



Deep Security 12.0ガイド

オンプレミスインストール

複数年契約について

お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

各製品のサポート提供期間は以下の Web サイトからご確認ください。

<https://success.trendmicro.com/jp/solution/000207383>

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend

Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Trend Micro Service One、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、先得、およびTrend Micro Oneは、トレンドマイクロ株式会社の登録商標です。

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

©2024 Trend Micro Incorporated.All rights reserved

個人情報保護方針

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシーに従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

最終更新日: 2022年10月

目次

目次	4
Trend Micro Deep Security について	78
Deep Securityトラストセンター	78
Deep Security製品使用状況データ収集	78
プライバシーと個人データの収集に関する規定	78
Deep Securityコンポーネントについて	79
Deep Securityのリリースライフサイクルとサポートポリシー	80
LTSリリースのサポート期間およびアップグレードの推奨事項	81
Feature Releaseのサポート期間およびアップグレードの推奨事項	82
サポートサービス	82
Agentプラットフォームサポートポリシー	84
このリリースについて	85
新機能	85
Deep Security 12.0（長期サポートリリース）の新機能	86
プラットフォームのサポートの強化	86
セキュリティの向上	87
管理と品質の向上	89
Deep Security Managerの新機能	91
Deep Security Manager - 12.0 update 30	91
新機能	92
セキュリティアップデート	92
Deep Security Manager-12.0 update 29	92
解決済みの問題	92
セキュリティアップデート	92
Deep Security Manager-12.0 update 28	93
解決済みの問題	93

セキュリティアップデート	93
Deep Security Manager - 12.0 update 27	93
解決済みの問題	93
セキュリティアップデート	93
Deep Security Manager-12.0 update 26	94
新機能	94
解決済みの問題	94
セキュリティアップデート	94
Deep Security Manager - 12.0 update 25	94
解決済みの問題	95
Deep Security Manager - 12.0 update 23	95
解決済みの問題	95
Deep Security Manager - 12.0 update 22	95
新機能	95
解決済みの問題	95
セキュリティアップデート	95
Deep Security Manager-12.0 update 21	96
解決済みの問題	96
Deep Security Manager-12.0 update 20	96
新機能	96
解決済みの問題	96
セキュリティアップデート	97
Deep Security Manager-12.0 update 19	97
新機能	97
Deep Security Manager-12.0 update 18	97
新機能	97
解決済みの問題	98
Deep Security Manager - 12.0 update 17	98
解決済みの問題	98

Deep Security Manager - 12.0 update 16	98
解決済みの問題	98
セキュリティアップデート	99
Deep Security Manager - 12.0アップデート15	99
新機能	99
解決済みの問題	99
Deep Security Manager - 12.0 update 14	100
解決済みの問題	100
Deep Security Manager 12.0 update 13	100
新機能	100
解決済みの問題	100
Deep Security Manager 12.0 update 12	101
解決済みの問題	101
セキュリティアップデート	101
Deep Security Manager 12.0 update 11	102
新機能	102
解決済みの問題	102
セキュリティアップデート	102
Deep Security Manager 12.0 update 10	102
新機能	103
管理と品質の向上	103
新機能	103
解決済みの問題	103
セキュリティアップデート	104
Deep Security Manager 12.0 update 9	104
新機能	104
解決済みの問題	104
セキュリティアップデート	105
Deep Security Manager-12.0 update 8	105

新機能	105
プラットフォームのサポートの強化	105
新機能	105
解決済みの問題	105
Deep Security Manager-12.0 update 7	106
拡張機能	106
解決された問題	106
セキュリティアップデート	107
Deep Security Manager-12.0 update 6	107
新機能	107
解決済みの問題	108
セキュリティアップデート	108
Deep Security Agentの新機能	108
Deep Security Agent - 12.0 update 30	109
解決済みの問題	109
Deep Security Agent-12.0 update 29	109
新機能	109
解決済みの問題	109
セキュリティアップデート	109
Deep Security Agent-12.0 update 28	110
セキュリティアップデート	110
解決済みの問題	110
Deep Security Agent - 12.0 update 27	110
セキュリティアップデート	110
Deep Security Agent-12.0 update 26	111
解決済みの問題	111
Deep Security Agent - 12.0 update 25	111
新機能	111
解決済みの問題	112

新機能	112
Deep Security Agent - 12.0 update 24	112
解決済みの問題	112
Deep Security Agent - 12.0 update 23	112
新機能	112
解決済みの問題	113
セキュリティアップデート	113
Deep Security Agent - 12.0 update 22	113
新機能	113
解決済みの問題	114
セキュリティアップデート	114
Deep Security Agent-12.0 update 21	114
解決済みの問題	115
Deep Security Agent-12.0 update 20	115
解決済みの問題	115
セキュリティアップデート	115
Deep Security Agent-12.0 update 19	116
解決済みの問題	116
Deep Security Agent-12.0 update 18	116
新機能	116
解決済みの問題	116
Deep Security Agent - 12.0 update 17	117
新機能	117
解決済みの問題	117
Deep Security Agent - 12.0 update 16	117
新機能	118
解決済みの問題	118
セキュリティアップデート	118
Deep Security Agent - 12.0アップデート15	119

新機能	119
解決済みの問題	119
セキュリティアップデート	119
Deep Security エージェント-12.0 update 14	120
解決済みの問題	120
Deep Security Agent-12.0 update 13	120
新機能	120
解決済みの問題	121
お知らせ	121
Deep Security Agent-12.0 update 12	121
プラットフォームのサポートの強化	122
新機能	122
解決済みの問題	122
セキュリティアップデート	123
Deep Security Agent-12.0 update 11	123
新機能	123
解決済みの問題	124
セキュリティアップデート	124
Deep Security Agent-12.0 update 10	124
新機能	125
プラットフォームのサポートの強化	125
管理と品質の向上	125
拡張機能	125
解決済みの問題	125
Deep Security Agent-12.0 update 9	126
新機能	126
解決済みの問題	126
セキュリティアップデート	127
Deep Security Agent-12.0 update 8	127

新機能	127
解決済みの問題	127
セキュリティアップデート	128
Deep Security Agent-12.0 update 7	128
新機能	128
解決済みの問題	128
セキュリティアップデート	129
Deep Security Agent-12.0 update 6	129
新機能	129
解決済みの問題	129
Deep Security Agent - 12.0 update 30	130
新機能	130
解決済みの問題	130
Deep Security Agent-12.0 update 29	131
新機能	131
解決済みの問題	131
セキュリティアップデート	131
Deep Security Agent-12.0 update 28	132
セキュリティアップデート	132
解決済みの問題	132
Deep Security Agent - 12.0 update 27	132
セキュリティアップデート	132
Deep Security Agent-12.0 update 26	133
解決済みの問題	133
Deep Security Agent - 12.0 update 25	133
新機能	133
解決済みの問題	133
新機能	134
Deep Security Agent - 12.0 update 24	134

Deep Security Agent - 12.0 update 23	134
解決済みの問題	134
セキュリティアップデート	134
Deep Security Agent - 12.0 update 22	135
解決済みの問題	135
セキュリティアップデート	135
Deep Security Agent-12.0 update 21	135
解決済みの問題	136
Deep Security Agent-12.0 update 20	136
プラットフォームのサポートの強化	136
解決済みの問題	136
セキュリティアップデート	136
Deep Security Agent-12.0 update 19	137
解決済みの問題	137
Deep Security Agent-12.0 update 18	137
解決済みの問題	137
Deep Security Agent - 12.0 update 17	137
プラットフォームのサポートの強化	138
新機能	138
解決済みの問題	138
Deep Security Agent - 12.0 update 16	138
新機能	138
解決済みの問題	139
セキュリティアップデート	139
Deep Security Agent - 12.0アップデート15	139
解決済みの問題	140
Deep Security エージェント-12.0 update 14	140
Deep Security Agent-12.0 update 13	140
新機能	140

解決済みの問題	140
Deep Security Agent-12.0 update 12	141
プラットフォームのサポート強化	141
新機能	141
解決済みの問題	141
セキュリティアップデート	142
Deep Security Agent-12.0 update 11	143
新機能	143
解決済みの問題	143
セキュリティアップデート	143
Deep Security Agent-12.0 update 10	143
新機能	143
管理と品質の向上	144
新機能	144
解決済みの問題	144
Deep Security Agent-12.0 update 9	144
解決済みの問題	144
セキュリティアップデート	145
Deep Security Agent-12.0 update 8	145
新機能	146
解決済みの問題	146
セキュリティアップデート	147
Deep Security Agent-12.0 update 7	147
新機能	147
解決済みの問題	147
セキュリティアップデート	148
Deep Security Agent-12.0 update 6	148
解決済みの問題	148
Deep Security Agent - 12.0 update 30	149

解決済みの問題	149
Deep Security Agent-12.0 update 29	149
新機能	149
解決済みの問題	149
セキュリティアップデート	149
Deep Security Agent-12.0 update 28	150
セキュリティアップデート	150
Deep Security Agent - 12.0 update 27	150
セキュリティアップデート	150
Deep Security Agent-12.0 update 26	151
解決済みの問題	151
Deep Security Agent - 12.0 update 25	151
解決済みの問題	151
新機能	151
Deep Security Agent - 12.0 update 24	151
Deep Security Agent - 12.0 update 23	152
解決済みの問題	152
Deep Security Agent - 12.0 update 22	152
解決済みの問題	152
セキュリティアップデート	152
Deep Security Agent-12.0 update 21	153
解決済みの問題	153
Deep Security Agent-12.0 update 20	153
解決済みの問題	153
セキュリティアップデート	154
Deep Security Agent-12.0 update 19	154
解決済みの問題	154
Deep Security Agent-12.0 update 18	154
拡張機能	154

解決済みの問題	155
Deep Security Agent - 12.0 update 17	155
解決済みの問題	155
Deep Security Agent - 12.0 update 16	155
新機能	155
解決済みの問題	156
セキュリティアップデート	156
Deep Security Agent - 12.0アップデート15	156
解決済みの問題	156
セキュリティアップデート	157
Deep Security エージェント-12.0 update 14	157
解決済みの問題	157
Deep Security Agent-12.0 update 13	157
新機能	157
解決済みの問題	158
Deep Security Agent-12.0 update 12	158
拡張機能	158
解決された問題	159
セキュリティアップデート	159
Deep Security Agent-12.0 update 11	160
拡張機能	160
Deep Security Agent-12.0 update 10	160
新機能	160
管理と品質の向上	160
拡張機能	160
解決された問題	161
Deep Security Agent-12.0 update 9	161
解決済みの問題	161
Deep Security Agent-12.0 update 8	161

新機能	162
解決された問題	162
セキュリティアップデート	162
Deep Security Agent-12.0 update 7	162
新機能	163
解決済みの問題	163
セキュリティアップデート	163
Deep Security Agent-12.0 update 6	163
解決済みの問題	164
Deep Security Virtual Applianceの新機能	165
Deep Security Virtual Appliance - 12.0 update 3	165
新機能	166
セキュリティアップデート	166
既知の問題	166
アーカイブ	166
Deep Security Managerのリリースノートのアーカイブ	166
Deep Security Manager-12.0 update 5	166
拡張機能	167
解決済みの問題	167
セキュリティアップデート	167
Deep Security Manager-12.0 update 4	167
解決済みの問題	167
セキュリティアップデート	167
Deep Security Manager-12.0 update 3	167
新機能	168
解決済みの問題	168
Deep Security Manager-12.0 update 2	169
新機能	169
解決済みの問題	169

Deep Security Manager-12.0 update 1	171
解決済みの問題	171
セキュリティアップデート	172
Deep Security Agentのリリースノートのアーカイブ	172
Deep Security エージェント-12.0 update 5	172
新機能	172
解決済みの問題	172
セキュリティアップデート	173
Deep Security エージェント-12.0 update 4	173
新機能	173
解決済みの問題	173
Deep Security エージェント-12.0 update 3	173
新機能	174
解決済みの問題	174
Deep Security エージェント-12.0 update 2	174
新機能	174
解決済みの問題	174
Deep Security エージェント-12.0 update 1	175
新機能	175
解決済みの問題	175
Deep Security エージェント-12.0 update 5	176
新機能	176
解決済みの問題	177
セキュリティアップデート	177
Deep Security エージェント-12.0 update 3	177
解決済みの問題	177
Deep Security エージェント-12.0 update 2	178
解決済みの問題	178
Deep Security エージェント-12.0 update 1	178

解決済みの問題	178
Deep Security エージェント-12.0 update 5	179
解決済みの問題	179
セキュリティアップデート	179
Deep Security エージェント-12.0 update 4	179
解決済みの問題	180
Deep Security エージェント-12.0 update 3	181
Deep Security エージェント-12.0 update 2	181
新機能	181
解決済みの問題	181
Deep Security エージェント-12.0 update 1	182
解決済みの問題	182
Deep Security Agentのプラットフォーム	182
各プラットフォームでサポートされている機能	183
Deep Security AgentのLinuxカーネルサポート	183
システム要件	184
サイジング	184
Deep Security Managerのサイジング	184
複数のサーバノード	185
データベースのサイジング	185
データベースのディスク容量の見積もり	187
Deep Security AgentおよびRelayのサイジング	188
Deep Security Virtual Applianceのサイジング	189
ポート番号、URL、およびIPアドレス	190
Deep Securityのポート番号	191
Deep SecurityのURL	196
法律上の免責事項	204
Hot Fix	205
メジャーリリース、Update、パッチ、Service Pack	205

はじめに	206
データベースを準備する	206
Deep Security Managerで使用するデータベースの準備	206
ハードウェア要件	207
専用のサーバ	207
ハードウェアに関する推奨事項	207
Microsoft SQL Server	208
一般的な要件	208
トランスポートプロトコル	208
マルチテナントを使用する場合	208
Oracle Database	209
Oracle RAC (Real Application Clusters) のサポート	209
データベースメンテナンス	209
インデックスのメンテナンス	209
バックアップと障害復旧	210
PostgreSQLの推奨設定	210
ログローテーション	212
例:日単位のデータベースのログローテーション	213
ロック管理	213
最大同時接続数	213
有効キャッシュサイズ	213
共有バッファ	214
ワークメモリとメンテナンスワークメモリ	214
チェックポイント	214
ログ先行書き込み (WAL)	214
自動バキューム設定	215
Linux版PostgreSQL	216
Transparent huge pages	216
ホストベース認証	216

Microsoft SQL Server Expressに関する注意事項	216
ソフトウェアパッケージのデジタル署名の確認	216
ソフトウェアZIPパッケージの署名の確認	217
インストーラファイル (EXE、MSI、RPM、またはDEBファイル) の署名の確認	218
EXEまたはMSIファイルの署名の確認	219
RPMファイルの署名の確認	219
DEBファイルの署名の確認	221
Deep Securityのインストール	223
Deep Securityのインストールまたはアップグレード	223
環境を準備する	224
ハードウェア要件	226
ネットワーク要件	227
ネットワークトポロジ	227
データベース要件	228
サポートされているデータベースへの移行	229
リモートSQLクエリタイムアウトの変更	229
Agentベースの保護とAgentレスによる保護のどちらを使用するかを選択する	230
サポート対象OSをインストールする	230
サポート対象外のDeep Security Managerをアップグレードする	231
サポートされていないRelayをアップグレードする	231
VMwareの要件	231
Virtual Applianceをアップグレードする	232
協調的保護からコンバインモードへの変換	236
VMware HAへのApplianceのピンニング	236
サポートされていないAgentをアップグレードする	237
インストーラを実行する	237
複数ノードでDeep Security Managerを実行する	238
LinuxにDeep Security Managerをインストールする	239
Deep Security ManagerをWindowsにインストールする	240

Deep Security ManagerのサーバにRelayをインストールする	240
スキーマのアップデート	242
マルチテナントデータベースの強制アップグレード	243
失敗したアップグレードをロールバックする	243
インストーラ実行後の処理	244
自己署名証明書	244
暗号化を強化する	244
イベントデータの移行	245
RelayをLinuxでアップグレードする (dpkg)	245
RelayをLinuxでアップグレードする (rpm)	246
RelayをWindowsでアップグレードする	246
WindowsでAgentをアップグレードする	247
LinuxでAgentのアップグレードをする	247
SolarisでのAgentのアップグレード	248
Deep Security Agentのセキュリティアップデートをダウンロードする	248
AIX上のエージェントのアップグレード	249
各保護機能をAgentとApplianceのどちらから提供するかを選択	249
新しいDeep Security AgentまたはRelayをインストールする	250
アラートを設定する	253
推奨設定の検索を実行する	254
Deep Security Managerのサイレントインストール	255
サイレントインストールのシステムチェックを実行する	255
Windowsプラットフォームでサイレントインストールを実行する	255
Linuxプラットフォームでサイレントインストールを実行する	255
パラメータ	256
プロパティファイルの例	256
Deep Security Managerの設定プロパティファイル	257
必須の設定	258
LicenseScreen	258

CredentialsScreen	258
オプションの設定	258
LanguageScreen	258
UpgradeVerificationScreen	258
OldDataMigrationScreen	259
DatabaseScreen	259
AddressAndPortsScreen	262
CredentialsScreen	262
MasterKeyConfigurationScreen	263
SecurityUpdateScreen	263
SoftwareUpdateScreen	264
SmartProtectionNetworkScreen	265
RelayScreen	267
プロパティファイルの例	267
インストール時の出力	268
インストールに成功した場合	268
インストールに失敗した場合	269
複数のノードでのDeep Security Managerの実行	270
ノードを追加する	270
ノードを削除する	271
ノードのステータスを表示する	271
アクティビティグラフ付きネットワークマップ	271
ノード別ジョブ	272
種類別ジョブ	273
ノードおよび種類別ジョブの総数	273
アクティベーションコードを追加	274
Deep Security Managerのメモリ使用量の設定	275
インストーラの最大メモリ使用量を設定する	275
Deep Security Managerの最大メモリ使用量を設定する	275

Deep Security Managerのパフォーマンス機能	276
パフォーマンスプロファイル	276
ディスク容量不足のアラート	276
データベースのディスク容量不足	276
Managerのディスク容量不足	276
ロードバランサの証明書のアップデート	277
マルチテナント環境の設定	279
マルチテナントの要件	280
マルチテナントを有効にする	281
テナントを作成する	281
テナントに送信されるメッセージの例	283
確認リンクをメール: アカウント確認要求	283
生成したパスワードをメール	283
スケーラビリティのガイドライン	284
マルチテナントに関するヒント	284
攻撃の予兆IPリスト	284
複数のデータベースサーバを使用する	284
テナントの「削除の保留中」状態	285
[システム設定] のマルチテナントオプション	285
テナントを管理する	285
テナントのプロパティ	285
一般	286
モジュール	286
機能	287
統計	287
Deep Security Agentの有効化	287
テナントに表示される内容	287
Agentからのリモート有効化	289
テナントの診断	289

使用状況の監視	289
マルチテナントのダッシュボード	290
マルチテナントのレポート	290
セキュリティモジュールの累積使用状況レポート	290
セキュリティモジュールの使用状況レポート	291
テナントレポート	291
データベースのユーザアカウントを設定する	291
データベースのユーザアカウントを設定する	292
SQL Server	292
Oracle	296
PostgreSQL	299
複数のデータベースサーバを設定する	299
セカンダリデータベースを削除または変更する	300
API	300
アップグレード	301
テナントをサポートする	301
ロードバランサ	302
Deep Security Virtual Appliance環境のマルチテナント	303
マルチテナント設定	304
データベースサーバ	306
新しいテナントテンプレート	306
保護の使用状況の監視	308
メール通知のSMTPの設定	308
Applianceのインストール	309
VMware環境の保護	309
Deep Security Virtual Applianceの機能	309
検索キャッシュ	309
検索ストームの最適化	310
管理の簡素化	310

Virtual ApplianceおよびNSXを使用するVMware環境	310
エージェントのみを使用したVMwareの配置	315
追加情報	315
Agentレスによる保護またはコンバインモードの保護の選択	315
Agentレスによる保護	316
コンバインモード	316
協調的保護からコンバインモードへの変換	317
各保護機能をAgentとApplianceのどちらから提供するかの選択	317
vCloud Director環境で、エージェント起動の有効化を使用して複合モードを有効にする	318
アプライアンスを配信する前に	319
Applianceのインストール (NSX-T)	320
手順1: Deep Security ManagerにApplianceパッケージをインポートする	320
手順2: ファブリック設定を準備する	321
手順3: Deep Security ManagerにvCenterを追加する	327
手順4: Deep Security Virtual ApplianceをNSX-Tにインストールする	327
手順5: エンドポイント保護を設定する	331
手順6: NSX-Tで有効化を準備する	334
方法1: 「コンピュータの作成」 イベントベースタスクを作成する	352
手順7: 有効化とポリシーの割り当てを開始する	353
手順8: 仮想マシンが有効化されて、ポリシーが割り当てられていることを確認する	354
次の手順 (新しい仮想マシンを追加する方法)	354
vCloud環境でのAgentレスによる保護の実施	354
開始前の準備	355
vCloud仮想マシンのAgentレスによる保護を有効にする	355
マルチテナント環境を作成する	355
vCenterを追加してDeep Security Virtual Applianceを配置する	355
Deep SecurityでVMware vCloudリソースを使用できるように設定する	356
vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する	356

新しい仮想マシンに一意的UUIDを割り当てる	357
ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする	357
仮想マシンでVirtual Appliance保護を有効にする	357
VMware vCloud Organizationアカウントからコンピュータをインポートする	357
VMware vCloud Air仮想データセンターからコンピュータをインポートする	358
仮想マシンでVirtual Appliance保護を有効にする	359
NSX環境での自動ポリシー管理	359
「NSXセキュリティグループの変更」 イベントベースタスク	359
タスクを実行する条件	360
実行可能な処理	361
vCenterがDeep Security Managerに追加されたときに作成されるイベントベースタスク	362
Deep Security ManagerからvCenterを削除する	363
Deep SecurityポリシーのNSXとの同期	364
NSXセキュリティタグの設定	365
NSXセキュリティタグを適用するように不正プログラム対策を設定する	366
NSXセキュリティタグを適用するように侵入防御を設定する	367
アプライアンスのOVFの場所を設定する	368
Deep Security Virtual Applianceのメモリ割り当て	370
vCenterに配置する前にApplianceのメモリ割り当てを設定する	370
配置済みのApplianceのメモリ割り当てを設定する	371
アプライアンスを起動または停止する	371
Agentのインストール	372
Deep Security Agentソフトウェアの入手	372
Deep Security ManagerにAgentソフトウェアパッケージをダウンロードする	372
ソフトウェアアップデートを自動的にインポートする	373
ソフトウェアアップデートを手動でインポートする	373
Agentのインストーラをエクスポートする	374
Deep Securityデータベースからソフトウェアパッケージを削除する	374

シングルテナントモードでAgentパッケージを削除する	375
マルチテナントモードでAgentパッケージを削除する	375
カーネルサポートパッケージを削除する	375
Deep Security Agentの手動インストール	376
WindowsにAgentをインストールする	376
Amazon WorkSpacesでのインストール	377
Windows 2012 Server Coreでのインストール	377
Red Hat、SUSE、Oracle Linux、またはCloudLinuxにAgentをインストールする	378
UbuntuまたはDebianにAgentをインストールする	378
SolarisにAgentをインストールする	379
AIXにAgentをインストールする	381
Microsoft Azure Virtual MachineへのAgentのインストール	382
インストールスクリプトを生成して実行する	383
カスタムスクリプト拡張機能を既存の仮想マシンに追加する	383
VMware vCloudへのAgentのインストール	383
vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する	384
新しい仮想マシンに一意的UUIDを割り当てる	384
ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする	385
VMware vCloud Organizationアカウントからのコンピュータのインポート	385
VMware vCloud Air仮想データセンターからコンピュータをインポートする	386
Amazon EC2およびWorkSpacesへのAgentのインストール	387
AWSアカウントをDeep Security Managerに追加する	387
通信方向を設定する	388
有効化の種類を設定する	388
ポートを開く	389
開くポート	390
AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする	390
Agentが適切にインストールされ有効化されたことを確認する	391

ポリシーを割り当てる	392
AgentのAMIまたはWorkSpaceバンドルへの統合	393
AWSアカウントをDeep Security Managerに追加する	394
通信方向を設定する	394
有効化の種類を設定する	394
「マスター」 Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する ..	394
Agentをマスターにインストールする	394
Agentが適切にインストールされ有効化されたことを確認する	395
(推奨) 自動ポリシー割り当てを設定する	395
マスターに基づいてAMIまたはカスタムWorkSpaceバンドルを作成する	396
AMIを使用する	397
Agentを有効化するときに自動的にアップグレードする	397
Agentの自動アップグレードを有効にする	398
Agentが正常にアップグレードされたことを確認する	398
コンポーネント間の通信の設定	399
AgentとManagerの通信	400
ハートビートを設定する	400
通信方向を設定する	401
AgentとManagerの通信でサポートされている暗号化スイート	404
Deep Security Agent 9.5の暗号化スイート	404
Deep Security Agent 9.6の暗号化スイート	405
Deep Security Agent 10.0の暗号化スイート	405
Deep Security Agent 11.0の暗号化スイート	406
Deep Security Agent 12.0の暗号化スイート	407
SSLの実装と資格情報のプロビジョニング	407
Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化し て保護する	408
Agentからのリモート有効化およびAgentからの通信を有効にする	408
Agentからの通信を有効にしたポリシーを作成または変更する	409

Agentからのリモート有効化を有効にする	409
Agentにポリシーを割り当てる	409
インストールスクリプトを使用してAgentを有効にする	410
プロキシの背後に配置されたAgentの接続	410
要件	410
Deep Security Managerでプロキシを登録する	411
プロキシを経由してAgent、Appliance、Relayをセキュリティアップデートに 接続する	411
プロキシを経由してAgentをセキュリティサービスに接続する	411
プロキシを経由してAgentをRelayに接続する	412
AgentをRelayのプライベートIPアドレスに接続する	412
プロキシ設定を削除する	413
Windows	413
Linux	413
以降のAgentのインストール	413
インターネットにアクセスできない エージェントを設定する	413
解決策	414
プロキシを使用する	414
Smart Protection Serverをローカルにインストールする	415
隔離されたネットワークでアップデートを取得する	416
隔離されたネットワークでルールのアップデートを取得する	418
トレンドマイクロのセキュリティサービスを使用する機能を無効にする	419
Deep Securityでサポートされるプロキシプロトコル	421
プロキシ設定	422
プロキシサーバの使用	422
プロキシサーバ	423
信頼された証明書の管理	424
信頼された証明書をインポートする	424
信頼された証明書を表示する	425

信頼された証明書を削除する	426
Smart Protection Networkの接続を無効にした場合のトレンドマイクロへの情報の送信について	427
Agent向けのLinux Secure Bootのサポート	427
トレンドマイクロの公開鍵をダウンロードする	428
Shim MOK Managerの鍵データベースを使用して鍵を登録する	428
Agentの有効化	430
Agentを無効化する	432
エージェントの起動または停止	432
Agent配信での問題の診断 (Windows)	433
NICチーミングの設定	433
Agentの設定	434
ホスト名	434
Agentからのリモート有効化	434
Agentのアップグレード	436
非アクティブなAgentのクリーンナップ	436
データプライバシー	437
AgentレスによるvCloud保護	437
Deep Security Notifierのインストール	437
インストールパッケージをコピーする	437
Windows版Deep Security Notifierをインストールする	437
Relayによるセキュリティとソフトウェアのアップデートの配布	438
Relayの仕組み	439
使用するRelayの数を決定する	439
Agentの地域	440
ネットワーク設定	440
ネットワーク帯域幅の使用	440
サイジングの推奨設定	440
1つ以上のRelayを設定する	441

1つ以上のRelayグループを作成する	441
1つ以上のRelayを有効にする	443
AgentをRelayグループに割り当てる	444
セキュリティアップデートとソフトウェアアップデートのためのRelay設定を指定する	444
セキュリティアップデート	444
ソフトウェアアップデート	445
AgentからRelay機能を削除する	445
開発、自動化、およびAPI	446
コマンドラインの基本	447
Deep Security Agent	447
dsa_control	448
使用方法	448
Agentからのリモート有効化 (「dsa_control -a」)	452
Agentからのハートビート有効化コマンド (「dsa_control -m」)	453
Agentを有効化する	461
Windows	461
Linux	461
不正プログラム対策およびルールアップデート用にプロキシを設定する	461
Windows	461
Linux	462
Managerへの接続用にプロキシを設定する	462
Windows	462
Linux	462
Agentからのハートビート有効化コマンド	462
Windows	462
Linux	462
不正プログラムの手動検索を開始する	463
Windows	463

Linux	463
診断パッケージを作成する	463
Agentをリセットする	463
Windows	463
Linux	464
dsa_query	464
使用方法	464
CPU使用率とRAM使用量を確認する	465
Windows	465
Linux	465
ds_agentプロセスまたはサービスが実行されていることを確認する	465
Windows	465
Linux	465
LinuxでAgentを再起動する	465
Deep Security Manager	466
使用方法	466
リターンコード	477
Deep Security APIを使用したタスクの自動化	478
従来のREST APIおよびSOAP API	478
ステータス監視APIを有効にする (オプション)	479
Webサービスユーザアカウントを作成する	479
Deep Security予約タスクの設定	479
予約タスクを作成する	479
予約タスクを有効または無効にする	481
定期レポートをセットアップする	482
コンピュータの追加または変更時のタスクの自動実行	482
イベントベースタスクを作成する	482
既存のイベントベースタスクを編集または停止する	482
監視できるイベント	482

条件	483
処理	486
実行順序	486
イベントベースタスクを一時的な無効にする	488
AWSオートスケーリングとDeep Security	488
Agentをプレインストールする	488
インストールスクリプトでAgentをインストールする	489
オートスケーリングの結果としてDeep Securityからインスタンスを削除する	491
Azure Virtual Machine Scale SetsとDeep Security	491
手順1: (推奨) AzureアカウントをDeep Security Managerに追加する	492
手順2: インストールスクリプトを準備する	492
手順3: カスタムスクリプト拡張機能を介してAgentをVMSSインスタンスに追加する	493
例1: Agentを含む新しいVMSSを作成する	493
例2: 既存のVMSSにAgentを追加する	496
インストールスクリプトを使用したコンピュータの追加と保護	498
Agentからのリモート有効化を有効にする	499
インストールスクリプトを生成する	499
トラブルシューティングおよびヒント	501
AWSインスタンスタグに基づくポリシーの自動割り当て	502
保護	504
侵入防御	504
不正プログラム対策	505
ファイアウォール	505
Webレピュテーション	505
変更監視	505
セキュリティログ監視	506
アプリケーションコントロール	506
保護対象コンピュータの管理	506

Deep Security Managerにコンピュータおよびその他のリソースの追加	506
Managerにコンピュータを追加する	507
コンピュータのグループ化	508
コンピュータリストをエクスポートする	508
コンピュータを削除する	509
ローカルネットワークコンピュータの追加	509
Agentからのリモート有効化	509
コンピュータを手動で追加する	509
コンピュータを検出する	510
VMware vCenterの追加	512
vCenterの追加	512
vCenter - FIPSモードを追加する	515
保護されたNSXクラスタへのESXiの追加	515
AWSクラウドアカウントの追加	516
AWSアカウントを追加することのメリットは何ですか?	517
サポートされるAWSリージョン	517
AWSアカウントを追加する方法の概要	518
方法: Managerインスタンスロールとクロスアカウントロール	519
AWS DSMアカウントを設定する	520
AWSアカウントAを設定する	522
AWSアカウントをDeep Security Managerに追加する	524
方法: IAMユーザとクロスアカウントロール	525
AWSアカウントXを設定する	526
AWSアカウントYを設定する	528
Deep Security Managerにアクセスキーを追加する	529
AWSアカウントをDeep Security Managerに追加する	530
方法: Managerインスタンスロール (1つのAWSアカウント)	531
方法: AWSアクセスキー	533
クラウドアカウントを編集する	535

Managerからクラウドアカウントを削除する	535
AWSアカウントを同期する	535
Amazon WorkSpacesの追加	536
Amazon WorkSpacesを保護する (AWSアカウントをすでに追加している場合) ...	536
Amazon WorkSpacesを保護する (AWSアカウントをまだ追加していない場合) ...	537
新しいクラウドコネクタ機能への移行方法	537
Deep SecurityへのMicrosoft Azureアカウントの追加	539
Azureアカウントを追加することのメリットは何ですか?	539
Azureアカウントのプロキシを設定する	540
Microsoft AzureアカウントからDeep Securityに仮想マシンを追加する	540
Azure Resource Managerコネクタを使用してAzureクラシック仮想マシンを管理 する	541
Azureアカウントを削除する	541
Azureアカウントを同期する	542
Deep Security用のAzureアプリケーションの作成	542
適切な役割を割り当てる	543
Azureアプリケーションを作成する	543
AzureアプリケーションID、Active Directory ID、およびパスワードを記録する ..	543
サブスクリプションIDを記録する	544
Azureアプリケーションに役割とコネクタを割り当てる	544
新しいAzure Resource Manager接続機能へのアップグレードについて	545
VMware vCloudでホストされる仮想マシンの追加	545
vCloudアカウントを追加することのメリットは何ですか。	546
クラウドアカウント用のプロキシ設定	547
Manager用のVMware vCloud Organizationアカウントを作成する	547
VMware vCloud Organizationアカウントからコンピュータをインポートする	548
VMware vCloud Airデータセンターからコンピュータをインポートする	548
クラウドアカウントのソフトウェアアップデートを設定する	549
クラウドアカウントを削除する	549

Microsoft Active Directoryからのコンピュータグループの追加	549
Active Directoryのその他のオプション	551
ディレクトリの削除	551
今すぐ同期	551
サーバ証明書を使用する	551
ユーザおよび連絡先をインポートする	552
Active Directoryオブジェクトの同期を維持する	553
Active Directoryとの同期を無効にする	554
Active Directoryとの同期からコンピュータグループを削除する	554
Active Directoryのユーザおよび連絡先を削除する	554
Dockerコンテナの保護	554
Deep SecurityによるDockerホストの保護	555
Deep SecurityによるDockerコンテナの保護	556
侵入防御の推奨検索に関する制限事項	556
コンピュータおよびAgentのステータス	556
[ステータス] 列 - コンピュータの状態	557
[ステータス] 列 - AgentまたはApplianceの状態	557
[タスク] 列	558
コンピュータのエラー	562
保護モジュールのステータス	563
コンピュータでその他の処理を実行する	564
コンピュータのアイコン	570
各種コンピュータのステータス情報	571
通常のコンピュータ	571
Relay	572
Deep Security Scanner	572
Dockerホスト	573
ESXiサーバ	573
Virtual Appliance	573

仮想マシンをAgentレスで保護する	574
Deep Securityでのiptablesの使用	574
Deep Security Managerの実行に必要なルール	575
Deep Security Agentの実行に必要なルール	575
Deep Securityによるiptablesルールの自動追加を防ぐ	576
Agentセルフプロテクションの有効化または無効化	576
Deep Security Managerを介してセルフプロテクションを設定する	576
コマンドラインを使用してセルフプロテクションを設定する	577
Deep Securityによる「オフライン」Agentの保護	578
Deep Security Notifier	578
Notifierの仕組み	579
コンピュータとその他のリソースを保護するためのポリシーの作成	583
新規ポリシーを作成する	583
ポリシーを作成するその他の方法	584
ポリシーまたは個々のコンピュータの設定を編集する	585
ポリシーをコンピュータに割り当てる	585
ポリシーの自動アップデートを無効にする	586
ポリシーの変更を手動で送信する	586
ポリシーをエクスポートする	587
ポリシー、継承、およびオーバーライド	587
継承	588
オーバーライド	589
オブジェクトのプロパティをオーバーライドする	590
ルールの割り当てをオーバーライドする	591
コンピュータまたはポリシーのオーバーライド項目をまとめて確認する	591
推奨設定の検索の管理と実行	592
検索内容	593
検索の制限	594
推奨設定の検索を実行する	595

予約タスクを作成して定期的に推奨設定の検索を実行する	596
継続検索を設定する	597
推奨設定の検索を手動で実行する	597
推奨設定の検索をキャンセルする	597
推奨設定の検索からルールまたはアプリケーションの種類を除外する	597
推奨設定を自動的に適用する	598
検索結果を確認して手動でルールを割り当てる	599
推奨ルールを設定する	600
一般的な脆弱性の追加ルールを実装する	600
トラブルシューティング: 推奨設定の検索失敗	602
通信	602
サーバリソース	602
タイムアウト値	602
コンピュータで使用可能なインタフェースの検出と設定	603
複数のインタフェースに対してポリシーを設定する	603
インタフェース制限を強制する	604
コンピュータエディタの [概要] セクション	605
[一般] タブ	605
コンピュータのステータス	606
保護モジュールのステータス	607
VMware仮想マシンの概要	608
[処理] タブ	608
有効化	608
ポリシー	609
Agentソフトウェア	609
サポート情報	610
[TPM] タブ	610
[システムイベント] タブ	611
ポリシーエディタの [概要] セクション	611

[一般] タブ	611
一般	611
継承	611
モジュール	611
[このポリシーを使用しているコンピュータ] タブ	612
[イベント] タブ	612
ネットワークエンジン設定	612
ポリシーのルール、リスト、およびその他の共通オブジェクトの定義	622
ルール	623
リスト	623
その他	623
ファイアウォールルールの作成	623
新しいルールを追加する	624
ルールの動作とプロトコルを選択する	624
パケットの送信元と送信先を選択する	627
ルールイベントとアラートを設定する	628
アラート	628
ルールのスケジュールを設定する	628
ルールにコンテキストを割り当てる	629
ルールが割り当てられているポリシーとコンピュータを確認する	629
ルールをエクスポートする	629
ルールを削除する	629
侵入防御ルールの設定	629
侵入防御ルールのリストを表示する	630
侵入防御ルールに関する情報を表示する	630
一般情報	631
詳細	631
侵入防御ルールのリストを表示する	631
一般情報	632

ID (トレンドマイクロのルールのみ)	632
関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ)	632
ルールを割り当てる/ルールの割り当てを解除する	633
アップデートされた必須ルールを自動割り当てする	633
ルールにイベントログを設定する	634
アラートを生成する	635
設定オプションを設定する (トレンドマイクロのルールのみ)	635
有効な時間を予約する	636
推奨設定から除外する	636
ルールのコンテキストを設定する	636
ルールの動作モードをオーバーライドする	637
ルールおよびアプリケーションの種類の設定をオーバーライドする	637
ルールをエクスポート/インポートする	638
変更監視ルールの作成	639
新しいルールを追加する	639
変更監視ルール情報を入力する	640
ルールテンプレートを選択し、ルールの属性を定義する	640
レジストリ値テンプレート	640
ファイルテンプレート	640
カスタム (XML) テンプレート	641
トレンドマイクロが発行する変更監視ルールを設定する	641
ルールイベントとアラートを設定する	642
リアルタイムのイベント監視	642
アラート	642
ルールが割り当てられているポリシーとコンピュータを確認する	643
ルールをエクスポートする	643
ルールを削除する	643
ポリシーで使用する セキュリティログ監視 ルールを定義する	643

新しいセキュリティログ監視ルールを作成する	644
デコーダ	646
サブルール	647
グループ	647
ルール、ID、およびレベル	648
説明	649
デコード形式	650
一致項目	650
条件文	651
評価の階層	652
ログエントリのサイズに関する制限	653
コンポジットルール	654
実際の使用例	655
セキュリティログ監視ルールの重要度レベルと推奨される使用法	664
strftime() 変換指定子	665
セキュリティログ監視ルールの確認	666
セキュリティログ監視 のルール構造とイベント照合プロセス	666
重複しているサブルール	668
ポリシーで使用するディレクトリリストの作成	669
ディレクトリリストをインポート/エクスポートする	672
ディレクトリリストを使用するポリシーを確認する	672
ポリシーで使用するファイル拡張子リストの作成	672
ファイル拡張子リストをインポート/エクスポートする	673
ファイル拡張子リストを使用する不正プログラム検索設定を確認する	673
ポリシーで使用するファイルリストの作成	674
ファイルリストをインポート/エクスポートする	676
ファイルリストを使用するポリシーを確認する	677
ポリシーで使用するIPアドレスリストの作成	677
IPリストをインポート/エクスポートする	678

IPリストを使用するルールを確認する	678
ポリシーで使用するポートリストの作成	678
ポートリストをインポート/エクスポートする	679
ポートリストを使用するルールを確認する	679
ポリシーで使用するMACアドレスリストの作成	679
MACリストをインポート/エクスポートする	680
MACリストを使用するポリシーを確認する	680
ポリシーで使用するコンテキストの定義	680
コンピュータがインターネットに接続されているかどうかを判別するオプション を設定する	681
コンテキストを定義する	681
ステートフルファイアウォールの設定の定義	682
ステートフル設定を追加する	682
ステートフル設定情報を入力する	683
パケットインスペクションオプションを選択する	683
IPパケットインスペクション	683
TCPパケットインスペクション	684
FTPオプション	685
UDPパケットインスペクション	685
ICMPパケットインスペクション	686
ステートフル設定をエクスポートする	687
ステートフル設定を削除する	687
ステートフル設定が割り当てられたポリシーとコンピュータを表示する	687
ルールに適用するスケジュールの定義	687
アプリケーションコントロールによるソフトウェアのロックダウン	688
主な概念	689
アプリケーションコントロールの仕組み	690
アプリケーションコントロールインタフェースの紹介	691
アプリケーションコントロール: ソフトウェア変更 ([処理])	692

アプリケーションコントロールルールセット	693
セキュリティイベント	694
アプリケーションコントロールで検出されるソフトウェア変更	694
Deep Security Agent 10と11におけるファイルの比較方法の相違点	695
アプリケーションコントロールの設定	696
アプリケーションコントロールを有効にする	696
新規および変更済みソフトウェアを監視する	698
変更の処理のヒント	700
変更の計画時にメンテナンスモードをオンにする	701
アプリケーションコントロールのヒントと注意事項	702
アプリケーションコントロールの有効化の確認	703
アプリケーションコントロールイベントの監視	705
ログに記録するアプリケーションコントロールイベントを選択する	706
アプリケーションコントロールイベントログを表示する	706
集約されたセキュリティイベントを解釈する	707
アプリケーションコントロールアラートを監視する	708
アプリケーションコントロールルールセットの表示と変更	709
アプリケーションコントロールルールセットを表示する	709
セキュリティイベント	711
アプリケーションコントロールルールの処理を変更する	711
個々のアプリケーションコントロールルールを削除する	712
アプリケーションコントロールルールセットを削除する	713
大量のソフトウェア変更後にアプリケーションコントロールをリセットする	713
共有ルールセットとグローバルルールセットを作成するためのAPIの使用	714
共有ルールセットを作成する	717
共有許可およびブロックルールからコンピュータ固有の許可およびブロックルールに切り替える	718
Relayを介してアプリケーションコントロール共有ルールセットをインストールする	719
単一テナント環境	719

Relayと共有ルールセットを使用する際の注意事項	721
不正プログラムの防止	722
不正プログラム検索の種類	723
リアルタイム検索	723
手動検索	723
予約検索	724
クイック検索	724
検索されるオブジェクトと順序	724
不正プログラム検索設定	725
不正プログラムイベント	725
スマートスキャン	725
機械学習型検索	726
Connected Threat Defense	727
不正プログラムの種類	727
ウイルス	727
トロイの木馬	727
パッカー	728
スパイウェア/グレーウェア	728
Cookie	729
その他の脅威	730
潜在的な不正プログラム	730
不正プログラム対策の有効化と設定	730
不正プログラム対策モジュールをオンにする	731
実行する検索の種類を選択する	731
検索除外を設定する	731
最新の脅威に対応できるようにDeep Securityを最新の状態に保つ	732
不正プログラム検索の設定	733
不正プログラム検索設定を作成または編集する	734
不正プログラム検索をテストする	735

特定の種類の不正プログラムを検索する	736
スパイウェア/グレーウェアを検索する	736
圧縮済み実行可能ファイルを検索する (リアルタイム検索のみ)	736
プロセスメモリを検索する (リアルタイム検索のみ)	737
圧縮ファイルを検索する	737
埋め込みのMicrosoft Officeオブジェクトを検索する	737
検索対象ファイルを指定する	738
検索対象	738
検索除外	739
ファイル除外のテスト	740
ディレクトリリストの構文	741
ファイルリストの構文	742
ファイル拡張子リストの構文	744
プロセスイメージファイルリストの構文 (リアルタイム検索のみ):	744
ネットワークディレクトリを検索する (リアルタイム検索のみ)	745
リアルタイム検索を実行するタイミングを指定する	745
不正プログラムの処理方法を設定する	745
不正プログラム修復処理をカスタマイズする	745
トレンドマイクロの推奨処理	747
不正プログラム検出のアラートを生成する	748
NSXセキュリティタグを適用する	748
ファイルのハッシュダイジェストにより不正プログラムファイルを特定する	749
コンピュータで通知を設定する	749
不正プログラム対策のパフォーマンスのヒント	750
ディスク使用量を最小限に抑える	750
CPU使用率を最適化する	751
RAM使用率を最適化する	752
Windows Server 2016へのDeep Security不正プログラム対策のインストール後の Windows Defenderの無効化	753

Windows Defenderが無効の状態での不正プログラム対策モジュールをインストールする	753
Virtual Applianceの検索キャッシュ	753
検索キャッシュ設定	754
不正プログラム検索のキャッシュ設定	755
変更監視の検索のキャッシュ設定	755
検索キャッシュの管理設定	755
初期設定を変更する場合の考慮事項	756
機械学習型検索を使用した脅威の検出	756
インターネットに接続されていることを確認する	757
機械学習型検索を有効にする	757
Connected Threat Defenseを使用した脅威の検出	758
Connected Threat Defenseの仕組み	759
Connected Threat Defenseの前提条件を確認する	759
Deep Discovery Analyzerへの接続をセットアップする	760
Trend Micro Apex Centralへの接続をセットアップする	762
Apex CentralがすでにDeep Securityを管理している場合に接続をセットアップする	762
Apex CentralがまだDeep Securityを管理していない場合に接続をセットアップする	763
Connected Threat Defenseで使用する不正プログラム検索設定を作成する	763
コンピュータでConnected Threat Defenseを有効にする	764
分析のためにファイルをDeep Discoveryへ手動で送信する	765
誤ったアラームを引き起こしたファイルを許可する	765
不審なファイルに対する検索処理を設定する	765
Deep Securityで不審オブジェクトリストをアップデートする	766
マルチテナント環境でConnected Threat Defenseを設定する	766
サポートされているファイルタイプ	766
挙動監視による不正プログラム/ランサムウェア検索の強化	767
強化された検索で実現される保護	768

強化された検索を有効にする方法	768
強化された検索で問題が検出された場合の動作	770
Agentをインターネットに直接接続できない場合の対処	774
Deep SecurityのSmart Protection	774
不正プログラム対策とSmart Protection	774
スマートスキャンの利点	774
スマートスキャンを有効にする	775
ファイルレピュテーションサービス用のSmart Protection Server	776
WebレピュテーションとSmart Protection	777
スマートフィードバック	777
不正プログラムの処理	778
検出した不正プログラムの確認と復元	778
検出ファイルのリストを参照する	779
検出ファイルを処理する	780
検出ファイルを検索する	781
検出ファイルを復元する	782
ファイルの検索除外を作成する	782
ファイルを復元する	785
検出ファイルを手動で復元する	785
不正プログラム対策の例外の作成	785
不正プログラム対策イベントから例外を作成する	786
不正プログラム対策の例外を手動で作成する	786
スパイウェア/グレーウェアの例外の処理方法	787
検索除外の推奨設定	787
保護対象のLinuxインスタンスにおける不正プログラム対策のデバッグログレベル の引き上げ	788
侵入防御を使用した攻撃のブロックをブロックする	789
侵入防御 ルール	789
アプリケーションの種類	790

ルールアップデート	790
推奨設定の検索	791
動作モードを使用してルールをテストする	791
ルールの動作モードをオーバーライドする	791
侵入防御 イベント	792
安全な接続のサポート	793
コンテキスト	793
インタフェースのタグ付け	793
侵入防御の設定	793
検出モードで侵入防御を有効にする	794
侵入防御のテスト	796
推奨ルールを適用する	797
システムを監視する	798
システムパフォーマンスを監視する	798
侵入防御イベントを確認する	799
パケットまたはシステムのエラーに対して「Fail-Open」を有効にする	799
予防モードに切り替える	799
個々のルールについてのベストプラクティスを実装する	799
HTTPプロトコルデコードルール	799
クロスサイトスクリプティングルールと汎用的なSQLインジェクションルール	800
NSXセキュリティタグを適用する	800
侵入防御ルールの設定	801
侵入防御ルールのリストを表示する	801
侵入防御ルールに関する情報を表示する	802
一般情報	802
詳細	802
侵入防御ルールのリストを表示する	802
一般情報	803
ID (トレンドマイクロのルールのみ)	803

関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ)	804
ルールを割り当てる/ルールの割り当てを解除する	804
アップデートされた必須ルールを自動割り当てする	805
ルールにイベントログを設定する	805
アラートを生成する	806
設定オプションを設定する (トレンドマイクロのルールのみ)	806
有効な時間を予約する	807
推奨設定から除外する	808
ルールのコンテキストを設定する	808
ルールの動作モードをオーバーライドする	808
ルールおよびアプリケーションの種類の設定をオーバーライドする	809
ルールをエクスポート/インポートする	810
SQLインジェクション防御ルールの設定	810
SQLインジェクション攻撃とは	811
SQLインジェクション攻撃に共通する文字および文字列	811
Generic SQL Injection Preventionルールの仕組み	813
ルールおよび評価システムの実例	814
例1: トラフィックのログ記録と破棄が発生	814
例2: トラフィックのログ/破棄が発生しない	815
Generic SQL Injection Preventionルールを設定する	817
文字エンコードのガイドライン	819
アプリケーションの種類	821
アプリケーションの種類の一覧を表示する	821
一般情報	821
接続	822
設定	822
オプション	822
割り当て対象	822

SSLまたはTLSトラフィックの検査	823
SSLインスペクションを設定する	823
ポート設定を変更する	824
トラフィックがPerfect Forward Secrecy (PFS)で暗号化されている場合に侵入防御 を使用する	825
Diffie-Hellman暗号化の特別な注意事項	825
サポートされている暗号化スイート	826
サポートされているプロトコル	827
回避技術対策の設定	827
侵入防御のパフォーマンスに関するヒント	832
設定パッケージの最大サイズ	834
ファイアウォールを使用したエンドポイントトラフィックの制御	835
ファイアウォールルール	835
Deep Securityファイアウォールの設定	836
ファイアウォールルールを配信前にテストする	836
タップモードでテストする	837
インラインモードでテストする	838
「Fail-Open」の動作を有効にする	838
ファイアウォールをオンにする	840
初期設定のファイアウォールルール	840
Deep Security Managerのトラフィックに関するバイパスルールの初期設定	842
厳格または寛容なファイアウォール設計	842
厳格なファイアウォール	842
寛容なファイアウォール	843
ファイアウォールルールの処理	843
ファイアウォールルールの優先度	844
許可ルール	844
強制的に許可ルール	845
バイパスルール	845

推奨されるファイアウォールポリシールール	845
ファイアウォールルールをテストする	845
攻撃の予兆検索	846
ステートフルインスペクション	848
例	848
重要事項	849
ファイアウォールルールの作成	850
新しいルールを追加する	851
ルールの動作とプロトコルを選択する	851
パケットの送信元と送信先を選択する	854
ルールイベントとアラートを設定する	855
アラート	855
ルールのスケジュールを設定する	855
ルールにコンテキストを割り当てる	856
ルールが割り当てられているポリシーとコンピュータを確認する	856
ルールをエクスポートする	856
ルールを削除する	856
信頼済みトラフィックに対するファイアウォールのバイパス許可	857
信頼済みトラフィックのソースの新しいIPリストを作成する	857
IPリストを使用して信頼済みトラフィックの受信用と送信用のファイアウォール ルールを作成する	857
信頼済みトラフィックが通過するコンピュータで使用されているポリシーにファイ アウォールルールを割り当てる	858
ファイアウォールルールの処理と優先度	858
ファイアウォールルールの処理	858
許可ルールの詳細	859
バイパスルールの詳細	859
Deep Security Managerのトラフィックに関するバイパスルールの初期設定	860
強制的に許可ルールの詳細	861
ファイアウォールルールのシーケンス	861

ログに関する注意	862
各ファイアウォールルールとの関係	863
ルール処理	863
ルール優先度	865
ルール処理およびルール優先度を集約する	865
ファイアウォールの設定	866
一般	866
ファイアウォール	866
ファイアウォールステートフル設定	866
ポート検索 (コンピュータエディタのみ)	866
割り当てられたファイアウォールルール	867
インタフェース制限	868
インタフェース制限	868
インタフェースパターン	868
攻撃の予兆	869
攻撃の予兆検索	869
詳細	871
イベント	871
イベント	871
Oracle RACでのファイアウォール設定	871
ノード間の接続を許可するルールを追加する	872
UDPポート42424を許可するルールを追加する	872
その他のRAC関連パケットを許可する	874
Oracle SQL Serverルールが割り当てられていることを確認する	877
回避技術対策の設定が「標準」に設定されていることを確認する	877
ステートフルファイアウォールの設定の定義	878
ステートフル設定を追加する	879
ステートフル設定情報を入力する	879
パケットインスペクションオプションを選択する	879

IPパケットインスペクション	879
TCPパケットインスペクション	880
FTPオプション	881
UDPパケットインスペクション	882
ICMPパケットインスペクション	882
ステートフル設定をエクスポートする	883
ステートフル設定を削除する	883
ステートフル設定が割り当てられたポリシーとコンピュータを表示する	883
オープンポートの検索	884
コンテナのファイアウォールルール	885
Kubernetesファイアウォールルール	885
Swarmファイアウォールルール	886
変更監視によるシステム変更の監視	886
変更監視の設定	887
変更監視を有効にする方法	887
変更監視をオンにする	887
推奨設定の検索を実行する	888
変更監視ルールを適用する	889
コンピュータのベースラインを構築する	891
変更を定期的に検索する	891
変更監視をテストする	891
変更監視検索を実行するタイミング	892
変更監視検索パフォーマンスの設定	893
CPUの使用率を制限する	893
コンテンツハッシュアルゴリズムを変更する	894
仮想マシンの検索キャッシュ設定を有効にする	894
変更監視イベントのタグ付け	894
変更監視ルールの作成	895
新しいルールを追加する	895

変更監視ルール情報を入力する	896
ルールテンプレートを選択し、ルールの属性を定義する	896
レジストリ値テンプレート	896
ファイルテンプレート	897
カスタム (XML) テンプレート	897
トレンドマイクロが発行する変更監視ルールを設定する	897
ルールイベントとアラートを設定する	898
リアルタイムのイベント監視	898
アラート	899
ルールが割り当てられているポリシーとコンピュータを確認する	899
ルールをエクスポートする	899
ルールを削除する	899
Virtual Applianceの検索キャッシュ	899
検索キャッシュ設定	900
不正プログラム検索のキャッシュ設定	901
変更監視の検索のキャッシュ設定	901
検索キャッシュの管理設定	901
初期設定を変更する場合の考慮事項	902
セキュリティログ監視によるログの分析	903
セキュリティログ監視の設定	903
セキュリティログ監視モジュールをオンにする	904
推奨設定の検索を実行する	904
推奨されるセキュリティログ監視ルールを適用する	905
セキュリティログ監視をテストする	906
セキュリティログ監視イベントの転送と保存を設定する	907
ポリシーで使用する セキュリティログ監視 ルールを定義する	907
新しいセキュリティログ監視ルールを作成する	908
デコーダ	910
サブルール	911

グループ	911
ルール、ID、およびレベル	912
説明	914
デコード形式	914
一致項目	914
条件文	915
評価の階層	916
ログエントリのサイズに関する制限	917
コンポジットルール	918
実際の使用例	920
セキュリティログ監視ルールの重要度レベルと推奨される使用法	928
strftime() 変換指定子	929
セキュリティログ監視ルールの確認	930
セキュリティログ監視のルール構造とイベント照合プロセス	930
重複しているサブルール	932
Webレピュテーションによる不正なURLへのアクセスのブロック	933
Webレピュテーションモジュールをオンにする	934
インラインモードとタップモードを切り替える	934
セキュリティレベルを適用する	935
セキュリティレベルを設定するには、次の手順に従います。	935
例外設定を作成する	936
URL例外設定を作成するには、次の手順に従います。	936
Smart Protection Serverを設定する	937
Smart Protection Serverへの接続の警告	938
詳細設定を編集する	938
ブロックページ	938
アラート	939
ポート	939
Webレピュテーションをテストする	939

SAP NetWeaverとの統合	940
Deep Security Scanner機能を有効にする	940
SAPサーバを追加する	941
コンピュータまたはポリシーでSAP統合機能を有効にする	941
SAP統合を設定する	941
Deep SecurityとSAPのコンポーネント	943
Agentをインストールする	944
SAPサーバをManagerに追加する	945
ManagerでSAPを有効化する	945
SAPサーバを追加する	945
Agentの有効化	945
セキュリティプロファイルを割り当てる	948
Agentを使用するようにSAPを設定する	954
トレンドマイクロのスキナグループを設定する	955
トレンドマイクロのウイルススキャンプロバイダを設定する	961
トレンドマイクロのウイルススキャンプロファイルを設定する	967
ウイルススキャンインタフェースをテストする	977
サポートされているMIMEタイプ	983
Deep Securityのベストプラクティスガイド	988
管理	988
ライセンス情報の確認	988
データベースのバックアップと復元	989
データベースをバックアップする	989
データベースのみを復元する	990
Deep Security Managerとデータベースの両方を復元する	990
オブジェクトをXML形式またはCSV形式でエクスポートする	990
オブジェクトをインポートする	992
Deep Security Managerの再起動	993
Linux	993

Windows	993
Windowsデスクトップ	993
コマンドプロンプト	993
PowerShell	994
Deep Securityのアップグレード	994
アップグレードについて	994
Agentによるアップデートの整合性の検証方法	995
Deep Security Managerによるソフトウェアアップグレードの確認方法	996
Deep Security Relayのアップグレード	997
Deep Security Agentのアップグレード	998
アラートからAgentをアップグレードする	999
Agentのアップグレードを開始する	1000
新しく有効化されたVirtual ApplianceのAgentを選択する	1001
Agentを手動でアップグレードする	1001
Windows上でAgentを手動でアップグレードする	1002
Linux上でAgentを手動でアップグレードする	1002
Solaris上でAgentを手動でアップグレードする	1002
ds_adm.fileの内容	1004
AIX上のエージェントを手動でアップグレードする	1005
Deep Security Virtual Applianceのアップグレード	1006
Applianceのサポート期間とアップグレードに関する推奨事項	1006
Appliance SVM、組み込みのAgent、およびDeep Security Managerのバージョン は一致している必要がありますか	1007
アップグレードする必要があるかどうかを確認する	1007
現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する ..	1008
新しいAppliance SVMがあるかどうかを確認する	1008
新しいAgentがあるかどうかを確認する	1009
Applianceをアップグレードする	1009
既存のAppliance SVMを自動的にアップグレードする	1010

開始前の準備	1010
手順1: 新しいVirtual ApplianceパッケージをManagerにインポートする	1011
手順2: ManagerでAppliance SVMをアップグレードする	1012
「Appliance (SVM) のアップグレード失敗」 システムイベントのトラブル シューティング	1015
手順4: 最後の手順	1015
既存のAppliance SVMを手動でアップグレードする	1015
手順1: 新しいVirtual ApplianceパッケージをManagerにインポートする	1016
手順2: 検出ファイルを確認または復元する	1017
手順3: ゲスト仮想マシンを別のESXiホストに移行する	1017
手順4: 古いAppliance SVMをアップグレードする	1019
NSX-Vの手順	1023
NSX-Tの手順	1025
手順5: メンテナンスモードがオフになっていることを確認する	1025
手順6: 新しいAppliance SVMが有効化されていることを確認する	1025
手順7: 最後の手順	1027
Appliance SVMに組み込まれているAgentをアップグレードし、OSパッチを適用 する	1028
互換性の表: Appliance、Agent、パッチ	1030
エラー: データベースサーバへの安全な接続を確立できませんでした	1030
NSXライセンスをアップグレードして、利用できるDeep Securityの機能を増やす ..	1031
手順1: NSXライセンスをアップグレードする	1032
手順2: Deep SecurityをNSXからすべて削除する	1038
手順3: Deep Security Virtual Applianceを再インストールする	1038
セキュリティアップデートの取得と配布	1039
セキュリティアップデート元および設定を指定する	1042
不正プログラム対策エンジンのアップデートを設定する	1043
セキュリティアップデートを実行する	1044
Special case: エアギャップ環境におけるRelay有効化済みAgentでのアップデー トを設定する	1044

セキュリティアップデートのステータスを確認する	1045
パターンファイルアップデートの詳細を確認する	1045
ルールアップデートの詳細を確認する	1046
ソフトウェアアップデートを配布するWebサーバの使用	1047
Webサーバのシステム要件	1048
フォルダ構造をコピーする	1048
新しいソフトウェアリポジトリを使用するようにAgentを設定する	1050
新しいパターンファイルアップデートアラートのメールの無効化	1051
エージェントパッケージの整合性チェック	1052
トラブルシューティング	1052
サポートされるDeep Security Relayのバージョン	1053
Deep Securityの強化	1053
Agentを使用したDeep Security Managerの保護	1054
Deep Security Agentの保護	1055
特定のDeep Security ManagerへのDeep Security Agentのバインド	1055
Deep Security Manager TLS証明書の置き換え	1057
Java Keystoresについて	1058
秘密鍵とキーストアを生成する	1058
CSRを生成して証明書を要求する	1060
署名された証明書をキーストアにインポートする	1060
署名付き証明書ストアを使用するようにDeep Securityを設定する	1062
Deep Security Managerとデータベース間の通信の暗号化	1063
Managerとデータベースの間の通信を暗号化する	1064
Microsoft SQL Serverデータベース (Linux)	1064
Microsoft SQL Server (Windows)	1066
Oracle Database	1068
PostgreSQL	1069
データベースサーバでAgentを実行する	1070
Managerとデータベース間の暗号化を無効にする	1070

Microsoft SQL Serverデータベース (Linux)	1071
Microsoft SQL Server (Windows)	1071
Oracle Database	1072
PostgreSQL	1072
Deep Security Managerのデータベースのパスワードの変更	1072
Microsoft SQL Serverのパスワードを変更する	1073
Oracleのパスワードを変更する	1073
PostgreSQLのパスワードを変更する	1074
HTTPセキュリティヘッダの設定	1075
カスタマイズ可能なセキュリティヘッダ	1075
HTTPの厳密なトランスポートセキュリティ (HSTS)	1076
Content Security Policy (CSP)	1076
HTTP公開鍵ピンニング (HPKP)	1078
カスタマイズ可能なセキュリティヘッダを有効化する	1078
設定をリセットする	1078
HTTPの厳密なトランスポートセキュリティ	1079
Content Security Policy (CSP)	1079
Public Key Pinning Policy	1079
強制的に適用されるセキュリティヘッダ	1079
Cache-ControlおよびPragma	1079
X-XSS-Protection	1080
X-Frame-Options	1080
サポートされていないセキュリティヘッダ	1080
X-Content-Type-Options	1081
ユーザパスワードルールの適用	1081
パスワード要件を指定する	1081
ログオンに別のIDプロバイダを使用する	1082
Deep Security Managerログオンページにメッセージを追加する	1083
ユーザに使用条件を提示する	1083

その他のセキュリティ設定	1083
多要素認証の設定	1083
多要素認証を有効にする	1084
多要素認証を無効にする	1086
サポートされる多要素認証 (MFA) アプリケーション	1087
MFAをトラブルシューティングする	1088
MFAデバイスを有効にしても機能しない場合の対処	1088
MFAデバイスが紛失または動作停止した場合の対処	1088
AWSリージョンの管理	1089
Amazon Web Servicesのリージョンを追加する	1089
Amazon Web Servicesのリージョンを表示する	1090
Amazon Web Servicesのリージョンを削除する	1090
アラートの設定	1091
Deep Security Managerにアラートを表示する	1091
アラートを設定する	1092
アラートのメール通知を設定する	1092
アラートメールのオンとオフを切り替える	1094
アラートメールを受信するユーザを個別に設定する	1099
すべてのアラートメールの受信者を設定する	1099
アラートやその他のアクティビティに関するレポートの生成	1099
単独レポートを設定する	1099
定期レポートを設定する	1103
ダッシュボードのカスタマイズ	1104
日時の範囲	1105
コンピュータおよびコンピュータグループ	1106
タグごとのフィルタ	1107
ダッシュボードのウィジェットを選択する	1108
監視:	1109
システム:	1110

ランサムウェア:	1110
不正プログラム対策:	1110
Webレピュテーション:	1111
ファイアウォール:	1111
侵入防御:	1112
変更監視:	1113
セキュリティログ監視:	1113
アプリケーションコントロール:	1114
レイアウトを変更する	1114
ダッシュボードのレイアウトを保存/管理する	1115
Deep Securityのイベント	1116
Agentでのイベントログの場所	1116
イベントがManagerに送信されるタイミング	1117
イベントが保持される期間	1118
システムイベント	1118
セキュリティイベント	1118
ポリシーまたはコンピュータに関連付けられたイベントを確認する	1119
イベントの詳細を表示する	1119
リストをフィルタしてイベントを検索する	1120
イベントをエクスポートする	1121
ログのパフォーマンスを向上する	1121
ログとイベントの保存に関するベストプラクティス	1122
トラブルシューティング	1124
ログファイルのサイズを制限する	1125
イベントログのヒント	1126
不正プログラム検索の失敗イベント	1127
イベントを識別およびグループ化するためのタグの適用	1129
手動によるタグ付け	1130
自動タグ付け	1130

自動タグ付けルールに優先度を設定する	1131
セキュリティログ監視イベントを自動でタグ付けする	1131
信頼済みのソースを使用したタグ付け	1132
信頼済みのローカルコンピュータ	1133
対象コンピュータのイベントと信頼済みのソースコンピュータのイベントの一 致をDeep Securityで判別する仕組み	1133
信頼済みのローカルコンピュータに基づいてイベントにタグを付ける	1134
トレンドマイクロのソフトウェア安全性評価サービスに基づいてイベントにタ グを付ける	1134
信頼済みの共通ベースラインに基づいてイベントにタグを付ける	1135
タグを削除する	1136
ログに記録するイベントの数を減らす	1136
イベントのランク付けによる重要度の数値化	1139
Webレピュテーションイベントのリスク値	1139
ファイアウォールルールの重要度の値	1140
侵入防御ルールの重大度の値	1140
整合性監視ルールの重大度値	1140
検査ルールの重大度の値の記録	1140
資産評価	1141
Deep SecurityイベントをSyslogまたはSIEMサーバに転送する	1141
イベント転送ネットワークトラフィックを許可する	1142
クライアント証明書を要求する	1142
Syslog設定を定義する	1142
システムイベントを転送する	1146
セキュリティイベントを転送する	1146
イベント転送のトラブルシューティング	1147
「Syslogメッセージの送信に失敗」アラート	1147
Syslog設定を編集できません	1148
証明書が期限切れのためにSyslogが転送されない	1148
サーバ証明書が期限切れであるか変更されたためにSyslogが配信されない	1148

互換性	1148
syslogメッセージの形式	1149
CEFのsyslogメッセージの形式	1149
LEEF 2.0のsyslogメッセージの形式	1152
マネージャーから発信されたイベント	1152
システムイベントログの形式	1152
Agentで発生するイベント	1154
不正プログラム対策イベントの形式	1154
アプリケーション制御イベントの形式	1172
ファイアウォールイベントログの形式	1180
整合性監視イベントのログ	1183
侵入防御イベントログの形式	1187
ログ検査イベントの形式	1194
Webレピュテーションイベントの形式	1196
Red Hat Enterprise Linuxでイベントログを受信するための設定	1198
Red Hat Enterprise Linux 6または7でSyslogを設定する	1198
Red Hat Enterprise Linux 5でSyslogを設定する	1200
Amazon SNSでのイベントへのアクセス	1200
AWSユーザを作成する	1201
Amazon SNSトピックを作成する	1202
SNSを有効にする	1202
サブスクリプションを作成する	1203
JSON形式でのSNS設定	1203
Version	1203
Statement	1204
Topic	1204
Condition	1204
Bool	1205
Exists	1206

IpAddress	1207
NotIpAddress	1208
NumericEquals	1209
NumericNotEquals	1210
NumericGreaterThan	1211
NumericGreaterThanEquals	1212
NumericLessThan	1213
NumericLessThanEquals	1213
StringEquals	1214
StringNotEquals	1215
StringEqualsIgnoreCase	1216
StringNotEqualsIgnoreCase	1216
StringLike	1216
StringNotLike	1217
複数の文と複数の条件	1219
複数の文	1219
複数の条件	1220
SNS設定の例	1221
重大なすべての侵入防御イベントをSNSトピックに送信する	1221
イベントごとに異なるSNSトピックに送信する	1222
JSON形式のイベント	1223
有効なイベントプロパティ	1223
イベントプロパティのデータタイプ	1243
JSON形式のイベントの例	1245
システムイベント	1245
不正プログラム対策イベント	1247
リモートコンピュータにSNMP経由でシステムイベントを転送	1248
イベントとアラートのリスト	1248
事前定義アラート	1249

Agentイベント	1265
システムイベント	1271
アプリケーションコントロールイベント	1317
アプリケーションコントロールイベントで表示される情報	1317
アプリケーションコントロールイベント一覧	1319
不正プログラム対策イベント	1319
不正プログラム対策イベントで表示される情報	1319
不正プログラム対策イベント一覧	1321
ファイアウォールイベント	1322
ファイアウォールイベントで表示される情報	1322
ファイアウォールイベント一覧	1324
侵入防御イベント	1331
侵入防御イベントで表示される情報	1332
侵入防御イベントの追加情報の表示。	1333
侵入防御イベント一覧	1334
変更監視イベント	1337
変更監視イベントで表示される情報	1337
変更監視イベント一覧	1338
セキュリティログ監視イベント	1340
セキュリティログ監視イベントで表示される情報	1340
セキュリティログ監視のセキュリティイベント一覧	1342
Webレピュテーションイベント	1342
Webレピュテーションイベントで表示される情報	1343
許可するURLのリストにURLを追加する	1343
共通イベント、アラート、およびエラーのトラブルシューティング	1343
ファイアウォールモジュールが無効であるにも関わらず、ファイアウォールイベントが発生する理由	1345
イベントID 771 「認識できないクライアントによる接続」のトラブルシューティング	1345
Deep Security Agentをアンインストールする	1345

コンピュータまたはクローンを再有効化する	1346
VMwareコネクタの同期の中断を修正する	1346
「Smart Protection Serverへの接続不能」エラーのトラブルシューティング	1346
エラーの詳細を確認する	1346
Deep Security Virtual Applianceの問題	1347
エラー: 有効化に失敗	1347
プロトコルエラー	1348
Agentから開始	1348
双方向の通信	1348
ホスト名解決不能	1348
エージェント/アプライアンスがありません	1349
ポートのブロック	1349
重複するコンピュータ	1350
プロキシ経由のエンドポイント	1351
再インストールが必要です	1351
エラー: サポートされていないAgentバージョン	1351
エラー: 不正プログラム検索エンジンオフライン	1351
Agentベースの保護	1352
エージェントがWindowsの場合:	1352
エージェントがLinuxにインストールされている場合:	1353
Agentレスによる保護	1353
エラー: ステータスの確認の失敗	1354
エラー: 機能「dpi」のインストール失敗: 使用不可: フィルタ	1355
追加情報	1355
エラー: 仮想マシンを有効化した後に「変更監視エンジンがオフライン」およびその他のエラーが発生する	1356
エラー: インタフェースが非同期	1356
仮想マシンのインタフェースを確認する	1357
vCenterで仮想マシンのインタフェース情報を確認する	1357

Deep Security Managerでvmxファイルと仮想マシンのインタフェース情報を確認する	1358
Deep Security Virtual Applianceの仮想マシンのインタフェース情報を確認する	1358
回避策	1359
回避策1	1359
回避策2	1360
回避策3	1360
詳細なトラブルシューティング手順	1360
エラー: 侵入防御ルールのコンパイルに失敗しました	1361
侵入防御のベストプラクティスを適用する	1362
ルールを管理する	1362
個々のポートからアプリケーションの種類の割り当てを解除する	1363
エラー: セキュリティログ監視ルールに必要なログファイル	1364
ファイルの場所が必要な場合:	1365
リストされたファイルが保護対象マシンに存在しない場合:	1365
エラー: モジュールのインストール失敗 (Linux)	1365
エラー: このコンピュータに1つ以上のアプリケーションの種類の競合がある	1366
解決方法	1367
ポートを統合する	1367
継承オプションを無効にする	1367
エラー: クラウドアカウントに接続できない	1368
AWSアカウントのアクセスキーIDまたは秘密アクセスキーが無効である	1368
Deep Securityで使用するアカウントに間違ったAWS IAMポリシーが適用されている	1369
NAT、プロキシ、またはファイアウォールのポートが開いていないか、設定が正しくない	1369
エラー: インスタンスのホスト名を解決できない	1370
アラート: 変更監視情報の収集が遅延しています	1370
アラート: Managerの時刻が非同期	1370
アラート: Managerノードのメモリの警告しきい値を超過しました	1371

イベント: 最大TCP接続数	1371
警告: Census、Good File Reputation、機械学習型検索サービスへの接続解除	1372
原因1: AgentまたはRelay有効化済みAgentがインターネットにアクセスできない	1373
原因2: プロキシは有効化されているが、適切に設定されていない	1373
警告: ディスク容量の不足	1374
ヒント	1374
警告: 攻撃の予兆の検出	1374
攻撃の予兆の検出の種類	1375
推奨処理	1375
ユーザの作成と管理	1376
Active Directoryと同期する	1377
ユーザを個別に追加または編集する	1378
ユーザのパスワードを変更する	1381
ユーザをロックアウトする/ロックアウトをリセットする	1381
ユーザに関連付けられたシステムイベントを表示する	1382
ユーザを削除する	1382
ユーザロールの定義	1382
役割を追加または編集する	1383
Full Access、Auditor、および新規の各役割の初期設定	1395
レポートのみを受信できるユーザの追加	1406
連絡先を追加または編集する	1406
連絡先を削除する	1406
ユーザ向けのAPIキーの作成	1407
既存のAPIキーをロックアウトする	1408
ロックアウトされたユーザ名のロック解除	1408
管理者としてユーザのロックを解除する	1408
コマンドラインから管理ユーザのロックを解除する	1409
SAMLシングルサインオン (SSO) を実装する	1409

SAMLとシングルサインオンとは	1409
Deep SecurityでのSAMLシングルサインオンの仕組み	1410
信頼関係を確立する	1410
ユーザIDからDeep Securityアカウントを作成する	1410
Deep SecurityでSAMLシングルサインオンを実装する	1411
SAMLシングルサインオンを設定する	1412
設定前の要件を設定する	1413
Deep SecurityをSAMLサービスプロバイダとして設定する	1413
Deep SecurityでSAMLを設定する	1414
IDプロバイダSAMLメタデータドキュメントをインポートする	1414
SAMLユーザのDeep Securityの役割を作成する	1414
IDプロバイダの管理者に情報を提供する	1415
Deep Security ManagerサービスプロバイダSAMLメタデータドキュメントを ダウンロードする	1415
URNおよびDeep Security SAMLメタデータドキュメントをIDプロバイダの管 理者に送信する	1415
SAMLクレームの構造	1415
Deep Securityユーザ名 (必須)	1416
SAMLデータの例 (簡略版)	1416
Deep Securityユーザの役割 (必須)	1416
SAMLデータの例 (簡略版)	1417
最大セッション期間 (オプション)	1417
SAMLデータの例 (簡略版)	1417
言語設定 (オプション)	1418
SAMLデータの例 (簡略版)	1418
SAMLシングルサインオンをテストする	1418
設定を確認する	1419
診断パッケージを作成する	1419
サービスとIDプロバイダの設定	1419
SAMLシングルサインオンをAzure Active Directoryで設定する	1419

誰がこのプロセスに関与していますか？	1420
Deep SecurityをSAMLサービスプロバイダとして設定する	1421
Deep SecurityサービスプロバイダのSAMLメタデータドキュメントをダウンロードする	1421
Azure Active Directoryを設定する	1421
Deep SecurityでSAMLを設定する	1422
Azure Active Directoryメタデータドキュメントをインポートする	1422
SAMLユーザのDeep Securityの役割を作成する	1423
URNを取得する	1423
Azure Active Directoryで役割を定義する	1423
サービスとIDプロバイダの設定	1424
SAMLクレームの構造	1424
Deep Securityユーザ名 (必須)	1424
SAMLデータの例 (簡略版)	1424
Deep Securityユーザの役割 (必須)	1425
SAMLデータの例 (簡略版)	1425
最大セッション期間 (オプション)	1425
SAMLデータの例 (簡略版)	1426
言語設定 (オプション)	1426
SAMLデータの例 (簡略版)	1426
Deep Security Managerの移動とカスタマイズ	1427
スマートフォルダによるコンピュータの動的なグループ化	1427
スマートフォルダを作成する	1428
スマートフォルダを編集する	1431
スマートフォルダのクローンを作成する	1431
サブフォルダを使用して検索を絞り込む	1431
サブフォルダを自動作成する	1432
検索可能なプロパティ	1433
一般	1433

AWS	1436
Azure	1439
vCenter	1440
vCloud	1441
フォルダ	1441
演算子	1442
アクティブなDeep Security Managerノードの表示	1444
詳細なシステム設定のカスタマイズ	1446
プライマリテナントアクセス	1446
ロードバランサ	1447
マルチテナントモード	1447
Deep Security Managerプラグイン	1448
SOAP WebサービスAPI	1448
ステータス監視API	1448
エクスポート	1449
Whois	1449
ライセンス	1449
推奨設定の検索中のCPU使用率	1449
NSX	1450
ロゴ	1450
Manager AWS ID	1450
アプリケーションコントロール	1451
コンプライアンスの推進	1456
Deep SecurityによるPCI DSS要件への対応	1456
Common Criteriaの設定	1457
GDPR	1457
FIPS 140-2のサポート	1457
FIPSモードでDeep Securityを操作する場合の違い	1458
FIPSモードのシステム要件	1459

Deep Security Managerの要件	1459
Deep Security Agentの要件	1460
Deep Security Virtual Applianceの要件	1460
Deep Security ManagerでFIPSモードを有効にする	1460
WindowsでDeep Security ManagerのFIPSモードを有効にする	1460
LinuxでDeep Security ManagerのFIPSモードを有効にする	1461
FIPSモードで外部サービスに接続する	1461
保護しているコンピュータのOSのFIPSモードを有効にする	1462
保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする	1462
Windows AgentのFIPSモードを有効にする	1462
RHEL 7またはCentOS 7 AgentのFIPSモードを有効にする	1462
Deep Security Virtual ApplianceでFIPSモードを有効にする	1463
PostgreSQLデータベースでFIPSモードを使用する	1463
Microsoft SQL ServerデータベースでFIPSモードを使用する	1467
FIPSモードを無効にする	1469
Deep Securityでの脆弱性管理検索トラフィックのバイパス	1470
脆弱性検索プロバイダのIP範囲またはアドレスから新しいIPリストを作成する	1470
受信および送信検索トラフィック用のファイアウォールルールを作成する	1471
新規ファイアウォールルールをポリシーに割り当てて、脆弱性検索をバイパスする	1472
Deep SecurityでのTLS 1.2の使用	1472
TLS 1.2のアーキテクチャ	1474
TLS 1.2を使用するようにコンポーネントをアップグレードする	1479
Deep Security Managerを確認してアップグレードする	1479
Deep Security Managerデータベースを確認する	1479
Deep Security Agentを確認する	1480
Deep Security Relayを確認する	1480
Deep Security Virtual Applianceを確認する	1481
TLS 1.2を強制する	1482

TLS 1.2を強制できるコンポーネント	1482
TLS 1.2を強制した場合の動作	1482
初期設定でTLS 1.2が強制されるかどうか	1483
TLS 1.2の強制が可能になる場合の条件	1483
Deep Security ManagerでTLS 1.2を強制する	1483
Deep Security RelayでTLS 1.2を強制する	1484
ManagerのGUIポート (4119) でのみTLS 1.2を強制する	1484
TLS 1.2の強制をテストする	1485
初期のTLS (1.0) を有効にする	1487
Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする	1487
ManagerのGUIポートでTLS 1.0を有効にする (4119)	1488
インストールスクリプトでTLS 1.0を有効にする	1488
TLS 1.2が強制されているかどうかを確認する	1489
TLS 1.2の強制後のAgent、Virtual Appliance、Relayのインストールに関するガイドライン	1489
TLS 1.2が強制されているときのAgent、Virtual Appliance、およびRelayのインストールに関するガイドライン	1490
TLS 1.2の強制後にインストールスクリプトを使用する場合のガイドライン	1490
TLS 1.2の強力な暗号化スイートの有効化	1491
Deep Securityコンポーネントをアップデートする	1491
TLS 1.2の強力な暗号化スイートを有効にするためのスクリプトを実行する	1492
スクリプトの動作を確認する	1493
nmapを使用してManagerを確認する	1494
nmapを使用してRelayを確認する	1495
nmapを使用してAgentを確認する	1496
TLS 1.2の強力な暗号化スイートを無効にする	1497
Deep Securityの暗号化アルゴリズムのアップグレード	1498
Windowsでアルゴリズムをアップグレードする	1498
Linuxでアルゴリズムをアップグレードする	1499
複数ノード環境でアルゴリズムをアップグレードする	1499

マルチテナント環境でアルゴリズムをアップグレードする	1500
Microsoft SQL Server ExpressデータベースのEnterpriseへの移行	1500
Deep Securityのアンインストール	1501
Deep Security Relayをアンインストールする	1502
Relayをアンインストールする (Windows)	1502
Relayをアンインストールする (Linux)	1503
Deep Security Agentをアンインストールする	1503
Agentをアンインストールする (Windows)	1503
Agentをアンインストールする (Linux)	1504
Agentをアンインストールする (Solaris 10)	1505
Agentをアンインストールする (Solaris 11)	1505
Agentをアンインストールする (AIX)	1505
Deep Security Notifierをアンインストールする	1506
Deep Security Managerをアンインストールする	1506
Managerをアンインストールする (Windows)	1506
Managerをアンインストールする (Linux)	1507
NSX環境からのDeep Securityのアンインストール	1507
NSX-V環境からのDeep Securityの自動アンインストール	1508
NSX-V環境からのDeep Securityの手動アンインストール	1511
最初に、Deep Security ManagerからNSX Managerを削除します	1511
次に、NSX Managerでトレンドマイクロのサービスを削除します	1511
NSX-T環境からのDeep Securityの手動アンインストール	1519
非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化	1523
非アクティブなAgentのクリーンナップを有効にする	1524
長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護	1524
オーバーライド設定による特定のコンピュータの削除の回避	1524
非アクティブなAgentのクリーンナップジョブによって削除されたコンピュータの監査証跡の確認	1525

システムイベントを検索する	1525
システムイベントの詳細	1526
2953 - 非アクティブなAgentのクリーンアップが正常に完了しました	1526
251 - コンピュータの削除	1527
716 - 不明なAgentの再有効化の試行	1527
Workload Securityへのポリシーの移行	1527
要件	1528
ポリシーの移行	1528
移行状態を確認する	1529
トラブルシューティング	1529
よくある質問	1530
保護をオンにするとWindowsマシンのネットワーク接続が失われる理由	1530
Deep Securityに関するニュースの取得方法	1530
Solarisゾーンでのエージェント保護はどのように機能しますか?	1531
侵入防御 (IPS)、ファイアウォール、およびWebレピュテーション	1531
共有IPネットワークインタフェースを使用する非グローバルゾーン	1532
専用IPネットワークインタフェースを使用する非グローバルゾーン	1532
不正プログラム対策、変更監視、およびセキュリティログ監視	1533
Solaris ControlドメインとLogical Domainsのエージェント保護はどのように機能しますか?	1533
Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか	1534
AWS GovCloud (US) インスタンスを保護するにはどうすればいいですか?	1535
AWS GovCloud (US) のAWSインスタンスの管理者によるインスタンスの保護	1536
Azure Governmentのインスタンスを保護するにはどうすればいいですか?	1536
AWS Elastic Beanstalk環境でオフライン環境に対するハートビートアラートを最小限に抑える方法	1539
Azureクラウドコネクタを使用してAzureサーバを追加できない	1540
Deep SecurityでAzureサブスクリプションの一部の仮想マシンが表示されない	1540
トラブルシューティング	1541

「オフライン」のAgent	1541
原因	1541
Agentが実行されていることを確認する	1543
DNSを検証する	1543
送信ポートを許可する (Agentからのハートビート)	1544
受信ポートを許可する (Managerからのハートビート)	1545
Amazon AWS EC2インスタンスでICMPを許可する	1545
Solaris 11でのアップグレードの問題を解決する	1546
CPU使用率が高い	1546
VMwareの「不正プログラム対策ドライバがオフライン」ステータス	1547
Windowsプラットフォーム用不正プログラム対策のアップデート失敗	1547
互換性のない他のトレンドマイクロ製品の不正プログラム対策コンポーネント	1548
互換性のないサードパーティ製品の不正プログラム対策コンポーネント	1548
その他のエラー/不明なエラー	1548
Agentレスによる仮想マシンのパフォーマンスの問題	1549
原因:限られたリソース	1549
原因:不正プログラム対策	1549
原因:ネットワークトラフィック	1549
原因:ポリシー	1549
原因:CPU使用率が高い	1550
原因:セキュリティアップデート	1550
セキュリティアップデートの接続	1551
SQL Serverドメイン認証の問題	1552
手順1: ホスト名とドメインを確認する	1552
手順2: servicePrincipalName (SPN) を確認する	1554
手順2a: SQL Serverサービスを実行しているアカウント (SID) を特定する	1555
手順2b: Active Directoryでアカウントを確認する	1557
手順2c: SPNで使用するFQDNを特定する	1558

手順2d: 初期設定のインスタンスを使用しているのか、名前付きインスタンスを使用しているのかを特定する	1558
ケース1: ローカル仮想アカウントでSPNを設定する	1559
ケース2: ドメインアカウントでSPNを設定する	1561
ケース3: 管理されたサービスアカウントでSPNを設定する	1563
ケース4: フェールオーバークラスタのSPNを設定する	1565
SPNリファレンス	1567
SPNのデバッグのヒント	1567
手順3: krb5.confファイルを確認する (Linuxのみ)	1568
手順4: システム時計を確認する	1570
手順5: ファイアウォールを確認する	1570
複数のAmazon Virtual Private Cloud (VPC) からのAgent通信でMTUが原因で発生する問題の回避	1571
診断パッケージとログの作成	1573
Deep Security Managerの診断	1573
Deep Security Managerの診断パッケージを作成する	1573
Deep Security Managerのデバッグログを有効にする	1573
Deep Security Agentの診断	1574
Deep Security Managerを使用してAgentの診断パッケージを作成する	1575
保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する	1576
DebugViewを使用してデバッグログを収集する	1577
詳細な診断パッケージのプロセスメモリを増やす	1578

Trend Micro Deep Securityについて

Deep Securityトラストセンター

Deep Security製品使用状況データ収集

Trend Micro Deep Security Managerの品質向上に役立てるため、パフォーマンスおよび機能の使用状況データを匿名で収集します。Trend Micro 収集したデータは、製品の品質向上を目的として社内でのみ使用されます。外部の関係者とデータを共有したり、個人が特定できる情報をデータに含めたりすることはありません。

Trend MicroがDeep Securityをより効果的にサポートできるように、データ収集は有効にしておくことをお勧めします。しかし、Deep Security Managerによるデータ収集を希望しない場合は、データ収集を無効にできます。

データ収集を無効にするには、[システム設定]→[詳細]→[製品使用状況データ収集]の順に選択し、[製品使用状況データ収集]の選択を解除します。

注意: データ収集を無効化するには、Deep Security Managerを再起動する必要があります。複数ノード構成でDeep Security Managerを実行している場合は、各ノードを再起動する必要があります。

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の条例において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Deep Securityにより収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次のWebサイトを参照してください。

<http://www.go-tm.jp/data-collection-disclosure>

※重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Deep Securityにおける無効化の影響をご確認の上、無効化はお客様の責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客様のデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

Deep Securityコンポーネントについて

Trend Micro Deep Security (以下、Deep Security) は、物理、仮想、およびクラウドサーバに高度なサーバセキュリティを提供し、企業のアプリケーションやデータを保護し、緊急でのパッチ適用を必要とすることなくデータ漏えいやビジネスの中断を防ぎます。この包括的な中央管理プラットフォームにより、セキュリティに関する処理を簡素化すると同時に、仮想化およびクラウドプロジェクトのROIを向上できます。

Deep Securityで利用できる保護モジュールの詳細については、"**保護**" on page 504を参照してください。

Deep Securityは、次のコンポーネントセットで構成されています。これらは連携して動作し、保護を提供します。

- Deep Security Manager: 管理者がセキュリティポリシーを設定し、Deep Security Virtual ApplianceおよびDeep Security Agentの保護を実施するのに使用する、Webベースの管理コンソールです。
- Deep Security Virtual Appliance: VMware vSphere環境用に構築されたセキュリティ仮想マシン。vShield環境の仮想マシンに対して不正プログラム対策や変更監視の保護モジュールをAgentレスで提供します。NSX環境では、不正プログラム対策、変更監視、ファイアウォール、侵入防御、Webレピュテーションの各モジュールをAgentレスで利用できます。
- Deep Security Agent: コンピュータ上に直接インストールされるセキュリティエージェント。アプリケーションコントロール、不正プログラム対策、Webレピュテーションサービス、ファイアウォール、侵入防御、変更監視、およびセキュリティログ監視保護を提供します。
- Deep Security AgentにはRelayモジュールが含まれています。Relay有効化済みAgentは、Deep Securityコンポーネントのネットワーク全体にソフトウェアアップデートとセキュリティアップデートを配信します。

- Deep Security Notifier (Notifier): 保護対象のコンピュータに関するセキュリティ通知をユーザに表示する、Windowsのシステムトレイアプリケーションです。Deep Securityが不正プログラムやWebページへのアクセスをブロックしたときにも、ポップアップ通知が表示されます。Notifierは、Virtual Applianceで保護されているコンピュータ上にインストールできます。Windows用Agentをインストールする際は一緒にインストールされません。Relay有効化済みAgentの場合、ローカルのコンピュータから配信されるセキュリティアップデートに関する情報も表示されます。

Deep Securityのリリースライフサイクルとサポートポリシー

Deep Securityのリリースには2種類あります。

- 長期間サポート (LTS) リリース: Deep SecurityのLTSリリースは毎年公開されます。これには新機能、既存の機能の強化、およびバグフィックスが含まれます。LTSリリースでは、下記の"[LTSリリースのサポート期間およびアップグレードの推奨事項](#)" [on the next page](#)で説明するように、長期間のサポートが提供されます。LTSリリースが一般公開されると、LTSリリースに対するアップデートは、修正と細かい機能強化のみに限定されます。LTSリリースの例: Deep Security 10.0、Deep Security 11.0、Deep Security 12.0
- Feature Release (FR): Feature Releaseでは、年間を通じて継続的にリリースされる新機能をいち早く利用できます。つまり、Feature Releaseでは、Deep Securityの次のLTSリリースを待たなくても、新機能をすぐに利用できます。Feature Releaseの機能は蓄積され、最終的には次のLTSリリースにまとめられます。FRは、下記の"[Feature Releaseのサポート期間およびアップグレードの推奨事項](#)" [on page 82](#)で説明するように、LTSリリースよりもはるかに頻繁にリリースされますが、サポート期間は短くなります。

LTSリリースは、環境への新機能の導入をより厳密に管理したいお客様やサポートを長期間受けることを希望するお客様に適しています。

Feature Releaseは、使用可能になった機能をすぐに利用したいお客様や、Deep Securityを定期的にアップグレードしてFeature Releaseの短いサポート期間に対応できるお客様に適しています。

どちらの種類のリリースを選択する場合も、Agentを定期的にアップグレードすることをお勧めします。新しいバージョンのAgentでは、追加のセキュリティ機能と保護、より高い品質、パフォーマンスの向上、および各プラットフォームの新しいバージョンとの連携を保つためのアップデートが提供されます。

LTSリリースのサポート期間およびアップグレードの推奨事項

コンポーネント	アップグレードのベストプラクティス	サポート
Deep Security Manager	年に1回以上のアップグレード。	3年間の標準サポート、5年間の延長サポート
Deep Security Agent	少なくとも2年ごとのアップグレード。 LTS Agentでは、2つ前までのメジャーリリースからのアップグレード (Deep Security Agent 10.0からDeep Security Agent 12 LTSへのアップグレードなど) をサポートします。 サポートされているリリースを使用し続けるためと、1回のアップグレードで最新のソフトウェアにアップグレードできるようにするために、定期的なアップグレードを計画してください。	3年間の標準サポート、5年間の延長サポート
Deep Security Agent (古いリリースのAgentがそのプラットフォームの「最新」のAgentであるプラットフォーム)	プラットフォームでサポートされているのが、古いリリースのDeep Security Agentのみである場合 (たとえば、Windows 2000では9.6のAgent、Red Hat Enterprise Linux 5では10.0のAgent)、そのプラットフォームの最新のAgentを使用し、アップデートがリリースされたらアップグレードしてください。 各プラットフォームでサポートされるAgentのバージョンの詳細については、" Deep Security Agentのプラットフォーム " on page 182 を参照してください。	プラットフォームに固有
Deep Security Relay	Deep Security Relayは、Relay機能を有効にしたDeep Security Agentです。 Agentのアップグレードの推奨事項とサポートポリシーがRelayにも適用されます。	Agentと同じ
Deep Security Virtual Appliance	" Deep Security Virtual Applianceのアップグレード " on page 1006 の「Applianceのサポート期間およびアップグレードの推奨事項」を参照してください。	

[サポート終了製品のリスト](#)を公開しています。

Feature Releaseのサポート期間およびアップグレードの推奨事項

すべてのアップデートは定期的に予定されているFeature Releaseで提供されます。Feature Releaseは「[Deep Security Software](#)」ページ (英語版) の [Feature Releases] タブから取得できます。

コンポーネント	アップグレードのベストプラクティス	サポート
Deep Security Manager	年に1回以上のアップグレード。	18か月間*
Deep Security Agent	年に1回以上のアップグレード。アップグレードは、機能のリリースから18か月間サポートされます。サポートされているリリースを使用し続けるためと、1回のアップグレードで最新のソフトウェアにアップグレードできるようにするために、定期的なアップグレードを計画してください。	18か月間*
Deep Security Relay	Deep Security Relayは、Relay機能を有効にしたDeep Security Agentです。Agentのアップグレードの推奨事項とサポートポリシーがRelayにも適用されます。	Agentと同じ
Deep Security Virtual Appliance	" Deep Security Virtual Applianceのアップグレード " on page 1006の「Applianceのサポート期間およびアップグレードの推奨事項」を参照してください。	

* Deep Securityチームでは、新しいAgentを使用するのに最小限必要なDeep Security Managerのバージョンを変更しないように努めていますが、一部の新しいAgentではManagerのアップグレードが必要な場合があります。

注意: 18か月を超えるFRでサポートケースを作成するお客様は、サポートが提供される前にサポート期間内のFRにアップグレードする必要があります。

サポートサービス

次の表に、Deep SecurityのLTSリリースおよびFRリリースのライフサイクル中に利用可能なサポート項目を示します。

サポート項目	LTS - 標準サポート	LTS - 延長サポート	FR (1)	配信メカニズム
新機能			✓	<ul style="list-style-type: none"> 新規FR
小規模な機能強化 (中心機能の変更なし)	✓		✓	<ul style="list-style-type: none"> LTSアップデート 新規FR
Linuxカーネルのアップデート	✓	要求に応じて提供	✓	<ul style="list-style-type: none"> Linuxカーネルサポートパッケージ (LKP)
一般的なバグフィックス	✓		✓	<ul style="list-style-type: none"> LTSアップデート 新規FR
重要なバグフィックス (システムクラッシュやハング、または主要機能の喪失)	✓	✓	✓	<ul style="list-style-type: none"> LTSアップデートまたはHotFix 新規FR
重大かつ高度な脆弱性の修正	✓	✓	✓	<ul style="list-style-type: none"> LTSアップデートまたはHotFix 新規FR
中程度および軽微な脆弱性の修正	✓		✓	<ul style="list-style-type: none"> LTSアップデート 新規FR

サポート項目	LTS - 標準サポート	LTS - 延長サポート	FR (1)	配信メカニズム
不正プログラム対策パターンのアップデート	✓	✓	✓	<ul style="list-style-type: none"> アップデートサーバ
侵入防御システムルール、変更監視ルール、およびセキュリティログ監視ルールのアップデート	✓	✓	✓	<ul style="list-style-type: none"> アップデートサーバ
新しいバージョンのサポート対象オペレーティングシステムにおけるAgentとDeep Security Managerのサポート	✓		✓	<ul style="list-style-type: none"> LTSアップデート 新規FR

(1) Deep Security 12 Feature Releaseから開始します。既存のDS 10.xおよびDS 11.xのFeature Releaseのサポートステートメントに変更はありません。これらのリリースのサポートポリシーのステートメントについては、DS 10.xおよびDS 11.xのドキュメントを参照してください。

Agentプラットフォームサポートポリシー

Deep Security Agentソフトウェアは、前述のとおり年に数回リリースされます。Agentプラットフォーム (OS) は、以下のポリシーに従ってサポートされています。トレンドマイクロでは、お客様が特定のプラットフォームを長期にわたって使い続けなければならないケースがあることを認識しています。そのような場合には、このポリシーを参照して将来を見据えたDeep Securityのインストールを行ってください。

- 「["Deep Security Agentのプラットフォーム" on page 182](#)」に示されているように、Agentは広範なプラットフォームでサポートされています。
- Agentソフトウェアの各リリースにおけるサポート期間は、上記の表で説明しています。たとえば、AgentのLTSリリース (10.0、11.0など) に関しては、3年間の標準サポートと5年間の延長サポートが提供されます。特定のOSプラットフォームを長期にわたって利用する場合は、Agentソフトウェアを定期的にアップグレードして、特定のDeep Securityソフトウェアリリースのサポートライフサイクルから外れないように計画を立てる必要があります。特定のプラットフォームで古いAgentが推奨されている場合、そのAgentはソ

ソリューション全体の一部と見なされ、そのソリューション全体のサポート期間が適用されます。詳細については、以下の各項目を参照してください。

- 各プラットフォームのサポート期間は、少なくともOSベンダによる延長サポートの終了日まで継続されます。トレンドマイクロでは、重要性に応じて、この終了日を大幅に超える長期サポートを提供する場合があります。
- OSベンダから提供される最新のパフォーマンスアップデートおよびセキュリティアップデートを常に適用できるように、トレンドマイクロでは、Agentに対応した最新バージョンのOSに移行することを強くお勧めします。
- トレンドマイクロは、すべてのサポート対象プラットフォーム向けに新しいバージョンのDeep Security Agentをリリースできるよう努めています。ただし、古いプラットフォームへの対応を目的に、古いリリースのAgentの利用を推奨する場合があります。たとえば、Deep Security 11.0におけるWindows 2000向けの最新のAgentは、Deep Security Agent 9.6です。この9.6 Agentは、Deep Security 11.0ソリューション全体の一部となり、このソリューション全体のサポート期間が適用されます。
- 特定のプラットフォームのサポートを終了する場合は必ず事前に通知します。また、一般提供 (GA) 開始後にソフトウェアリリースのサポートライフサイクルを短縮することは一切ありません。*

* OSベンダによるプラットフォームのサポートが終了すると、OSベンダのサポートなしでは解決できない技術的問題が発生するリスクが生じます。このような状況に陥った場合、トレンドマイクロは、その状況下での制限事項をただちにお客様にお伝えします。こうした状況は、機能喪失につながる可能性がありますのでご注意ください。どのような技術的問題が発生した場合でも、トレンドマイクロは最善を尽くし、その問題に対処します。

このリリースについて

新機能

Deep SecurityのLTSリリースは、機能強化とバグ修正によって頻繁にアップデートされています。[LTSリリースのサポート期間とアップグレードの推奨事項](#)で説明されているように、LTSリリースには長期間のサポートが含まれます。

最新のアップデートの詳細については、次を参照してください。

- [Deep Security Managerの新機能](#)
- [Deep Security Agentの新機能](#)

- [Deep Security Virtual Applianceの新機能](#)

Deep Security 12.0（長期サポートリリース）の新機能

Deep Security 12.0の主な変更を以下に示します。

注意: Deep Security 12.0には、これまでDeep Security 11.3,11.2、および11.1で提供されていた機能も含まれています。

ヒント: 必要に応じて、YouTubeで[Deep Security 12 - 新機能](#)を視聴できます。

プラットフォームのサポートの強化

Deep Security 12.0でリリースされた機能：

Deep Security Agent:

- Red Hat Enterprise Linux 8 (64ビット)
- SUSE Linux Enterprise Server 15 (64ビット)
- Windows 10 Version 1903 (64ビット)

Deep Security Manager:

- Amazon Aurora (PostgreSQL) データベースのサポート
- GovCloud向けAzure Marketplace (BYOL)

Deep Security Virtual Appliance:

- NSX-T向けAgentレス不正プログラム対策: Deep Securityでは、ハイパーバイザレベルのVMware NSX-TでVMware仮想マシンに対して不正プログラム対策保護を実行できます。詳細については、"[Applianceのインストール \(NSX-T\)](#)" on page 320を参照してください。
- NSX-T不正プログラム対策タグ付け: Deep Securityでは、NSX-Tの不正プログラム対策イベントに基づいてNSXセキュリティタグを適用できます。詳細については、"[NSXセキュリティタグを適用するように不正プログラム対策を設定する](#)" on page 366を参照してください。
- UEFIブート、NSX-T、およびNSX-V向けの新しいAppliance: 同じApplianceを使用して、NSX-TインフラストラクチャとNSX-Vインフラストラクチャの両方にSVMをインストール

Trend Micro Deep Security(オンプレミス) 12.0

できます。このApplianceは、仮想UEFIまたはBIOSをサポートしているvSphereにインストールすることもできます。詳細については、"[Deep Security Virtual Applianceのアップグレード](#)" on page 1006を参照してください。

元々 Deep Security 11.3,11.2,11.1でリリースされた機能：

Deep Security Agent:

- Windows 10 Embedded (Windows 10 IoT (64ビット) とも呼ばれる)
- Windows 8.1 Embedded (32ビット)
- Windows 7 Embedded (32ビット)

Windows Embeddedのサポートに関する重要な詳細については、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。

Deep Security Manager:

- SQL Server 2017データベースのサポート
- PostgreSQL 10.xデータベースのサポート

セキュリティの向上

Deep Security 12.0でリリースされた機能：

- TLS 1.2の強化:
 - Deep Securityには、TLS 1.2と強力な暗号を強制する機能があります (暗号の評価は「A+」となっており、[こちらの表](#)に記載されています)。詳細については、"[TLS 1.2の強力な暗号化スイートの有効化](#)" on page 1491を参照してください。
 - 新しくDeep Securityをインストールした場合には必ずTLS 1.2が初期設定となります。詳細については、"[Deep SecurityでのTLS 1.2の使用](#)" on page 1472を参照してください。
 - `dsm_c`コマンドには、`settlsprotocol`と呼ばれる新しい`-action`パラメータが含まれています。このパラメータによって、Deep Security Managerで許可される最小のTLSバージョンを設定および確認できます。詳細については、"[コマンドラインの基本](#)" on page 447を参照してください。
- Agentのアップグレード中に不正プログラム対策をオンラインのままにして保護を実行する: この機能によって、AgentをアップグレードするときにWindows Serverを強制的に再起動する必要がなくなります。Agentのアップグレード後も、コンピュータを再起動できるタイミングまで、既存のAgentの不正プログラム対策を使用して不正プログラム対策保

護が引き続き実行されます。新しいAgentへのアップグレードを完了するために再起動が必要なことは変わりません。今回の改善は、ユーザが自由にこの再起動のタイミングを将来の日付に設定したり、多くのWindows Serverでよく行われているように、アップグレードの完了を次に予定されている再起動まで待って、そのタイミングで新しい不正プログラム対策モジュールをインストールしたりできるようにするものです。

- 署名済みインストーラパッケージ: Deep Securityソフトウェアにデジタル署名がない場合、または正常に確認できない署名が含まれている場合、Deep Security Managerは、Deep Securityソフトウェアのインポートをブロックします。

注意: AIXまたはSolaris用にDeep Security Agent 9.0が必要な場合は、[Deep Securityソフトウェア] ページの [12.0] タブから、署名されたバージョンを入手できます。

元々 Deep Security 11.3,11.2,11.1でリリースされた機能：

- コンテナトラフィックスキャンの向上: Deep Security Agent 11.1以前では、ホストコンピュータのネットワークインタフェースを通過してコンテナに向かうトラフィックがファイアウォールと侵入防御モジュールによって監視されます。Deep Security Agent 11.2以降では、コンテナ間のトラフィックを監視することもできます。この機能を有効にする方法については、"[侵入防御の設定](#)" on page 793と"[Deep Securityファイアウォールの設定](#)" on page 836を参照してください。
- 変更監視 - リアルタイム検索の改善: LinuxおよびWindows Serverプラットフォーム上でのリアルタイムファイル変更監視では、監視対象のファイルに変更を加えたユーザの情報を取得します。この機能は、LinuxではDeep Security Agent 11.1以降でサポートされています。Windows ServerプラットフォームではDeep Security Agent 11.2以降でサポートされています。この機能をサポートしているプラットフォームの詳細については、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。
- 非アクティブなAgentのクリーンナップ: 新しい機能である非アクティブなAgentのクリーンナップを利用して、所定の期間非アクティブなコンピュータを自動的に削除できます。詳細については、"[非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化](#)" on page 1523を参照してください。
- 署名済みインストーラパッケージ: Deep Security Manager、Deep Security Agent、およびDeep Security Notifierのインストーラはデジタル署名されています。"[ソフトウェアパッケージのデジタル署名の確認](#)" on page 216を参照してください。
- トレンドマイクロのライセンスおよび登録サーバのセキュリティの強化: Deep Security 11.1以降、トレンドマイクロのライセンスおよび登録サーバとの通信はすべて、HTTPSを使用して保護されます。

- Smart Protection Serverのセキュリティの強化: AWSのSmart Protection Server CloudFormationテンプレートに、WebレピュテーションサービスのHTTPS URLが含まれるようになりました。詳細については、[「AWSでのSmart Protection Serverの配置」](#)を参照してください。

管理と品質の向上

Deep Security 12.0でリリースされた機能：

- 正しくないプラットフォームへのAgentのインストール防止: Deep Security Agentインストーラがインストールプラットフォームを確認して、プラットフォームに一致しないAgentのインストールを防止します。この機能は以下でサポートされています。
 - Amazon LinuxおよびAmazon Linux 2
 - Red Hat Enterprise Linux 6および7
 - CentOS 6および7
 - Cloud Linux 7
 - Oracle Linux 6および7
 - SUSE Linux Enterprise Server 11および12
- VMwareの信頼性とスケーラビリティの向上: VMwareのインスタントクローン技術を使用する大規模なVMware Horizon VDI環境に対応するために、Deep Security Virtual Applianceのスケーラビリティと信頼性の向上が図られました。この強化は、VDIゲストマシンの動的な運用に対処するためのものです。
- Azureの「クイック」モードの削除: Deep Security 12.0では、Azureクラウドアカウントを追加するためのクイックモードが削除されました。クイックモードでは、Deep Security Managerに対する過剰な権限の付与が求められていたためです。以前のリリースでクイックモードを使用した場合でも、お使いの環境に影響はありません。新しいAzureクラウドアカウントのすべてで、詳細方式を使用する必要があります。詳細については、["Microsoft AzureアカウントからDeep Securityに仮想マシンを追加する" on page 540](#)を参照してください。

元々 Deep Security 11.3,11.2,11.1でリリースされた機能：

- アプリケーションコントロールの向上:
 - アプリケーションコントロールのハッシュベースのルール: Deep Security Agent 11.1以降を使用した場合、アプリケーションコントロールルールは、ファイル名やパスではなく、ソフトウェアファイルのSHA-256ハッシュ値に基づきます。この機能強

化により、各ルールの対象範囲が大幅に改善され、同じハッシュ値を持つファイルに対する複数のルールを作成および管理する際の運用のオーバーヘッドが削減されます。詳細については、"[アプリケーションコントロールで検出されるソフトウェア変更](#)" on page 694を参照してください。また、Deep Security APIを使用して共有ルールセットを使用する場合は、"[共有ルールセットとグローバルルールセットを作成するためのAPIの使用](#)" on page 714を参照してください。

- アプリケーションコントロールの簡略化: 冗長な判定ログの表示を削除することで、アプリケーションコントロールのユーザインタフェースが簡略化されました。アプリケーションコントロール判定を元に戻す方法については、"[アプリケーションコントロールルールセットの表示と変更](#)" on page 709を参照してください。
- Deep Security APIのアップデート:
 - Deep Security 11.1では、新しいDeep Security Automation Centerが導入されました。ここでは、Deep Security APIを使用する方法について、役に立つ情報を入手できます。詳細については、[Deep Security Automation Center](#)をご覧ください。
 - リリースごとの自動化のアップデート内容については、[Automation Changelog](#)を参照してください。
 - Deep Security 11.1では、Deep Securityを使用したセキュリティのプロビジョニングとメンテナンスを自動化できる新しいRESTful APIが提供されています。[Deep Security Automation Center](#)にアクセスし、任意の言語でSDKをダウンロードして、APIの使用方法を資料で確認します。
 - Deep Security APIにはPython SDK、APIリファレンスにはPythonの例が含まれるようになりました。詳細については、[Deep Security Automation Center](#)を参照してください。
- 不正プログラム対策エンジンの自動アップデート: 不正プログラムは絶えず進化しています。そのため、Deep Securityで使用する不正プログラム対策エンジンを定期的にアップデートする必要があります。これまで、不正プログラム対策エンジンをアップデートするには、Deep Security Agentをアップグレードする必要があり、場合によっては、コンピュータを再起動する必要もありました。今回のリリースでは、Deep Security Agentとは別に不正プログラム対策エンジンをアップデートできるようになりました。このアップデートが自動的に行われるように設定すると、ユーザが手動で操作することなく、また、システムを再起動することなく、不正プログラム対策エンジンを最新の状態に維持することができます。詳細については、"[セキュリティアップデートの取得と配布](#)" on page 1039を参照してください。
- 有効化時にアップグレード: Deep Security Manager 11.3以降には、Agentを有効化したときに、Deep Security Agentを互換性がある最新バージョンのAgentソフトウェアに自

動的にアップグレードするよう設定するオプションが用意されました。詳細については、"[Agentを有効化するとき自動的にアップグレードする](#)" on page 397を参照してください。

注意: 有効化時のアップグレードは、最初Linuxプラットフォームのみでサポートされています (この機能を有効にするとWindowsプラットフォームとUNIXプラットフォームはスキップされます)。これは、グローバルなシステム設定で制御されています。

- Applianceをシームレスにアップグレード: Deep Security Virtual Applianceのアップグレードプロセスが簡略化されました。選択したDeep Security Virtual Applianceを自動的にアップグレードできるようになりました。新しいアップグレードプロセスにより、手動でアップグレードする場合に必要な複雑な手順が軽減されます。"[Deep Security Virtual Applianceのアップグレード](#)" on page 1006を参照してください。
- アラートの向上: アラート名「Relayアップデートサービスを利用不可」が「Deep Security Relayのセキュリティコンポーネントをダウンロードできません」に変更され、より正確な説明と解決策を含むようになりました。
- コマンドの向上: `dsa_query`コマンドと`dsa_control`コマンドに、AgentのバージョンとDeep Security保護モジュールの情報が示されるようになりました。詳細については、"[コマンドラインの基本](#)" on page 447を参照してください。
- ログの向上: トラブルシューティングに使用したり、Deep Security ManagerとDeep Security Agentの間でのイベントの相関関係を考慮し、イベントにタイムゾーンを含めることができるようになりました。"[Deep SecurityイベントをSyslogまたはSIEMサーバに転送する](#)" on page 1141を参照してください。

詳細については、各ソフトウェアのダウンロードに伴う[リリースノート](#)を参照してください。

Deep Security Managerの新機能

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Manager 12.0 README](#)を参照してください。

注意: 以前のリリースノートについては、「Deep Security Managerのリリースノート」 ("[Deep Security Managerのリリースノートのアーカイブ](#)" on page 166)

Deep Security Manager - 12.0 update 30

リリース日：2023年5月4日

Trend Micro Deep Security(オンプレミス) 12.0

ビルド番号：12.0.544

新機能

- Deep Security Managerは、Azureコード署名の検証が原因でAgentのアップグレードがインストールに失敗したときにイベントを受信するようになりました。DSSEG-7837

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-7771 / DSSEG-7841

CVSSの最高値: 8.8

最高の重大度: 高

Deep Security Manager-12.0 update 29

リリース日：2022年10月4日

ビルド番号：12.0.540

解決済みの問題

- Deep Securityコンソールに不正プログラム対策がオフラインと表示されている場合、不正プログラム対策ホストのレポートに不正プログラム対策がオンラインと誤って表示される問題。SF05780825 / SEG-149707 / DSSEG-7706
- Deep Security Managerで予期しない「コンピュータのアップデート」システムイベントが生成されることがありました。SF05496967 / SEG-138407 / DSSEG-7678

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-7705

最高のCVSS：9.1

最高の重大度：重大

Deep Security Manager-12.0 update 28

リリース日：2022年7月4日

ビルド番号：12.0.537

解決済みの問題

- セキュリティログ監視ルール「1003613-DHCPサーバ」のイベントが取得されていませんでした。SEG-125264 / DSSEG-7630

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-7561

最高のCVSS：7.5

最高の重大度：高

Deep Security Manager - 12.0 update 27

リリース日：2022年5月26日

ビルド番号：12.0.535

解決済みの問題

- 列が「グループ別」にソートされている場合、一部のルールがDeep Security Managerで正しく表示されませんでした ([ポリシー]→[共通オブジェクト]→[ルール] または [コンピュータ]→[コンピュータ])。

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-7532

最高CVSS：9.8

最高の重大度：重大

Deep Security Manager-12.0 update 26

リリース日：2022年4月28日

ビルド番号：12.0.533

新機能

- Smart Protection Networkと共有されるトレンドマイクロのフィードバックについて、「匿名」ではなく「保護」という用語が使用されるようにDeep Security Managerがアップデートされました。 DSSEG-7536

解決済みの問題

- Simple Network Management Protocol (SNMP) を使用する一部のシステム設定で、Deep Security Managerが「systemEventID」エラーに関連付けられた数を受信していませんでした。 04711592 / SEG-122864 / DSSEG-7263
- [ポリシー]→(ポリシーを選択)→[設定]→[一般]で、ポリシーの一般設定を変更した後、すべての設定をリセットして継承するために使用される[リセット]ボタンが、[ポリシーの変更をコンピュータに自動的に送信]と[推奨設定の継続的な検索を実行]で機能しませんでした。 DSSEG-7439
- Deep Security Managerの[コンピュータ]または[ポリシー]→[オーバーライド]に、誤った数のオーバーライドが表示されました。 03513073 / SEG-83802 / DSSEG-7455

セキュリティアップデート

本リリースには、セキュリティアップデートが含まれています。脆弱性からの保護方法の詳細については、[脆弱性対策](#)を参照してください。責任ある開示の慣行に従い、CVEの詳細は、該当するすべてのリリースのパッチが利用可能になった時点で、一部のセキュリティアップデートでのみ利用可能になります。 DSSEG-7391

最高CVSS：7.5

最高の重大度：高

Deep Security Manager - 12.0 update 25

リリース日：2022年3月8日

Trend Micro Deep Security(オンプレミス) 12.0

ビルド番号：12.0.527

解決済みの問題

- Deep Security Managerでは、以前に削除された古いカーネルサポートパッケージ (KSP) が再ダウンロードされることがありました。 DSSEG-7483

Deep Security Manager - 12.0 update 23

リリース日：2021年11月29日

ビルド番号：12.0.522

解決済みの問題

- Deep Security Managerの [コンピュータ] タブで、[前回の通信] 列が正しくソートされないことがありました。 SEG-120751 / SF04862693 / DSSEG-7281

Deep Security Manager - 12.0 update 22

リリース日：2021年11月1日

ビルド番号：12.0.521

新機能

- Deep Security Managerがアップデートされ、(dsm_c) コンソールコマンドを使用してシステムイベントとセキュリティイベントにAWSインスタンスIDフィールドを追加できるようになりました。 SEG-109291 / SF04487365 / DSSEG-7055

解決済みの問題

- Deep Security Managerで、有効化されていないエージェントに関するアラートが受信されることがありました。 SEG-112134 / SF04588645 / DSSEG-6962

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセ

Trend Micro Deep Security(オンプレミス) 12.0

セキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-6534 / 04742276 / DSSEG-7231

最高のCVSS：6.1

最高の重大度：中

Deep Security Manager-12.0 update 21

リリース日：2021年9月15日

ビルド番号：12.0.516

解決済みの問題

- Deep Security Managerの [コンピュータ] 画面で、一部の列（「不正プログラムの前回の手動検索」および「不正プログラムの前回の予約検索」）が正しくソートされませんでした。SF04406374 / SEG-107465 / DSSEG-6885
- プライマリテナントで資格情報を使用してプロキシサーバを有効にすると、テナントがライセンスをアップデートできないことがありました（管理 > システム設定 > プロキシ > Deep Security Manager (ソフトウェアアップデート、CSSS、ニュースアップデート、製品登録とライセンス)）。VRTS-6038 / 04588945 / DSSEG-6987

Deep Security Manager-12.0 update 20

リリース日：2021年8月4日

ビルド番号：12.0.515

新機能

- Deep Security Managerがアップデートされ、[最大TCP接続数]（Computers > Computers > Details > Settings > Advanced）が初期設定で1000000に増えました。DSSEG-6995

解決済みの問題

- マルチテナント環境では、プライマリテナントでDeep Security Manager（管理 > システム設定 > プロキシ > Deep Security Manager（ソフトウェアアップデート、CSSS、ニュースアップデート、製品登録とライセンス））のプロキシが有効になっていると、ライセンスのアップデートが失敗することがありました。SEG-112726 / 04453369 /

DSSEG-6971

- 複数の「セキュリティアップデートの確認」予約タスクを同時に実行すると、アップデートがスキップされることがありました。SEG-110107 / SF04490101 / DSSEG-6930

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-6743/DSSEG-6997/DSSEG-7009

最も高いCVSSスコア: 9.1

最高の重大度: 高

Deep Security Manager-12.0 update 19

リリース日: 2021年7月6日

ビルド番号: 12.0.509

新機能

- Deep Security Relayのダウンロードが失敗すると、Deep Security Managerは、リレーの問題の詳細が欠落している「ソフトウェアアップデート」イベントをトリガーしました。SF04443281 / SEG-111629 / DSSEG-6965

Deep Security Manager-12.0 update 18

リリース日: 2021年5月27日

ビルド番号: 12.0.503

新機能

- 不正プログラム対策の「Identified Files」データを.CSVファイルにエクスポートする際に、Deep Security ManagerがSHA-1値を含むようにアップデートしました。DSSEG-6911

解決済みの問題

- データベース接続が不安定な場合、Deep Security Managerで予約タスクの処理が停止することがありました。SEG-102044 / SF04236155 / DSSEG-6689

Deep Security Manager - 12.0 update 17

リリース日：2021年4月26日

ビルド番号：12.0.501

解決済みの問題

- タグによるスマートフォルダのフィルタ処理が、自動タグ設定（イベント&レポート>（イベントタイプの選択）>自動タグ設定）で追加された新しいイベントに対して正しく機能していませんでした。SEG-103100 / SF04264168 / DSSEG-6732
- Azureコネクタ（コンピュータ>コンピュータ>右クリックAzureコネクタ>プロパティ>接続）のパスワードをアップデートすると、Deep Security Managerとの接続が切断されることがあります。SEG-97244 / SF04027400 / DSSEG-6628
- Deep Security Managerの「セキュリティ更新プログラムの概要」（管理>アップデート>セキュリティは）時々、管理>予約タスクがあった場合でも、「予約タスクなし」を示しました。SEG-97381 / DSSEG-6764
- マルチテナント設定では、Deep Security Managerに接続に問題があります。DSSEG-6469
- 「ライセンス情報の表示」URLが、[ライセンスのプロパティ]メニュー（[管理] [>ライセンス] [>の詳細の表示]）で破損しています。SEG-104258 / SF04308332 / DSSEG-6768

Deep Security Manager - 12.0 update 16

リリース日: 2021年3月22日

ビルド番号: 12.0.493

解決済みの問題

- Deep Security Managerは、いくつかのケースでは、Relayの間違ったバージョンをインストールしました。DSSEG-6604

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。 DSSEG-6574

最も高いCVSSスコア：7.5

最高の重大度：高

Deep Security Manager - 12.0アップデート15

リリース日：2021年1月28日

ビルド番号：12.0.490

新機能

- Deep Security Managerがアップデートされ、スマートフォルダの[コンピュータの説明]フィールドが検索条件として使用可能になりました (Computers&スマートフォルダ)。 SEG-85288 / DSSEG-6436

解決済みの問題

- 複数のIPを持つDeep Security Agentの優先IPアドレスの設定に使用されるDeep Security Managerコンソールコマンドが機能しない場合があり、一部のエージェントを接続できないことがありました。 DSSEG-6521
- セキュリティログ監視 ルールまたは 侵入防御 ルールを追加したときに、Webアプリケーション ファイアウォール によってページがブロックされることがありました。 SEG-87396 / SF03668760 / DSSEG-6283
- 不正プログラム対策 [予約タスク Skipped]イベントが発生せず、タイムアウトになった予約検索タスクが再度開始されることがありました。 SEG-95139/03837423 / DSSEG-6548
- の管理 > システム設定 > ストレージでの [次の期間を超過したサーバログを自動的に削除する] 設定が、テナントに表示されました (プライマリテナントにのみ登場するはずでした)。 DSSEG-6483
- 不正プログラム対策 リアルタイム検索を使用してDeep Security Agentが実行されていた場合、関連のないアプリに対してランダムな障害が発生することがありました。 SEG-85142/03527705 / DSSEG-6082

Deep Security Manager - 12.0 update 14

リリース日：2020年11月12日

ビルド番号：12.0.484

解決済みの問題

- vCloud Director VMでの予約検索が機能しませんでした。SEG-82971 / SF03421234 / DSSEG-6037
- ダッシュボードの[不正プログラム検索ステータス]ウィジェットで間違っただータが表示されることがありました。SEG-81776/03398406 / DSSEG-6359
- Deep Security ManagerとDeep Security Agentとの間のTLS通信に使用される証明書の自動更新メカニズムが期待どおりに機能していません。有効期限が切れた証明書が原因で、マネージャとエージェントが互いに通信できなくなり、多くのオフラインクライアントがWebコンソールに表示されていました。SEG-79146 / SF03240076 / DSSEG-6321
- vCentersがDeep Security Managerとの同期を試行したときに問題が発生することがありました。SEG-90204 / SF03773453 / DSSEG-6382

Deep Security Manager 12.0 update 13

リリース日：2020年10月1日

ビルド番号：12.0.480

新機能

- Deep Security Managerの[ユーザのプロパティ]ページに表示されるポケットベル番号、電話番号、またはモバイル番号は、30桁を超えるように設定できます。SEG-80854 / SF03098096 / DSSEG-5890
- Deep Securityは、ソフトウェア・ファイルが署名時以降に変更されていないことを確実にするためのDeep Securityエージェントの署名を検証します。DSSEG-5874

解決済みの問題

- 一部の侵入防御ルールは、[検出のみ]モードでのみ動作するように設計されていますが、ポリシーとコンピュータページでその動作を変更できました。SEG-83700 / SF03456778 / DSSEG-5998

Trend Micro Deep Security(オンプレミス) 12.0

- ダッシュボードの「ランサムウェアイベント履歴」ウィジェットに、間違った情報が表示されました。SEG-86045 / SF03618147 / DSSEG-6142
- MasterAdminがすべてのコンピュータに対して予約タスクを作成できませんでした。SEG-86413 / SF03320936 / DSSEG-6131

Deep Security Manager 12.0 update 12

リリース日：2020年8月19日

ビルド番号：12.0.473

解決済みの問題

- セキュリティログ監視データベース破損の問題が発生した場合、Deep Security Managerのセキュリティログ監視のステータスには影響しませんでした。SEG-77081/02984526 / DSSEG-5726
- タスクの作成時に不正な挙動が発生した、予約タスクに関する権限の問題がありました。SEG-78610 / SF03320936 / DSSEG-5752
- vCloudでインポートされたVMをアクティブ化できませんでした。SEG-75542/03189161 / DSSEG-5813
- Deep Security Virtual ApplianceをESXi 7.0のNSX-V 6.4.7にインストールした場合、Deep Security Manager 12へのアップグレードがブロックされました。SEG-82636,/SEG-82637 / DSSEG-5926
- Deep Security Managerのダッシュボードにあるコンピュータステータスウィジェットに、管理下のコンピュータの正しい数が表示されませんでした。SEG-80171/03189161 / DSSEG-5885

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-5814 / VRTS-4652/03296737 / DSSEG-5772

最も高いCVSSスコア：9.8

重大度が最も高い：重大

Deep Security Manager 12.0 update 11

リリース日：2020年7月9日

ビルド番号：12.0.466

新機能

- 「活性化にアップグレード」機能は、最後の二つのメジャーリリースから、コンピュータ上のエージェントをアップグレードします。エージェントが条件を満たしていない場合、エンドツーエンドのメジャーリリース内のリリースにエージェントを手動でアップグレードする必要があります。その後、「アクティベーション時のアップグレード」機能が新しいバージョンを検出し、指定されたリリースへのアップグレードを完了します。DSSEG-5715

解決済みの問題

- 別のソフトウェアパッケージを同じ名前でも再インポートした場合、パッケージは変更されていないと見なされます。DSSEG-5707
- 初期設定のSSL設定の説明が誤解を招くようになりました。SEG-68686 / DSSEG-5191
- ポリシーの[共通オブジェクト]→[セキュリティログ監視 ルールの セキュリティログ監視 ルール「1002729 - 初期設定ルールの設定」]でプロパティが変更されたときにエラーが発生しました。SEG-77260 / SF03263573 / DSSEG-5727

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。

- 最も高いCVSSスコア：8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
- 最高の重大度：高

DSSEG-5738 / DSSEG-5886 / DSSEG-5744

Deep Security Manager 12.0 update 10

リリース日：2020年5月28日

ビルド番号：12.0.458

新機能

管理と品質の向上

インスタンスメタデータサービスバージョン2 (IMDSv2) のサポート: IMDSv2は、Deep Security Agent 12.0アップデート10でサポートされます。詳細については、「["Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか" on page 1534](#)」を参照してください。DSSEG-5463

新機能

- イベント&レポート>予約レポートページが更新されました。これにより、失敗の可能性のあるレポートを作成できなくなります。予約レポートを作成する前に設定する必要があるアラートが表示されます。SEG-72578/02958064 / DSSEG-5525
- 次の非表示設定コマンドが追加されました。

```
dsm_c -action changesetting -name  
com.trendmicro.ds.antimalware:settings.configuration.maxSelfExtractRT  
ScanSizeMB -value 512
```

Deep Security Agentが対象ファイルの種類を判別できない場合、検索エンジンはそのファイルをメモリにロードして、自己解凍型ファイルかどうかを判別しました。これらのファイルの数が多い場合、検索エンジンはメモリを消費します。上記の隠しコマンド設定を使用すると、対象ファイルをロードする際のファイルサイズの制限が512MBに設定されます。ファイルサイズが設定された制限を超えると、検索エンジンはこのプロセスをスキップしてファイルを直接検索します。DSSEG-5097

この機能を実装するには以下の手順を実行します。

1. Deep Security Managerでこのコマンドを実行して、データベース内の値を変更します。
2. 対象のDeep Security Agentにポリシーを送信して設定を配信します。

解決済みの問題

- リアルタイムの不正プログラム対策検索で検出の問題が発生しました。SEG-72928 / SF03050515 / DSSEG-5452
- 大規模なボディを持ついくつかのメールがキューに入れられたとき、バッチではなくすべてを一度にロードしていたため、大量のメモリが使用されていました。SEG-71863 / SF03024164 / DSSEG-5628

Trend Micro Deep Security(オンプレミス) 12.0

- ファイアウォールルール、侵入防御ルール、変更監視ルール、またはセキュリティログ監視ルールが、APIを使用してコンピューターで追加、更新、または削除されましたが、ポリシーはコンピューターに送信されませんでした。SEG-74583 / SF03099843 / DSSEG-5481

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-5540 / DSSEG-5605 / SEG-70989 / SF02964497 / DSSEG-5653 / DSSEG-5652

最も高いCVSSスコア：6.5

重大度：中

Deep Security Manager 12.0 update 9

リリース日：2020年5月4日

ビルド番号：12.0.446

新機能

- メモリ消費量を削減し、ページのロードに費やされた時間を削減することで、[Computers]ページが改善されました。SEG-69380 / DSSEG-5437
- Deep Security Managerがアップデートされ、仮想マシンのハードウェア情報が不足していてもvCloudアカウントを追加できるようになりました。SEG-72729 / SF03054267 / DSSEG-5354
- Windows Server 2019のサポートが追加されました。DSSEG-5213

解決済みの問題

- Active Directoryとの同期が終了しないことがある問題がありました。SEG-52485 / DSSEG-5477
- 「放置」とマークされた不正プログラム対策イベントは、ダッシュボードまたは不正プログラム対策イベントで正しくカウントされませんでした。SEG-70872 / SF02904003 / DSSEG-5278

Trend Micro Deep Security(オンプレミス) 12.0

- Deep Security Agentは、複数のコンポーネントを同時に使用できる場合に、ソフトウェアコンポーネントをリレーからダウンロードできないことがありました。SEG-66691 / DSSEG-5444
- ダッシュボードで+ボタンをクリックしたときに、[新規ダッシュボード名]フィールドに新しいエントリを入力できませんでした。DSSEG-5535
- Oracleデータベースで問題が発生したため、ルールのアップデートを適用できませんでした。DSSEG-5357

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。DSSEG-5307 / DSSEG-5580

Deep Security Manager-12.0 update 8

リリース日：2020年4月1日

ビルド番号：12.0.426

新機能

プラットフォームのサポートの強化

- Red Hat Enterprise Linux 8 (64ビット)

新機能

- [システム情報]画面のメモリに関連する説明が更新され、より正確で理解しやすくなりました。(DSSEG-5134)
- 不正プログラム対策の処理に失敗すると、結果が[Syslog結果]フィールドに表示されません。(SEG-69456/SF02896227/DSSEG-5300)
- Deep Security Managerのインストールログのローテーションが追加されました。(SEG-66918/02765043/DSSEG-5126)

解決済みの問題

- Deep Security Managerでは、パートナーOVFがVMwareによって署名されている場合、NSX-TがNSX-Tで確認する必要があるファイルをダウンロードできませんでした。その結果、DSVAのOVFを適切に配置できませんでした。(DSSEG-5195)

- 変更監視が有効になっていると、次の警告メッセージが表示されました：「セキュリティアップデート：Agents/Appliance でのパターンファイルのアップデート失敗」。(SEG-67859/DSSEG-5265)
- 複数のレポートを同時に生成している場合、レポートデータが正しくないことがあります。(SEG-71688/SF03011491/DSSEG-5289)

Deep Security Manager-12.0 update 7

リリース日：2020年2月28日

ビルド番号：12.0.416

拡張機能

- 管理>ユーザ管理>の役割>新しい>コンピュータ権限>の選択されたコンピュータに進行状況バーが追加され、ページのロード状況を確認できます。(SEG-61331/DSSEG-4941)
- 画像ファイルが繰り返しブラウザにダウンロードされると、パフォーマンスが向上します。(SEG-64280/DSSEG-5141)

解決された問題

- ダッシュボードで「タグなし」フィルタが選択された場合、一部のウィジェットでは引き続きタグ付きアイテムが表示されます。(SEG-63290/SF02585007/DSSEG-4910)
- コンピュータリストで「ソフトウェアアップデートステータス」が正しく検索されない問題がありました。これにより、コンピュータリストおよび該当するコンピュータを表示するためにリストを使用していた「旧版」のコンピュータレポートとウィジェットに影響が生じました。(SEG-62740/DSSEG-4840)
- テナントでのPortScanの実行が許可されていない場合、仮想マシンのファイアウォールのステータスはアップデートされませんでした。(SEG-63713/SF02554452/DSSEG-5041)
- マルチテナントのセットアップのテナントは、リレーをプライマリテナントの中継グループに移動できます。これにより、リレーが「Relay」画面から消えてしまいます。テナントは現在、リレーをプライマリテナントリレーグループに移動できません。(SEG-57715/02322762/DSSEG-5240)
- PostgreSQLを使用しているDeep Security Managerによって、イベントがAWS SNSに転送されていないことがありました。(SEG-67362/SF02798561/DSSEG-5077)

Trend Micro Deep Security(オンプレミス) 12.0

- ウイルス検索とリビルドベースラインのボタンがグレー表示され、[コンピュータ] [>コンピュータの詳細]で無効になりました。対応する操作が完了した後であっても、>変更監視>一般を参照してください。(SEG-69921/02932025/DSSEG-5229)
- 推奨設定に基づいて侵入防御ルールが割り当てまたは割り当て解除された場合、ポリシーエディタのパフォーマンスが低下し、推奨事項が適用されませんでした。(SEG-63540/SF02573474/DSSEG-4965)
- Deep Security Managerで、要約レポートの生成に失敗することがありました。(SEG-68840/SF02850674/DSSEG-5165)
- vCloudコネクタを追加すると、vCloud Directorのバージョン9.7以降でSDKがサポートされていないため失敗しました。(DSSEG-5185)
- Agentレス保護は、vCloud Directorバージョン9.5以降では機能しませんでした。(DSSEG-5185)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。(DSSEG-5230/DSSEG-5140/DSSEG-5171)

- JREを最新のバンドルパッチリリース (8.0.241 / 8.43.0.6.) にアップデートしました。(DSSEG-5180)

Deep Security Manager-12.0 update 6

リリース日：2020年1月17日

ビルド番号：12.0.393

新機能

- 「TrendMicroDsPacketData」フィールドがDeep Security Manager経由でSyslog転送されるファイアウォールイベントに追加されました。(DSSEG-4856)
- 挙動監視で.dllsが検出されないようにするには、次のhiddenコマンドを追加しました。

```
dsm_c -action changesetting -name  
com.trendmicro.ds.antimalware:settings.configuration.bmExploitLoadRem  
oteLibExceptionList -value "abc.dll;123.dll"
```

この強化を実装するには、ポリシーをDeep Security Agentに送信します。

基本名「123.dll」に加えて、ワイルドカードもサポートされています。「\10.1.1.1\remote *」などの値を追加できます。このリモートパス内のすべての.dllは検出されません。(DSSEG-4976)

解決済みの問題

- 「セキュリティモジュール使用状況レポート」のCSV出力の列名の一部がデータ列とずれています。(SEG-66258/SF02718206/DSSEG-5029)
- [不正プログラム検索設定]画面 (Computers/Policies>不正プログラム対策>一般>手動検索>編集>Advanced)を選択し、圧縮圧縮ファイルを選択) 抽出するファイルの最大数設定を0に設定できませんでした。意味は無制限です。(SEG-65997/02685854/DSSEG-5040)
- 拡張イベントの説明を送信するオプションが有効になっていると、外部Syslogサーバへのイベント配信が遅くなりました。これにより、Syslogサーバにイベントが到着するまでに許容されない遅延が発生します。(DSSEG-4984)
- Deep Security Managerで新しいダッシュボードを追加するときに、[ダッシュボード]画面で[+]をクリックしてEnterキーを何回か押した場合、複数のダッシュボードが作成され、最初のダッシュボードがウィジェットを失います。(DSSEG-5089)
- [バージョン]フィールドに値が含まれていて、値が「N/A」の場合、[コンピュータ]ページの詳細検索が正常に実行されませんでした。(SEG-66513/02740746/DSSEG-5106)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。(DSSEG-5056)

Deep Security Agentの新機能

注意: 以前のリリースノートについては、「["Deep Security Agentのリリースノートのアーカイブ" on page 172](#)

Linux

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Agent - Linux 12.0 Readme](#)を参照してください。

Deep Security Agent - 12.0 update 30

リリース日：2023年5月4日

ビルド番号：12.0.0-2932

解決済みの問題

- コンポーネントのアップデート中に問題が発生し、エンジンのアップデートが無効になっていても、検索エンジンがアップデートされることがありました。SF06390800 / SEG-165036 / DSSEG-7802

Deep Security Agent-12.0 update 29

リリース日：2022年10月4日

ビルド番号：12.0.0-2626

新機能

- 「Bypass Network Scanner」ルール適用時の侵入防御のパフォーマンスが向上しました。SEG-132057 / DSSEG-7621

解決済みの問題

- エージェントのアップグレード中に、「新しく適用されたルールセットによって、再起動時に一部の実行中のプロセスがブロックされます」というメッセージが誤って表示されました。DSSEG-7653
- 一致または正規表現フィールドで変数に「\$」文字を使用すると、セキュリティセキュリティログ監視エンジンがオフラインになる問題を修正しました。SEG-146965 / SEG-146966 / DSSEG-7665
- IPv4 / IPv6変換用に予約された有効なIPv6アドレスがあると、「無効なIPv6アドレス」エラーが発生しました。SEG-147969 / DSSEG-7673

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示さ

れ、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7090 / DSSEG-7647

最高のCVSS：4.6

最高の重大度：中

Deep Security Agent-12.0 update 28

リリース日：2022年7月4日

ビルド番号：12.0.0-2487

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7385 / DSSEG-7563、VRTS-7647 / DSSEG-7625、VRTS-7633 / DSSEG-7599

最高CVSS：9.8

重大度が最も高い：重大

解決済みの問題

- ・アプリケーションコントロールは、インベントリ検索が完了するまで、ハッシュによるプロセスのブロックに失敗しました。

Deep Security Agent - 12.0 update 27

リリース日：2022年5月26日

ビルド番号：12.0.0-2416

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣

行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7130 / DSSEG-7528

CVSS : 7.5

重大度 : 高

Deep Security Agent-12.0 update 26

リリース日 : 2022年4月28日

ビルド番号 : 12.0.0-2380

解決済みの問題

- 侵入防御が有効になっていると、パケット転送エラーによって一部のシステム設定がクラッシュしました。SEG-136843 / DSSEG-7524
- 不正プログラム対策を有効にすると、イベントレポートの配信で問題が発生し、Deep Security Agentで大量のシステムメモリが使用されるようになりました。SF05247760 / SEG-132286 / DSSEG-7514
- Deep Security Agentのセキュリティアップデートが開始され、「セキュリティアップデートの実行中」イベントが作成されることがありますが、完了しませんでした。SF05253107 / SEG-131983 / DSSEG-7513

Deep Security Agent - 12.0 update 25

リリース日 : 2022年3月8日

ビルド番号 : 12.0.0-2265

新機能

Debian 11 : Debian 11 : Deep Security Agent (バージョン12.0-2265+) がDebian 11でサポートされるようになりました。これにはDeep Security Managerバージョン12.0.527+が必要です。

解決済みの問題

- Deep Security Managerコンソールから起動したときに、Deep Security Agent for Debian 11 (64ビット) をアップグレードできませんでした。DSSEG-7465
- アプリケーションコントロールは、一部のシステム設定でソフトウェアの変更や実行を適切に検出できませんでした。DSSEG-7441

新機能

- Deep Security Agentがアップデートされ、「メンテナンスモード」での実行時のアプリケーションコントロールのパフォーマンスが向上しました。DSSEG-7354

Deep Security Agent - 12.0 update 24

リリース日：2022年1月24日

ビルド番号：12.0.0-2201

解決済みの問題

- 変更監視の検索がタイムアウトすると、誤った「ユーザ」、「グループ」、「作成」、または「削除」イベントが生成されることがありました。DSSEG-7349
- Deep Security Agentがネットワークインタフェースコントローラ (NIC) と競合して、複数のNICを備えたシステムがクラッシュすることがありました。SEG-126094 / 05048124 / DSSEG-7401

Deep Security Agent - 12.0 update 23

リリース日：2021年11月29日

ビルド番号：12.0.0-2112

新機能

- 不正プログラム対策 リアルタイム検索を有効にすると、変更されていないファイルがDeep Security Agentで検索されることがありました。DSSEG-7311

解決済みの問題

- Deep Security Agentで、オンデマンドの不正プログラム対策 検索時にファイルのアクセス時間が変更されることがありました。 SEG-79766 / 03352457 / DSSEG-5817
- Deep Security Managerに接続できない場合、 Deep Security Agentがクラッシュすることがありました。 DSSEG-7305
- Deep Security Agentによって接続の問題、CPU使用率の増加、またはシステムのクラッシュが発生することがありました。 SEG-123885 / SF04973642 / DSSEG-7298
- ファイアウォール カーネルモジュールのダウンロードに失敗すると、 Deep Security Agentがダウンロードを再試行せず、「ファイアウォール エンジンがオフライン」 イベントが発生することがありました。 SEG-122270 / SF04907791 / DSSEG-7261

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。 DSSEG-7260

最高のCVSS：7.8

最高の重大度：高

Deep Security Agent - 12.0 update 22

リリース日：2021年11月1日

ビルド番号：12.0.0-2072

新機能

- Deep Security Agentがアップデートされ、バージョン10.0から12.0にアップグレードしたエージェントの「NICバイパス」設定が失われないようになりました

([ネットワークインタフェースのバイパス](#)で使用)。SEG-111757 / SF04574021 / DSSEG-7087

解決済みの問題

- 証明書失効リスト (CRL) が一致しないため、アップグレード中にDeep Security Agentでパッケージ署名エラーが表示されることがありました。DSSEG-7214
- プラグインバージョンの競合により、Deep Security AgentがRelayからKSP (カーネルサポートパッケージ) ファイルを取得できないことがありました。DSSEG-7244
- 非アクティブなネットワーク接続のリソースをクリーンアップする際に、問題によってDeep Security Agentがクラッシュすることがありました。SEG-113291 / DSSEG-7035
- 不正プログラム対策 の検索中にDeep Security Agentサービス (ds_agent) を停止すると、再起動時にAgentがクラッシュすることがありました。DSSEG-7228

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-6489 / DSSEG-7237

最高のCVSS：7.8

最高の重大度：高

Deep Security Agent-12.0 update 21

リリース日：2021年9月15日

ビルド番号：12.0.0-1993

解決済みの問題

- ネットワークインタフェースカード (NIC) の接続の問題により、Deep Security Agentが複数の「セキュリティログ監視 エンジン初期化」または「ポリシー送信」イベントをトリガすることがありました。 SF03968169 / SEG-95731 / DSSEG-7039
- 変更監視を有効にすると、一部のシステムでDeep Security Managerの認証サーバのCPU使用率が高くなりました。 SEG-110088 / 04488319 / DSSEG-7072

Deep Security Agent-12.0 update 20

リリース日：2021年8月4日

ビルド番号：12.0.0-1908

解決済みの問題

- コンソールコマンドを使用して以前の (RPMパッケージ) アップグレードが実行された場合、Deep Security Agentのアップグレード (管理>アップデート>ソフトウェア) が失敗することがありました。 SEG-113583 / SF04586071 / DSSEG-7029
- SSL接続の確立中に、Deep Security Agentの接続が切断されることがありました。 SEG-107451 / DSSEG-7016
- 古いバージョンのOSを使用しているシステムでは、Deep Security AgentがWebアプリケーションに接続できないことがありました。 SEG-109652 / DSSEG-6992

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。 VRTS-6032 / DSSEG-6967

最も高いCVSSスコア: 9.8

最高の重大度：高

Deep Security Agent-12.0 update 19

リリース日：2021年7月6日

ビルド番号：12.0.0-1845

解決済みの問題

- 侵入防御が有効になっている場合、互換性の問題により、一部の構成でシステムがクラッシュしました。03368009 / SEG-81702 / DSSEG-6898
- Webレピュテーションを有効にすると、Deep Security Agentによって一部のサードパーティのソフトウェアで接続の問題が発生しました。SF04072723 / SEG-97952 / DSSEG-6810

Deep Security Agent-12.0 update 18

リリース日：2021年5月27日

ビルド番号：12.0.0-1789

新機能

- Entrust Root Certificate Authority (G2) 証明書のサポートを追加するために、Deep Security Agent (バージョン12.0.0-1789+) がアップデートされました。G2以外のセキュリティ証明書の有効期限は2022/07/09です。その後は、バージョン12.0.0-1789以降にアップグレードされたエージェントのみが最新の不正プログラム対策スマートスキャン保護を使用します。DSSEG-6904
- Deep Security Agentのアップデート不正プログラム対策初期設定では、ローカルホストからのファイルアクセスのみを監視し、一部のファイルシステムの互換性を向上させます。DSSEG-6831

解決済みの問題

- 侵入防御がSSL検査用に設定されていると、Deep Security Agentがクラッシュすることがありました。DSSEG-6909
- Deep Security Agent 不正プログラム対策リアルタイム検索は、一部のサードパーティアプリケーションの実行を妨げていました。SEG-104512 / SF04245456 / DSSEG-6894

- 不正プログラム対策リアルタイム検索により、一部の設定で意図しないファイルの変更が発生しました。 SEG-94769 / SF03806819 / DSSEG-6783
- カーネルサポートパッケージの圧縮方法をUbuntuのサイズを縮小するように変更しました。 DSSEG-6897

Deep Security Agent - 12.0 update 17

リリース日：2021年4月26日

ビルド番号：12.0.0-1735

新機能

- Deep Security Agentがアップデートされ、リアルタイムの変更監視パフォーマンスが向上しました。 SEG-102276 / SF04205359 / DSSEG-6759

解決済みの問題

- アップグレード失効リスト（CRL）が一致していないため、Deep Security Agentでパッケージシグネチャエラーが発生することがありました。 DSSEG-6826
- アプリケーションコントロールは、特定の種類のドライブ上のファイルに対して適切なソフトウェアインベントリを追加しないことがあります。 SEG-103667 / SF04227412 / DSSEG-6756
- Deep Security Agentは、1つの侵入防御イベントの重複を報告することがあります。 SEG-93125 / SF03595899 / DSSEG-6723
- Deep Security Agentでは、通常、これらのイベントを発生させる条件は存在しませんでした。複数の「レコード層メッセージ（未処理）」侵入防御イベントが発生することがありました。「Record Layer Message (not ready)」イベントは通常、セッションの初期化前にSSLステートエンジンでSSLレコードが検出されたことを示します。 SEG-101697 / SF04203096 / DSSEG-6739

Deep Security Agent - 12.0 update 16

リリース日: 2021年3月22日

ビルド番号: 12.0.0-1655

新機能

- アップデートされた不正プログラム対策リアルタイム検索により、互換性が向上しました。 DSSEG-5899
- Deep Security Agentがアップデートされ、アプリケーションコントロールのインベントリ検索のパフォーマンスが向上しました。 SEG-78295/03234667 / DSSEG-6303

解決済みの問題

- リアルタイムの変更監視は、ユーザによって指定された正確なディレクトリに一致しない場合がありますが、ベースディレクトリで開始されたすべてのパスに一致することがあります。 SEG-97758 / SF04046718 / DSSEG-6636
- Webレピュテーションが有効になっていると、システムがクラッシュすることがありました。 SF04258834 / SEG-102756 / DSSEG-6712
- アプリケーションコントロールがロックダウンモードの場合、場合によっては適切なソフトウェアインベントリを構築できませんでした。 SEG-94173 / SF03946250 / DSSEG-6503
- アプリケーションコントロールは、".install4j" ディレクトリ内のファイルをインベントリに追加できないため、一部のアプリケーションのインストールを妨げていました。 SEG-100706 / SF04166919 / DSSEG-6674
- Deep Security Agentが侵入防御の実行中にデータベースに接続できないことがあります。 DSSEG-6641
- アプリケーションコントロールは、認識されたソフトウェアインベントリにファイル拡張子「.ksh」を持つスクリプトを含めていないため、許可されたときにこれらのスクリプトがブロックされていました。 SEG-100706 / SF04166919 / DSSEG-6658
- Deep Security AgentがWebサーバへのSSL接続を確立できないことがあります。 SEG-93807 / SF03773176 / DSSEG-6624

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示さ

れ、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。 DSSEG-6440

最も高いCVSSスコア: 5.3

最高の重大度：中

Deep Security Agent - 12.0アップデート15

リリース日：2021年1月28日

ビルド番号：12.0.0-1546

新機能

- 不正プログラム対策 リアルタイム検索は、Dockerコンテナで動作しないことがありました。 DSSEG-6476

解決済みの問題

- Deep Security Agent SAP検索サービスで、特定のファイルの形式が正しく識別されていません。 DSSEG-6180
- アプリケーションコントロールにより、CPUのソフトロックアップが発生することがありました。 SEG-93033 / SF03882268 / DSSEG-6429
- 場合によっては、AWSインスタンスで大量のメモリが消費されていました。 SEG-86654 / SF03616828 / DSSEG-6405
- SSLインスペクションが有効になっていると、SSL接続が確立されないことがあります。 DSSEG-6407
- 不正プログラム対策 リアルタイム検索が有効になっていた場合、Rancher Kubernetesポッドを正常に終了できないことがありました。 SEG-87824 / SF03695639 / DSSEG-6454
- Deep Security AgentがWebサーバへのSSL接続を確立できないことがありません。 SEG-93807 / SF03773176 / DSSEG-6556

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣

行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。

Deep Security エージェント-12.0 update 14

リリース日：2020年11月12日

ビルド番号：12.0.0-1436

解決済みの問題

- エラー "atomic during scheduling during" dsa_filterが原因でカーネルパニックが発生しました。SEG-83207 / SF03470132 / DSSEG-6282
- 不正プログラム対策ドライバは、初期化中に警告メッセージを表示しました。SEG-92204/03784490 / DSSEG-6389

Deep Security Agent-12.0 update 13

リリース日：2020年10月1日

ビルド番号：12.0.0-1373

新機能

- 不正プログラムとサードパーティのセキュリティ保護機能との互換性が向上しました。SEG-84563/03564043 / DSSEG-6039
- VMware NSX 6.4.8をサポートするようにバージョンアップされたVMware NetX SDK
- Deep Securityは、ソフトウェア・ファイルが署名時以降に変更されていないことを確実にするためのDeep Securityエージェントの署名を検証します。DSSEG-5935
- HTTPヘッダの「X-Forwarded-For」タグに複数のIPアドレスがある場合、そのうちの最初のIPアドレスが取得されます。DSSEG-6183
- 変更監視Deep Security Managerの 検索完了時刻が秒単位で1000単位の区切り文字で表示されるようにアップデートしました。SEG-83194 / SF03429936 / DSSEG-6029

解決済みの問題

- ファイルシステムのフックを有効にしたリアルタイム不正プログラムは、旧バージョンのカーネルでは機能しませんでした。SEG-82411 / DSSEG-5991
- Deep Security Agentが、[Scan for Integrity]検索の実行中にクラッシュすることがありました。SEG-82795/03462751 / DSSEG-6008
- dsa_queryコマンドで、不正プログラムパターンが正しく表示されませんでした。DSSEG-6073
- Deep Security Anti-Malware カーネルモジュールは、ds_agentサービスが停止したときに正常にアンロードされませんでした。SEG-83209 / SF03512620 / DSSEG-6043
- 不正プログラム および アプリケーションコントロール が有効になっている場合、ds_agentサービスを停止するとCPU使用率が高くなる可能性があります。SEG-85738 / SF03595067 / DSSEG-6157
- Deep Security Agentのイベント「9105：エージェントの停止時に リレー Web サーバの失敗が有効になりました。SEG-79615/03326180 / DSSEG-6022
- 作成および実行された実行可能ファイルは、アプリケーションコントロールによってブロックされていました。DSSEG-6173
- Linuxで不正プログラムリアルタイム検索が有効になっていた場合、カーネルシステムコールフックに基づくサードパーティのセキュリティソフトウェアとの互換性の問題により、システムがクラッシュすることがありました。SEG-88135 / SF03700563 / DSSEG-6247
- 「Out of Connection」ファイアウォールイベントは、ネットワークエンジンが「タップモード」に設定されたときに発生しました。SEG-87155 / SF03644367 / DSSEG-6270
- 一部の 侵入防御 イベントにXFFヘッダが含まれていませんでした。SEG-81986/03419140 / DSSEG-5936

お知らせ

Deep Security 9.5がEnd of Supportに達しました。このリリースにアップグレードすることはできません。DSSEG-5938

Deep Security Agent-12.0 update 12

リリース日：2020年8月19日

ビルド番号：12.0.1278

プラットフォームのサポートの強化

- CloudLinux 8 (64ビット)

新機能

- パケットデータをDeep Security Managerに送信しないように選択するには、管理>エージェント>データプライバシーに進み、いいえを選択します。
SF03237033 / DSSEG-6017

注意: この機能強化には、Deep Security Manager FR 2019-10-23以降が必要です。

解決済みの問題

- Linuxで不正プログラム対策のリアルタイム検索が有効になっていた場合、procfsのバッファが検証されなかったため、システムがクラッシュすることがありました。SEG-80183 / DSSEG-5884
- アプリケーションコントロールによって、許可されているはずのアプリケーションが、信頼済みアップデートによって作成されたときにブロックされることがありました。SEG-77446/03206632 / DSSEG-5840
- エージェントの自己保護でDeep Security Notifierを保護できませんでした。
SEG-76015 / SF03168155 / DSSEG-5920
- Deep Security Agentが無効化されると、不正プログラム対策モジュールの言語が英語に切り替わりました。Deep Securityエージェントが日本語で再アクティベートされた場合、不正プログラム対策コンポーネントのアップデートが失敗することがありました。SEG-79963/03184072 / DSSEG-5811
- 新しいパケットを含む再送信パケットが送信された場合、「サポートされていないSSLバージョン」の侵入防御 event./DSSEG-5879が生成されることがあります。
- セキュリティログ監視データベース破損の問題が発生した場合、Deep Security Managerのセキュリティログ監視のステータスには影響しませんでした。SEG-77081/02984526 / DSSEG-5726

- Deep Security Agentがセキュリティアップデートとして除外を受信したため、Deep Security Managerによってセキュリティアップデートのタイムアウトが報告されました。SEG-82072/03273761 / DSSEG-5953
- setuid/setgid 形式のため、Deep Security Agentで偽のファイル変更イベントが検出されました。また、 /usr/bin では、ファイルの作成時に change./DSSEG-5928が原因でアップグレード時にファイル属性の変更が不正に発生しています。
- 「アプリケーションコントロールリレーからのルールセットを提供」が有効になっていると、不要なリレーエラーイベント occurred./DSSEG-5988
- Kerberosキャッシュファイルが削除されて再追加されたときに、「ユーザが追加しました」および「ユーザが削除しました」変更監視イベントが多数発生しました。SEG-80629/03402557 / DSSEG-5981

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-5255

CVSSスコア：7.8

重大度：高

- curl 7.67.0にアップデートされました。
- openssl-1.0.2tにアップデートされました。

Deep Security Agent-12.0 update 11

リリース日：2020年7月9日

ビルド番号：12.0.1186

新機能

- アプリケーションコントロールには、拡張子「.cron」を持つスクリプトファイルが含まれています。SEG-76680 / SF03240341 / DSSEG-5685

- 変更監視では、LinuxおよびUnixプラットフォームの「setuid」属性と「setgid」属性に対する変更が検出されます。SEG-78797 / DSSEG-5732
- リアルタイム変更監視は、ベースディレクトリで指定されたディレクトリと明示的に一致します。以前は、ベースディレクトリで開始されたすべてのパスに一致していました。SEG-79112/03301290 / DSSEG-5767

解決済みの問題

- autofsが使用されたLinuxプラットフォームでは、不正プログラム対策ドライバによりシステムハングが発生しました。SEG-78320 / SF03199934 / DSSEG-5718
- Deep Securityリアルタイムの不正プログラム対策の検索がLinuxプラットフォームで有効になっていたため、大量のCPUが使用されていました。SEG-75739 / SF03036857 / DSSEG-5836
- アプリケーションコントロールが有効になっていると、エージェントが定期的に再起動されることがあります。SEG-79922 / DSSEG-5823 / SEG-75985 / SF03184883 / DSSEG-5843
- Webレピュテーション、ファイアウォール、または侵入防御が有効になったときにカーネルパニックが発生しました。SEG-80201 / SF03332691 / DSSEG-5846

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。

- Nginxが1.18.0にアップデートされました。

SEG-78524 / SF03321021 / DSSEG-5749

Deep Security Agent-12.0 update 10

リリース日：2020年5月28日

ビルド番号：12.0.1090

新機能

プラットフォームのサポートの強化

- Ubuntu 20.04 (64ビット)

管理と品質の向上

インスタンスメタデータサービスバージョン2 (IMDSv2) のサポート：IMDSv2は、Deep Security Manager 12.0アップデート10でサポートされます。詳細については、「["Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使いますか" on page 1534](#)」を参照してください。DSSEG-5422

拡張機能

- カーネルパニックを防ぐためにファイルシステムのカーネルフックからCephを除外しました。DSSEG-5584
- Account Domain Authenticationの環境を改善し続けました。SEG-73480 / SF02989282 / DSSEG-5661

解決済みの問題

- Deep Security Agentのアップグレードに問題があり、変更監視またはセキュリティログ監視が有効になっていると、エージェントがオンラインにならないことがあります。SEG-75769 / SF03196478 / DSSEG-5596
- Deep Security Agentからネットワークインタフェース情報が正しくないことが報告されました。SEG-77161 / DSSEG-5644
- リアルタイムの不正プログラム対策検索で検出の問題が発生しました。SEG-72928 / SF03050515 / DSSEG-5362
- アプリケーションコントロールでは、拡張子「.bash」のスクリプトはインベントリに含まれていませんでした。その結果、これらのスクリプトはロックダウンモードでブロックされます。SEG-73174 / SF03063609 / DSSEG-5381
- 状況によっては、アプリケーションコントロールによってエージェントがオフラインになって再起動してしまいました。SEG-74143 / SF03119820 / DSSEG-5524

- Linux上のDeep Security Agentがクラッシュすることがある問題。SEG-76460 / SF03218198 / DSSEG-5623
- リアルタイムの不正プログラム対策の検索後、システムが応答しなくなることがありました。SEG-76430 / SF02537903 / DSSEG-5629

Deep Security Agent-12.0 update 9

リリース日：2020年5月4日

ビルド番号：12.0.1026

新機能

- Red Hat Enterprise Linux 7およびRed Hat Enterprise Linux 8でのSecurity-Enhanced Linux (SELinux) 強制モードのサポートが追加されました。Deep Security Agentは、初期設定のSELinuxポリシーと互換性があります。

注意: ds_agentなどの不正プログラム対策ソフトウェアは、システムを保護するために一意のドメインで実行する必要があります。追加のSELinuxポリシーのカスタマイズまたは設定は、ds_agentのためにブロックまたは失敗することがあります。

解決済みの問題

- ワイルドカードを使用した不正プログラム対策ディレクトリの除外が、サブディレクトリと正しく一致していませんでした。SF03131855 / SEG-74892 / DSSEG-5543
- リアルタイムの変更監視を有効にした場合、アカウントドメイン認証が遅くなることがあります。SEG-73480 / DSSEG-5592
- 不正プログラム対策エンジンのアップデートが実行されたときに、不正プログラム対策が正常に適用されないことがありました。DSSEG-5483
- アプリケーションコントロールと不正プログラム対策が有効になっていると、アプリケーションコントロールがオフラインで表示されることがありました同時に。(DSSEG-5383/SEG-72885)
- [Actions]タブのアプリケーションコントロールに、承認または拒否のために保留中のソフトウェア変更があるコンピュータが表示されました。ただし、コン

コンピュータの詳細ウィンドウが開いたときにイベントが報告されませんでした。
SEG-74084 / SF03106203 / DSSEG-5449

- アプリケーションコントロールと不正プログラム対策が有効になっていると、アプリケーションコントロールがオフラインで表示されることがありました同時に。SEG-72885/03036072 / DSSEG-5383
- Deep Security Virtual Applianceの不正プログラム対策エンジンは、Censusサーバの応答の署名者フィールドが空の場合にオフラインになりました。SEG-73047 / SF03065452 / DSSEG-5447

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。DSSEG-5280

Deep Security Agent-12.0 update 8

リリース日：2020年4月1日

ビルド番号：12.0.0-967

新機能

- Deep Security Agent 不正プログラム対策が、IntelliScanが無効になっているときにデータタイプに関係なく圧縮ファイルを検索できるようになりました。(SEG-71425/02971395/DSSEG-5306)
- 強化された不正プログラム対策 file/folder 除外設定には、「(」または「)」などの角カッコが含まれる環境変数のサポートが追加されています。(DSSEG-5260)

解決済みの問題

- Webレピュテーション、ファイアウォール、侵入防御、およびセキュリティログ監視を有効にできませんでした。(SEG-71825/SF03021819/DSSEG-5351)
- ルール「1002875：Unix Add/Remove Software」が適用されたリアルタイム変更監視が有効になっている場合、RPMデータベースはロックされている可能性があります。(SEG-67275/SF02663756/DSSEG-5308)

- 不正プログラム対策の準備が完了する前にセキュリティ更新プログラムが実行された場合、セキュリティ更新プログラムは失敗しました。(DSSEG-5361)
- セキュリティログ監視を有効にすると、Deep Security Agentがクラッシュしました。(SEG-61106/SEG-42752/DSSEG-5225)
- 一部のリアルタイム変更監視の変更が/varディレクトリで検出されませんでした。(SEG-72584/02982752/DSSEG-5346)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。(DSSEG-3771)

Deep Security Agent-12.0 update 7

リリース日：2020年2月28日

ビルド番号：12.0.0-911

新機能

- 検索エンジンのURIパスの長さの制限が増加しました。(SEG-61309/DSSEG-5245)

解決済みの問題

- Deep Security Agentのリアルタイム不正プログラム対策の検索が、Linuxカーネル5.5で正しく機能していません。(DSSEG-5209)
- Deep Security Agentのリアルタイム不正プログラム対策検索がDebian 10カーネル5.4で正しく機能しませんでした。(DSSEG-5153)
- 表示されたパケットヘッダデータには、冗長ペイロードデータが含まれていません。(DSSEG-4762)
- ルール1006540「X-Forwarded-For HTTPヘッダロギングを有効にする」を適用すると、Deep Securityは侵入防御イベントのX-Forwarded-Forヘッダを正しく抽出します。ただし、「無効なトラバーサル」などのURL侵入は、ヘッダが解析される前にHTTP要求文字列で検出されます。侵入防御エンジンが強化され、ヘッダが解析された後にX-Forwarded-Forヘッダが検索されます。(DSSEG-5156)

- Deep Security Virtual Applianceがオフラインになることがありました。(DSSEG-5184)
- Deep Security Agent 不正プログラム対策が、不正プログラム対策イベントに無効なコンテナIDのコンテナ情報を取得しようとしてしました。(SEG-69502/SF02915821/DSSEG-5186)
- SSL処理の欠陥のため、SSL復号化中にメモリがリークしました。(DSSEG-5142)
- Deep Security Agentのリアルタイム不正プログラム対策検索がDebian 10カーネル5.3.0-0.bpo.2-amd64で正しく機能しませんでした。(DSSEG-5135)
- セキュリティログ監視イベント処理により、Deep Security Agentが異常再起動しました。(DSSEG-5228)
- 特定のDeep Security Agent Serverで、CPU使用率が100%に達し、アクティブなアップデートプロセスでパターンマージに失敗しました。(SEG-66210/02711299/DSSEG-5152)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。

- SQLiteが3.30.1にアップデートされました。(DSSEG-5103)

Deep Security Agent-12.0 update 6

リリース日：2020年1月17日

ビルド番号：12.0.0-817

新機能

- LinuxでDocker pullコマンドを実行すると、リアルタイムの不正プログラム対策のパフォーマンスが向上しました。(SF02181241/SEG-54744/DS-38060)

解決済みの問題

- 検索ディレクトリのインクルードリストでルートディレクトリが「/」に設定されていると、不正プログラム対策のオンデマンド検索が正しく機能しませんでした。(SEG-66679/02756807/DSSEG-5052)

- ファイル属性を取得できなかった場合、不正プログラム対策でメモリリークが発生しました。(SEG-67374/DSSEG-5063)
- Deep Security AgentがDeep Security Managerへの応答として無効なJSONオブジェクトを送信したことが原因で、Deep Security Managerのログファイルでエラーが発生する問題がありました。(SEG-48728/SF01919585/DSSEG-4995)
- ルール1006540「X-Forwarded-For HTTPヘッダロギングを有効にする」を適用すると、Deep Securityは侵入防御イベントのX-Forwarded-Forヘッダを正しく抽出します。ただし、「無効なトラバーサル」などのURL侵入は、ヘッダが解析される前にHTTP要求文字列で検出されます。侵入防御エンジンが強化され、ヘッダが解析された後にX-Forwarded-Forヘッダが検索されます。(SEG-60728/DSSEG-5094)

Windows

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Agent - Windows 12.0 Readme](#)を参照してください。

Deep Security Agent - 12.0 update 30

リリース日：2023年5月4日

ビルド番号：12.0.0-2932

新機能

- Deep Security Agentのインストールで、オペレーティングシステムがAzureコード署名 (ACS) の要件を満たしているかどうかを確認されるようになりました。詳細については、「[Trend Micro Server and Endpoint Protection AgentのWindowsの最小バージョン要件](#)」を参照してください。DSSEG-7813

解決済みの問題

- Windows Active Directoryドメインコントローラ上のDeep Security Agentに対して、「UserSet」または「GroupSet」を使用する変更監視ルールを有効にすると、CPUとメモリが過剰に消費されることがありました。Deep Security Agent 12.0.0-2932では、Windows Active Directoryドメインコントローラでこれらの種

類の変更監視ルールがブロックされ、「適用変更監視ルール」イベントが生成されません。SF06082644 / SEG-155804 / DSSEG-7725

- コンポーネントのアップデート中に問題が発生し、エンジンのアップデートが無効になっていても、検索エンジンがアップデートされることがありました。SF06390800 / SEG-165036 / DSSEG-7802

Deep Security Agent-12.0 update 29

リリース日：2022年10月4日

ビルド番号：12.0.0-2626

新機能

- 「Bypass Network Scanner」ルール適用時の侵入防御のパフォーマンスが向上しました。SEG-132057 / DSSEG-7621

解決済みの問題

- エージェントのアップグレード中に、「新しく適用されたルールセットによって、再起動時に一部の実行中のプロセスがブロックされます」というメッセージが誤って表示されました。DSSEG-7653
- 一致または正規表現フィールドで変数に「\$」文字を使用すると、セキュリティセキュリティログ監視エンジンがオフラインになる問題を修正しました。SEG-146965 / SEG-146966 / DSSEG-7665
- IPv4 / IPv6変換用に予約された有効なIPv6アドレスがあると、「無効なIPv6アドレス」エラーが発生しました。SEG-147969 / DSSEG-7673

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7090 / DSSEG-7647

最高のCVSS：4.6

最高の重大度：中

Deep Security Agent-12.0 update 28

リリース日：2022年7月4日

ビルド番号：12.0.0-2487

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7385 / DSSEG-7563、VRTS-7647 / DSSEG-7625、VRTS-7633 / DSSEG-7599

最高CVSS：9.8

重大度が最も高い：重大

解決済みの問題

- アプリケーションコントロールは、インベントリ検索が完了するまで、ハッシュによるプロセスのブロックに失敗しました。

Deep Security Agent - 12.0 update 27

リリース日：2022年5月26日

ビルド番号：12.0.0-2416

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7130 / DSSEG-7528

CVSS：7.5

重大度：高

Deep Security Agent-12.0 update 26

リリース日：2022年4月28日

ビルド番号：12.0.0-2380

解決済みの問題

- 不正プログラム対策を有効にすると、イベントレポートの配信で問題が発生し、Deep Security Agentで大量のシステムメモリが使用されるようになりました。SF05247760 / SEG-132286 / DSSEG-7514
- 侵入防御が有効になっていると、パケット転送エラーによって一部のシステム設定がクラッシュしました。SEG-136843 / DSSEG-7524

Deep Security Agent - 12.0 update 25

リリース日：2022年3月8日

ビルド番号：12.0.0-2265

新機能

Windows 10 21H2：Deep Security Agent（バージョン12.0-2265+）がWindows 10 21H2でサポートされるようになりました。

解決済みの問題

- ドライバが競合しているため、VMwareを実行しているシステムで、手動、予約、およびリアルタイムの不正プログラム対策が機能しませんでした。DSSEG-7397
- パスワードの確認に失敗した場合でも、Deep Security Agentでポリシーの変更パラメータが受け入れられることがありました。SEG-129643 / DSSEG-7431
- 不正プログラム対策ドライバの競合により、Citrix仮想アプリケーションおよびデスクトップアプリケーションがフリーズしました。SEG-131549 / DSSEG-7495

新機能

- Deep Security Agentがアップデートされ、「メンテナンスモード」での実行時のアプリケーションコントロールのパフォーマンスが向上しました。DSSEG-7354

Deep Security Agent - 12.0 update 24

リリース日：2022年1月24日

ビルド番号：12.0.0-2201

このリリースには、一般的な改善が含まれます。

Deep Security Agent - 12.0 update 23

リリース日：2021年11月29日

ビルド番号：12.0.0-2112

解決済みの問題

- Deep Security Managerに接続できない場合、Deep Security Agentがクラッシュすることがありました。DSSEG-7305
- Deep Security Agentによって接続の問題、CPU使用率の増加、またはシステムのクラッシュが発生することがありました。SEG-123885 / SF04973642 / DSSEG-7298

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。DSSEG-7255

最高のCVSS：7.8

最高の重大度：高

Deep Security Agent - 12.0 update 22

リリース日：2021年11月1日

ビルド番号：12.0.0-2072

解決済みの問題

- 証明書失効リスト（CRL）が一致しないため、アップグレード中にDeep Security Agentでパッケージ署名エラーが表示されることがありました。 DSSEG-7214
- プラグインバージョンの競合により、Deep Security AgentがRelayからKSP（カーネルサポートパッケージ）ファイルを取得できないことがありました。 DSSEG-7244
- 非アクティブなネットワーク接続のリソースをクリーンナップする際に、問題によってDeep Security Agentがクラッシュすることがありました。 SEG-113291 / DSSEG-7035
- 不正プログラム対策の検索中にDeep Security Agentサービス（ds_agent）を停止すると、再起動時にAgentがクラッシュすることがありました。 DSSEG-7228

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。 VRTS-6489 / DSSEG-7237

最高のCVSS：7.8

最高の重大度：高

Deep Security Agent-12.0 update 21

リリース日：2021年9月15日

ビルド番号：12.0.0-1993

解決済みの問題

- 不正プログラム対策を有効にすると、一部のシステムでDeep Security Agentによってサードパーティ製ソフトウェアの接続の問題が発生していました。SF04087024 / SEG-100464 / DSSEG-7069
- ネットワークインタフェースカード (NIC) の接続の問題により、Deep Security Agentが複数の「セキュリティログ監視 エンジン初期化」または「ポリシー送信」イベントをトリガすることがありました。SF03968169 / SEG-95731 / DSSEG-7039

Deep Security Agent-12.0 update 20

リリース日：2021年8月4日

ビルド番号：12.0.0-1908

プラットフォームのサポートの強化

- Windows 10 21H2：Deep Security Agent（バージョン12.0.0-1908+）でWindows 10 21H1がサポートされるようになりました。

解決済みの問題

- SSL接続の確立中に、Deep Security Agentの接続が切断されることがありました。SEG-107451 / DSSEG-7016
- 古いバージョンのOSを使用しているシステムでは、Deep Security AgentがWebアプリケーションに接続できないことがありました。SEG-109652 / DSSEG-6992

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-6032 / DSSEG-6967

最も高いCVSSスコア: 9.8

最高の重大度：高

Deep Security Agent-12.0 update 19

リリース日：2021年7月6日

ビルド番号：12.0.0-1845

解決済みの問題

- Webレピュテーションを有効にすると、Deep Security Agentによって一部のサードパーティのソフトウェアで接続の問題が発生しました。 SF04072723 / SEG-97952 / DSSEG-6810

Deep Security Agent-12.0 update 18

リリース日：2021年5月27日

ビルド番号：12.0.0-1789

解決済みの問題

- Deep Security Agentで「ユーザ（作成/削除）」イベントまたは「グループ（追加/削除/アップデート）イベント」イベントが作成されることがありました。 SEG-96947 / SF04034198 / DSSEG-6837
- 侵入防御がSSL検査用に設定されていると、Deep Security Agentがクラッシュすることがありました。 DSSEG-6909
- Deep Security Agentで「Invalid Flag」ファイアウォール イベントが重複して表示されることがありました。 DSSEG-6835
- 不正プログラム対策 モジュールが実行されていた場合、Deep Security Agentがいくつかの設定でクラッシュしました。 SEG-101968 / SF04225628 / DSSEG-6791

Deep Security Agent - 12.0 update 17

リリース日：2021年4月26日

ビルド番号：12.0.0-1735

プラットフォームのサポートの強化

- Windows 10 20H2

新機能

- Deep Security Agentが最新のWindowsクロスサインオプションを使用するようにアップデートされました。 DSSEG-6820

解決済みの問題

- アップグレード失効リスト (CRL) が一致していないため、Deep Security Agentでパッケージングネチャエラーが発生することがありました。 DSSEG-6826
- アプリケーションコントロールは、特定の種類のドライブ上のファイルに対して適切なソフトウェアインベントリを追加しないことがあります。 SEG-103667 / SF04227412 / DSSEG-6756
- Deep Security Agentは、1つの侵入防御イベントの重複を報告することがあります。 SEG-93125 / SF03595899 / DSSEG-6723
- Deep Security Agentでは、通常、これらのイベントを発生させる条件は存在しませんでした。複数の「レコード層メッセージ (未処理)」侵入防御イベントが発生することがありました。「Record Layer Message (not ready)」イベントは通常、セッションの初期化前にSSLステートエンジンでSSLレコードが検出されたことを示します。 SEG-101697 / SF04203096 / DSSEG-6739

Deep Security Agent - 12.0 update 16

リリース日: 2021年3月22日

ビルド番号: 12.0.0-1655

新機能

- Deep Security Agentがアップデートされ、アプリケーションコントロールのインベントリ検索のパフォーマンスが向上しました。 SEG-78295/03234667 / DSSEG-6303

解決済みの問題

- リアルタイムの変更監視は、ユーザによって指定された正確なディレクトリに一致しない場合がありますが、ベースディレクトリで開始されたすべてのパスに一致することがあります。 SEG-97758 / SF04046718 / DSSEG-6636
- アプリケーションコントロールがロックダウンモードの場合、場合によっては適切なソフトウェアインベントリを構築できませんでした。 SEG-94173 / SF03946250 / DSSEG-6503
- 侵入防御をパッシブモードで実行していると、Deep Security Agentがクラッシュすることがありました。 DSSEG-6385
- アプリケーションコントロールは、".install4j" ディレクトリ内のファイルをインベントリに追加できないため、一部のアプリケーションのインストールを妨げていました。 SEG-100706 / SF04166919 / DSSEG-6674
- 挙動監視の除外が正しく機能しない場合があります。 SEG-89899 / SF03775351 / DSSEG-6485
- アプリケーションコントロールは、認識されたソフトウェアインベントリにファイル拡張子「.ksh」を持つスクリプトを含めていないため、許可されたときにこれらのスクリプトがブロックされていました。 SEG-100706 / SF04166919 / DSSEG-6658

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。 DSSEG-6440

最も高いCVSSスコア: 5.3

最高の重大度: 中

Deep Security Agent - 12.0アップデート15

リリース日: 2021年1月28日

ビルド番号: 12.0.0-1546

解決済みの問題

- 場合によっては、AWSインスタンスで大量のメモリが消費されていました。SEG-86654 / SF03616828 / DSSEG-6405
- SSLインスペクションが有効になっていると、SSL接続が確立されないことがあります。DSSEG-6407

Deep Security エージェント-12.0 update 14

リリース日：2020年11月12日

ビルド番号：12.0.0-1436

このリリースのWindows Deep Security Agentには変更がありません。

Deep Security Agent-12.0 update 13

リリース日：2020年10月1日

ビルド番号：12.0.0-1373

新機能

- Deep Securityは、ソフトウェア・ファイルが署名時以降に変更されていないことを確実にするためのDeep Securityエージェントの署名を検証します。DSSEG-5935
- 変更監視Deep Security Managerの 検索完了時刻が秒単位で1000単位の区切り文字で表示されるようにアップデートしました。SEG-83194 / SF03429936 / DSSEG-6029

解決済みの問題

- Deep Security AgentがWindows Server上のDockerエンジンのバージョンを検出できなかったため、予期せずクラッシュしました。DSSEG-6075
- Deep Security Notifierは、Windowsのアクションセンターで[ウイルス対策]のステータスをオン/オフにしていたため、CPU使用率が高くなりました。SEG-73189 / SF03037857 / DSSEG-6004

- Deep Security Agentが、[Scan for Integrity]検索の実行中にクラッシュすることがありました。SEG-82795/03462751 / DSSEG-6008
- 作成および実行された実行可能ファイルは、アプリケーションコントロールによってブロックされていました。/ DSSEG-6173
- HTTPヘッダの「X-Forwarded-For」タグに複数のIPアドレスがある場合、そのうちの最初のIPアドレスが取得されます。/ DSSEG-6183
- 「Out of Connection」ファイアウォールイベントは、ネットワークエンジンが「タップモード」に設定されたときに発生しました。SEG-87155 / SF03644367 / DSSEG-6270
- 一部の侵入防御イベントにXFFヘッダが含まれていませんでした。SEG-81986/03419140 / DSSEG-5936

Deep Security Agent-12.0 update 12

リリース日：2020年8月19日

ビルド番号：12.0.1278

プラットフォームのサポート強化

- Windows 10 20H1 v2004 (64 & 86)
- Windows Server Core 20H1 v2004

新機能

- パケットデータをDeep Security Managerに送信しないように選択するには、管理>エージェント>データプライバシーに進み、いいえを選択します。。
SF03237033 / DSSEG-6017

注意: この機能強化には、Deep Security Manager FR 2019-10-23以降が必要です。

解決済みの問題

- アプリケーションコントロールによって、許可されているはずのアプリケーションが、信頼済みアップデートによって作成されたときにブロックされることがありました。SEG-77446/03206632 / DSSEG-5840

- エージェントの自己保護がDeep Security通知機能SEG-76015 / SF03168155 / DSSEG-5920を保護していません
- Deep Security Agentが無効化されると、不正プログラム対策モジュールの言語が英語に切り替わりました。Deep Securityエージェントが日本語で再アクティベートされた場合、不正プログラム対策コンポーネントのアップデートが失敗することがありました。SEG-79963/03184072 / DSSEG-5811
- 新しいパケットを含む再送信パケットが送信されると、「サポートされていないSSLバージョン」の侵入防御イベントが生成されることがありました。 / DSSEG-5879
- セキュリティログ監視データベース破損の問題が発生した場合、Deep Security Managerのセキュリティログ監視のステータスには影響しませんでした。SEG-77081/02984526 / DSSEG-5726
- Deep Security Agentがセキュリティアップデートで例外を受信したため、Deep Security Managerによってセキュリティアップデートのタイムアウトが報告されました。SEG-82072/03273761 / DSSEG-5953
- 「Served アプリケーションコントロールルールセットをリレーから」が有効になっている場合、不要なリレーエラーイベントが発生しました。 / DSSEG-5988
- Kerberosキャッシュファイルが削除されて再追加されたときに、「ユーザが追加しました」および「ユーザが削除しました」変更監視イベントが多数発生しました。SEG-80629/03402557 / DSSEG-5981

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。

CVSSスコア：7.8

重大度：高

- curl 7.67.0にアップデートされました。
- openssl-1.0.2tにアップデートされました。

Deep Security Agent-12.0 update 11

リリース日：2020年7月9日

ビルド番号：12.0.1186

新機能

- アプリケーションコントロールには、拡張子「.cron」を持つスクリプトファイルが含まれています。SEG-76680 / SF03240341 / DSSEG-5685
- リアルタイム変更監視は、ベースディレクトリで指定されたディレクトリと明示的に一致します。以前は、ベースディレクトリで開始されたすべてのパスに一致していました。SEG-79112/03301290 / DSSEG-5767

解決済みの問題

- 変更監視が有効な場合、ファイルの所有者が存在しないユーザに誤って変更されています。DSSEG-5731

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。

- Nginxが1.18.0にアップデートされました。

SEG-78524 / SF03321021 / DSSEG-5749

Deep Security Agent-12.0 update 10

リリース日：2020年5月28日

ビルド番号：12.0.1090

新機能

管理と品質の向上

インスタンスメタデータサービスバージョン2 (IMDSv2) のサポート：IMDSv2は、Deep Security Manager 12.0アップデート10でサポートされます。詳細については、「["Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使いますか" on page 1534](#)」を参照してください。DSSEG-5422

新機能

- Account Domain Authenticationの環境を改善し続けました。SEG-73480 / SF02989282 / DSSEG-5661

解決済みの問題

- リアルタイムの不正プログラム対策検索で検出の問題が発生しました。SEG-72928 / SF03050515 / DSSEG-5362
- 不正プログラム対策が有効になっていると、エージェントコンピュータがクラッシュすることがありました。SEG-75451 / SF03174016 / DSSEG-5602
- 状況によっては、アプリケーションコントロールによってエージェントがオフラインになって再起動してしまいました。SEG-74143 / SF03119820 / DSSEG-5524
- リアルタイムの不正プログラム対策の検索後、システムが応答しなくなることがありました。SEG-76430 / SF02537903 / DSSEG-5629

Deep Security Agent-12.0 update 9

リリース日：2020年5月4日

ビルド番号：12.0.1026

解決済みの問題

- 侵入防御が有効になっていて、同じ位置でペイロードが異なるIPフラグメンテーションパケットが受信された場合、エンジンはペイロードを組み立てるために以前のパケットではなく、後のパケットを使用することを選択しました。この場合、ペイロードの整合性チェックにより、この接続のパケットが破棄されます。SEG-70386 / DSSEG-5428

- 不正プログラム対策ドライバによって、RDPプロセスが停止することがありました。

注意: 最新のOSを使用している場合 (Windows 7より新しいバージョン、たとえば), の場合は、不正プログラム対策ドライバを適用した後にシステムを再起動してください)。

SF03060355 / SEG-72751 / DSSEG-5391

- アプリケーションコントロールと不正プログラム対策が有効になっていると、アプリケーションコントロールがオフラインで表示されることがありました同時に。DSSEG-5383 / SEG-72885
- [Actions]タブのアプリケーションコントロールに、承認または拒否のために保留中のソフトウェア変更があるコンピュータが表示されました。ただし、コンピュータの詳細ウィンドウが開いたときにイベントが報告されませんでした。SEG-74084 / SF03106203 / DSSEG-5449
- アプリケーションコントロールと不正プログラム対策が有効になっていると、アプリケーションコントロールがオフラインで表示されることがありました同時に。SEG-72885/03036072 / DSSEG-5383
- Deep Security Virtual Applianceの不正プログラム対策エンジンは、Censusサーバの応答の署名者フィールドが空の場合にオフラインになりました。SEG-73047 / SF03065452 / DSSEG-5447
- 不正プログラム対策ドライバによって、RDPプロセスが停止することがありました。

注意: 注意：最新のOS (Windows 7より新しいバージョン、たとえば,) を使用している場合は、不正プログラム対策ドライバが適用された後にシステムを再起動してください。

SEG-72751 / SF03060355 / DSSEG-5391

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。DSSEG-5280

Deep Security Agent-12.0 update 8

リリース日：2020年4月1日

ビルド番号：12.0.0-967

新機能

- Deep Security Agent 不正プログラム対策が、IntelliScanが無効になっているときにデータタイプに関係なく圧縮ファイルを検索できるようになりました。(SEG-71425/02971395/DSSEG-5306)
- 強化された不正プログラム対策 file/folder 除外設定には、「 (」または「) 」などの角カッコが含まれる環境変数のサポートが追加されています。(DSSEG-5260)

解決済みの問題

- Webレピュテーション、ファイアウォール、侵入防御、およびセキュリティログ監視を有効にできませんでした。(SEG-71825/SF03021819/DSSEG-5351)
- ルール「1002875：Unix Add/Remove Software」が適用されたリアルタイム変更監視が有効になっている場合、RPMデータベースはロックされている可能性があります。(SEG-67275/SF02663756/DSSEG-5308)
- 不正プログラム対策の準備が完了する前にセキュリティ更新プログラムが実行された場合、セキュリティ更新プログラムは失敗しました。(DSSEG-5361)
- セキュリティログ監視を有効にすると、Deep Security Agentがクラッシュしました。(SEG-61106/SEG-42752/DSSEG-5225)
- 一部のリアルタイム変更監視の変更が/varディレクトリで検出されませんでした。(SEG-72584/02982752/DSSEG-5346)
- 不正プログラム対策の挙動監視機能により、誤検出が発生することがありました。(SEG-61282/SF02431397/DSSEG-4997)
- Deep Security Agentが予期せず再起動しました。これは、セキュリティログ監視がSQLiteデータベースにアクセスしていたためです。(SEG-71302/02970735/DSSEG-5309)
- Windowsインストーラのeulaファイルの上部に空白行があります。(DSSEG-5348)
- 不正プログラム対策により、メモリリークが発生することがありました。(DSSEG-5323)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。(DSSEG-3771)

Deep Security Agent-12.0 update 7

リリース日：2020年2月28日

ビルド番号：12.0.0-911

新機能

- 検索エンジンのURIパスの長さの制限が増加しました。(SEG-61309/DSSEG-5245)

解決済みの問題

- アプリケーションコントロールが有効な場合に、分散ファイルシステムの複製が原因で大量のソフトウェア変更が発生する問題がありました。(SEG-60169/DSSEG-5031)
- 表示されたパケットヘッダデータには、冗長ペイロードデータが含まれていません。(DSSEG-4762)
- Using Octopus Deploy with アプリケーションコントロールの結果、Powershellの実行エラーが発生しました。(SEG-67037/02655196/DSSEG-5084)
- Deep Security Agent 不正プログラム対策が、不正プログラム対策イベントに無効なコンテナIDのコンテナ情報を取得しようとしてしました。(SEG-69502/SF02915821/DSSEG-5186)
- セキュリティログ監視イベント処理により、Deep Security Agentが異常再起動しました。(DSSEG-5228)
- 特定のDeep Security Agent Serverで、CPU使用率が100%に達し、アクティブなアップデートプロセスでパターンマージに失敗しました。(SEG-66210/02711299/DSSEG-5152)
- アプリケーションコントロールが有効な場合に、分散ファイルシステムの複製が原因で大量のソフトウェア変更が発生する問題がありました。(SEG-60169/DSSEG-5031)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。

- SQLiteが3.30.1にアップデートされました。(DSSEG-5103)

Deep Security Agent-12.0 update 6

リリース日：2020年1月17日

ビルド番号：12.0.0-817

解決済みの問題

- Windows Server 2019 19H2 1909およびWindows 10 19H2 1909のプラットフォームが追加されました。(DSSEG-4782)
- Deep Security AgentがDeep Security Managerへの応答として無効なJSONオブジェクトを送信したことが原因で、Deep Security Managerのログファイルでエラーが発生する問題がありました。(SEG-48728/SF01919585/DSSEG-4995)
- 変更監視では、リアルタイムで検索されたファイルでロシア文字が正しく処理されませんでした。(SEG-64071/SF02608976/DSSEG-4983)
- ルール1006540「X-Forwarded-For HTTPヘッダロギングを有効にする」を適用すると、Deep Securityは侵入防御イベントのX-Forwarded-Forヘッダを正しく抽出します。ただし、「無効なトラバーサル」などのURL侵入は、ヘッダが解析される前にHTTP要求文字列で検出されます。侵入防御エンジンが強化され、ヘッダが解析された後にX-Forwarded-Forヘッダが検索されます。(SEG-60728/DSSEG-5094)

UNIX

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Agent - Unix 12.0 Readme](#)を参照してください。

Deep Security Agent - 12.0 update 30

リリース日：2023年5月4日

ビルド番号：12.0.0-2932

解決済みの問題

- コンポーネントのアップデート中に問題が発生し、エンジンのアップデートが無効になっていても、検索エンジンがアップデートされることがありました。
SF06390800 / SEG-165036 / DSSEG-7802

Deep Security Agent-12.0 update 29

リリース日：2022年10月4日

ビルド番号：12.0.0-2626

新機能

- 「Bypass Network Scanner」ルール適用時の侵入防御のパフォーマンスが向上しました。 SEG-132057 / DSSEG-7621

解決済みの問題

- エージェントのアップグレード中に、「新しく適用されたルールセットによって、再起動時に一部の実行中のプロセスがブロックされます」というメッセージが誤って表示されました。 DSSEG-7653
- 一致または正規表現フィールドで変数に「\$」文字を使用すると、セキュリティセキュリティログ監視エンジンがオフラインになる問題を修正しました。 SEG-146965 / SEG-146966 / DSSEG-7665
- IPv4 / IPv6変換用に予約された有効なIPv6アドレスがあると、「無効なIPv6アドレス」エラーが発生しました。 SEG-147969 / DSSEG-7673

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示さ

れ、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7090 / DSSEG-7647

最高のCVSS：4.6

最高の重大度：中

Deep Security Agent-12.0 update 28

リリース日：2022年7月4日

AIXビルド番号：12.0.0-2504

Solarisビルド番号：12.0.0-2487

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7385 / DSSEG-7563、VRTS-7647 / DSSEG-7625、VRTS-7633 / DSSEG-7599

最高CVSS：9.8

重大度が最も高い：重大

Deep Security Agent - 12.0 update 27

リリース日：2022年5月26日

ビルド番号：12.0.0-2416

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-7130 / DSSEG-7528

CVSS：7.5

重大度：高

Deep Security Agent-12.0 update 26

リリース日：2022年4月28日

ビルド番号：12.0.0-2380

解決済みの問題

- 不正プログラム対策を有効にすると、イベントレポートの配信で問題が発生し、Deep Security Agentで大量のシステムメモリが使用されるようになりました。SF05247760 / SEG-132286 / DSSEG-7514
- 侵入防御が有効になっていると、パケット転送エラーによって一部のシステム設定がクラッシュしました。SEG-136843 / DSSEG-7524

Deep Security Agent - 12.0 update 25

リリース日：2022年3月8日

ビルド番号：12.0.0-2265

解決済みの問題

- セキュリティログ監視は、1桁の日付形式を含むシステムログを解析できませんでした。SF04562942 / SEG-115435 / DSSEG-7476

新機能

- Deep Security Agentがアップデートされ、「メンテナンスモード」での実行時のアプリケーションコントロールのパフォーマンスが向上しました。DSSEG-7354

Deep Security Agent - 12.0 update 24

リリース日：2022年1月24日

ビルド番号：12.0.0-2201

このリリースには、一般的な改善が含まれます。

Deep Security Agent - 12.0 update 23

リリース日：2021年11月29日

ビルド番号：12.0.0-2112

解決済みの問題

- Deep Security Managerに接続できない場合、Deep Security Agentがクラッシュすることがありました。DSSEG-7305
- Deep Security Agentによって接続の問題、CPU使用率の増加、またはシステムのクラッシュが発生することがありました。SEG-123885 / SF04973642 / DSSEG-7298

Deep Security Agent - 12.0 update 22

リリース日：2021年11月1日

ビルド番号：12.0.0-2072

解決済みの問題

- 証明書失効リスト（CRL）が一致しないため、アップグレード中にDeep Security Agentでパッケージ署名エラーが表示されることがありました。DSSEG-7214
- 非アクティブなネットワーク接続のリソースをクリーンナップする際に、問題によってDeep Security Agentがクラッシュすることがありました。SEG-113291 / DSSEG-7035
- 不正プログラム対策の検索中にDeep Security Agentサービス（ds_agent）を停止すると、再起動時にAgentがクラッシュすることがありました。DSSEG-7228

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-6489 / DSSEG-7237

最高のCVSS：7.8

最高の重大度：高

Deep Security Agent-12.0 update 21

リリース日：2021年9月15日

ビルド番号：12.0.0-1993

解決済みの問題

- ネットワークインタフェースカード (NIC) の接続の問題により、Deep Security Agentが複数の「セキュリティログ監視 エンジン初期化」または「ポリシー送信」 イベントをトリガすることがありました。 SF03968169 / SEG-95731 / DSSEG-7039
- 変更監視を有効にすると、Deep Security Agentで、実際には作成または削除されていないユーザおよびグループの作成イベントと削除イベントが生成されることがありました。 SEG-100159 / SF04158229 / DSSEG-6806
- 変更監視を有効にすると、一部のシステムでDeep Security Managerの認証サーバのCPU使用率が高くなりました。 SEG-110088 / 04488319 / DSSEG-7072

Deep Security Agent-12.0 update 20

リリース日：2021年8月4日

ビルド番号：12.0.0-1908

解決済みの問題

- 変更監視を有効にすると、Deep Security Agentで、実際には作成または削除されていないユーザおよびグループの作成イベントと削除イベントが生成されることがありました。 SF04158229 / SEG-100159 / DSSEG-7015
- SSL接続の確立中に、Deep Security Agentの接続が切断されることがありました。 SEG-107451 / DSSEG-7016
- 古いバージョンのOSを使用しているシステムでは、Deep Security AgentがWebアプリケーションに接続できないことがありました。 SEG-109652 / DSSEG-6992

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。VRTS-6032 / DSSEG-6967

最も高いCVSSスコア: 9.8

最高の重大度: 高

Deep Security Agent-12.0 update 19

リリース日: 2021年7月6日

ビルド番号: 12.0.0-1845

解決済みの問題

- Webレピュテーションを有効にすると、Deep Security Agentによって一部のサードパーティのソフトウェアで接続の問題が発生しました。SF04072723 / SEG-97952 / DSSEG-6810

Deep Security Agent-12.0 update 18

リリース日: 2021年5月27日

ビルド番号: 12.0.0-1789

拡張機能

- Entrust Root Certificate Authority (G2) 証明書のサポートを追加するために、Deep Security Agent (バージョン12.0.0-1789+) がアップデートされました。G2以外のセキュリティ証明書の有効期限は2022/07/09です。その後は、バージョン12.0.0-1789以降にアップグレードされたエージェントのみが最新の不正プログラム対策スマートスキャン保護を使用します。DSSEG-6904
- Deep Security Agentがアップデートされ、AIX用のネットワークドライバのデバッグログが出力されるようになりました。DSSEG-6896

解決済みの問題

- Deep Security Agent for AIX 6.1でソフトウェアのアップデートが12.0から20.0に失敗することがありました。 DSSEG-6805
- 侵入防御 がSSL検査用に設定されていると、 Deep Security Agentがクラッシュすることがありました。 DSSEG-6909

Deep Security Agent - 12.0 update 17

リリース日：2021年4月26日

ビルド番号：12.0.0-1735

解決済みの問題

- アップグレード失効リスト（CRL）が一致していないため、 Deep Security Agentでパッケージシグネチャエラーが発生することがありました。 DSSEG-6826
- アプリケーションコントロールは、特定の種類のドライブ上のファイルに対して適切なソフトウェアインベントリを追加しないことがあります。 SEG-103667 / SF04227412 / DSSEG-6756
- Deep Security Agentでは、通常、これらのイベントを発生させる条件は存在しませんが、複数の「レコード層メッセージ（未処理）」侵入防御イベントが発生することがありました。「Record Layer Message (not ready)」イベントは通常、セッションの初期化前にSSLステートエンジンでSSLレコードが検出されたことを示します。 SEG-101697 / SF04203096 / DSSEG-6739

Deep Security Agent - 12.0 update 16

リリース日: 2021年3月22日

ビルド番号: 12.0.0-1655

新機能

- Deep Security Agentがアップデートされ、アプリケーションコントロールのインベントリ検索のパフォーマンスが向上しました。 SEG-78295/03234667 / DSSEG-6303

解決済みの問題

- リアルタイムの変更監視は、ユーザによって指定された正確なディレクトリに一致しない場合がありますが、ベースディレクトリで開始されたすべてのパスに一致することがあります。 SEG-97758 / SF04046718 / DSSEG-6636
- アプリケーションコントロールがロックダウンモードの場合、場合によっては適切なソフトウェアインベントリを構築できませんでした。 SEG-94173 / SF03946250 / DSSEG-6503
- アプリケーションコントロールは、認識されたソフトウェアインベントリにファイル拡張子「.ksh」を持つスクリプトを含めていないため、許可されたときにそれらのスクリプトがブロックされていました。 SEG-100706 / SF04166919 / DSSEG-6658

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。 DSSEG-6440

最も高いCVSSスコア: 5.3

最高の重大度：中

Deep Security Agent - 12.0アップデート15

リリース日：2021年1月28日

ビルド番号：12.0.0-1546

解決済みの問題

- 場合によっては、AWSインスタンスで大量のメモリが消費されていました。 SEG-86654 / SF03616828 / DSSEG-6405

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。

Deep Security エージェント-12.0 update 14

リリース日：2020年11月12日

ビルド番号：12.0.0-1436

解決済みの問題

- Solarisサーバでカーネルパニックが発生することがありました。DSSEG-4698

Deep Security Agent-12.0 update 13

リリース日：2020年10月1日

ビルド番号：12.0.0-1373

新機能

- Deep Securityは、ソフトウェア・ファイルが署名時以降に変更されていないことを確実にするためのDeep Securityエージェントの署名を検証します。DSSEG-5935
- 変更監視Deep Security Managerの 検索完了時刻が秒単位で1000単位の区切り文字で表示されるようにアップデートしました。SEG-83194 / SF03429936 / DSSEG-6029
- HTTPヘッダの「X-Forwarded-For」タグに複数のIPアドレスがある場合、そのうちの最初のIPアドレスが取得されます。DSSEG-6183

解決済みの問題

- Deep Security Agentが、[Scan for Integrity]検索の実行中にクラッシュすることがありました。SEG-82795/03462751 / DSSEG-6008
- 作成および実行された実行可能ファイルは、アプリケーションコントロールによってブロックされていました。DSSEG-6173
- Deep Security AgentをSolarisで使用する場合に、変更監視モジュールのポート検索機能が動作しない問題がありました。この問題は、指定されたポートを開くためのユーザID情報へのアクセス権限がAgentになく、リスニングポートの情報を保存できないことに起因して発生していました。本Updateの適用後は、Solaris Agentのポート検索機能が変更され、useridの「n/a」文字列が保存されるようになり、この問題が修正されます。これにより残りのポート情報を保存して、ポート検索機能で使えるようになります。ただし、ユーザIDに基づく検索除外/対象については、この情報を使用できないため正常に機能しません。DSSEG-6151
- 「Out of Connection」ファイアウォール イベントは、ネットワークエンジンが「タップモード」に設定されたときに発生しました。SEG-87155 / SF03644367 / DSSEG-6270
- 一部の 侵入防御 イベントにXFFヘッダが含まれていませんでした。SEG-81986/03419140 / DSSEG-5936

Deep Security Agent-12.0 update 12

リリース日：2020年8月19日

ビルド番号：12.0.1278

拡張機能

- パケットデータをDeep Security Managerに送信しないように選択するには、管理>エージェント>データプライバシーに進み、いいえを選択します。。SF03237033 / DSSEG-6017

注意: この機能強化には、Deep Security Manager FR 2019-10-23以降が必要です。

解決された問題

- アプリケーションコントロールによって、許可されているはずのアプリケーションが、信頼済みアップデートによって作成されたときにブロックされることがありました。SEG-77446/03206632 / DSSEG-5840
- エージェントの自己保護でDeep Security Notifierを保護できませんでした。SEG-76015 / SF03168155 / DSSEG-5920
- Deep Security Agentが無効化されると、不正プログラム対策モジュールの言語が英語に切り替わりました。Deep Security Agentが日本語で再アクティベートされると、不正プログラム対策コンポーネントのアップデートが失敗することがありました。SEG-79963/03184072 / DSSEG-5811
- Deep Security Agentがセキュリティアップデートで例外を受信したため、Deep Security Managerによってセキュリティアップデートのタイムアウトが報告されました。SEG-82072/03273761 / DSSEG-5953
- setuid/setgid 形式のため、Deep Security Agentで偽のファイル変更イベントが検出されました。また、 /usr/bin では、ファイルの作成日時の変更によってアップグレード時にファイル属性の変更が不正に発生しています。 / DSSEG-5928
- 「Served アプリケーションコントロールルールセットをリレーから」が有効になっている場合、不要なリレーエラーイベントが発生しました。 / DSSEG-5988
- Deep Security Agentがインストールされ、不正プログラム対策に対してデバッグログが有効になっているSolaris 10サーバでは、Deep Security Agentのプロセスで異常な再起動が発生することがありました。SEG-80989 / SF03420394 / DSSEG-5880
- Kerberosキャッシュファイルが削除されて再追加されたときに、「ユーザが追加しました」および「ユーザが削除しました」変更監視イベントが多数発生しました。SEG-80629/03402557 / DSSEG-5981

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。CVEの詳細は、「責任ある開示」の慣行に沿って、影響を受ける全てのリリースに対するパッチが公開された後に開示され、脆弱性対策は特定のセキュリティアップデートでのみ利用可能となる点にご注意ください。

CVSSスコア：7.8

重大度：高

- curl 7.67.0にアップデートされました。
- openssl-1.0.2tにアップデートされました。

Deep Security Agent-12.0 update 11

リリース日：2020年7月9日

ビルド番号：12.0.1186

拡張機能

- アプリケーションコントロールには、拡張子「.cron」を持つスクリプトファイルが含まれています。SEG-76680 / SF03240341 / DSSEG-5685
- 変更監視では、LinuxおよびUnixプラットフォームの「setuid」属性と「setgid」属性に対する変更が検出されます。SEG-78797 / DSSEG-5732

Deep Security Agent-12.0 update 10

リリース日：2020年5月28日

ビルド番号：12.0.1090

新機能

管理と品質の向上

インスタンスメタデータサービスバージョン2 (IMDSv2) のサポート：IMDSv2は、Deep Security Manager 12.0アップデート10でサポートされます。詳細については、「["Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使いますか" on page 1534](#)」を参照してください。DSSEG-5422

拡張機能

- Account Domain Authenticationの環境を改善し続けました。SEG-73480 / SF02989282 / DSSEG-5661

解決された問題

- リアルタイムの不正プログラム対策検索で検出の問題が発生しました。SEG-72928 / SF03050515 / DSSEG-5362
- 状況によっては、アプリケーションコントロールによってエージェントがオフラインになって再起動してしまいました。SEG-74143 / SF03119820 / DSSEG-5524
- リアルタイムの不正プログラム対策の検索後、システムが応答しなくなることがありました。SEG-76430 / SF02537903 / DSSEG-5629

Deep Security Agent-12.0 update 9

リリース日：2020年5月4日

ビルド番号：12.0.1026

解決済みの問題

- ワイルドカードを使用した不正プログラム対策ディレクトリの除外が、サブディレクトリと正しく一致していませんでした。SF03131855 / SEG-74892 / DSSEG-5543
- 特定のライブラリのリンクが正しくないと、Deep Security Agentが不安定になる可能性があります。SEG-72958/03071960 / DSSEG-5382
- [Actions]タブのアプリケーションコントロールに、承認または拒否のために保留中のソフトウェア変更があるコンピュータが表示されました。ただし、コンピュータの詳細ウィンドウが開いたときにイベントが報告されませんでした。SEG-74084 / SF03106203 / DSSEG-5449
- Deep Security Virtual Applianceの不正プログラム対策エンジンは、Censusサーバの応答の署名者フィールドが空の場合にオフラインになりました。SEG-73047 / SF03065452 / DSSEG-5447

Deep Security Agent-12.0 update 8

リリース日：2020年4月1日

ビルド番号：12.0.0-967

新機能

- Deep Security Agent 不正プログラム対策が、IntelliScanが無効になっているときにデータタイプに関係なく圧縮ファイルを検索できるようになりました。(SEG-71425/02971395/DSSEG-5306)
- 強化された不正プログラム対策 file/folder 除外設定には、「(」または「)」などの角カッコが含まれる環境変数のサポートが追加されています。(DSSEG-5260)

解決された問題

- Webレピュテーション、ファイアウォール、侵入防御、およびセキュリティログ監視を有効にできませんでした。(SEG-71825/SF03021819/DSSEG-5351)
- ルール「1002875：Unix Add/Remove Software」が適用されたリアルタイム変更監視が有効になっている場合、RPMデータベースはロックされている可能性があります。(SEG-67275/SF02663756/DSSEG-5308)
- 不正プログラム対策の準備が完了する前にセキュリティ更新プログラムが実行された場合、セキュリティ更新プログラムは失敗しました。(DSSEG-5361)
- セキュリティログ監視を有効にすると、Deep Security Agentがクラッシュしました。(SEG-61106/SEG-42752/DSSEG-5225)
- 一部のリアルタイム変更監視の変更が/varディレクトリで検出されませんでした。(SEG-72584/02982752/DSSEG-5346)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。(DSSEG-3771)

Deep Security Agent-12.0 update 7

リリース日：2020年2月28日

ビルド番号：12.0.0-911

新機能

- 検索エンジンのURIパスの長さの制限が増加しました。(SEG-61309/DSSEG-5245)

解決済みの問題

- 表示されたパケットヘッダデータには、冗長ペイロードデータが含まれていません。(DSSEG-4762)
- ルール1006540「X-Forwarded-For HTTPヘッダロギングを有効にする」を適用すると、Deep Securityは侵入防御イベントのX-Forwarded-Forヘッダを正しく抽出します。ただし、「無効なトラバーサル」などのURL侵入は、ヘッダが解析される前にHTTP要求文字列で検出されます。侵入防御エンジンが強化され、ヘッダが解析された後にX-Forwarded-Forヘッダが検索されます。(DSSEG-5156)
- SSL処理の欠陥のため、SSL復号化中にメモリがリークしました。(DSSEG-5142)
- セキュリティログ監視イベント処理により、Deep Security Agentが異常再起動しました。(DSSEG-5228)
- 特定のDeep Security Agent Serverで、CPU使用率が100%に達し、アクティブなアップデートプロセスでパターンマージに失敗しました。(SEG-66210/02711299/DSSEG-5152)
- Deep Security Agent 12.0.0.817にアップグレードした後、Solarisシステムがクラッシュしました。(SF02871943/SEG-68654/DSSEG-5139)

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細については、[脆弱性対策](#)を参照してください。

- SQLiteが3.30.1にアップデートされました。(DSSEG-5103)

Deep Security Agent-12.0 update 6

リリース日：2020年1月17日

ビルド番号：12.0.0-817

解決済みの問題

- ファイル属性を取得できなかった場合、不正プログラム対策でメモリリークが発生しました。(SEG-67374/DSSEG-5063)
- ルール1006540「X-Forwarded-For HTTPヘッダロギングを有効にする」を適用すると、Deep Securityは侵入防御イベントのX-Forwarded-Forヘッダを正しく抽出します。ただし、「無効なトラバーサル」などのURL侵入は、ヘッダが解析される前にHTTP要求文字列で検出されます。侵入防御エンジンが強化され、ヘッダが解析された後にX-Forwarded-Forヘッダが検索されます。(SEG-60728/DSSEG-5094)
- Deep Security AgentがDeep Security Managerへの応答として無効なJSONオブジェクトを送信したことが原因で、Deep Security Managerのログファイルでエラーが発生する問題がありました。(SEG-48728/SF01919585/DSSEG-4995)
- クラスタを持つSolarisサーバでは、Deep Security 侵入防御モジュールの負荷が高くなり、クラスタのプライベートトラフィックが検査されます。余分な負荷が原因で、レイテンシの問題、ノードの追いつき、および同期イベントの損失が発生しました。

これで、エージェント上のPacket Processing Engineを設定して、指定されたインターフェイスでトラフィック検査をバイパスできるようになりました。コンピュータの特定のインタフェースがクラスタのプライベートトラフィック専用の場合、この設定を使用して、このインタフェースとの間で送受信されるパケットの検査をバイパスできます。これにより、バイパスされたインタフェースやその他のインタフェースでパケット処理が高速化されます。

この設定を使用してトラフィック検査をバイパスすることはセキュリティ上の危険です。潜在的な遅延のメリットが関連するリスクを上回るかどうかは、エンドユーザが決定します。また、クラスタ内のノードだけが、そのインタフェースがバイパスされているサブネットにアクセスできるかどうかを判断する必要があります。

バイパスを実装するには、次の手順を実行します。

1. Deep Security Agentを、この修正が含まれている最新のビルドにアップグレードします。
2. /etcディレクトリに「ds_filter.conf」という名前のファイルを作成します。
3. /etc/ds_filter.conf ファイルを開きます。

4. クラスタ通信に使用されるすべてのNICカードのMACアドレスを次のように追加します。

```
MAC_EXCLUSIVE_LIST=XX:XX:XX:XX:XX,XX:XX:XX:XX:XX
```

5. 保存します。
6. 変更が有効になるまで60秒間待ちます。

/etc/ds_filter.conf ファイル内：

- MAC_EXCLUSIVE_LIST行は、ファイル内の最初の行である必要があります。
- MACアドレスのすべての文字は大文字である必要があります。
- 各バイトの先行ゼロを含める必要があります。

有効なMAC_EXCLUSIVE_リスト：

```
MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E
```

```
MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E,6A:23:F0:0F:AB:34
```

無効なMAC_EXCLUSIVE_リスト：

```
MAC_EXCLUSIVE_LIST=B:3A;12:F8:32:5E
```

```
MAC_EXCLUSIVE_LIST=0b:3a;12:F8:32:5e,6a:23:F0:0F:ab:34
```

```
MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E
```

- MACアドレスが有効でない場合、インタフェースはバイパスされません。正確な文字列「MAC_EXCLUSIVE_LIST =」が行の先頭でない場合、インタフェースはバイパスされません。(DSSEG-4055)

Deep Security Virtual Applianceの新機能

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Virtual Appliance 12.0 Readme](#)を参照してください。

Deep Security Virtual Appliance - 12.0 update 3

リリース日：2019年12月5日

ビルド番号：12.0.0-682

新機能

- VMwareによるvmdkおよびOVFファイルの認証により、ファイルの整合性が確保されま
す。(DS-44354)
- 環境要件に応じて、小、中、大規模のOVF設定を複数追加 (DS-40008)
- 新しいNSX-Tのエージェントレス機能のための新しいネットワークインタフェースが追加
されました。このアプライアンスは、現在のエージェントレス機能 (DSSEG-4763) と互
換性があります。

セキュリティアップデート

本Updateには、セキュリティアップデートが含まれています。脆弱性への対策の詳細について
は、[脆弱性対策](#)を参照してください。(DS-37505)

- Deep Security Virtual Applianceでカーネルをアップデートして、脆弱性に対する対策を
実施しました。

既知の問題

- インポートされたOVFを使用してDeep Security Virtual Applianceを配信すると失敗する
ことがあります。
- OVF設定のリードを変更すると、Deep Security Virtual Applianceの配信が失敗します。

アーカイブ

Deep Security Managerのリリースノートのアーカイブ

注意: 今年のリリースノートについては、"[Deep Security Managerの新機能](#)" on page 91を
参照してください。

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Manager 12.0
Readme](#)を参照してください。

Deep Security Manager-12.0 update 5

リリース日：2019年12月16日

ビルド番号：12.0.383

Trend Micro Deep Security(オンプレミス) 12.0

拡張機能

- サポート>配信スクリプトのエージェントインストーラへの署名の検証チェックボックスが追加されました。詳細については、"[ソフトウェアパッケージのデジタル署名の確認](#)" on page 216を参照してください。(DSSEG-4934)

解決済みの問題

- 「Deep Security Managerの新しいバージョンが使用可能です」というアラートが表示されましたが、使用可能なアラートはありません。(DSSEG-4724)
- [アクティビティ概要] ウィジェットでデータベースのサイズが正しく表示されないことがある問題がありました。(DSSEG-4908)

セキュリティアップデート

本Updateには、次のセキュリティに関するアップデートが含まれています。脆弱性に対する対策の詳細については、[脆弱性対策](#)にアクセスしてください。

- JREが最新のCritical Patch Update (8.0.232) にアップデートされます。(DSSEG-4881)

Deep Security Manager-12.0 update 4

リリース日：2019年11月28日

ビルド番号：12.0.372

解決済みの問題

- システムに使用可能なメモリがあるにもかかわらず、メモリしきい値アラートが発令される問題がありました。(DSSEG-4882)

セキュリティアップデート

本Updateには、次のセキュリティに関するアップデートが含まれています。脆弱性に対する保護の詳細については、次のWebサイトを参照してください。

<https://success.trendmicro.com/vulnerability-response>(DSSEG-4822)

Deep Security Manager-12.0 update 3

リリース日：2019年11月5日

ビルド番号：12.0.366

新機能

- Oracle19cがサポート対象のデータベースとして追加されました。(DSSEG-4723)
- AWSコネクタに関連する機能の診断ログオプションが改善されました。(DSSEG-4615)
- Deep Security Managerがアップデートされて、署名済みのAgentインストーラをDeep Security Managerからエクスポートしたり、インストールスクリプトを使用してインストールしたりできるようになりました。署名済みのAgentインストーラのファイル名(拡張子は「.rpm」)の先頭部分は、「Agent-Core」から「Agent-PGPCore」に変更されました。(DSSEG-4570)

解決済みの問題

- Linuxシステムでは、同時にオープンされたファイルの初期設定の最大数がDeep Security Managerのニーズを満たしていなかったため、マネージャはファイルハンドルの取得に失敗しました。その結果、Deep Security Managerの機能がランダムに失敗し、ログに「ファイルが多すぎます」というメッセージが表示されていました。(DSSEG-4748/SEG-59895)
- ポリシーエディタ>の親ポリシーでカスタム回避技術対策の状態が選択されている場合設定>詳細>ネットワークエンジンの設定>Anti-Evasionポスチャ>でカスタム), を選択した場合、子ポリシーに設定が表示されませんでした。(DSSEG-4676/02434648 / SEG-60410)
- Syslogイベントに対して正しくないログ送信元識別子が送信されることがありました。(SF02422793 / DSSEG-4665 / SEG-59969およびSEG-60314)
- コンピュータまたはポリシーエディタで、不正プログラム>General>リアルタイム検索>Schedule>Editの下にある割り当て対象スケジュールがコンピュータとポリシーに正しく割り当てられていても、このタブが空でないことがありました。(SF02374723/DSSEG-4613/SEG-58761)
- [管理]→[システム設定]→[イベントの転送]→[SNMP] で無効または解決不能なSNMPサーバ名が設定されていた場合に、SIEMおよびSNSでも失敗する問題がありました。(SF02339427/DSSEG-4554/SEG-57996)
- Deep Security Managerは、 イベントの取得 および Agent/Applianceエラー が System Settings> System Eventsに記録されていない場合に、内部ソフトウェアエラーシステムイベントを多数示しました。(DSSEG-4433/SEG-39714)
- 多数のホストおよび保護ルールが設定された環境にDeep Security Managerを配置した場合、ユーザが一部のホストからのみデータを要求した場合でも、マネージャはすべてのホストのデータをロードすることがあります。(SF02552257/SEG-62563/DSSEG-4812)

Trend Micro Deep Security(オンプレミス) 12.0

- Deep Securityの管理者は、未解決の推奨設定の検索結果を、ポリシー画面の [侵入防御]、[変更監視]、および [セキュリティログ監視] タブで非表示にできるようになります。未解決の推奨検索結果を非表示にするには、次のコマンドを使用します。

侵入防御:

```
dsm_c -action changesetting -name  
com.trendmicro.ds.network:settings.configuration.showUnresolvedRecomm  
endationsInfoInPolicyPage -value false
```

変更監視:

```
dsm_c -action changesetting -name  
com.trendmicro.ds.integrity:settings.configuration.showUnresolvedRecom  
mendationsInfoInPolicyPage -value false
```

セキュリティログ監視:

```
dsm_c -action changesetting -name  
com.trendmicro.ds.loginspection:settings.configuration.showUnresolvedR  
ecommentationsInfoInPolicyPage -value false
```

(DSSEG-4391)

Deep Security Manager-12.0 update 2

リリース日：2019年9月13日

ビルド番号：12.0.347

新機能

- Oracle 18がサポート対象データベースに追加されました。(DSSEG-4494)
- 以前のバージョンのDeep Security Managerは、VMware vCloud Director 9.0以前をサポートするvCloud SDK 1.5を使用していました。今回のリリースでは、VMware vCloud Director 9.5以降をサポートするvCloud SDK 5.5がマネージャで使用されるようになりました。(DSSEG-4430)

解決済みの問題

- バージョンが12.0以上のすべてのDeep Security エージェントで、すべてのDeep security Manager バージョンが必要です。必要なバージョンよりも前のバージョンの非

互換エージェントをインポートすると、現在のマネージャバージョンよりも小さいものがブロックされます。(DSSEG-4560)

- Deep Security では、現在は維持またはサポートされていない SIGAR というオープンソースライブラリが使用されています。これにより、今後アプリケーションがクラッシュしたり、その他の予期しない問題が発生する可能性があります。同等の置換は JRE に同梱されているライブラリに含まれている必要があり、識別された同等の機能を使用するために SIGAR のすべての用法をリファクタリングする必要があります。(SF02184158/DSSEG-4544/SEG-54629)
- Deep Security Managerで互換性のない侵入防御の設定の作成が許可されてしまう問題がありました(DSSEG-4533)
- Deep Security Manager をアップグレードできませんでした。お客さまが Microsoft Azure SQL データベースを初期設定の照合順序では使用していません。(SF02345050/DSSEG-4531/SEG-58319)
- Deep Security Manager ではリージョン名として使用されているため、Amazon WorkSpaces のインライン同期が機能しない場合があります。(DSSEG-4514)
- \$ 記号が含まれるローカルキーシークレットを使用すると、Deep Security Manager のアップグレードまたは新規インストールが停止します。(SF02013831/DSSEG-4462/SEG-57243)
- Security module usage レポートを生成すると、レポート内のホストの多くに、そのホストに関連付けられている正しいクラウドアカウントが表示されません。(SF01802147/DSSEG-4442/SEG-46978)
- 仮想 Uuid がデータベースに保存されていると、Deep Security エージェントがオフラインになることがあります。(SF01722554/DSSEG-4415/SEG-41425)
- このオプションが利用できなかったため、攻撃の予兆アラートを無効にできませんでした。(DSSEG-4388)
- 管理>Updates>Relay Management>Relay Groupのプロパティのリレーグループのアップデートコンテンツとして[セキュリティアップデートのみ]を選択した場合、期待どおりに機能しませんでした。(DSSEG-4343)
- 有効期限を延長したアクティベーションコード ;マルチテナントアカウントのライセンスは できませんでした。マルチテナント機能を有効にするために、Deep Security Managerはライセンスステータス ;onlineを確認していないため、入力することはできません。(DSSEG-4332/02223786/SEG-55842)
- DNS 解決で Deep Security Manager のホスト名を取得できなかった場合、SIEM イベント転送による [Deep Security Manager を使用したイベントの転送] は機能しません。(SF01992435/DSSEG-4099/SEG-50655)

Deep Security Manager-12.0 update 1

リリース日：2019年8月9日

ビルド番号：12.0.327

解決済みの問題

- AWSコネクタに追加された新しいグループが、そのコネクタに割り当てられている既存の権限を継承していませんでした。(SF01112604/SEG-35024/DSSEG-4205)
- Relay機能が有効なDeep Security Agentに基づいてポリシーを作成すると、ポリシーにRelayの状態が含まれ、そのポリシーを割り当てたすべてのDeep Security Agentで自動的にRelay機能が有効になる問題がありました。(DSSEG-3550)
- アプリケーションコントロールイベントについて「サイズ」列が表示されない問題がありました。(DSSEG-4256)
- Deep Security Managerでは、リリースノート列のエンタリは#160ですが、readme.txtからリリースノートに置き換えられています。(DSSEG-4331)
- Deep Security Managerでは、AWSクラウドコネクタの同期時に多くのホストを削除する必要がある場合に、一部のAWS EC2ホストがクラウドインスタンスのレコードに一致しないまま残りました。(DSSEG-4317)
- Deep Security Managerが大文字と小文字が区別されるMicrosoft SQLデータベースとVMware NSXの両方に接続されている場合に、アップグレード時のシステムチェックに失敗してアップグレードがブロックされることがある問題がありました。(SF02060051/DSSEG-4268/SEG-52044)
- 一部のLinux OS (RHEL7やAmazon Linuxなど) の最新カーネルアップデートにより、エージェントが開始した通信ハートビートの間に障害が発生します。(DSSEG-4315)
- Deep Security Managerのポリシー>侵入防御ルール>アプリケーションの種類> (DNSクライアントの選択) >のプロパティ>の一般設定で、ポート設定が「すべて」に変更されます。ポートリスト。(DSSEG-4370/SEG-55634)
- Deep Security Managerは、[すべての機能を無効にする]ログをINFOレベルでログに記録し、無効になった機能が何も示されませんでした。(DS-33927)
- VMware仮想マシンのBIOS UUIDが変更されたときに、不正プログラム対策エンジンのステータスがオフラインに変わる問題がありました。(DS-36259)
- 多数のvMotionタスクを実行した後に、Deep Security Managerの管理コンソールにvCenterコネクタの仮想マシンが重複して表示される問題がありました。(SEG-47565/DS-36331)

セキュリティアップデート

本Updateには、次のセキュリティに関するアップデートが含まれています。脆弱性に対する保護の詳細については、次のWebサイトを参照してください。

[https://success.trendmicro.com/vulnerability-response\(SF02112629/SEG-53014/DSSEG-4097\)](https://success.trendmicro.com/vulnerability-response(SF02112629/SEG-53014/DSSEG-4097))

- Tomcatを8.5.43にアップグレードしました。(DSSEG-4335)

Deep Security Agentのリリースノートのアーカイブ

注意: 今年のリリースノートについては、"[Deep Security Agentの新機能](#)" on page 108を参照してください。

Linux

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Agent - Linux 12.0 Readme](#)を参照してください。

Deep Security エージェント-12.0 update 5

リリース日：2019年12月16日

ビルド番号：12.0.0-767

新機能

- カーネルパニック防止のためにファイルシステムのカーネルフックからAWS Lustreが除外されます。(SEG-65127/SF02650803/DSSEG-4955)

解決済みの問題

- Zenossを使用してアプリケーションコントロールを有効にすると、大量のファイルイベントが作成され、CPU使用率が高くなりました。(SEG-56946 / SEG-62440 / SEG-64764 / DSSEG-4792)
- vMotionによる仮想マシンの移行後、Deep Security Virtual Applianceにおけるファイル記述子のリリースに時間がかかる問題がありました。(DSSEG-4817)
- リアルタイムの変更監視では、変更監視ルールに環境変数を使用できませんでした。(SF02611220 / SEG-64777 / SEG-65541 / DSSEG-4953)

セキュリティアップデート

本Updateには、次のセキュリティに関するアップデートが含まれています。脆弱性に対する対策の詳細については、[脆弱性対策](#)にアクセスしてください。

- curl 7.67.0にアップデートされました。(DSSEG-4906)
- openssl-1.0.2tにアップデートされました。(DSSEG-4906)

Deep Security エージェント-12.0 update 4

リリース日：2019年11月28日

ビルド番号：12.0.0-725

新機能

- Linuxでの不正プログラム対策カーネルレベルの除外が強化されました。ネットワークディレクトリ検索が無効になっていると、リモートファイルシステムからのファイルイベントはDeep Security Agentによって処理されなくなります。(SEG-50838/DSSEG-4652)

解決済みの問題

- Deep Security Agentのコアからのみアップグレードした場合、セキュリティアップデートに失敗しました。(DSSEG-4870/SEG-63999)
- Deep Security Agent Red Hat 8 64ビットカーネル4.18.0-147.el8.x86_64では、アプリケーションコントロールが正常に動作しませんでした。(DSSEG-4858)
- リアルタイム変更監視ルールは、ベースディレクトリ内の末尾にあるワイルドカードアスタリスクをサポートしていませんでした。(DSSEG-4842)
- Linux 5.3カーネルでDeep Security Agentのリアルタイム不正プログラム対策の検索が正しく機能しませんでした。(DSSEG-4611)

Deep Security エージェント-12.0 update 3

リリース日：2019年11月5日

ビルド番号：12.0.0-682

新機能

- CentOS 8がサポート対象プラットフォームとして追加されました。(DSSEG-4671)

解決済みの問題

- ApacheのHadoopサーバでアプリケーションコントロールが有効にされ、Yarn ユーザキャッシュに大量の非実行可能ファイルが作成された場合、CPU使用率が高くなりました。(DSSEG-4631)
- トロイの木馬ファイルは隔離されていません。(DSSEG-4644)
- データベースがロックされたため、vMotionの後に仮想マシンがオフラインになりました。(DSSEG-4638)
- RATTツールを使用してドライバログを収集すると、オペレーティングシステムがクラッシュすることがありました。(DSSEG-4435)
- Deep Securityがセキュリティ更新プログラムのダウンロードに失敗しました。(SF02043400/SEG-52069DSSEG-4431)

Deep Security エージェント-12.0 update 2

リリース日：2019年9月13日

ビルド番号：12.0.0-563

新機能

- Oracle Linux 8がサポートされるプラットフォームとして追加されました。(DS-37687)
- PGP 署名されたパッケージ用の新しい rpm ファイルがインストーラパッケージに追加されました。詳細については、"[ソフトウェアパッケージのデジタル署名の確認](#)" on page 216を参照してください。(SF02287602/SEG-57033/DSSEG-4607)

解決済みの問題

- Red Hat Enterprise Linux 5または6、CentOS 5または6の環境で、ユーザまたはグループが作成/削除されていない場合でも、次のルールに関連する変更監視イベントが表示される問題がありました: 1008720-ユーザとグループ-アクティビ

ティを作成および削除します。(DSSEG-4548)

- 複数のSmart Protection Serverが設定されている場合、無効なsps_indexが原因で、Deep Security Agentのプロセスがクラッシュすることがある問題がありました。(DSSEG-4386)
- Deep Security AgentでGetDockerVersionコマンドエラーが発生したため、[ポリシーの送信]処理に失敗しました。(DSSEG-4082)
- Deep Security AgentがアプリケーションコントロールのインベントリにPython拡張モジュール (PYD) ファイルを追加しない問題がありました。(DSSEG-3588)
- 明示モードでのTLS/SSL接続で、Deep Security AgentのSSLインスペクションが機能しない問題がありました。(DSSEG-4464)
- Deep Security 不正プログラム対策 サンプル不正プログラムファイルが自動的に削除されませんでした。(SF02230778/SEG-55891/DSSEG-4569)
- 特定の設定の場合、エージェントがAzureファブリックサーバの位置を特定できないため、Azureコネクタに適切に移動できません。(DSSEG-4547)

Deep Security エージェント-12.0 update 1

リリース日：2019年8月9日

ビルド番号：12.0.0-481

新機能

- このリリースでは、Debian Linux 10がサポートされています。(DSSEG-4262)

解決済みの問題

- Red Hat Enterprise Linux 8では、DHCPの初期設定の動作が変更されました。Deep Security AgentがAzure VMインスタンス上で動作しているかどうかを検出するために影響します。したがって、エージェントはHostInfoのDeep Security Managerに十分な情報を保持せず、Azureコネクタへのリホームに失敗します。(DSSEG-4085)
- ネットワークエンジンの詳細オプションの [パケットデータがキャプチャされたときに格納する最大データサイズ] が機能しない問題がありました。(DSSEG-4113/SEG-48011)

- Deep Security Agentの不正プログラムのリアルタイム検索とアプリケーションコントロールがカーネルバージョン5.0.0-15-genericで動作しない問題がありました。(DSSEG-4228)
- Deep Security AgentをUbuntu 18.04にインストールできませんでした。(SF01593513/SEG-43300/DSSEG-4119)
- UbuntuでNetplanネットワークインタフェースを使用している場合に、Deep Securityの不正プログラム対策およびネットワークフィルタドライバが正常に起動しない問題がありました。(DSSEG-4306)
- 場合によっては、変更監視イベントにエンティティ名は含まれません。(SF00889757/DSSEG-3761/SEG-31021)
- ds_filterでクラスタ間通信の検査の除外設定を行った際にAgentのOSがクラッシュする問題がありました。(DSSEG-4377)
- ゲストVMが頻繁にESXiホスト間で移行された場合 (vMotion), を使用して、VMが状態ファイルを保存できないことがあります。このため、新しいESXiサーバの下でDeep Security ManagerによってVMが自動的に再アクティベートされるまで、Deep Security Virtual Applianceの保護期間は数分かかります。(DSSEG-4341)

UNIX

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Agent - Unix 12.0 Readme](#)を参照してください。

Deep Security エージェント-12.0 update 5

リリース日：2019年12月16日

ビルド番号：12.0.0-767

新機能

- このリリースには、AIXオペレーティングシステムバージョン6.1,7.1、および7.2用のDeep Security Agentが追加されています。このエージェントでサポートされるセキュリティコントロールは、Deep Security 9.0 Agent for AIXのものと同じです。つまり、ファイアウォール、侵入防御、変更監視、セキュリティログ監視を実行します。詳細なサポート情報については、Deep Securityのヘルプセン

ターを参照してください。Deep Security 12.0 Agent for AIXには、Deep Security 9.0とDeep Security 12.0の間にDeep Security Agentの多くの機能強化が組み込まれています。このエージェントには、Deep Security 12.0 LTSリリースと同じサポートライフサイクルもあります。(DS-17159)

解決済みの問題

- Zenossを使用してアプリケーションコントロールを有効にすると、大量のファイルイベントが作成され、CPU使用率が高くなりました。(SEG-56946 / SEG-62440 / SEG-64764 / DSSEG-4792)
- vMotionによる仮想マシンの移行後、Deep Security Virtual Applianceにおけるファイル記述子のリリースに時間がかかる問題がありました。(DSSEG-4817)
- デバッグログにより、Deep Security Agentが異常再起動しました。(DSSEG-4948)
- リアルタイムの変更監視では、変更監視ルールに環境変数を使用できませんでした。(SF02611220 / SEG-64777 / SEG-65541 / DSSEG-4953)

セキュリティアップデート

本Updateには、次のセキュリティに関するアップデートが含まれています。脆弱性に対する対策の詳細については、[脆弱性対策](#)にアクセスしてください。

- curl 7.67.0にアップデートされました。(DSSEG-4906)
- openssl-1.0.2tにアップデートされました。(DSSEG-4906)

Deep Security エージェント-12.0 update 3

リリース日：2019年11月5日

ビルド番号：12.0.0-682

解決済みの問題

- ApacheのHadoopサーバでアプリケーションコントロールが有効にされ、Yarn ユーザキャッシュに大量の非実行可能ファイルが作成された場合、CPU使用率が高くなりました。(DSSEG-4631)
- Deep Securityがセキュリティ更新プログラムのダウンロードに失敗しました。(SF02043400/SEG-52069DSSEG-4431)

Deep Security エージェント-12.0 update 2

リリース日：2019年9月13日

ビルド番号：12.0.0-563

解決済みの問題

- 複数のSmart Protection Serverが設定されている場合、無効なsps_indexが原因で、Deep Security Agentのプロセスがクラッシュすることがある問題がありました。(DSSEG-4386)
- AIX用のDeep Security Agentの場合、が変更監視ルールに含まれている場合、GroupSetおよびUserSetの「エンティティセット」タイプが正しく機能していませんでした。(DSSEG-4239)
- AIX用 Deep Security エージェントで、多数のルールセットを含むポリシーを受信できませんでした。(DSSEG-4207)
- AIX サーバでは、Deep Security エージェントのインタフェースバイパス機能が、3文字以外の名前のインタフェースのために AIX で提供されているインタフェースの mac アドレスを誤って読み取っています。そのため、これらのインタフェースをバイパスすることはできませんでした。(DSSEG-4118)
- Deep Security AgentがアプリケーションコントロールのインベントリにPython 拡張モジュール (PYD) ファイルを追加しない問題がありました。(DSSEG-3588)
- 明示モードでのTLS/SSL接続で、Deep Security AgentのSSLインスペクションが機能しない問題がありました。(DSSEG-4464)
- 特定の設定の場合、エージェントがAzureファブリックサーバの位置を特定できないため、Azureコネクタに適切に移動できません。(DSSEG-4547)

Deep Security エージェント-12.0 update 1

リリース日：2019年8月9日

ビルド番号：12.0.0-481

解決済みの問題

- 特定の状況でネットワークイベントが失われることがありました。(DSSEG-4159)

- 場合によっては、変更監視イベントにエンティティ名は含まれません。
(SF00889757/DSSEG-3761/SEG-31021)

Windows

注意: 長期サポートLTSリリースのリリースノートについては、[Deep Security Agent - Windows 12.0 Readme](#)を参照してください。

Deep Security エージェント-12.0 update 5

リリース日：2019年12月16日

ビルド番号：12.0.0-767

解決済みの問題

- Zenossを使用してアプリケーションコントロールを有効にすると、大量のファイルイベントが作成され、CPU使用率が高くなりました。(SEG-56946 / SEG-62440 / SEG-64764 / DSSEG-4792)
- vMotionによる仮想マシンの移行後、Deep Security Virtual Applianceにおけるファイル記述子のリリースに時間がかかる問題がありました。(DSSEG-4817)
- リアルタイムの変更監視では、変更監視ルールに環境変数を使用できませんでした。(SF02611220/SEG-64777/DSSEG-4953)
- サーバが断続的にハングアップし、大量のメモリが使用されました。(SF02351375/SEG-59668/DSSEG-4747)

セキュリティアップデート

本Updateには、次のセキュリティに関するアップデートが含まれています。脆弱性に対する対策の詳細については、[脆弱性対策](#)にアクセスしてください。

- curl 7.67.0にアップデートされました。(DSSEG-4906)
- openssl-1.0.2tにアップデートされました。(DSSEG-4906)

Deep Security エージェント-12.0 update 4

リリース日：2019年11月28日

ビルド番号：12.0.0-725

解決済みの問題

- Deep Security 不正プログラム対策 for Windowsが繰り返しクラッシュし、不正プログラム対策のクラッシュダンプを作成しようとしたのですが、これによりCPUが高くなりました。(SF02621665/SEG-63997/DSSEG-4889)
- ApacheのHadoopサーバでアプリケーションコントロールが有効にされ、Yarn ユーザキャッシュに大量の非実行可能ファイルが作成された場合、CPU使用率が高くなりました。(DSSEG-4631)
- コンピュータがドキュメントファイルをファイルサーバに書き込んだ場合、不正プログラム対策が頻繁にファイルを検索する必要があり、ファイルの検索中に別のコンピュータでファイルの書き込みに失敗することがありました。

注意: Windows Server 2016やWindows Server 2012などの最新のOSでは、Deep Security Agentのアップグレード後にマシンを再起動して、この機能を適用してください。

(SF02497125/DSSEG-4746/SEG-61541)

- レジストリ値の変更を監視するために初期設定の「STANDARD」属性が設定されている場合に、変更監視イベントに「種類」属性が表示されない問題がありました。(DSSEG-4625)
- 不正プログラム対策解決策プラットフォーム (AMSP) のログサーバがクラッシュすることがありました。(DSSEG-4620/SEG-51877)
- RATTツールを使用してドライバログを収集すると、オペレーティングシステムがクラッシュすることがありました。(DSSEG-4435)
- Deep Security Agentが「Notifierアプリにデータを送信できません。」とともに異常的に再起動しました。ds_agent.logのエラーメッセージ。(DSSEG-2089)
- Deep Securityの不正プログラム対策ドライバは、多くのページプールメモリを占有していました。(SF02185196/SEG-54652/DSSEG-4224)

注意: 最新のOS (Windows Server 2016またはWindows Server 2012など) を使用している場合は、コンピュータを再起動して、Deep Security Agentのバージョンアップ後にこの修正プログラムを適用してください。

- Deep Securityがセキュリティ更新プログラムのダウンロードに失敗しました。(SF02043400/SEG-52069DSSEG-4431)

Deep Security エージェント-12.0 update 3

リリース日：2019年11月5日

ビルド番号：12.0.0-682

このビルドは高CPUでの問題により廃止予定です。より新しいビルドを使用するか、[サポート担当者にお問い合わせ](#)ください。

詳細については、[Trend Micro Deep Security Agent 12.0 Update 3 for Windowsの削除 \(ビルド：12.0.0-682\)](#) を参照してください。

Deep Security エージェント-12.0 update 2

リリース日：2019年9月13日

ビルド番号：12.0.0-563

新機能

- Windows Server 2019 バージョン1903がサポート対象プラットフォームとして追加されました。

解決済みの問題

- システムの地域設定が「中国語 (繁体字、香港特別行政区)」の場合に、Deep Security Notifierで繁体字中国語でなく簡体字中国語が表示される問題がありました。(DSSEG-4432/SEG-48075)
- 複数のSmart Protection Serverが設定されている場合、無効なsps_indexが原因で、Deep Security Agentのプロセスがクラッシュすることがある問題がありました。(DSSEG-4386)
- Deep Security AgentでGetDockerVersionコマンドエラーが発生したため、[ポリシーの送信]処理に失敗しました。(DSSEG-4082)
- Deep Security AgentがアプリケーションコントロールのインベントリにPython拡張モジュール (PYD) ファイルを追加しない問題がありました。(DSSEG-3588)
- 明示モードでのTLS/SSL接続で、Deep Security AgentのSSLインスペクションが機能しない問題がありました。(DSSEG-4464)
- 特定の設定の場合、エージェントがAzureファブリックサーバの位置を特定できないため、Azureコネクタに適切に移動できません。(DSSEG-4547)

Deep Security エージェント-12.0 update 1

リリース日：2019年8月9日

ビルド番号：12.0.0-481

解決済みの問題

- ネットワークエンジンの詳細オプションの [パケットデータがキャプチャされたときに格納する最大データサイズ] が機能しない問題がありました。(DSSEG-4113/SEG-48011)
- 場合によっては、変更監視イベントにエンティティ名は含まれません。(SF00889757/DSSEG-3761/SEG-31021)
- 誤った再起動要求イベントが発生することがある問題がありました。(DSSEG-3722)

Deep Security Agentのプラットフォーム

本バージョンのDeep Security Managerで管理対象となるエージェントおよびプラットフォームの一覧は下記のページでご確認ください。

https://help.deepsecurity.trendmicro.com/12_0/on-premise/Manage-Components/Software-Updates/compatibility.html

以下のプラットフォームについては日本語版ではサポート対象外となります。

- Windows 2000
- Windows XP
- Windows 2003

各プラットフォームでサポートされている機能

Deep Security 12.0でサポートされる機能は、OSとプラットフォーム、仮想環境のOSとプラットフォーム、およびインストールされているDeep Security Agent (ある場合) のバージョンによって異なります。

詳細については以下を参照してください。 https://help.deepsecurity.trendmicro.com/12_0/on-premise/supported-features-by-platform.html

Deep Security AgentのLinuxカーネルサポート

- [Deep Security Agent 12.0のLinuxカーネルサポート](#)
- [Deep Security Agent 11.3のLinuxカーネルサポート](#)
- [Deep Security Agent 11.2のLinuxカーネルサポート](#)
- [Deep Security Agent 11.1のLinuxカーネルサポート](#)
- [Deep Security Agent 11.0のLinuxカーネルサポート](#)
- [Deep Security Agent 10.3のLinuxカーネルサポート](#)
- [Deep Security Agent 10.2のLinuxカーネルサポート](#)
- [Deep Security Agent 10.1のLinuxカーネルサポート](#)
- [Deep Security Agent 10.0のLinuxカーネルサポート](#)
- [Deep Security Agent 9.6 SP1のLinuxカーネルサポート](#)
- [Deep Security Agent 9.5 SP1のLinuxカーネルサポート](#)

スクリプトと自動ワークフローに対応したDeep Security Agent 10.0以降でサポートされているLinuxカーネルの完全なリストの[JSON版](#)も使用できます。

システム要件

システム要件については、次のWebサイトを参照してください。

Deep Security:

<https://www.go-tm.jp/tmds/req>

Cloud One - Workload Security:

<https://www.go-tm.jp/tmdsaas/req>

サイジング

Deep Security環境のサイジングガイドラインは、ネットワーク、ハードウェア、およびソフトウェアの規模によって異なります。

Deep Security Managerのサイジング

Deep Security Managerのサイジングの推奨値は、エージェントの数によって異なります。

ヒント: 希望する場合は、YouTubeで [Deep Security 12 - DSMシステム要件と](#) のサイズを確認できます。

Agentの数	CPUの数	RAM	JVMプロセスメモリ	Managerノードの数	推奨ディスク容量
<500	2	8GB	4GB	2	200GB
500~1000	4	8GB	4GB	2	200GB
1000~5000	4	12GB	8GB	2	200GB

Trend Micro Deep Security On-Premise 12.0

Agentの数	CPUの数	RAM	JVMプロセスメモリ	Managerノードの数	推奨ディスク容量
5000~10000	8	16GB	12GB	2	200GB
10000~20000	8	24GB	16GB	2	200GB

最大限のパフォーマンスを発揮するには、Deep Security Managerプロセスに十分なJava仮想マシン (JVM) メモリを割り当てることです。"[Deep Security Managerのメモリ使用量の設定](#)" on page 275を参照してください。

Deep Security Managerの推奨設定の検索はCPU負荷が高くなります。推奨設定の検索を実行する頻度を決定する際には、パフォーマンスへの影響を考慮してください。"[推奨設定の検索の管理と実行](#)" on page 592を参照してください。

多数の仮想マシンが同時に再起動され、各AgentがDeep Security Managerとの接続を同時に再確立すると、リソースの使用量が急増する場合があります。

複数のサーバノード

可用性とスケーラビリティを向上させるために、ロードバランサを使用して、同じバージョンのDeep Security Managerを2つのサーバ(「ノード」)にインストールします。これらを同じデータベースに接続します。

ヒント: データベースサーバの負荷が高くないように、データベースサーバ1台につき接続するDeep Security Managerノードは2個までにしてください。

各Managerノードがすべてのタスクを実行できます。あるノードが他のノードよりも重要ということはありません。すべてのノードにログインでき、Agent、Appliance、およびRelayはどのノードにも接続できます。1つのノードで障害が発生してもサービスは継続され、データが失われることはありません。

データベースのサイジング

必要となるデータベースのCPU、メモリ、およびディスク容量は、以下の要素によって異なります。

Trend Micro Deep Security On-Premise 12.0

- 保護されているコンピュータの数
- Deep Security Agentをインストールするプラットフォームの数
- 1秒あたりに記録されるイベント (ログ) の数 (有効になっているセキュリティ機能に関連)
- イベントの保持期間
- データベーストランザクションログのサイズ

最小ディスク容量 = (2 x Deep Securityのデータサイズ) + トランザクションログ

たとえば、データベースとトランザクションログのサイズが合計40GBの場合は、データベーススキーマのアップグレード中に80GB (40 x 2) の空きディスク容量が必要です。

ディスクの空き容量を増やすには、使用されていないプラットフォーム用の不要なAgentパッケージ("Deep Securityデータベースからソフトウェアパッケージを削除する" on page 374を参照)、トランザクションログ、不要なイベントレコードを削除します。

イベントの保持期間は設定可能です。セキュリティイベントの場合、保持期間はポリシー、個々のコンピュータ設定、またはその両方で設定されます。"ポリシー、継承、およびオーバーライド" on page 587と"ログとイベントの保存に関するベストプラクティス" on page 1122を参照してください。

イベントによるディスク使用量を最小限に抑えるには、次の操作を行います。

- イベントをローカルではなくリモートに保存します。イベントの保持期間を長くする必要がある場合は (コンプライアンスのためなど)、イベントをSIEMまたはSyslogサーバに転送してから、削除機能を使用してローカルコピーを削除します("Deep SecurityイベントをSyslogまたはSIEMサーバに転送する" on page 1141を参照)。

注意: アプリケーションコントロールと変更監視の一部の操作 (ベースラインの再構築、変更の検索、およびインベントリの変更の検索) では、すべてのレコードがローカルに保持され、削除されることも転送されることもありません。

- 侵入防御を有効にする前に、保護されているコンピュータのソフトウェアにパッチを適用します。推奨設定の検索では、脆弱なOSを保護するために、より多くのIPSルールが割り当てられます。セキュリティイベントが増えると、ローカルまたはリモートのディスク使用量が増加します。
- TCP、UDP、ICMP用のステートフルファイアウォールなど、頻繁にログを記録する不要なセキュリティ機能を無効にします。

Deep Securityファイアウォールまたは侵入防御機能を使用する、トラフィックの多いコンピュータでは、1秒あたりに記録するイベント数が多くなるため、パフォーマンスの高いデータベースが必要になることがあります。また、ローカルのイベント保持期間の調整も必要になる場合があります。

ヒント: 大量のファイアウォールイベントが予想される場合は、「ポリシーで未許可」イベントを無効にすることを検討してください("ファイアウォールの設定" on page 866を参照)。

"Deep Security Managerのパフォーマンス機能" on page 276も参照してください。

データベースのディスク容量の見積もり

次の表には、イベントの保持期間に初期設定を使用した場合のデータベースのディスク容量の見積もりを示します。有効にする保護モジュールの合計ディスク容量が「2つ以上のモジュール」の値を超える場合は、より小さい見積もりを使用してください。たとえば、Deep Securityの不正プログラム対策、侵入防御システム、変更監視を使用して750のAgentを配置するとします。個々の推奨の総数は320 GB (20 + 100 + 200) ですが、「2つ以上のモジュール」の推奨は300 GB未満です。そのため、300GBと見積もります。

Agentの数	不正プログラム対策	Webレピュテーションサービス	セキュリティログ監視	ファイアウォール	侵入防御	アプリケーションコントロール	変更監視	2つ以上のモジュール
1~99	10GB	15GB	20GB	20GB	40GB	50GB	50GB	100GB
100~499	10GB	15GB	20GB	20GB	40GB	100GB	100GB	200GB
500~999	20GB	30GB	50GB	50GB	100GB	200GB	200GB	300GB
1000~9999	50GB	60GB	100GB	100GB	200GB	500GB	400GB	600GB
10,000~20,000	100GB	120GB	200GB	200GB	500GB	750GB	750GB	1 TB

データベースのディスク容量は、個々のDeep Security Agentプラットフォームの数に伴って増加します。たとえば、30のAgent (Agentプラットフォームごとに最大5つのバージョン) がある場合、データベースサイズが約5GB増加します。

Deep Security AgentおよびRelayのサイジング

ヒント: 必要に応じて、YouTubeで [Deep Security 12 - Agentのシステム要件と](#) のサイズを確認できます。

プラットフォーム	有効になっている機能	最小RAM	推奨RAM	最小ディスク容量
Windows	すべての保護	2GB	4GB	1GB
Windows	Relayのみ	2GB	4GB	30GB
Linux	すべての保護	1GB	5GB	1GB
Linux	Relayのみ	2GB	4GB	30GB
Solaris	すべての保護。Relayはサポート対象外	4GB	4GB	2 GB
AIX	すべての保護。Relayはサポート対象外	4GB	4GB	2 GB

OSバージョンによっては、必要なRAMが少なくなります。また、一部のDeep Security機能だけを有効にする場合も同様です。

保護されたコンピュータでVMware vMotionを使用する場合は、エージェントが接続されているDeep Security Relay に10 GBのディスク領域を追加して、合計推奨サイズを40 GBに設定します。

さまざまなプラットフォームにDeep Security Agentをインストールする場合、Relayで必要となるディスク容量が増加します(Relayではプラットフォームごとにアップデートパッケージが保存されます)。詳細については、"[Deep Security Agentソフトウェアの入手](#)" on page 372を参照してください。必要なRelayの数を確認するには、"[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照してください。

Deep Security Virtual Applianceのサイジング

初期設定では、Deep Security Virtual Applianceに割り当てられるメモリは4GBだけです。Applianceは、同じESXiサーバにある仮想マシン (VM) を保護します。Applianceに最小限割り当てる必要があるvCPU数とメモリ容量は、保護されている仮想マシンの数と、割り当てられている侵入防御 (IPS) ルールの数によって異なります。以下の表の要件では、仮想マシンごとに350～400のIPSルールを想定しています。"[Deep Security Virtual Applianceのメモリ割り当て](#)" on page 370も参照してください。

保護されている仮想マシンの数	最小vCPU	最小vRAM	最小ディスク容量
1～25	2	6GB	20GB
26～50	2	8GB	20GB
51～100	2	10GB	20GB
101～150	4	12GB	20GB
151～200	4	16GB	20GB
201～250	6	20GB	20GB
251～300	6	24GB	20GB

注意:

上記の要件は、以下の機能によって変化する場合があります。

- [変更監視](#): 大規模なVDI環境 (ESXiホストあたりの仮想マシンが50以上) では、Deep Security Virtual Applianceではなく、Deep Security Agentを使用してください。

- [不正プログラム対策](#): 要件は、VMware Guest Introspectionのバージョンによって異なる場合があります。[VMware Configuration Maximumsツール](#)を使用してください。
- [ファイアウォール](#)、[Webレピュテーション](#)、または[侵入防御](#): 要件は、VMware Network Introspection (NSX) のバージョンによって異なる場合があります。[「NSX for vSphere Recommended Configuration Maximum」](#)を参照してください。

ヒント:

侵入防御を有効にする前に、保護されているコンピュータのソフトウェアにパッチを適用します。推奨設定の検索では、脆弱なOSを保護するために、より多くのIPSルールが割り当てられます。これによって、Applianceのメモリ使用量が増加します。たとえば、次の表では、300の仮想マシン (仮想デスクトップインフラストラクチャ (VDI) としてのフル、リンク、またはインスタントクローン) でのIPSルールの数によってvRAMの使用量がどのように増加するかを示しています。

侵入防御ルールの数	ApplianceのvRAM使用量
350~400	24GB
500~600	30GB
600~700	40GB
700以上	50GB以上

Applianceが多数の仮想マシンを保護していて、タイムアウトエラーにより推奨設定の検索が失敗する場合は、"[推奨設定の検索の管理と実行](#)" on page 592を参照してタイムアウト値を大きくしてください。

ポート番号、URL、およびIPアドレス

ヒント: YouTubeで [Deep Security 12 - Scoping Environment Pt2 - Network Communication](#) を視聴すると、さまざまなDeep Securityコンポーネントに関連するネットワーク通信を確認できます。

Deep Securityの初期設定のポート番号、URL、IPアドレス、およびプロトコルは、以下のセクションに示されています。ポート、URL、またはIPアドレスが設定可能な場合は、関連する設定ページへのリンクが用意されています。

- ["Deep Securityのポート番号" below](#)
- ["Deep SecurityのURL" on page 196](#)

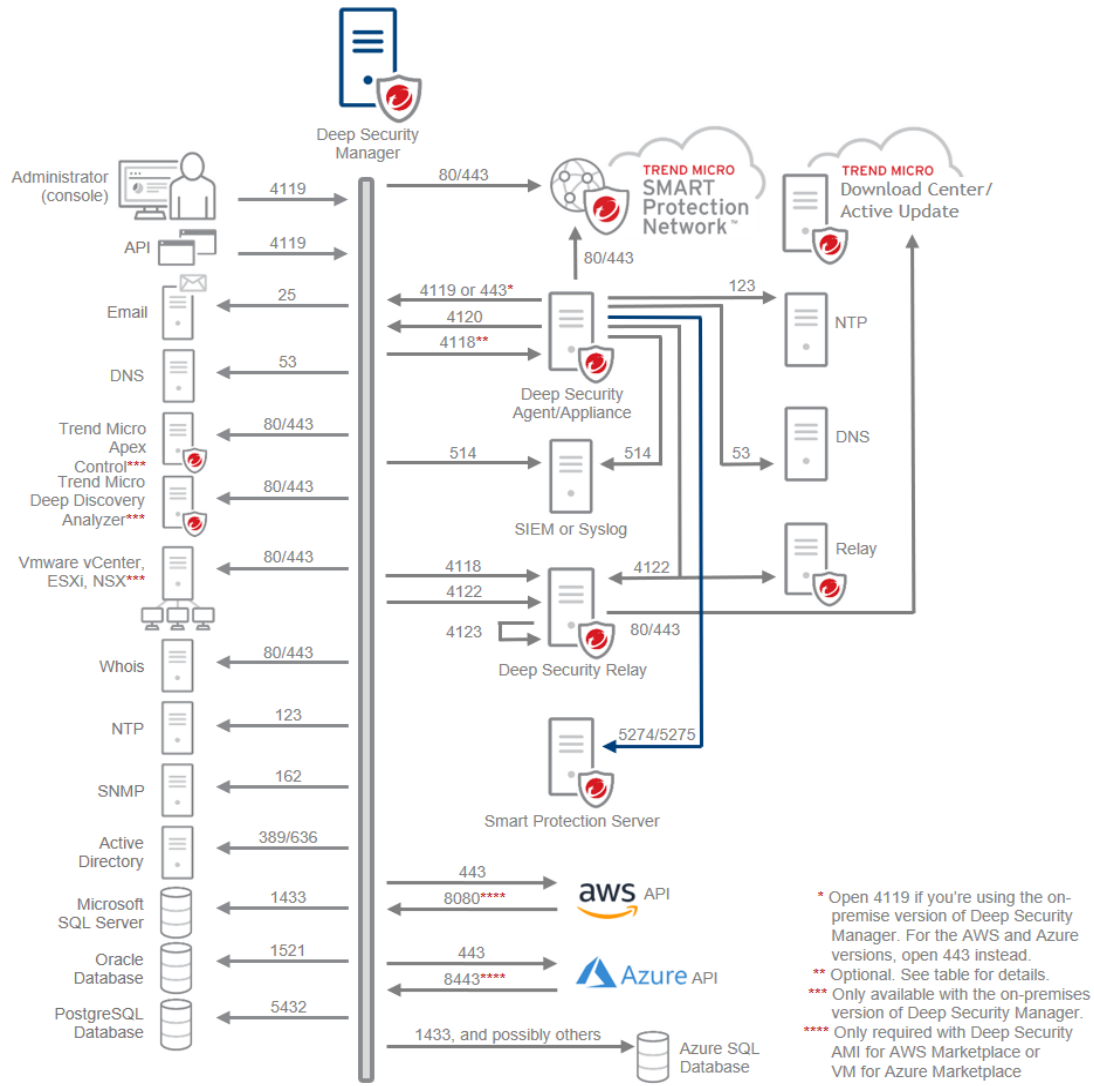
注意: ネットワークでプロキシまたはロードバランサを使用する場合は、このページに記載されている初期設定のポートとURLの代わりにそれを使用するように、Deep Securityを設定できます。詳細については、「["プロキシ設定" on page 422](#)」と「["ロードバランサ" on page 1447](#)」を参照してください。

注意: このページのポートの他に、Deep Securityでは、ソケット (送信元ポート) を開くときにエフェメラルポートが使用されます。まれに、これらがブロックされて接続の問題が生じることがあります。詳細については、「["ポートのブロック" on page 1349](#)」を参照してください。

Deep Securityのポート番号

次の図は、Deep Securityシステムの初期設定のポートを示しています。詳細については、図の下の表を参照してください。

Trend Micro Deep Security On-Premise 12.0



ポートの種類

初期設定のポート番号

Managerリスンポート

- 4119/HTTPS (Deep Security ManagerのGUIおよびAPIのリスニングポート)。また、ルールセットがリレーからダウン

ポートの種類	初期設定のポート番号
	<p>ロードされない限り、共有およびグローバル アプリケーションコントロール ルールセットにも使用されます。)</p> <ul style="list-style-type: none"> 4120/HTTPS (Deep Security Managerのハートビートおよびアクティベーション)
Manager宛先ポート	<ul style="list-style-type: none"> 25/SMTP* (メールサーバポート) 53/DNS (DNSサーバポート) 443 / HTTPS* (これらのポートは、さまざまなDeep Securityクラウドサービス、 Smart Protection Network サービス、Trend Micro Apex Central, Deep Discovery Analyzer、VMwareコンポーネント (vCenter、ESXi、NSX), AWS API) で使用されます。 Azure API) 123/NTP* (NTPサーバポート。NTPサーバは、Trend Micro Apex Centralにすることができます) 162/SNMP* (SNMP Managerポート) 389/LDAP、636/LDAPS* (Active Directory) 514/Syslog* (SIEMまたはSyslogサーバポート) 1433 / SQL (Microsoft SQLデータベース、Azure SQLデータベースポート) 1521 / SQL ("Oracle Database" on page 209 ポート) 5432/SQL (PostgreSQLデータベースポート) 4118/HTTPS* (Deep Security Agentポート) 4119 / HTTPS (ガディープセキュリティ仮想アプライアンスの展開中にOVF を取得するために使用) 4122/HTTPS (Deep Security Relay ポート) 11000-11999/SQL、14000-14999/SQL* (Azure SQLデータベースポート) 80/HTTP、443/HTTPS (Whoisサーバ) <p>* 備考:</p>

ポートの種類	初期設定のポート番号
	<ul style="list-style-type: none"> • メール通知が必要な場合はポート25を許可します。はManagerで設定可能です。 • 80および443は、アクセスされるサービスによっては設定可能です。Trend Micro Apex CentralおよびDeep Discovery Analyzerのポートを設定するには、ここをクリックしてください。NSXおよびvCenterのポートについては、ここをクリックしてください。Whoisポートを設定するには、ここをクリックしてください。 • ManagerとNTPサーバを同期する場合は、ポート123を許可します。 • "リモートコンピュータにSNMP経由でシステムイベントを転送" on page 1248を使用してシステムイベントをリモートコンピュータに転送します。 • ポート389と636を許可する場合Active Directory からマネージャにコンピュータを追加します。389および636は、Active Directoryサーバが別のポートを使用している場合、マネージャで設定可能な です。 • ポート514を許可する場合Deep Securityイベントを外部SIEMまたはSyslogサーバに転送します。514 はマネージャで設定可能な です。 • 双方向またはマネージャが開始した通信を使用している場合は、ポート4118を許可します。（初期設定では、双方向通信がに使用されます。）詳細については、「"AgentとManagerの通信" on page 400」を参照してください。 • Allow port 11000-11999 and 14000-14999-1433に加えて - Azure SQLデータベースを使用していてマネージャが稼働している場合 内でAzure Cloudの境界を指定します（Azure MarketplaceにDeep Security Manager VMを使用している場合も同様です）。管理者が実行されている場合 のAzureクラウド境界外にある場合、ポート1433のみがAzure SQL Databaseに許可する必要があります。Azure SQL Databaseポートの詳細については、Microsoft AzureのこちらのWebサイトを参照してください。
Deep Security Agent/Applianceの待機ポート	<ul style="list-style-type: none"> • 4118 / HTTPS（Agent/ appliance がハートビートおよびアクティベーションを待機するポート） <p>注意: Agentからの通信を使用している場合は、4118を閉じることができます。初期設定では双方向通信が使用されるため、4118を開く必要があります。詳細については、「"AgentとManagerの通信" on page 400」を参照してください。</p>

ポートの種類	初期設定のポート番号
Deep Security Agent/Applianceの送信先ポート	<ul style="list-style-type: none"> • 53/DNS (DNSサーバポート) • 443/HTTPS (Smart Protection Network ポート、 Smart Protection Server (ファイルレピュテーション) 、 Deep Security Managerポート) • 123/NTP* (NTPサーバポート) • 514/Syslog* (SIEMまたはSyslogサーバポート) • 4119/HTTPS (Deep Security ManagerのGUIとAPIのポート) () このポートは、 配信スクリプトを使用する場合にエージェントソフトウェアをダウンロードするためにも使用されます。 • 4120/HTTPS* (Deep Security Managerのハートビートおよびアクティベーションポート) • 4122/HTTPS(Deep Security Relayポート) • 5274/HTTP、 5275/HTTPS* (Webレピュテーション用のSmart Protection Server) <p>注意: AWS AMIおよびAzure VMバージョンのManagerを使用する場合は、ポート4119ではなくポート443を開きます。</p> <p>* 備考:</p> <ul style="list-style-type: none"> • ポート5274および5275は、ファイアウォールではなく、 Webレピュテーションにのみ必要です。 • エージェントをNTPサーバと同期する場合は、ポート123を許可します。 • エージェントがSIEMまたはSyslogサーバにセキュリティイベントを直接送信するようにする場合は、ポート514を許可します。ポート番号 は、マネージャで設定可能な です。 • 双方向またはエージェントが開始した通信を使用している場合は、ポート4120を許可します。(初期設定では、双方向通信が使用されます。) "AgentとManagerの通信" on page 400を参照してください。 • ポート5274および5275を許可する場合は、ポート5274および5275を許可します。 Smart Protection Serverローカルネットワークまたは仮想プライベートネットワーク (VPC,) でビジネスセキュリティクライアントを使用する代わりに/アプラ

ポートの種類	初期設定のポート番号
	<p>イアンスクラウドベースに接続するSmart Protection Network 443 / HTTPSを超えています。詳細については、Smart Protection Serverのドキュメントまたは「AWSでのSmart Protection Serverの配置」を参照してください。</p>
Deep Security Relayの待機ポート	<ul style="list-style-type: none"> • すべてのエージェント待機ポートを許可する（リレーにも適用されるため） • 4122/HTTPS (Relayポート) • 4123 (Agentと独自の内部Relay間の通信用ポート) <p>注意: ポート4123は他のコンピュータからの接続を待機しないでください。また、ネットワークファイアウォールポリシーで設定する必要はありません。ただし、Managerのサーバ自体にファイアウォールソフトウェア (Windowsファイアウォールやiptablesなど) がある場合は、ソフトウェアがそれ自身に対してこの接続をブロックしていないことを確認してください。また、他のアプリケーションが同じポートを使用していない (ポートが競合していない) ことを確認してください。</p>
Deep Security Relayの送信先ポート	<ul style="list-style-type: none"> • すべてのエージェント宛先ポートを許可する（リレーにも適用されるため）。 • 443/HTTPS (Trend Micro Update Server / Active UpdateおよびDownload Centerポート) • 4119/HTTPS — Deep Security Manager GUIおよびAPIポート • 4122 (他のRelayのポート) <p>注意: AWS AMIおよびAzure VMバージョンのManagerを使用する場合は、ポート4119ではなくポート443を開きます。</p>

Deep SecurityのURL

お使いの環境で許可されるURLを制限する必要がある場合は、このセクションを確認してください。

ファイアウォールで次のトラフィックを許可する必要があります：トレンドマイクロ、Deep Security、AWS、AzureサーバのURL（ポート443（HTTPS））。

送信元	送信先のサーバまたはサービスの名前	送信先URL
APIクライアント	Deep Security API	<ul style="list-style-type: none"> • <ManagerのFQDNまたはIP>:4119/webservice/Manager?WSDL • <ManagerのFQDNまたはIP>:4119/api • <ManagerのFQDNまたはIP>:4119/rest
従来のREST APIクライアント	Deep Securityの従来のREST APIの ステータス監視API	<ul style="list-style-type: none"> • <ManagerのFQDNまたはIP>:4119/rest/status/manager/ping
マネージャ、エージェント/アプライアンス、およびリレー	ダウンロードセンターまたは Webサーバ ソフトウェアをホストします。	<ul style="list-style-type: none"> • files.trendmicro.com
マネージャー	Smart Protection Network - ソフトウェア安全性評価サービス (CSSS) イベントのタグ付けと変更監視 のために使用されます。	<ul style="list-style-type: none"> • gacl.trendmicro.com • grid-global.trendmicro.com • grid.trendmicro.com
Agent/Appliance	Smart Protection Network - Global Censusサービス 挙動監視 、および 機械学習型検索 のために使用されます。	<p>12.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds1200-en-census.trendmicro.com • ds1200-jp-census.trendmicro.com <p>11.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds1100-en-census.trendmicro.com • ds1100-jp-census.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先URL
		<p>10.2および10.3エージェント/ appliance に接続先：</p> <ul style="list-style-type: none"> • ds1020-en-census.trendmicro.com • ds1020-jp-census.trendmicro.com • ds1020-sc-census.trendmicro.com <p>10.1および10.0エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds1000-en.census.trendmicro.com • ds1000-jp.census.trendmicro.com • ds1000-sc.census.trendmicro.com • ds1000-tc.census.trendmicro.com
Agent/Appliance	<p>Smart Protection Network - Good File Reputationサービス</p> <p>挙動監視、機械学習型検索、およびプロセスメモリ検索のために使用されます。</p>	<p>12.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • deepsec12-en.gfrbridge.trendmicro.com • deepsec12-jp.gfrbridge.trendmicro.com <p>11.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • deepsec11-en.gfrbridge.trendmicro.com • deepsec11-jp.gfrbridge.trendmicro.com <p>10.2および10.3エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • deepsec102-en.gfrbridge.trendmicro.com • deepsec102-jp.gfrbridge.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先URL
		10.1および10.0エージェント/ appliance 接続先： <ul style="list-style-type: none"> • deepsec10-en.grid-gfr.trendmicro.com • deepsec10-jp.grid-gfr.trendmicro.com • deepsec10-cn.grid-gfr.trendmicro.com
Agent/Appliance	Smart Protection Network - スマートフィードバック	12.0以降のクライアント/ appliance 接続先： <ul style="list-style-type: none"> • ds120-en.fbs25.trendmicro.com • ds120-jp.fbs25.trendmicro.com 11.0以降のクライアント/ appliance 接続先： <ul style="list-style-type: none"> • deepsecurity1100-en.fbs25.trendmicro.com • deepsecurity1100-jp.fbs25.trendmicro.com 10.0エージェント/ appliance 接続先： <ul style="list-style-type: none"> • deepsecurity1000-en.fbs20.trendmicro.com • deepsecurity1000-jp.fbs20.trendmicro.com • deepsecurity1000-sc.fbs20.trendmicro.com
Agent/Appliance	Smart Protection Network - スマートスキャンサービス	12.0以降のクライアント/ appliance 接続先： <ul style="list-style-type: none"> • ds120.icrc.trendmicro.com • ds120-jp.icrc.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先URL
		<p>11.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds110.icrc.trendmicro.com • ds110-jp.icrc.trendmicro.com <p>10.2および10.3エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds102.icrc.trendmicro.com • ds102-jp.icrc.trendmicro.com • ds102-sc.icrc.trendmicro.com.cn <p>10.1および10.0エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds10.icrc.trendmicro.com • ds10.icrc.trendmicro.com/tmcSS/ • ds10-jp.icrc.trendmicro.com/tmcSS/ • ds10-sc.icrc.trendmicro.com.cn/tmcSS/ <p>9.6および9.5エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • iaufdbk.trendmicro.com • ds96.icrc.trendmicro.com • ds96-jp.icrc.trendmicro.com • ds96-sc.icrc.trendmicro.com.cn • ds95.icrc.trendmicro.com • ds95-jp.icrc.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先URL
		<ul style="list-style-type: none"> • ds95-sc.icrc.trendmicro.com.cn
Agent/Appliance	Smart Protection Network - 機械学習型検索	<p>12.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds120-en-b.trx.trendmicro.com • ds120-jp-b.trx.trendmicro.com • ds120-en-f.trx.trendmicro.com • ds120-jp-f.trx.trendmicro.com <p>11.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds110-en-b.trx.trendmicro.com • ds110-jp-b.trx.trendmicro.com • ds110-en-f.trx.trendmicro.com • ds110-jp-f.trx.trendmicro.com <p>10.2および10.3エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds102-en-f.trx.trendmicro.com • ds102-jp-f.trx.trendmicro.com • ds102-sc-f.trx.trendmicro.com
Agent/Appliance	Smart Protection Network - Webレピュテーションサービス	<p>12.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds12-0-en.url.trendmicro.com • ds12-0-jp.url.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先URL
		<p>11.0以降のクライアント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds11-0-en.url.trendmicro.com • ds11-0-jp.url.trendmicro.com <p>10.2および10.3エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds10-2-en.url.trendmicro.com • ds10-2-sc.url.trendmicro.com.cn • ds10-2-jp.url.trendmicro.com <p>10.1および10.0エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds100-jp.url.trendmicro.com • ds100-sc.url.trendmicro.com • ds100-jp.url.trendmicro.com <p>9.6および9.5エージェント/ appliance 接続先：</p> <ul style="list-style-type: none"> • ds96-jp.url.trendmicro.com • ds96-jp.url.trendmicro.com • ds95-jp.url.trendmicro.com • ds95-jp.url.trendmicro.com
マネージャー	ヘルプとサポート	<ul style="list-style-type: none"> • help.deepsecurity.trendmicro.com • success.trendmicro.com/product-support/deep-security

送信元	送信先のサーバまたはサービスの名前	送信先URL
マネージャー	ライセンスと登録サーバ	<ul style="list-style-type: none"> • licenseupdate.trendmicro.com • clp.trendmicro.com • olr.trendmicro.com
マネージャー	ニュースフィード	<ul style="list-style-type: none"> • news.deepsecurity.trendmicro.com • news.deepsecurity.trendmicro.com/news.atom • news.deepsecurity.trendmicro.com/news_ja.atom
エージェントコンピュータ上のブラウザおよびマネージャへのログインに使用するコンピュータ	Site Safety	<p>(任意)以下のURLへのリンクがマネージャUI内と、クライアントの[管理者がこのページへのアクセスをブロックしました]ページにあります。</p> <ul style="list-style-type: none"> • sitesafety.trendmicro.com • jp.sitesafety.trendmicro.com
リレー、およびエージェント/appliance	アップデートサーバ セキュリティアップデートをホストします。	<ul style="list-style-type: none"> • iaus.activeupdate.trendmicro.com • iaus.trendmicro.com • ipv6-iaus.trendmicro.com • ipv6-iaus.activeupdate.trendmicro.com
マネージャー	AWSとAzure URL AWSアカウント と Azureアカウント をDeep Security Managerに追加するために使用されます。	<p>AWS URL</p> <ul style="list-style-type: none"> • AWSのこちらのページ内にある、下記の各見出しの下に表示されているAWSエンドポイントのURL。 <ul style="list-style-type: none"> • Amazon Elastic Compute Cloud (Amazon EC2)

送信元	送信先のサーバまたはサービスの名前	送信先URL
		<ul style="list-style-type: none"> • AWS Security Token Service (AWS STS) • AWS Identity and Access Management (IAM) • Amazon WorkSpaces <p>Azure URL</p> <ul style="list-style-type: none"> • login.windows.net (認証) • management.azure.com (Azure API) • management.core.windows.net (Azure API) <p>注意: management.core.windows.net URLは、AzureアカウントをManagerに追加するためにDeep Security Manager 9.6で利用可能なv1 Azureコネクタを使用した場合にのみ必要です。Deep Security Manager 10.0以降では、v2コネクタが使用され、このURLにアクセスする必要はありません。</p>
マネージャー	テレメトリサービス 匿名 "Deep Security製品使用状況データ収集" on page 78。	<ul style="list-style-type: none"> • telemetry.deepsecurity.trendmicro.com

法律上の免責事項

以下は、次のリリースに関する免責事項です。

- ["Hot Fix" below](#)
- ["メジャーリリース、Update、パッチ、Service Pack" below](#)

Hot Fix

本HotFixは、お客様の使用環境で実際に発生している不具合を修正するために提供いたします。トレンドマイクロでは、発生している不具合に関する動作テストのみ実施していますので、本HotFixの適用によりその他の不具合が発生する可能性があることをご理解いただき、本HotFixをご利用いただきますようお願いいたします。

■ 保証および責任の限定 ■

1. トレンドマイクロ株式会社は、本HotFixに関して一切の保証を行いません。またトレンドマイクロ株式会社は、本ソフトウェアの機能がお客様の特定の目的に適合することを保証するものではなく、本HotFixの物理的な紛失、盗難、事故および誤用等に起因するお客様の損害につき一切の補償をいたしません。
2. お客様が期待する成果を得るためのソフトウェアプログラム (本HotFixを含むがこれに限られない) の選択、導入、使用および使用結果につきましては、お客様の責任とさせていただきます。本HotFixの使用に起因してお客様またはその他の第三者に生じた結果的損害、付随的損害および逸失利益に関してトレンドマイクロ株式会社は一切の責任を負いません。

メジャーリリース、Update、パッチ、Service Pack

プログラムの仕様は予告なしに変更される場合があります。あらかじめご了承ください。また、本製品をご利用いただく前に、使用許諾契約に同意していただく必要があります。

製品の最新情報については、弊社ホームページをご覧ください。

URL: <https://www.trendmicro.com>

本製品を体験版としてお使いの場合には、30日以内に製品版を購入していただき、製品版にアップグレードしていただくことをお勧めします。製品版の購入については、トレンドマイクロの営業部または販売代理店にお問い合わせください。

はじめに

データベースを準備する

Deep Security Managerで使用するデータベースの準備

ヒント: YouTubeの [Deep Security 12 - データベースに関する考慮事項](#) を参照して、データベースの要件、設定、および認証のセットアップを確認できます。

Deep Security Managerをインストールする前に、Deep Security Managerで使用するデータベースを準備する必要があります。データベースのインストールおよび使用手順については、データベースプロバイダのドキュメントを参照してください。ただし、Deep Securityとの統合に関して、次の点にも注意してください。

1. "ハードウェア要件" on the next pageを確認します。
2. データベースの種類を選択します。サポートされるデータベースのリストについては、[「データベース」](#)を参照してください。

選択したデータベースに応じて、["Microsoft SQL Server" on page 208](#)、["Oracle Database" on page 209](#)、または["PostgreSQLの推奨設定" on page 210](#)を参照してください。

注意: Microsoft SQL Server Expressは、限られた構成でのみサポートされます。詳細については、["Microsoft SQL Server Expressに関する注意事項" on page 216](#)を参照してください。

3. 時刻とタイムゾーンの両方を同期させます。データベースとDeep Security Managerサーバーの両方で、同じタイムソースを使用します。
4. Deep Security Managerとデータベース間のネットワーク接続を許可します。["ポート番号、URL、およびIPアドレス" on page 190](#)を参照してください。

インストール中に、準備したデータベースのデータベース接続と認証資格情報を入力します。

インストール後に、["データベースメンテナンス" on page 209](#)を参照してください。

ハードウェア要件

専用のサーバ

データベースは、Managerノードから独立した専用のサーバにインストールします。また、データベースとDeep Security Managerを1GbpsのLAN接続を使用する同じネットワーク上に配置して、両者間の通信が妨げられずに確実に行われるようにすることも重要です。(WAN接続は推奨されません)。これは、Deep Security Managerノードを追加する場合にも該当します。Deep Security Managerからデータベースへの接続の待ち時間は、2ミリ秒以内が推奨されます。

そのためには、Managerとデータベースを仮想マシンにインストールする場合に、それらが必ず同じESXiホストで実行されるようにしてください。

1. vCenter Web Clientで、[Host and Clusters] に移動してクラスタを選択します。
2. [Manage] タブに移動して、[VM/Host Rules]→[Add] をクリックします。
3. ルールの名前を入力します。
4. [Enable rule] を選択します。
5. [Type] で [Keep Virtual Machines Together] を選択します。
6. [Add] をクリックし、Managerとデータベースの仮想マシンを選択します。

スケーラビリティとサービスの稼働時間のために、データベースロードバランシング、ミラーリング、および高可用性 (HA) が推奨されています。[Amazon Aurora](#)、[PostgreSQL](#)、[Microsoft SQL Server](#)などのベンダのドキュメントを参照してください。

警告: データベース複製ではなく、データベースミラーとHAを使用してください。フェイルオーバーでは、データベーススキーマを変更しないでください。一部の種類の複製では、複製中にデータベーステーブルに列が追加されるため、スキーマが変更され、重大なデータベース障害が発生します。

クラウドでホストされているデータベースの場合、複数の可用性ゾーン(「multi-AZ」)はネットワーク待ち時間を増加させることがあるため、推奨しません。

ハードウェアに関する推奨事項

アップデートや推奨設定の検索など、Deep Security Managerの処理の多くは、多くのCPUリソースとメモリリソースを必要とします。大規模な環境の場合、トレンドマイクロでは、各Managerノードに4コアおよび十分なメモリを持たせることを推奨します。

データベースは、最適なDeep Security Managerノードの仕様と同等か、それ以上のハードウェアにインストールしてください。十分なパフォーマンスのためには、データベースに

8~16GBのメモリと、ローカルまたはネットワーク接続されたストレージへの高速アクセスが必要です。可能であれば、最適なデータベースサーバの設定と実施されるメンテナンス計画について、データベース管理者に確認してください。

Microsoft SQL Server

一般的な要件

- Deep Securityで使用される空のデータベースを作成する必要があります。
- リモートTCP接続を有効にする"([https://docs.microsoft.com/en-us/previous-versions/bb909712\(v=vs.120\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/bb909712(v=vs.120)?redirectedfrom=MSDN)).を参照してください。
- Deep Security Managerのデータベースユーザにdb_owner権限を付与します。

注意:

Microsoft SQL Serverを使用する場合は、Deep Security ManagerがMicrosoft Active DirectoryドメインまたはSQLユーザとして接続する必要があります。Windowsのワークグループ認証はサポート対象外になりました。

トランスポートプロトコル

- サポートされている[トランスポートプロトコル](#)は、新しくインストールされたDeep Security 10.2以降のバージョンの場合はTCPです。
- Deep Security 10.1以前のバージョンからアップグレードし、トランスポートプロトコルとして名前付きパイプを使用する場合、DSMはアップグレード時に引き続き名前付きパイプを使用します。トレンドマイクロでは、TCPを使用して通信を暗号化することをお勧めします("Deep Security Managerとデータベース間の通信の暗号化" on page 1063を参照してください)。

マルチテナントを使用する場合

- メインデータベース名を短くします。これにより、テナントのデータベース名が読み取りやすくなります(たとえば、メインデータベースが「MAINDB」の場合、最初のテナントのデータベース名は「MAINDB_1」、2番目のテナントのデータベース名は「MAINDB_2」になります(以下同様))。
- Deep Security Managerのデータベースユーザアカウントにdbcreator権限を付与します。マルチテナントについては、"[マルチテナント環境の設定](#)" on page 279を参照してください。

Oracle Database

- 「Oracle Listener」サービスを開始します。TCP接続が許可されていることを確認します。
- Deep Security Managerのデータベースユーザ名に特殊文字は使用しないでください。Oracleでは、引用符で囲めばデータベースユーザオブジェクトの設定時に特殊文字を使用できますが、Deep Securityでは、データベースユーザの特殊文字がサポートされていません。
- Deep Security ManagerのデータベースユーザにCONNECTロールとRESOURCEロール、およびUNLIMITED TABLESPACE、CREATE SEQUENCE、CREATE TABLE、CREATE TRIGGERの各権限を付与します。

マルチテナントを使用する場合は、Deep Security ManagerのデータベースユーザにCREATE USER、DROP USER、ALTER USER、GRANT ANY PRIVILEGE、GRANT ANY ROLEの権限も付与します。

注意: Oracleコンテナデータベース (CDB) の設定は、Deep Security Managerのマルチテナントではサポートされません。

Oracle RAC (Real Application Clusters) のサポート

Deep Securityでは次の構成がサポートされます。

- SUSE Linux Enterprise Server 11 SP3とOracle RAC 12c Release 1 (v12.1.0.2.0)
- Red Hat Linux Enterprise Server 6.6とOracle RAC 12c Release 1 (v12.1.0.2.0)

初期設定のLinux Server Deep SecurityポリシーはOracle RAC環境に対応していますが、ファイアウォールの設定だけは例外です。ファイアウォール自体を無効にするか、"[Oracle RACでのファイアウォール設定](#)" on page 871の手順に従ってファイアウォールの設定をカスタマイズしてください。

データベースメンテナンス

Deep Security環境の状態を正常に維持するには、データベースメンテナンスが不可欠です。

インデックスのメンテナンス

Deep Security Managerのパフォーマンスを向上させるには、Deep Securityデータベースでインデックスのメンテナンスを定期的に実行して、過度のフラグメント化を防止することをお勧めします。

めします。組織のベストプラクティスに従ってデータベースのインデックスを再作成するか、データベースベンダが提供する以下のドキュメントを参照してください。

- PostgreSQL: PostgreSQLのインデックス再作成コマンドの詳細については、<https://www.postgresql.org/docs/10/sql-reindex.html>を参照してください。このコマンドを実行すると一部の処理がブロックされるため、アップグレード時にオフラインで実行することをお勧めします。このコマンドを既存のスナップショットに対してオフラインで実行する場合、完了までに約45分かかります。
- Microsoft SQL: インデックス管理のベストプラクティスについては、Microsoftのドキュメントを参照してください: <https://docs.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes?view=sql-server-ver15>。
- Oracle Database: インデックスの管理に関するOracleのベストプラクティスに従ってください。たとえば、https://docs.oracle.com/cd/B28359_01/server.111/b28310/indexes002.htm#ADMIN11713を参照してください。

このタスクに役立つスクリプトは、オープンソースのWebサイトでも提供されています。

バックアップと障害復旧

高可用性やロードバランシングとは別に、ベストプラクティスとして、定期的なデータベースのバックアップや障害復旧プランがあります。バックアップは、重大な障害が発生した場合にデータベースを復元するために使用できます。ベンダのドキュメントのほか、"[データベースのバックアップと復元](#)" on page 989を参照してください。

注意: PostgreSQLデータベースの場合、pg_dumpやpg_basebackupのような基本的なツールは、エンタープライズ環境でのバックアップと復元には適していません。[Barman](#)など、別のツールの使用を検討してください。

PostgreSQLの推奨設定

すべての種類のデータベースに適用される要件については、"[Deep Security Managerで使用するデータベースの準備](#)" on page 206を参照してください。

1. Deep Security Manager用のPostgreSQLデータベースを準備するには、データベースユーザアカウントを作成し、権限を付与します。

```
CREATE DATABASE "<database-name>";
```

```
CREATE ROLE "<dsm-username>" WITH PASSWORD '<password>' LOGIN;
```

```
GRANT ALL ON DATABASE "<database-name>" TO "<dsm-username>";
```

```
GRANT CONNECT ON DATABASE "<database-name>" TO "<dsm-username>";
```

Deep Security Managerに複数のテナントがある場合は、それらのテナントに新しいデータベースと役割を作成する権限も付与します。

```
ALTER ROLE <dsm-username> CREATEDB CREATEROLE;
```

2. Deep Security ManagerとPostgreSQLの間の接続で信頼できないネットワークが使用されている場合は、TLSを使用してセキュリティを強化することを検討してください。["Deep Security Managerとデータベース間の通信の暗号化" on page 1063](#)を参照してください。

3. データベースログのローテーションとパフォーマンス設定を行います。

ベストプラクティスについては、["ログローテーション" on the next page](#), ["ロック管理" on page 213](#), ["最大同時接続数" on page 213](#), ["自動バキューム設定" on page 215](#)などを参照してください。

手順は、ディストリビューションや管理対象のホスティングによって異なります。

- 自己ホスト型データベースの場合:初期設定は、PostgreSQL Core Distributionの汎用値となります。特に大規模環境では、初期設定がデータセンターやカスタマイズされたクラウドインストールに適していないこともあります。

設定を変更するには、次の手順に従います。

- プレーンテキストエディタで[postgresql.confファイル](#)を開きます。
 - パラメータを編集します。
 - ファイルを保存します。
 - PostgreSQLサービスを再起動します。
- Amazon RDSの場合:初期設定は、インスタンスのサイズによって異なります。多くの場合、`autovacuuming`、`max_connections`、`effective_cache_size`を微調整するだけです。設定を変更するには、[データベースパラメータグループ](#)を使用し、データベースインスタンスを再起動します。
 - Amazon Auroraの場合:初期設定は、インスタンスのサイズによって異なります。多くの場合、`autovacuuming`、`max_connections`、`effective_cache_size`を微調整するだけです。設定を変更するには、[データベースパラメータグループ](#)を使用し、データベースインスタンスを再起動します。

ヒント: パフォーマンスを微調整する場合は、Amazon CloudWatchなどのサービスを使用してデータベースIOPSを監視し、設定を確認してください。

ヒント: 追加の支援が必要な場合は、PostgreSQLから[プロフェッショナルサポート](#)が提供されています。

ログローテーション

PostgreSQL Core Distributionの初期設定では、データベースのローカルログファイルに保持期間やファイルサイズの制限がありません。そのため、ログで消費されるディスク容量は徐々に増加していきます。

これを防ぐには、[Syslogのlog_destinationへのリモートログ出力](#)またはローカルのログローテーションについてパラメータを設定します。

ログファイルは、保持期間の制限、ファイルサイズの制限、またはその両方(先に達した方)に基づいてローテーションされます。制限に達した場合は、その時点でファイル名のパターンに一致するログファイルが存在するかどうかに応じて、PostgreSQLでは、新しいファイルが作成されるか、既存のファイルが再利用されます。再利用の場合は、追記するか(保持期間の制限の場合は)上書きすることができます。

ログローテーションのパラメータは次のとおりです。

- `logging_collector`:データベースのログ出力を有効にするには、「on」を入力します。
- `log_filename`:ログファイル名のパターン。ほとんどの場合、パターンでは[IEEE標準の日時形式](#)が使用されます。
- `log_truncate_on_rotation`:既存ログファイルに追記する場合は「off」、既存のログファイルを上書きする場合は「on」を入力します。適用されるのは、時間ベースのログローテーションが発生した場合のみです(ファイルサイズベースのログローテーションでは、常に追記されます)。
- `log_rotation_age`:ログファイルの最大保持期間(分)。「0」を入力すると、時間ベースのログローテーションが無効になります。
- `log_rotation_size`:ログファイルの最大サイズ(KB)。「0」を入力すると、ファイルサイズベースのログローテーションが無効になります。

例:日単位のデータベースのログローテーション

以下のパラメータを使用して、ローテーションしたデータベースログファイルを7つ作成します。つまり、ファイルは各曜日に1つずつ作成されます(たとえば、月曜日のファイル名は「postgresql-Mon.log」となります)。

1日(1440分)ごとに、その曜日の名前が付いたファイルを作成するか(ファイルが存在しない場合)、その前の週で使用されたその曜日のログファイルを上書きします。

負荷が高い状況では、ファイルサイズの制限が無効になるため、ログ出力が「割り当てられたディスク容量を一時的に超過する」ことがあります。ただし、ファイルの数や名前は変更されません。

```
log_collector = on
```

```
log_filename = 'postgresql-%a.log'
```

```
log_rotation_age = 1440
```

```
log_rotation_size = 0
```

```
log_truncate_on_rotation = on
```

ロック管理

`deadlock_timeout`の値を大きくすると、現在の環境で設定されている通常のトランザクション時間を超過することができます。

クエリによるロックの待機時間が`deadlock_timeout`の値を超えるたびに、PostgreSQLはデッドロック状態を確認し、(設定されている場合は)エラーを記録します。ところが、負荷の高い大規模環境では、多くの場合、待機時間が1秒を超えることは正常です(エラーではありません)。こうした正常なイベントが記録されると、パフォーマンスは低下します。

最大同時接続数

`max_connections = 500`に引き上げてください。

有効キャッシュサイズ

有効キャッシュサイズ(`effective_cache_size`)の値を大きくすることを検討してください。この設定は、クエリによりキャッシュの効果を推定するために使用されます。これは、クエリ計画中のコスト見積もりにのみ影響し、RAMの使用量が増加することはありません。

共有バッファ

`shared_buffers`の値をRAMの25%まで引き上げてください。この設定では、PostgreSQLがデータのキャッシュに使用できるメモリ容量を指定します。これによりパフォーマンスが向上します。

ワークメモリとメンテナンスワークメモリ

`work_mem`の値を大きくしてください。この設定では、一時ディスクファイルへの書き込み前に、内部ソート操作とハッシュテーブルで使用できるRAMのサイズを指定します。複雑なクエリを実行する場合は、多くのメモリが必要になります。

`maintenance_work_mem`の値を大きくすることを検討してください。この設定では、ALTER TABLEなどのメンテナンス操作に使用される最大メモリ容量を決定します。

チェックポイント

チェックポイントの作成頻度を減らしてください。通常は、チェックポイントにより、データファイルへの書き込みのほとんどが行われます。パフォーマンスを最適化するには、大半のチェックポイントを「requested」（使用可能なすべてのWALセグメントを入力することによるトリガ、または明示的なCHECKPOINTコマンドによるトリガ）ではなく、「timed」（`checkpoint_timeout`によるトリガ）にする必要があります。

パラメータ名	推奨値
<code>checkpoint_timeout</code>	15min
<code>checkpoint_completion_target</code>	0.9
<code>max_wal_size</code>	16GB

ログ先行書き込み (WAL)

データベース複製を使用する場合は、`wal_level = replica`を使用することを検討してください。

自動バキューム設定

PostgreSQLには、「バキューム」と呼ばれる定期的なメンテナンスが必要です。通常、`autovacuum_max_workers`の初期設定値を変更する必要はありません。

`entitys` および `attribute2s` 表で、頻繁な書き込みによって多くの行が頻繁に変更される場合（短時間のクラウドインスタンス）、を使用する大規模な配置では、ディスク領域の使用を最小限に抑えてパフォーマンスを維持するために、自動バッファの実行頻度を増やす必要があります。パラメータはデータベース全体と特定のテーブルの両方に設定する必要があります。

データベースレベルのパラメータ名	推奨値
<code>autovacuum_work_mem</code>	1GB

テーブルレベルのパラメータ名	推奨値
<code>autovacuum_vacuum_cost_delay</code>	10
<code>autovacuum_vacuum_scale_factor</code>	0.01
<code>autovacuum_analyze_scale_factor</code>	0.005

データベースレベルの設定を変更するには、設定ファイルまたはデータベースパラメータグループを編集し、データベースサーバを再起動する必要があります。データベースが実行されている間、コマンドはその設定を変更できません。

テーブルレベルの設定を変更するには、設定ファイルまたはデータベースパラメータグループを編集するか、次のコマンドを入力します。

```
ALTER TABLE public.entitys SET (autovacuum_enabled = true, autovacuum_vacuum_cost_delay = 10, autovacuum_vacuum_scale_factor = 0.01, autovacuum_analyze_scale_factor = 0.005);
```

```
ALTER TABLE public.attribute2s SET (autovacuum_enabled = true, autovacuum_vacuum_cost_delay = 10, autovacuum_vacuum_scale_factor = 0.01, autovacuum_analyze_scale_factor = 0.005);
```

Linux版PostgreSQL

Transparent huge pages

Transparent Huge Pages (THP) は、RAMのサイズが大きいコンピュータでより大きなメモリページを使用することにより、Translation Lookaside Buffer (TLB) 検索のオーバーヘッドを削減するLinuxのメモリ管理システムです。初期設定ではTHPが有効になっていますが、PostgreSQLデータベースサーバには推奨されていません。この機能を無効にするには、OSベンダのドキュメントを参照してください。

ホストベース認証

ホストベース認証 (HBA) により、許可されたIPアドレスの範囲に含まれていないコンピュータからデータベースへの不正アクセスを防ぐことができます。Linuxの初期設定では、データベースに対するHBAの制限はありません。ただし、通常はセキュリティグループやファイアウォールを使用することをお勧めします。

Microsoft SQL Server Expressに関する注意事項

製品Q&A「[Deep Security 10 以降でサポートされる無償版データベースについて](#)」内の「Microsoft SQL Server Express使用時の注意点」をご確認ください。

ソフトウェアパッケージのデジタル署名の確認

Deep Securityをインストールする前に、ソフトウェアZIPパッケージおよびインストーラファイルのデジタル署名を確認する必要があります。デジタル署名が正しいことは、ソフトウェアがTrend Microからのもので、壊れていないか、または改ざんされていないことを示しています。

あなたは：

- "[ソフトウェアZIPパッケージの署名の確認](#)" on the next page
- "[インストーラファイル \(EXE、MSI、RPM、またはDEBファイル\) の署名の確認](#)" on page 218

ソフトウェアのチェックサム、およびセキュリティアップデートおよびDeep Security Agentモジュールのデジタル署名も検証できます。"[Agentによるアップデートの整合性の検証方法](#)" on page 995 および"[Agent向けのLinux Secure Bootのサポート](#)" on page 427。

ソフトウェアZIPパッケージの署名の確認

Deep Security Agent、Deep Security Virtual Appliance、およびオンラインヘルプは、ZIPパッケージで提供されます。これらのパッケージはデジタル署名されています。ZIPファイルのデジタル署名は、次の方法で確認できます。

ZIPを管理者との間でインポートまたはエクスポートすることで

"[Deep Security ManagerにAgentソフトウェアパッケージをダウンロードする](#)" on page 372 または "[Agentのインストーラをエクスポートする](#)" on page 374をエクスポートします。

インポートまたはエクスポートすると、マネージャはZIP ファイルのデジタル署名をチェックします。署名が良好な場合、マネージャはインポートまたはエクスポートを続行します。署名が不正の場合、または存在しない場合、マネージャは処理を禁止し、ZIPを削除してイベントをログに記録します。

注意: ファイルの削除およびイベントログの生成には、Deep Security Managerのビルド12.5.752以降が必要です。

ZIPのプロパティファイルを表示することで

1. Deep Security Managerにログインします。
2. 上部の [管理] をクリックします。
3. 左側で、[アップデート> ソフトウェア> ローカル]を展開します。
4. デジタル署名を確認するZIPパッケージを見つけてダブルクリックします。（見つからない場合は、[ダウンロードしてください](#)。）
5. ZIPファイルのプロパティページが開き、マネージャがデジタル署名を確認します。署名が良好な場合は、署名フィールドに緑色のチェックマークが表示されます。シグネチャが不良であるか、存在しない場合、マネージャはZIPを削除し、イベントをログに記録します。

注意: ファイルの削除およびイベントログの生成には、Deep Security Managerのビルド12.5.752以降が必要です。

jarsignerを使用する

jarsigner Javaユーティリティを使用して、a ZIP上の署名がマネージャから確認でき

ない場合にチェックします。たとえば、マネージャ以外のソースからエージェントのZIPパッケージ（例：[Deep Security Software](#)）を取得した後、エージェントを手動でインストールする場合を考えてみましょう。このシナリオでは、managerが関与していないため、jarsignerユーティリティを使用します。

jarsignerを使用して署名をチェックするには

1. お使いのコンピュータに最新の[Java Development Kit](#)をインストールしてください。
2. ZIPをダウンロードします。
3. JDK内の[jarsignerユーティリティ](#)を使用して、署名を確認します。コマンドは次のとおりです。

```
jarsigner -verify -verbose -certs -strict <ZIP_file>
```

例:

```
jarsigner -verify -verbose -certs -strict Agent-RedHat_EL7-11.2.0-124.x86_64.zip
```

4. エラー (エラーがある場合) と証明書の内容を読んで、署名が信頼できるかどうかを判断します。

インストーラファイル (EXE、MSI、RPM、またはDEBファイル) の署名の確認

Deep Security Agent、Deep Security Manager、およびDeep Security Notifierのインストーラは、RSAを使用してデジタル署名されています。インストーラは、Windows上のEXEまたはMSIファイル、Linux OS上のRPMファイル (Amazon、CloudLinux、Oracle、Red Hat、およびSUSE,) またはDebian上のDEBファイルおよびUbuntu。

注意: 以下の手順では、インストーラファイルでデジタル署名を手動で確認する方法について説明します。この確認を自動化したい場合は、これをAgentインストールスクリプトに含めることができます。インストールスクリプトの詳細については、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498を参照してください。

確認するインストーラファイルの種類に対応する指示に従います。

- "EXEまたはMSIファイルの署名の確認" below
- "RPMファイルの署名の確認" below
- "DEBファイルの署名の確認" on page 221

EXEまたはMSIファイルの署名の確認

1. EXEファイルまたはMSIファイルを右クリックして、[のプロパティ]を選択します。
2. [デジタル署名] タブをクリックし、署名を確認します。

RPMファイルの署名の確認

まず、GnuPGをインストールします。

あなたはそれが既にインストールされていない場合は、署名をチェックするつもりエージェント上で[GnuPG](#)のしてインストールします。このユーティリティにはGPGコマンドラインツールが含まれています。このツールは、署名キーをインポートしてデジタル署名を確認するために必要なツールです。

注意: GnuPGは、ほとんどのLinuxディストリビューションに初期設定でインストールされています。

次に、署名キーをインポートします。

1. エージェントのZIPファイルのルートフォルダにある3trend_public.ascファイルを探します。ASCファイルには、デジタル署名の検証に使用できるGPG公開署名キーが含まれています。
2. (オプション) 任意のハッシュユーティリティを使用して、ASCファイルのSHA-256ハッシュダイジェストを確認します。ハッシュは次のとおりです。

```
c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7
```

3. シグネチャをチェックするエージェントコンピュータで、ASCファイルをインポートします。次のコマンドを使用します。

注意: コマンドでは大文字と小文字が区別されます。

```
gpg --import 3trend_public.asc
```

次のメッセージが表示されます。

```
gpg: directory `/home/build/.gnupg' created
gpg: new configuration file `/home/build/.gnupg/gpg.conf'
created
gpg: WARNING: options in `/home/build/.gnupg/gpg.conf' are not
yet active during this run
gpg: keyring `/home/build/.gnupg/secring.gpg' created
gpg: keyring `/home/build/.gnupg/pubring.gpg' created
gpg: /home/build/.gnupg/trustdb.gpg: trustdb created
gpg: key E1051CBD: public key "Trend Micro (trend linux sign)
<alloftrendetscodesign@trendmicro.com>" imported
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
```

4. GPGパブリック署名キーをASCファイルからエクスポートします。

```
gpg --export -a 'Trend Micro' > RPM-GPG-KEY-CodeSign
```

5. GPGパブリック署名鍵をRPMデータベースにインポートします。

```
sudo rpm --import RPM-GPG-KEY-CodeSign
```

6. GPGパブリック署名キーがインポートされたことを確認します。

```
rpm -qa gpg-pubkey*
```

7. インポートされたGPG公開鍵のフィンガープリントが表示されます。トレンドマイクロの鍵を次に示します。

```
gpg-pubkey-e1051cbd-5b59ac99
```

署名鍵がインポートされ、エージェント RPMファイルのデジタル署名のチェックに使用できます。

最後に、RPMファイルの署名を確認します。

ヒント: RPMファイルの署名を手動で確認するのではなく、次に説明するように、配

信スクリプトで署名を確認することもできます。詳細については、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498を参照してください。

次のコマンドを使用します。

```
rpm -K Agent-PGPCore-<OS agent version>.rpm
```

例:

```
rpm -K Agent-PGPCore-RedHat_EL7-11.0.0-950.x86_64.rpm
```

Agent-PGPCore-<...>.rpmファイルで上記のコマンドを実行してください。

(Agent-Core-<...>.rpmで実行すると.)を使用できない) エージェント ZIPで Agent-PGPCore-<...>.rpmファイルが見つからない場合は、新しいZIPを使用する必要があります。具体的には次のとおりです。

- Deep Security Agent 11.0 Update 15以降のアップデート
- or
- Deep Security Agent 12 Update 2以降

署名の検証に成功すると、次のメッセージが表示されます。

```
Agent-PGPCore-RedHat_EL7-11.0.0-950.x86_64.rpm: rsa sha1 (md5) pgp  
md5 OK
```

DEBファイルの署名の確認

まず、dpkg-sigユーティリティをインストールします。

あなたはそれが既にインストールされていない場合は、署名をチェックするつもりエージェント上で[dpkg-SIG](#)をインストールします。このユーティリティにはGPGコマンドラインツールが含まれています。このツールは、署名キーをインポートしてデジタル署名を確認するために必要なツールです。

次に、署名キーをインポートします。

1. エージェントのZIPファイルのルートフォルダにある3trend_public.ascファイルを探します。ASCファイルには、デジタル署名の検証に使用できるGPG公開署名キーが含まれています。
2. (オプション) 任意のハッシュユーティリティを使用して、ASCファイルのSHA-256ハッシュダイジェストを確認します。ハッシュは次のとおりです。

```
c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7
```

3. あなたが署名をチェックするつもりエージェントで、GPGキーリングにASCファイルをインポートします。次のコマンドを使用します。

```
gpg --import 3trend_public.asc
```

次のメッセージが表示されます。

```
gpg: key E1051CBD: public key "Trend Micro (trend linux sign)
<alloftrendetscodesign@trendmicro.com>" imported
```

```
gpg: Total number processed: 1
```

```
gpg: imported: 1 (RSA: 1)
```

4. (オプション) Trend Micro Key情報を表示します。次のコマンドを使用します。

```
gpg --list-keys
```

次のようなメッセージが表示されます。

```
/home/user01/.gnupg/pubring.gpg
```

```
-----
```

```
pub 2048R/E1051CBD 2018-07-26 [expires: 2021-07-25]
```

```
uid Trend Micro (trend linux sign)
<alloftrendetscodesign@trendmicro.com>
```

```
sub 2048R/202C302E 2018-07-26 [expires: 2021-07-25]
```

最後に、DEBファイルの署名を確認します。

ヒント: 以下で説明するように、手動でDEBファイルの署名を検証する代わりに、配置スクリプトで署名を検証することもできます。詳細については、["インストールス](#)

[クリプトを使用したコンピュータの追加と保護" on page 498](#)を参照してください。

次のコマンドを入力します。

```
dpkg-sig --verify <agent_deb_file>
```

ここで、<agent_deb_file>はエージェントの DEBファイルの名前とパスです。たとえば、次のとおりです。

```
dpkg-sig --verify Agent-Core-Ubuntu_16.04-12.0.0-563.x86_64.deb
```

処理メッセージが表示されます。

```
Processing Agent-Core-Ubuntu_16.04-12.0.0-563.x86_64.deb...
```

署名が正常に確認されると、次のメッセージが表示されます。

```
GOODSIG _gpgbuilder CF5EBBC17D8178A7776C1D365B09AD42E1051CBD  
1568153778
```

Deep Securityのインストール

Deep Securityのインストールまたはアップグレード

このドキュメントでは、Deep Security 12.0のインストールまたはアップグレードに必要な手順を説明します。

ヒント: YouTube 2012のDeep Security Managerのインストールプロセスを確認するには、[Deep Security 12 - GUIベースのインストール](#) をYouTubeで視聴できます。このビデオでは、いくつかのインストール前のタスク、インストールの準備状況の確認、インストールの方法についても説明します。

ヒント: [Deep Security 12 - YouTubeのDSMおよび](#) エージェントのアップグレードを参照して、Deep Security Manager、Agent、Relay のアップグレードを確認できます。

ヒント: 以前のバージョンのDeep Securityからアップグレードする場合は、Deep Security Managerインストーラを実行し、お使いの環境に合ったバージョンのドキュメントをご利用

ください。インストール前にインストーラによって環境が確認され、それに応じたアップグレード手順へのリンクが提供されます。

環境を準備する

このドキュメントはチェックリストとして使用できます。Deep Securityプラットフォームを選択し、次の手順に従って基本的なインストールを実行します。この手順が完了すると、セキュリティポリシーを実装する準備が整います。



1. ソフトウェアのダウンロード: ライセンスのアクティベーションコードを入手します。
 - vCenter、ESXi、VMware Tools、NSX Managerなど、必要なソフトウェアを[VMware](#)からダウンロードします。
 - 最新のパッチおよびDeep Security Managerインストーラ (<https://help.deepsecurity.trendmicro.com/ja-jp/software.html>) をダウンロードします。
 - AgentおよびRelayのインストーラは必要ありません。これらはManagerを通じてダウンロードできます。Agent、Relay、Deep Security Virtual Applianceのインストーラまたはアップデートに関する詳細については、"[アップグレードについて](#)" on [page 994](#)を参照してください。

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。最初にRelayをアップグレードしないと、セキュリティコンポーネントのアップグレードとソフトウェアのアップグレードが失敗することがあります。

2. Deep Securityインストーラが正規のものであることを確認します (ハッシュのチェック)。

ソフトウェアが正規のものであることを確認するには、SHA256ハッシュ (フィンガープリント) をチェックします。トレンドマイクロでは、[Deep Securityソフトウェア](#)のページでこのハッシュを公開しています。ハッシュを表示するには、ソフトウェアの横にあるプラス記号をクリックする必要があります (下の図を参照)。

Manager Linux

ソフトウェア	リリースの種類	ビルド	リリース日	サイズ	ダウンロード
 Deep Security Manager 12.0.296 for Linux-x64	GM: 12.0	12.0.296	2019-06-19	402 MB	

ファイル名: [Manager-Linux-12.0.296.x64.sh](#)

SHA256: c01cbf51bcb6c4ee3372aef3d38b11580384ee121554f8fd50be96aa75dd3f42

MD5: d1cbb15e57f832aaf55fabdb3f00867b

[Readme](#)

3. 互換性の確認: インストーラを起動します。インストーラにより、使用している環境が[システム要件](#)に準拠しているかどうかの確認が行われます。また、インストーラでも既存のすべてのコンポーネントが新しいバージョンのDeep Security Managerと互換性があることを確認します。システムチェックが完了すると、対処する必要がある互換性の問題のリストが生成されます。

たとえば、空きディスク容量を確保したり、vRAMの割り当てを増やしたり、旧バージョンのDeep Security Agentをサポート対象のバージョンにアップグレードしたりといった処理が必要になることがあります。準備ができていない場合は、インストールをキャンセルし、準備が整ってから再度実行できます。

また、「アップグレード手順を表示」をクリックすると、システムチェックは環境のニーズに合わせてこの手順もカスタマイズします。インストールを開始する前に、["環境を準備する" on the previous page](#)のすべてのタスクを完了してください。

注意: サポートされるDeep Securityの機能は、プラットフォームによって異なります。["各プラットフォームでサポートされている機能" on page 183](#)を参照してください。

4. データのバックアップ: インストールを開始する前に、サーバおよび各保護対象コンピュータのシステム復元ポイントまたは仮想マシンのスナップショットを作成します。(複数ノード構成でDeep Security Managerを実行している環境では、各サーバノードのバックアップが必要です)。さらに、アップグレードの場合は、サービスを停止して既存のDeep SecurityManagerデータベースもバックアップします。

警告: バックアップを検証してください。バックアップがなく、インストーラの処理が何らかの理由で中断された場合、[環境を元に戻す](#)ことができません。この場合、環境全体の再インストールが必要になることがあります。

注意:

マルチテナント環境を使用している場合は、すべてのデータベースをバックアップします。

- Microsoft SQLおよびPostgreSQLでは、メインのデータベースが1つとテナントごとのデータベースがあります。
- Oracleでは、すべてのテナント情報が1つのDeep Security Managerデータベースに格納されていますが、テナントごとにユーザが作成され、各ユーザに専用のテーブルがあります。

ハードウェア要件

推奨されるハードウェアは、有効になっている機能、環境の規模、将来の拡張によって異なります。[サイジングガイドライン](#)を参照してください。

インストーラを実行するDeep Security Managerサーバでは、インストール前にシステムチェックによってハードウェアが検証されます。ハードウェアが[最小システム要件](#)を満たしていない場合は、パフォーマンスの低下に関する警告が表示されるか、インストールがブロックされます。

ローカルサーバのハードウェアと、データベースに保存されている他のいくつかのインストール情報のみがテストされます。手動でその他のサーバのハードウェアを確認したり、その他のManagerノードでシステムチェックを実行する必要があります。

注意:

Linuxでは、予約済みシステムメモリはプロセスメモリから独立しています。そのため、大きな差異はありませんが、インストーラではコンピュータに実際に搭載されているよりも少ないRAMが検出されます。コンピュータに実際に搭載されているRAMの合計を確認するには、スーパーユーザアカウントでログインして次のコマンドを入力します。

```
grep MemTotal /proc/meminfo
```

Deep Security 12.0のインストール後に、パフォーマンスを最適化できる場合があります。["Deep Security Managerのメモリ使用量の設定" on page 275](#)、["ディスク容量不足のアラート" on page 276](#)、["パフォーマンスプロファイル" on page 276](#)を参照してください。

ネットワーク要件

インストーラを実行する前に、Deep Security Managerサーバが必要なネットワークサービスを使用できることを確認します。これには、信頼できるタイムスタンプを提供するNTP、名前解決に使用するDNSが含まれます。プロトコル、関連する機能、想定される送信元や送信先、必要なネットワークポート番号については、"[ポート番号、URL、およびIPアドレス](#)" on [page 190](#)を参照してください。

注意: ManagerOSのシステムの時計はデータベースの時計と同期する必要があります。両方のコンピュータで同じNTPサービスを使用する必要があります。

Deep Security Managerのインストール後、新しいAgent、Appliance、Relayを配置すると、必要なポートを開くファイアウォールルールが自動的に適用されます。

警告: 必要なポートでネットワーク接続が不安定な状態の場合、一部の機能が適切に機能しなかったり失敗したりすることがあります。

一部の機能では、Deep Securityがホスト名をIPアドレスに解決する必要があります。Managerで各コンピュータまたは仮想マシンのホスト名をIPアドレスに解決できるようにDNSサーバにエントリを登録していない場合は、代わりにIPアドレスを使用するか、または次のどちらかの処理を実行します。

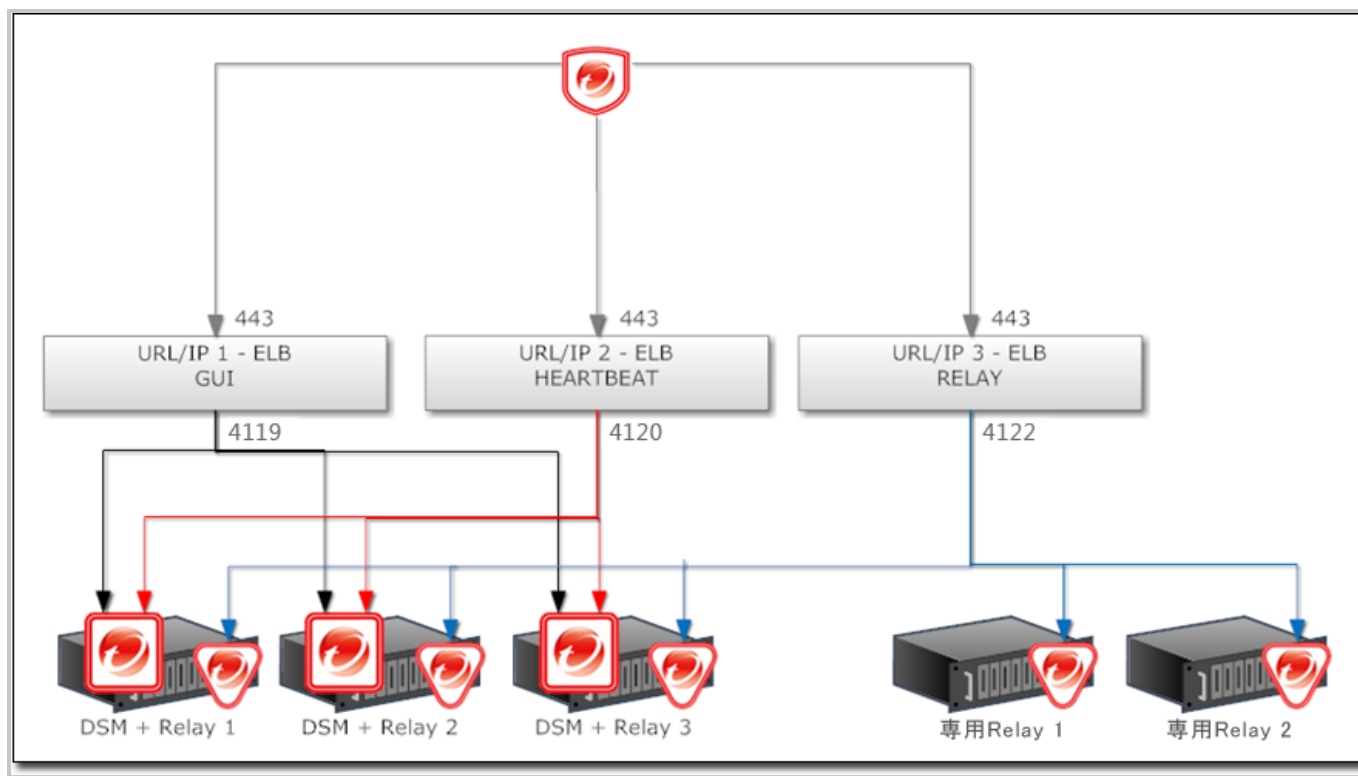
- DNSサーバにAレコード、AAAAレコード、または両方を登録し、Manager、Agent、Appliance、およびRelayがDNSルックアップクエリを実行できるようにします。
- AgentまたはApplianceコンピュータのhostsファイルにエントリを追加します。

注意: Deep Security ManagerのSSLまたはTLS接続用証明書ジェネレータでは、サーバがRFC 1034準拠のFQDNを使用する必要があります。サーバのDNS名は、0000-dsm.example.comのように数字から始まることはできません。数字から始まると、インストールログに次のエラーメッセージが表示されます。

```
java.io.IOException: DNSName components must begin with a letter
```

ネットワークトポロジー

大規模な環境でDeep Security Managerのサーバノードを複数配置している場合は、ロードバランサを使用してDeep Security AgentおよびVirtual Applianceとの接続を分散すると便利です。また、ロードバランサの仮想IPを使用すると、通常であればDeep Securityで複数のポート番号が必要になる構成において、着信ポート番号が1つ (TCP 443など) で済みます。



データベース要件

Deep Security Managerは、データベースと同じネットワーク上に配置し、接続速度が1Gbps以上のLANを使用する必要があります。WAN経由での接続はお勧めしません。Deep Security Managerはデータベースを使用して機能します。待ち時間が増えると、Deep Security Managerのパフォーマンスと可用性に重大な悪影響が出る可能性があります。

要件はデータベースの種類によって異なります。"[システム要件](#)" on page 184と"[Deep Security Managerで使用するデータベースの準備](#)" on page 206を参照してください。

Deep Securityを新規にインストールするときは、インストーラを実行する前に、Deep Security Managerのデータを格納するデータベースに対する権限を作成して付与します。

注意:

Microsoft SQL Serverを使用する場合は、Deep Security ManagerがMicrosoft Active DirectoryドメインまたはSQLユーザとして接続する必要があります。Windowsのワークグループ認証はサポート対象外になりました。

警告:

Microsoft SQL Server Expressは、特定の限られた構成でのみサポートされます。詳細については、"[Microsoft SQL Server Expressに関する注意事項](#)" on page 216を参照してください。

Microsoft SQL Server 2008を使用していて、Deep Security Managerをアップグレードする場

Trend Micro Deep Security(オンプレミス) 12.0

合は、データベースをサポートされているバージョンにアップグレードしてからDeep Security Managerをアップグレードすることをお勧めします。

サポートされているデータベースへの移行

データベースに互換性がない場合は、サポートされているデータベースに移行してからDeep Security Manager 12.0をインストールする必要があります。

Deep Securityをアップグレードする場合は、Deep Security Manager 12.0をインストールする準備ができるまでに発生したデータを引き続き保存するために、現在のソフトウェアと将来のソフトウェアの両方と互換性のあるデータベースに移行します。各バージョンでサポートされているデータベースについては、[システム要件](#)を参照してください。

たとえば、現在Microsoft SQL Server 2008データベースとDeep Security Manager 10.0を使用している場合は、まずデータベースをSQL Server 2014 (Deep Security Manager 10.0と12.0の両方でサポートされているため)に移行してから、Deep Security Manager 12.0にアップグレードします。

1. Deep Security Managerのサービスを停止します。

Deep Security Agentは、Managerの停止中も引き続き現在の保護ポリシーを使用します。

2. データベースをバックアップします。
3. 次のデータベース接続設定ファイルをバックアップします。

```
[Deep Securityのインストールディレクトリ]/webclient/webapps/ROOT/WEB-INF/dsm.properties
```

4. 現在のDeep Security ManagerのバージョンとDeep Security 12.0の両方でサポートされているデータベースに移行します。
5. 移行の際に既存のデータベースが保持されなかった場合は、新しいデータベースエンジンにデータベースのバックアップを読み込みます。
6. 必要に応じて、移行後のデータベースを使用するようにdsm.propertiesを編集します。
7. Deep Security Managerサービスを再起動します。

リモートSQLクエリタイムアウトの変更

Microsoft SQL Serverデータベースを使用する場合、[SQL Management Studio]→[サーバーのプロパティ]→[接続]→[リモートクエリのタイムアウト]に移動し、[0] (タイムアウトなし) を選択します。この設定により、各データベーススキーマの移行処理に時間がかかっても、アップグレード時にデータベース接続がタイムアウトしなくなります。

Agentベースの保護とAgentレスによる保護のどちらを使用するかを選択する

Deep Securityを新規にインストールするときは、仮想マシンを保護する方法について、Deep Security AgentをインストールせずにDeep Security Applianceを使用して保護を提供するか、両方を使用して保護を提供する(「コンバインモード」)かを選択します。"[Agentレスによる保護またはコンバインモードの保護の選択](#)" on page 315と"[vCloud環境でのAgentレスによる保護の実施](#)" on page 354を参照してください。

サポート対象OSをインストールする

サーバのオペレーティングシステム(OS)がDeep Security Manager 12.0でサポートされていない場合、Managerのインストール前に[サポート対象OSをインストールする](#)必要があります。

複数ノード環境をアップグレードする場合は、ロードバランサがあるかどうかによって、ダウンタイムなしでサーバを別のOSに移行できる場合があります。

たとえば、Windows 2003でDeep Security Manager 9.5をすでに使用している場合、OSを移行するには、次の手順を実行します。

1. Windows Server 2012 (64-bit) など、Deep Security Manager 9.5と12.0の両方でサポートされている新しいOSを実行しているManagerノードを追加します。

ヒント: Deep Security Managerの各バージョンでサポートされるOSのリストについては、[システム要件](#)を参照してください。

新しいノードを追加するには、Windows 2012 ServerでDeep Security Manager 9.5インストーラを実行します。インストーラウィザードでデータベース画面が表示された場合は、他のDeep Security Managerノードと同じデータベース接続設定を入力します。次の画面では、追加する新しいManagerノードを指定できます。または、サイレントインストールを実行して新しいノードを追加することもできます。手順については、"[Deep Security Managerのサイレントインストール](#)" on page 255を参照してください。

2. すべてが正常に動作していることを確認します。
3. Deep Security Managerで、[管理]→[Managerのノード] に移動し、古いWindows 2003ノードを右クリックして、[廃止] を選択して削除します。
4. 廃止したノードのOSをアップグレードしてから、プールに戻します。
5. サポートされていないOSを使用している他のすべてのノードに対して、この手順を繰り返します。

サポート対象外のDeep Security Managerをアップグレードする

インストーラは、Deep Security Managerの最新の2つのメジャーリリース（11.0および10.0.）からのアップグレードをサポートしています。

管理者が古い場合、インストーラは続行できません。最初にManagerをサポート対象バージョンにアップグレードする必要があります。その後、Deep Security Manager 12.0をインストールできます。

サポートされていないバージョンからサポートされるバージョンへのアップグレード方法については、[サポートされていないバージョンのインストールドキュメント](#)を参照してください。

サポートされていないRelayをアップグレードする

使用しているRelayが[最小システム要件](#)を満たしていない場合は、Manager自体をアップグレードする前に、Relayをアップグレードして新しいバージョンのManagerとの互換性を確保する必要があります。互換性のないバージョンがある場合は、構成の一部に障害が発生するためインストーラから警告が表示されますが、ある特定のRelayに互換性がない場合でもインストールは停止されません。これにより、そのRelayが現在使用されていない場合やオフラインの場合に作業を続行できます。

注意: Deep Securityには64ビットのRelayが必要です。

サポートされているバージョンにアップグレードする方法については、[のそれらのバージョンのインストールドキュメント](#)を参照してください。

Managerをアップグレード後に新しい機能を使用するには、RelayをDeep Security Relay 12.0に再度アップグレードします。

VMwareの要件

Agentレスによる保護やコンバインモードの保護を使用する場合は、新しいDeep Securityをインストールする前に、次の手順に従って[互換性のあるVMwareコンポーネントをインストール](#)します。

アップグレードする場合で、既存のApplianceに新しいDeep Securityとの互換性がない場合は、互換性のあるバージョンをインストールする手順も実行します。

- vSphere or ESXi — ESXi 6.0以降が必要です。

- vCNS - vCloud Networking& Security (vCNS) はサポートされていません。Deep Security Virtual Applianceを使用したAgentレスによる不正プログラム対策と変更監視でvCNSインフラストラクチャを使用している場合は、VMwareがvCNSのサポートを終了したため、Deep Security Manager12.0でもサポートされません。VMwareの新しいソリューションであるNSXにvCNSをアップデートする必要があります。

次のいずれかを使用します。

- NSX AdvancedまたはEnterpriseライセンス - Agentレスによるすべての保護機能。Deep SecurityVirtual Appliance 10.0以降およびESXi 6.0以降が必要です。
- NSX vShield EndpointまたはStandardライセンス - Agentレスによる不正プログラム対策および変更監視のみ(ネットワーク保護: ファイアウォール、侵入防御、Webレピュテーションなし)。また、Deep Security ManagerとNSX ManagerまたはvCenterを手動で同期して、NSXセキュリティグループのメンバーシップを特定する必要があります。Deep SecurityVirtual Appliance 10.0以降およびESXi 6.0以降が必要です。または、ネットワーク保護機能を含めた完全な保護を行うには、各ゲスト仮想マシンにVirtual Applianceに加えてDeep SecurityAgentを配置します (「コンバインモード」)。

vCNSのアップグレード時には、ESXiサーバごとにネットワークフィルタドライバをNetX APIに置き換えることも必要です。各ゲスト仮想マシン上のEPSec用のVMware Toolsドライバもアップグレードが必要です。新しいドライバの名前はGuest Introspectionです。

- NSX — NSX 6.3以降が必要です。
- Deep SecurityVirtual Appliance — Deep Security Virtual Appliance 10.0以降が必要です。[最小システム要件](#)および"[Deep Security Virtual Applianceのアップグレード](#)" on [page 1006](#)を参照してください。

Virtual Applianceをアップグレードする

互換性のないバージョンのVirtual Applianceがある場合は、構成の一部に障害が発生するためインストーラから警告が表示されますが、ある特定のApplianceに互換性がない場合でもインストールは停止されません(これにより、そのVirtual Applianceが使用されていない場合やオフラインの場合に作業を続行できます)。ただし、互換性のないバージョンのESXi、vShield Manager、NSX Managerがある場合は、インストールを続行できません。

VMwareの依存関係が存在します。互いに互換性のあるバージョンを選択する必要があります。互換性のあるバージョンを簡単に選択するには、トレンドマイクロのサポートのVMware互換性マトリックス (リリースごとにアップデート) を参照してください。

<https://success.trendmicro.com/solution/1060499>

警告: あるインフラストラクチャコンポーネントを他のコンポーネントと互換性のないバージョンにアップグレードして接続が失われることがないように、およびダウンタイムを最小限にするために、次の順序でアップデートします。

1. [vCenterデータベースをバックアップします](#)。方法はバージョンおよびストレージによって異なります。
2. [vCenterをアップグレードします](#)。
3. アップグレードする場合は、Deep Security Managerで、[コンピュータ]に移動します。AgentレスのコンピュータまたはコンバインモードのAgentを無効にします。

Deep Security Virtual Applianceを無効にします。

NSX Managerで、各ESXi上のVirtual Applianceも削除します。

ヒント: または、NSX、ESXi、Virtual Applianceのアップグレード中も保護を継続するために、Agentベースの保護を代わりに使用するようコンピュータを設定します。そうしないと、ApplianceとAgentを再度インストールして有効にするまでは、コンピュータは保護されません。

4. 保護されているゲスト仮想マシン (存在する場合) で、VMware Tools EPSecドライバをアンインストールします。ESXiサーバで、VMsafe-net API (ネットワークフィルタドライバ) をアンインストールします。

Deep Security Managerで、vShield ManagerまたはNSX 6.2.3以前 (vCenterではない) を切断します。

次に、[vShield Managerまたは古いNSXバージョンをNSX 6.3.xにアップグレードします](#)。

旧式のvShield Managerやそのコンポーネント (Filter Driverなど) がなく、NSX 6.3.x以降がある場合は、この手順をスキップしてください。

警告: vShield ManagerをNSXに置き換える必要があります。置き換えないと、設定済みのAgentレスによる保護はすべてDeep Security 12.0へのアップグレード後に機能しなくなります。これにより、保護対象のコンピュータのセキュリティが危険にさらされる可能性があります。

5. [ESXiをアップグレードします](#)。

アーキテクチャによっては、次のアップグレードも必要な場合があります。

- [dvSwitch](#)
- [vShield App \(NSX Distributed Firewallに\)](#)
- [vShield Edge](#)

6. Deep Security Managerのインストーラを実行します ("インストーラを実行する" on [page 237](#)を参照)。
7. [手順4](#)でNSX Managerを切断した場合は、Deep Security Managerで、[コンピュータ]→[vCenter] に移動します。NSX Managerを再接続します。[接続テスト] をクリックして接続を確認します。

これで、「Trend Micro Deep Securityサービス」がNSX Managerに追加されます。

8. Deep Security Virtual Applianceで不正プログラムなどのファイルベースの脅威から仮想マシンを保護するには、[Guest Introspectionをインストール](#)します。

VMware Tools 5.xのVMware vShield Endpointドライバは、NSX 6.2.4以降ではGuest Introspectionという名前に変更されています。

9. 保護対象のゲスト仮想マシンごとに、不正プログラムなどのファイルベースの脅威から保護するには、VMware Toolsのカスタムインストールを実行します。NSX File Introspectionオプションが選択されていることを確認します(vSphereドキュメントの [「VMware Tools のインストール」](#)を参照)。

警告: VMware Toolsをインストールする必要があります。そうしないと、Deep Security Managerは、仮想マシンの正しいホスト名とIPアドレスを取得できません。Managerが正しくないデータをTrend Micro Apex Centralに転送した場合、Apex Centralはそのエンドポイントを表示できません。

10. NSX Managerで、各ESXiに[新しいDeep Security Virtual Applianceを配信](#)します。このApplianceをアップグレードする場合は、"[Appliance SVMに組み込まれているAgentをアップグレードし、OSパッチを適用する](#)" on [page 1028](#)を参照してください。

注意: Virtual ApplianceのVMware Toolsはアップグレードしないでください。互換性のあるバージョンと一緒にパッケージされているため、アップグレードすると接続できなくなる場合があります。

通信が成功しても、「VMware Network Fabric」のサービス依存関係のアラートが表示される場合があります。このアラートを消去するには、[Failed] をクリックしてから [Resolve] をクリックします。

11. ESXiとNSXが統合され、通信していることを確認します。

12. [NSXセキュリティグループを作成します。](#)

vShield EndpointまたはStandardライセンスを使用している場合は、Deep Security ManagerとvCenterまたはvShield Endpointを手動で同期し、NSXセキュリティグループメンバーシップを取得して保護を開始します。

13. [NSXセキュリティポリシーを作成](#)します。

仮想マシンがセキュリティグループを変更する可能性がある場合は、[NSXセキュリティポリシーの自動管理](#)を設定するか、「Deep SecurityポリシーのNSXとの同期」 on page 364

14. vCloud仮想マシンのAgentレスによる保護を有効にします ("vCloud仮想マシンのAgentレスによる保護を有効にする" on page 355を参照)。

Deep SecurityでVMware vCloudリソースを使用できるように設定します ("Deep SecurityでVMware vCloudリソースを使用できるように設定する" on page 356を参照)。

15. [新しいDeep Security Virtual Applianceをインストールして有効化](#)します。

(Deep Security Virtual Applianceのアップグレードについては、「Deep Security Virtual Applianceのアップグレード」 on page 1006を参照)。

High Availability (HA) 用にVMware Distributed Resource Scheduler (DRS) を使用している場合は、[優先順位ルールを使用して](#)各Virtual Applianceを特定のESXiホストに「ピンニング」します。

16. [新しいDeep Security Agentをインストールして有効化](#)します。

NSXにNSX vShield EndpointまたはStandardライセンスがある場合、ネットワークベースの保護機能 (ファイアウォール、侵入防御、Webレピュテーション) は、新しいNSXライセンスではサポートされません。保護を維持してこれらの機能を提供するには、Agentをコンバインモードで設定します。セキュリティ機能が再度有効になったことを確認するために、各機能の設定をテストできます。

<https://success.trendmicro.com/solution/1098449>

ヒント: ファイアウォール機能はNSX Distributed Firewallを使用して提供できます。Deep Security12.0のファイアウォールは無効にすることができます。または、NSX Distributed Firewallから仮想マシンを除外し、代わりにDeep Securityのファイアウォールを使用することもできます ([「ファイアウォールによる保護からの仮想マシンの除外」](#)を参照)。

アップグレードを実行していて新しい機能を使用したい場合は、Deep Security Manager 12.0のインストール後にVirtual Appliance、Agent、RelayもDeep Security 12.0にアップグレードします。

協調的保護からコンバインモードへの変換

- 協調的保護: Deep Security 9.5では、仮想マシン上のAgentがオフラインの場合、代わりにDeep Security Virtual Applianceから保護機能が提供されます。ただし、各機能についてどちらを使用するかを個別に設定することはできません。
- コンバインモード: Deep Security 9.6では、それぞれの保護機能について、AgentまたはApplianceのどちらを使用するかを個別に設定できます。ただし、優先する保護ソースがオフラインの場合、もう一方の保護ソースが代わりに使用されることはありません。

Deep Security 10.0以降では、「保護ソース」の設定で両方の動作を設定できます。

- 各機能をAgentとApplianceのどちらから提供するか
- 優先する保護 (AgentまたはAppliance) を利用できない場合にもう一方を代わりに使用するかどうか

そのため、以前の協調的保護と同様の動作が必要な場合、Deep Security 9.6にアップグレードするのではなく、Deep Security 9.5からDeep Security 10.0にアップグレードしてから12.0にアップグレードすることをお勧めします。

VMware HAへのApplianceのピンニング

[Agentレス](#)の保護を実装するケースで、VMware Distributed Resource Scheduler (DRS) を使用してHigh Availability (HA) 環境を構築する場合は、Deep Securityをインストールする前に設定します。次に、すべてのESXiハイパーバイザ (バックアップハイパーバイザを含む) にDeep Security Virtual Applianceをインストールして、各ESXiサーバに「ピンニング」優先順位設定を使用します。これにより、HAフェイルオーバー後もAgentレスによる保護が適用されます。

警告: DRSによってApplianceのあるESXiからApplianceのないESXiに仮想マシンが移動された場合、その仮想マシンは保護されなくなります。その後仮想マシンが元のESXiに戻っても、vMotionによってApplianceのあるESXiに仮想マシンが移動されたときに仮想マシンを再び有効化して保護するイベントベースタスクを作成しないかぎり、その仮想マシンは保護されません。詳細については、"[コンピュータの追加または変更時のタスクの自動実行](#)" on [page 482](#)を参照してください。

注意: ApplianceにはvMotionを適用しないでください。各Applianceは固有のESXiサーバに固定します。DRS設定では、[Disabled] (推奨) または [Manual] を選択します。(または、共有ストレージではなくローカルストレージにApplianceをインストールします。Virtual Applianceがローカルストレージにインストールされている場合、DRSはvMotionを適用しません)。詳細については、VMwareのドキュメントを参照してください。

サポートされていないAgentをアップグレードする

使用しているAgentが[最小システム要件](#)を満たしていない場合は、Manager自体をアップグレードする前に、Agentをアップグレードして新しいバージョンのManagerとの互換性を確保する必要があります。互換性のないバージョンがある場合は、構成の一部に障害が発生するためインストーラから警告が表示されますが、ある特定のAgentに互換性がない場合でもインストールは停止されません。これにより、そのAgentが現在使用されていない場合やオフラインの場合に作業を続行できます。

サポートされているバージョンにアップグレードする方法については、[のそれらのバージョンのインストールドキュメント](#)を参照してください。

Managerをアップグレード後に新しい機能を使用するには、AgentをさらにDeep Security Agent 12.0に再度アップグレードします。

インストーラを実行する

環境の準備が完了したら、最新のパッチがある場合はそれらをインストールしてから、root、スーパーユーザ、または (Windowsの場合) 管理者としてインストーラを実行します。次のいずれかを使用できます。

- 対話形式のインストーラ (ウィザードに従って実行)
- サイレントインストーラ ("[Deep Security Managerのサイレントインストール](#)" on [page 255](#)を参照)

Microsoft SQL Serverを使用する場合、Deep Security Managerの接続設定は認証の種類によって異なります。

- SQL Server: ユーザ名とパスワードを入力します。
- Active Directory: ユーザ名 (ドメインなし) とパスワードを入力し、[詳細] をクリックして [ドメイン] を別途入力します。Kerberos認証またはWindowsドメイン認証とも呼ばれます。

["SQL Serverドメイン認証の問題"](#) on page 1552も参照してください。

iptablesが有効になっているLinuxにDeep Security Managerをインストールする場合は、Agentのハートビートポート番号および管理トラフィックを許可するようにiptablesの設定も行います。 ["ポート番号、URL、およびIPアドレス"](#) on page 190を参照してください。

新しいDeep Security Managerにアップグレードする場合で、新しい機能を使用するには、Virtual Appliance、Agent、およびRelayをManagerも同じバージョンにアップグレードします。

複数ノードでDeep Security Managerを実行する

大規模環境での高可用性とスケーラビリティを確保するために、[ロードバランサを使用](#)して、同じバージョンのDeep Security Managerを、同じマスターキー (設定されている場合) を持つ複数のサーバ (ノード) にインストールします。これらのノードを同じデータベースストレージに接続します。

同じデータベースを使用するすべてのノードで、同じソフトウェアバージョンを使用する必要があります。これにより、データの互換性が確保され、保護対象のコンピュータを一貫した方法で処理できます。また、すべてのノードが同じマスターキー (設定されている場合) を使用し、そのキーを常に使用できるようにしておく必要があります。これにより、すべてのノードが、暗号化された設定プロパティと個人データを必要に応じて復号化して読み取ることができます。詳細については、[「masterkey」](#)を参照してください。

警告: 複数のノードで同時にインストーラを実行しないでください。アップグレードを同時に実行すると、データベースが破損する可能性があります。その場合は、バックアップからデータベースを復元するか (アップグレードの場合)、データベースを再作成 (新規インストールの場合) してから、インストーラをもう一度開始する必要があります。

複数ノードのDeep Security Managerをアップグレードする場合は、次の手順を実行します。

1. すべてのノードを停止します。
2. 最初に1つのノードでインストーラを実行します。

最初のノードのアップグレードが完了すると、そのノードはサービスを開始します。他のノードがアップグレードされるまでは、このノードのソフトウェアだけがデータベースと互換性があるため、最初は唯一利用可能なManagerとなります。このノードがすべてのジョブを実行する必要があるため、この間はパフォーマンスが低下する場合があります。[管理]→[システム情報]の[アクティビティグラフ付きネットワークマップ]に、他のノードがオフラインであり、アップグレードが必要なことが表示されます。

3. 他のノードをアップグレードします。

アップグレードしたノードはオンラインに戻り、負荷の共有を再開します。

4. カスタムのマスターキーを設定した場合は、[masterkey](#)コマンドを実行して、既存のデータをいずれか1つのノードでのみ暗号化します。

警告: 複数のノードで同時にインストーラを実行しないでください。アップグレードを同時に実行すると、データベースが破損する可能性があります。破損した場合は、データベースのバックアップを復元し、再度アップグレードを開始する必要があります。

インストールやアップグレードのその他の手順は、サーバが1台か複数かにかかわらず同じです。

LinuxにDeep Security Managerをインストールする

コマンドラインを使用して[サイレントインストール](#)を実行するか、X Windowsをインストールしている場合は対話形式のインストーラを使用できます。

1. インストールパッケージを実行します。セットアップウィザードの指示に従います。
2. サーバにインストールされている既存のDeep Security Managerが検出されます。次のいずれかを選択します。
 - 新規インストール (既存または新規のデータベースを使用可能): Deep Securityソフトウェアをインストールします。データベースを初期化します。
 - アップグレード: 新規のDeep Securityソフトウェアをインストールしますが、既存のコンピュータの詳細、ポリシー、侵入防御ルール、ファイアウォールルールなどは維持します。必要に応じてデータを新しい形式に移行します。

警告: [新規インストール (既存または新規のデータベースを使用可能)] を選択すると、以前のインストールからすべてのデータが削除されます。

3. iptablesが有効な場合は、ルールを設定して、Agentのハートビートおよび管理トラフィックのポート番号からの受信接続を許可します。"[ポート番号、URL、およびIPアドレス](#)" on page 190も参照してください。

Deep Security ManagerをWindowsにインストールする

コマンドラインを使用して[サイレントインストール](#)を実行するか、対話形式のインストーラを使用できます。

1. インストールパッケージを実行します。セットアップウィザードの指示に従います。
2. サーバにインストールされている既存のDeep Security Managerが検出されます。次のいずれかを選択します。
 - 新規インストール (既存または新規のデータベースを使用可能): Deep Securityソフトウェアをインストールします。データベースを初期化します。
 - アップグレード: 新規のDeep Securityソフトウェアをインストールしますが、既存のコンピュータの詳細、ポリシー、侵入防御ルール、ファイアウォールルールなどは維持します。必要に応じてデータを新しい形式に移行します。

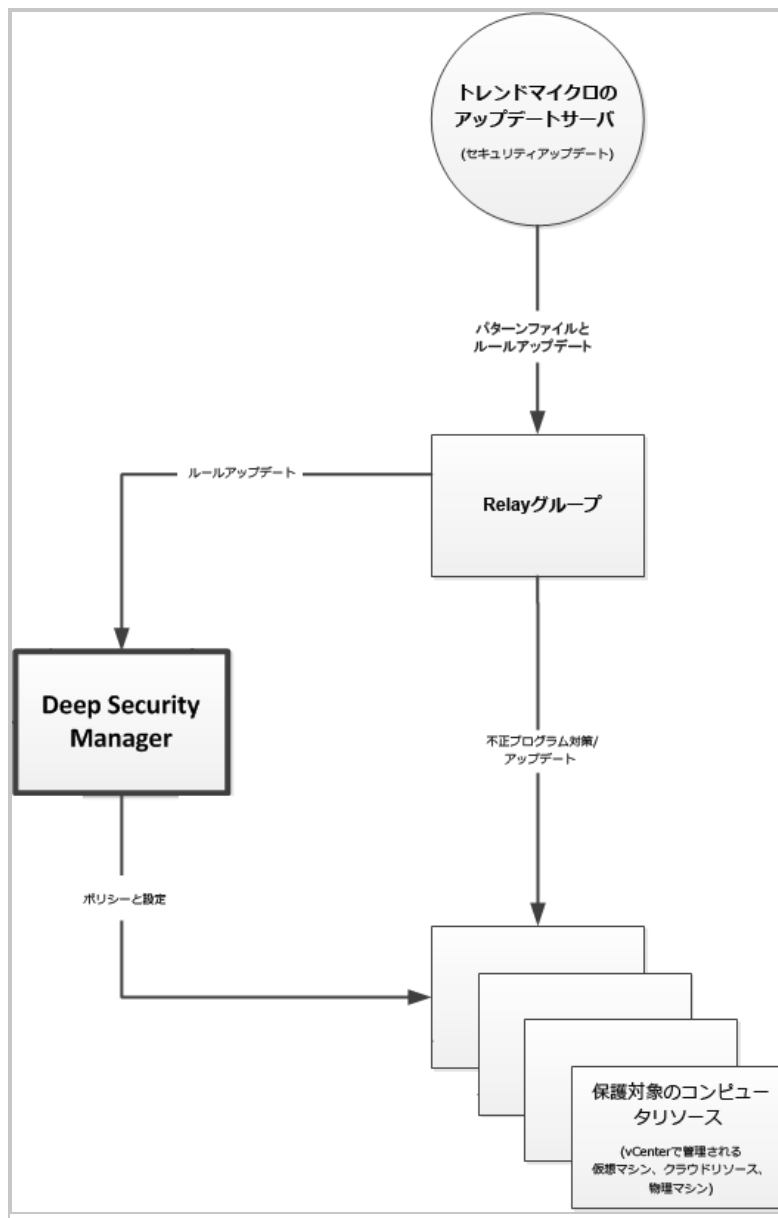
警告: [新規インストール (既存または新規のデータベースを使用可能)] を選択すると、以前のインストールからすべてのデータが削除されます。

Deep Security ManagerのサーバにRelayをインストールする

Deep SecurityにはRelayが少なくとも1つ必要です。Relayは保護対象のコンピュータに[セキュリティアップデート](#)を配布します。Relayの詳細については、"[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照してください。

Deep Security Managerインストーラを実行すると、Agentインストーラの完全なZIPパッケージ用にローカルディレクトリを検索します。(Relayはその機能を有効にしたAgentです。)見つからなかった場合は、Managerのインストーラがインターネット上にあるトレンドマイクロのダウンロードセンターからダウンロードします。

- どちらかの場所でAgentインストーラが見つかった場合、Managerのインストーラは、最新のRelayをインストールするよう提案します。



ヒント:

次の理由から、トレンドマイクロではサーバ上にRelayをインストールすることを推奨します。

- ManagerにとってローカルなRelayを提供する。
- Relayがインストールされた古いコンピュータを廃止した場合も、少なくとも1つのRelayが常に使用可能となる。

警告: ManagerのインストーラがAgentをそのサーバに追加しても、Relay機能が有効になるだけです。セキュリティの初期設定は適用されません。サーバを保護するには、Deep Security Managerで自身のAgentに[セキュリティポリシーを適用](#)します。

- Agentインストーラが見つからない場合は、ダウンロードして、[AgentやRelayを後からインストール](#)できます。

スキーマのアップデート

Deep Security Manager 9.6までとは異なり、アップデートの場合にデータベース管理者 (DBA) が最初に手動でデータベーススキーマをアップデートする必要はありません。データベーススキーマの変更は、必要に応じてインストーラで自動的に実行されます。この処理が何らかの理由で中断された場合は、バックアップからデータベースを復元して再試行してください。処理が中断する原因はいくつか考えられますが、負荷の上昇やネットワークのメンテナンスなど、その多くは一時的なものです。問題が解決しない場合は、サポート担当者に問い合わせてください。エラーが発生した場合、ログは次の場所に保存されます。

<インストールディレクトリ>/DBUpgrade/SchemaUpdate

<インストールディレクトリ> は、初期設定では/opt/dsm (Linux) またはC:\Program Files\Trend Micro\Deep Security Manager (Windows) です。次の2種類のファイルが作成されます。

- T-00000-Plan.txt - インストーラがスキーマのアップデートに使用するすべてのデータ定義言語 (DDL) SQL文。
- T-00000-Progress.txt - スキーマのアップデートの進捗状況ログ。処理が完了すると、ファイル名がT-00000-Done.txt (アップデートに成功した場合) またはT-00000-Failed.txt (アップデートに失敗した場合) に変更されます。

t0 (ルートテナント) でスキーマのアップデートに失敗した場合、インストーラの処理は中止されます。バックアップからデータベースを復元して再試行する必要があります。

ただし、マルチテナントが有効になっている場合は、ルート以外のテナントでアップグレードに失敗してもインストーラの処理は続行されます。それぞれの種類のログファイルがテナントごとに1つずつ作成され、テナントt1の場合は「00001」のように、テナント番号を示す「00000」の部分が変更されます。バックアップからデータベースを復元して再試行するか、該当するテナントのスキーマのアップデートを再試行できます (「マルチテナントを強制的にアップグレードする」を参照してください)。

マルチテナントデータベースの強制アップグレード

マルチテナント環境のDeep Security Managerをアップグレードする手順は次のとおりです。

1. インストーラがデータベーススキーマをアップデートします。
2. インストーラが、プライマリテナント (t0) 用の新しい構造にデータを移行します。
t0の移行が失敗した場合、インストーラは回復できません。この場合、処理は停止します。バックアップからデータベースを復元し、再度実行する必要があります。
3. インストーラが、他のテナントのデータを移行します (5個ずつのバッチで)。
プライマリ以外のテナントの移行が失敗してもインストーラは処理を続行しますが、[管理]→[テナント]にはこれらのテナントの状態が [データベースのアップグレードが必要 (オフライン)] と表示されます。バックアップから復元してインストーラを再度実行するか、該当するテナントの移行を再試行できます。

テナントの移行を再試行するには、テナントのインターフェースを使用します。強制的な再試行がうまくいかない場合は、サポート担当者に問い合わせてください。

失敗したアップグレードをロールバックする

アップグレードでのDeep Security Manager 12.0のインストールで問題が発生しても、次の場合はすぐに正常な状態に戻すことができます。

- アップグレード前にデータベースをバックアップしている。
 - Agent、Relay、Virtual Applianceをアップグレードしていない (またはアップグレード前に作成した仮想マシンスナップショットやシステムバックアップがある)。
1. Deep Security Managerのサービスを停止します。
 2. データベースを復元します。
 3. Deep Security Managerのすべてのサーバノードを復元します。
 4. アップグレード中にDeep Security Managerのホスト名、FQDN、またはIPアドレスを変更した場合は、それらを復元します。
 5. Agent、Relay、Virtual Applianceを復元します。
 6. Deep Security Managerのサービスを開始します。
 7. ManagerとAgentの間の接続も含めて、Deep Security Managerへの接続を確認します。

インストーラ実行後の処理

インストーラの処理が完了すると、「Trend Micro Deep Security Manager」サービスが自動的に開始されます。Deep Security ManagerのGUIにログインするには、Webブラウザを開いて次のアドレスにアクセスします。

```
https://[host_name]:[port]/
```

[host_name] はDeep Security ManagerをインストールしたサーバのIPアドレスまたはドメイン名で、[port] はインストール時に指定したManagerのポートです。

最後に次のコンポーネントをインストールすれば完了です。

1. Relay
2. Virtual Appliance (ある場合)
3. Agent (ある場合)

注意: Relay、Appliance、およびAgentを12.0にアップグレードする場合は、先にDeep Security Manager 12.0にアップグレードしてください。バージョンがManagerと同じかそれ以下でないと、ManagerをアップグレードするまではManagerと通信できないことがあります。

自己署名証明書

Deep Securityを新規にインストールする場合、インストーラによって自己署名サーバ証明書が作成されます。この証明書は、Deep Security ManagerがAgent、Appliance、Relay、およびWebブラウザとの安全な接続で自身の証明に使用します。有効期間は10年です。ただし、この証明書には信頼できる認証局の署名がないため、Managerを自動で認証することはできず、Webブラウザに警告が表示されます。このエラーメッセージが表示されないようにするとともにセキュリティを強化するには、Deep Securityのサーバ証明書を信頼できる認証局によって署名された証明書に置き換えます。認証局の証明書の使用については、"[Deep Security Manager TLS証明書の置き換え](#)" on page 1057を参照してください。

アップグレードでは、Managerの既存のサーバ証明書が保持されます。新規インストールの場合を除き、毎回インストールし直す必要はありません。

暗号化を強化する

アップグレードでは、Managerの既存のサーバ証明書が保持されます。新規インストールの場合を除き、毎回インストールし直す必要はありません。ただし、暗号化が強力でないと、通常はコンプライアンスを満たせません。攻撃コードや高速なブルートフォース攻撃には、古い認

証方式、暗号化方式、およびプロトコルを標的にしたものが含まれます。これには、SHA-1も含まれます。そのため、いずれにせよDeep Securityの証明書の置き換えが必要になる可能性があります。"[Deep Securityの暗号化アルゴリズムのアップグレード](#)" on page 1498および"[Deep Security Manager TLS証明書の置き換え](#)" on page 1057を参照してください。

イベントデータの移行

アップグレードの場合、データベーススキーマの変更は必要に応じてインストーラで自動的に実行されます。そのうえで、保護対象コンピュータのデータが新しいスキーマに移行されます。

データベースにはイベントデータも含まれています。イベントデータは、インストーラで保持するように選択したデータの量によっては大量になることがあります。ただしイベントデータはポリシーおよびコンピュータの管理機能には必要でないため、インストーラではすべてのイベントデータが移行されるのを待たずに処理が進められます。

その後インストーラを終了するとDeep Security Managerサービスが再起動され、古いイベントデータの新しいスキーマへの移行が続行されます。画面下部のステータスバーに、新しいイベントおよびアラート(エラーが発生した場合)と一緒に進捗状況が表示されます。移行が完了するまでの時間は、データの量、ディスク速度、RAM、および処理能力によって異なります。

移行処理の実行中も、新しいイベントデータは通常どおり記録され、利用できます。

注意: データベースアップグレードの移行が完了するまで、古いシステムイベントデータの表示は不完全になる可能性があります。

RelayをLinuxでアップグレードする (dpkg)

dpkgパッケージマネージャ (DebianまたはUbuntu) を使用するLinuxディストリビューションに関しては、コマンドは同じです。

1. [管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]の順に選択します。Deep Security Agentソフトウェアをダウンロードします ("[Deep Security Agentソフトウェアの入手](#)" on page 372を参照)。
2. [コンピュータ]に移動します。
3. アップグレードするコンピュータを探します。
4. コンピュータを右クリックして、[処理]→[Agentソフトウェアのアップグレード]を選択します。

新しいAgentソフトウェアがコンピュータに送信され、Relayがアップグレードされます。

または、Agentのインストーラファイルをコンピュータに手動でコピーして実行します。

- a. Agentのインストーラファイルをコンピュータにコピーします。

次のコマンドを入力します。

- b. `sudo dpkg -i <インストーラファイル>`

RelayをLinuxでアップグレードする (rpm)

RPMパッケージマネージャ (Red Hat、CentOS、Amazon Linux、Cloud Linux、SUSE) を使用するLinuxディストリビューションに関しては、コマンドは同じです。

1. [管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター] の順に選択します。Deep Security Agentソフトウェアをダウンロードします ("[Deep Security Agentソフトウェアの入手](#)" on page 372を参照)。
2. [コンピュータ] に移動します。
3. アップグレードするコンピュータを探します。
4. コンピュータを右クリックして、[処理]→[Agentソフトウェアのアップグレード] を選択します。

新しいAgentソフトウェアがコンピュータに送信され、Relayがアップグレードされます。

または、Agentのインストーラファイルをコンピュータに手動でコピーして実行します。

- a. Agentのインストーラファイルをコンピュータにコピーします。

次のコマンドを入力します。

- b. `sudo rpm -U <インストーラのrpm>`

(「-U」引数は、インストーラでアップグレードを実行するように設定します。)

RelayをWindowsでアップグレードする

1. Deep Security Managerで、[設定]→[一般]→[Agentセルフプロテクション] の順に選択します。
2. Agentでアップグレードが許可されるように、Agentセルフプロテクションを無効にします。
3. [コンピュータ] に移動します。
4. アップグレードするコンピュータを探します。
5. コンピュータを右クリックして、[処理]→[Agentソフトウェアのアップグレード] を選択します。

新しいAgentソフトウェアがコンピュータに送信され、Relayがアップグレードされます。

または、Agentのインストーラファイルをコンピュータに手動でコピーして実行します。ウィザードの指示に従います。

WindowsでAgentをアップグレードする

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。そうしないと、Relayのアップグレードが失敗する可能性があります。

1. Deep Security Managerで、[設定]→[一般]→[Agentセルフプロテクション]の順に選択します。
2. Agentでアップグレードが許可されるように、Agentセルフプロテクションを無効にします。
3. [コンピュータ]に移動します。
4. アップグレードするコンピュータを探します。
5. コンピュータを右クリックして、[処理]→[Agentソフトウェアのアップグレード]を選択します。

新しいAgentソフトウェアがコンピュータに送信され、Agentがアップグレードされます。

または、Agentのインストーラファイルをコンピュータに手動でコピーして実行します。ウィザードの指示に従います。

6. 不正プログラム対策が有効な場合に、Windows Server 2012以降 (またはWindows 8以降)でAgentをアップグレードしたときは、コンピュータを再起動します。

警告: 再起動するまでは、アップグレードは完了せず、保護が機能しない場合があります。

LinuxでAgentのアップグレードをする

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。そうしないと、Relayのアップグレードが失敗する可能性があります。

1. [管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]の順に選択します。Deep Security Agentソフトウェアをダウンロードします ("[Deep Security Agentソフトウェアの入手](#)" on page 372を参照)。
2. [コンピュータ]に移動します。
3. アップグレードするコンピュータを探します。
4. コンピュータを右クリックして、[処理]→[Agentソフトウェアのアップグレード]を選択します。

新しいAgentソフトウェアがコンピュータに送信され、Relayがアップグレードされます。

または、Agentのインストーラファイルをコンピュータに手動でコピーして実行します。

- a. Agentのインストーラファイルをコンピュータにコピーします。

RPMパッケージマネージャ (Red Hat、CentOS、Amazon Linux、Cloud Linux、SUSE) を使用しているコンピュータの場合は、次のコマンドを入力します。

- b. `sudo rpm -U <インストーラファイル>`

(「-U」引数は、インストーラでアップグレードを実行するように設定します。)

dpkgパッケージマネージャ (DebianまたはUbuntu) を使用しているコンピュータの場合は、次のコマンドを入力します。

```
sudo dpkg -i <インストーラファイル>
```

SolarisでのAgentのアップグレード

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。そうしないと、Relayのアップグレードが失敗する可能性があります。

Solaris上のDeep Security Agentをアップグレードする方法については、「"[Deep Security Agentのアップグレード](#)" on page 998」を参照してください。Deep Security Managerから「"[Agentのアップグレードを開始する](#)" on page 1000」ことも、「[Solaris上でAgentを手動でアップグレードする](#)" on page 1002」こともできます。

Deep Security Agentのセキュリティアップデートをダウンロードする

エージェントの最新のセキュリティ更新プログラムをダウンロードする必要があります。手順については、「[セキュリティアップデートの取得と配布](#)" on page 1039。

いくつかのプラットフォームでは、Deep Security Manager 12.0は古いバージョンをサポートしています。

- Deep Security Agent 9.0 (AIX 5.3、6.1、7.1、または7.2)

セキュリティアップデートパッケージの形式はバージョンによって異なります。初期設定では、ディスク容量を節約するために、Deep Security Relayはこれらの一般的ではないパッケージのダウンロードと配布は行いませんが、これらの古いバージョンが使用されている環境の場合は、このパッケージが必要になります。有効にするには、[管理]→[システム設定]→[アップデート]の順に選択します。[8.0および9.0のAgentのアップデートを許可]を選択します。

注意: Deep Security Agent 12.0ではないため、古いバージョンのAgentでは**新機能**はサポートされません。

AIX上のエージェントのアップグレード

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。そうしないと、Relayのアップグレードが失敗する可能性があります。

AIXでDeep Security Agentをアップグレードする方法については、"[Deep Security Agentのアップグレード](#)" on page 998のアップグレードを参照してください。"[Agentのアップグレードを開始する](#)" on page 1000のエージェントを手動でアップグレードしてください。

各保護機能をAgentとApplianceのどちらから提供するかを選択

コンピュータをApplianceまたはAgentで保護できる場合は、各保護機能をどちらが提供するかを選択できます。

注意: セキュリティログ監視とアプリケーションコントロールには、この設定はありません。VMwareの最新の統合テクノロジーでは、これらの機能をDeep Security Virtual Applianceから提供することはできません。

保護ソースを設定するには、VMware vCenterをDeep Security Managerにインポートしてから、**コンピュータエディタまたはポリシーエディタ**¹で、[設定]→[一般]の順に移動します。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

コンバインモードの場合の保護ソース

AgentとApplianceの両方が存在する場合に保護を提供するコンポーネントを選択してください。

不正プログラム対策:	継承 (Appliance優先)
Webレピュテーション / ファイアウォール / 侵入防御:	継承 (Agent優先)
変更監視:	継承 (Appliance優先)

ここに表示されていない保護モジュールでは、コンバインモードの設定はサポートされません。

各保護モジュールまたはモジュールグループに対して、次のいずれかを選択します。

- **Applianceのみ:**仮想マシンにAgentがあり、Deep Security Virtual Applianceが無効化または削除されている場合でも、Applianceからのみ保護を提供します。

警告: Scanner (SAP) が必要な場合、Applianceは使用しないでください。ScannerにはDeep Security Agentの不正プログラム対策が必要です。

ヒント: Agentで不正プログラム対策が有効になっている場合、Anti-malware Solution Platform (AMSP) がダウンロードされてサービスとして起動されます。このサービスが不要な場合は、**[不正プログラム対策]** で **[Applianceのみ]** を選択してください。これにより、Applianceが無効化されている場合でも、AMSPサービスが起動されることはありません。

- **Appliance優先:**ESXiサーバに有効化されたApplianceがある場合は、そのApplianceが保護を提供します。ただし、Applianceが無効化または削除された場合は、Agentが代わりに保護を提供します。
- **Agentのみ:** 有効化されたApplianceがある場合でも、Agentからのみ保護を提供します。
- **Agent優先:**仮想マシンに有効化されたAgentがある場合は、そのAgentが保護を提供します。しかし、有効化されたAgentがない場合は、Applianceが代わりに保護を提供します。

新しいDeep Security AgentまたはRelayをインストールする

新しい機能を使用するには、Deep Security AgentまたはRelay12.0をインストールする必要があります。ただし、最新の機能が不要な場合や旧システムとの互換性が必要な場合は、サポートされる任意のバージョンをインストールできます。各プラットフォームでサポートされ

るDeep Security Agentのバージョンについては、"[Deep Security Agentのプラットフォーム](#)" on page 182を参照してください。

Deep Security AgentとRelayのインストール手順はほとんど同じです。Relayとは、Relay機能を有効にしているDeep Security Agentのことです。RelayではAgentをより迅速にアップデートしたり、インターネット接続やWAN帯域幅を節約したりできます。Relayが1つ以上ある必要があります。RelayはトレンドマイクロおよびManagerからソフトウェアとセキュリティアップデートをダウンロードし、保護対象コンピュータに再配信します。

1. [管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]の順に移動します。
"[Deep Security Agentソフトウェアの入手](#)" on page 372します。

警告: サードパーティの配信システムを使用する場合でも、インストールされているすべてのDeep Security AgentソフトウェアをDeep Security Managerのデータベースにインポートする必要があります。Deep Security Agentを初めて有効化する際には、セキュリティポリシーで現在有効になっている保護モジュールだけがインストールされます。新しい保護モジュールを後から有効にすると、Deep Security AgentはDeep Security Managerからプラグインをダウンロードしようとしています。そのソフトウェアが見つからない場合、Agentは保護モジュールをインストールできないことがあります。

2. コンピュータにAgentソフトウェアをインストールします。これには複数の方法があります。
 - 手動インストール: コンピュータでインストールパッケージを実行し、有効化してポリシーを割り当てます。手順については、"[Deep Security Agentの手動インストール](#)" on page 376を参照してください。
 - インストールスクリプト: スクリプトをアップロードし、Linux/UnixシェルスクリプトまたはMicrosoft PowerShellを使用してインストーラを実行します。

注意: インストールスクリプトを使用する場合は、この手順の残りの操作は不要です。Agentのインストールは、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498の手順に従うと完了できます。

- Deep Security API: このAPIを使用して、コンピュータへのAgentのインストールを自動化するためのインストールスクリプトを生成します。Deep Security Automation Centerに [スクリプトを使用してDeep Security ManagerおよびAgent](#) を配信するを参照してください。

- SCCM: Microsoft System Center Configuration Manager (SCCM) を使用して、Agentのインストールと有効化からポリシーの適用までを実行できます。SCCMを使用するには、[管理]→[システム設定]→[Agent] の順に選択し、Agentからのリモート有効化を有効にします。
 - テンプレートまたはElastic Beanstalk: Agentを仮想マシンテンプレートに含めません。"[AgentのAMIまたはWorkSpaceバンドルへの統合](#)" on page 393および[AWS Elastic Beanstalkスクリプト](#)を参照してください。AWS Elastic Beanstalkスクリプト
3. Agentを有効化します ("[Agentの有効化](#)" on page 430を参照してください)。
 4. ポリシーをコンピュータに割り当てます ("[ポリシーをコンピュータに割り当てる](#)" on page 585を参照してください)。
 5. AgentをDeep Security Relayとして使用する場合は、"[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照してください。また、すでにWebサーバがある場合は、Relay有効化済みAgentではなくWebサーバ経由でAgentソフトウェアアップデートを提供できます。そのためには、Relay有効化済みAgentのソフトウェアリポジトリのミラーをWebサーバに作成する必要があります。独自のソフトウェア配布Webサーバの設定の詳細については、"[ソフトウェアアップデートを配布するWebサーバの使用](#)" on page 1047を参照してください。

Relayは、再配信するコンポーネントをダウンロードできる必要があります。Relayをテストするには、[管理]→[アップデート]→[セキュリティ] の順に選択します。[パターンファイルアップデート]と[ルールアップデート]の両方で、[アップデートを確認してダウンロード]をクリックします。

Relayがアップデートを確認する頻度を設定するには、[管理]→[予約タスク] の順に選択します。

警告: インストールにはRelayが少なくとも1つ必要です。AgentがRelayに接続できない場合は、重要なソフトウェアおよびセキュリティアップデートをダウンロードできません。

Deep SecurityManagerのインストール時、同じサーバにRelayを追加できます。追加しなかった場合は、少なくとも1つ以上の64ビットAgentでRelay機能を有効にします。Relayの数を確認するには、[管理]→[アップデート]→[Relayの管理] の順に選択し、各グループ内に含まれるRelayの数を調べます。詳細については、"[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照してください。

6. 古いAgentのセキュリティアップデートパッケージが必要な場合は、[管理]→[システム設定]→[アップデート]の順に選択し、[8.0および9.0のAgentのアップデートを許可]を選択します。

アラートを設定する

重要なシステムイベントが発生したときにDeep Security Managerから通知を受け取ることができます。

外部SIEMを使用している場合は、イベントを転送することもできます。[ポリシー]→[共通オブジェクト]→[その他]→[Syslog設定]に移動し、[管理]→[システム設定]→[イベントの転送]の順に選択します ("[Deep SecurityイベントをSyslogまたはSIEMサーバに転送する](#)" on page 1141を参照してください)。

1. [管理]→[システム設定]→[SMTP]の順に選択します。Deep Security Managerのメールサーバへの接続方法を設定します。
テストすると、「SMTPサーバへの接続テストに成功しました」というメッセージが表示されます。テストが失敗した場合は、[SMTP設定](#)を確認し、[必要なポート番号](#)での通信がサーバとネットワークで許可されていることを確認します。
2. [管理]→[ユーザ管理]→[ユーザ]の順に選択します。ユーザアカウントをダブルクリックし、[アラートメールを受信]を選択します。
3. [アラート]に移動し、[管理]→[システム設定]→[アラート]の順に選択します ("[アラートの設定](#)" on page 1091を参照してください)。各アラートをダブルクリックして、メール

を送信する条件を選択します。

一般

アラート情報

アラート: 不正プログラム対策アラート

説明: 1台以上のコンピュータで、アラートを発するように設定された不正プログラム検索設定によってイベントが発生しました。

消去可能: はい

オン
 オンのとき、条件を満たす場合、アラートが発令されます。

オプション



重要度:

(ルール設定に関係なく) すべてのルールでアラート

このアラートの発令時、通知のメールを送信する

このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

このアラートが存在しなくなったとき、通知のメールを送信する



オフ
 オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

推奨設定の検索を実行する

セキュリティポリシーをどのように設定すればよいかわからない場合は、Deep Security Managerで保護対象コンピュータを検索して脆弱なソフトウェアや設定を探し、推奨されるセキュリティ設定を確認することができます。[コンピュータ]に移動し、[処理]→[推奨設定の検索]の順に選択します ("[推奨設定の検索の管理と実行](#)" on page 592を参照してください)。

Deep Security Managerのサイレントインストール

ヒント: [Deep Security 12 - Linux - Silent Install](#) (YouTube) を視聴すると、Deep Security ManagerのサイレントインストールプロセスをRed Hat 7サーバで確認できます。

サイレントインストールのシステムチェックを実行する

インストーラをシステムチェックモードで実行すると、環境がDeep Securityのインストール要件を満たしているかどうかを確認できます。実際のインストールは実行されずにインストール環境に関するレポートが作成され、そのレポートに基づいてDeep Security Managerを実際にインストールする前に問題を修正することができます。

Windowsプラットフォームでサイレントシステムチェックを開始するには、インストールパッケージと同じフォルダでコマンドプロンプトを開いて、次のコマンドを入力します。

```
Manager-Windows-<Version>.x64.exe -q -console -Dinstall4j.language=<ISO code>-varfile <PropertiesFile> -t
```

Linuxプラットフォームでサイレントシステムチェックを開始するには、インストールパッケージと同じディレクトリで次のコマンドを入力します。

```
Manager-Linux-<Version>.x64.sh [-q] [-console] -t [-Dinstall4j.language=<ISO code>] [-varfile <PropertiesFile>]
```

Windowsプラットフォームでサイレントインストールを実行する

Windowsプラットフォームでサイレントインストールを開始するには、インストールパッケージと同じフォルダでコマンドプロンプトを開いて、次のコマンドを入力します。

```
Manager-Windows-<Version>.x64.exe -q -console -Dinstall4j.language=<ISO code> -varfile <PropertiesFile>
```

Linuxプラットフォームでサイレントインストールを実行する

注意: このコマンドを実行する前に、インストールパッケージに対する実行権限を付与してください。

Linuxプラットフォームでサイレントインストールを開始するには、インストールパッケージと同じディレクトリで次のコマンドを入力します。

```
Manager-Linux-<Version>.x64.sh [-q] [-console] [-Dinstall4j.language=<ISO code>] [-varfile <PropertiesFile>]
```

パラメータ

`-q`を指定すると、インストーラが無人(サイレント)モードで実行されます。

`-console`を指定すると、コンソール(stdout)にメッセージが表示されます。

`-Dinstall4j.language=<ISO code>`を指定すると、他の言語を利用できる場合に初期設定のインストール言語(英語)を変更できます。ISOの標準の言語識別子を使用して言語を指定します。

- 日本語: ja
- 簡体字中国語: zh_CN

`-varfile <PropertiesFile>`では、Deep Security Managerのインストール中に適用する各種設定を含んだ標準Javaプロパティファイルへのフルパスを<PropertiesFile>に指定します。各プロパティは、対応するGUI画面や、WindowsのDeep Security Managerインストールの設定を指定します。たとえば、[アドレスとポート]画面のDeep Security Managerのアドレスは、次のように指定されています。

```
AddressAndPortsScreen.ManagerAddress=
```

このファイル内のほとんどのプロパティには初期設定値が割り当てられているため、省略できます。

使用可能な設定の詳細については、"[Deep Security Managerの設定プロパティファイル](#)" on [the next page](#)を参照してください。

`-t`を指定すると、通常のインストールではなく、インストーラによるシステムチェックが実行されます。

プロパティファイルの例

一般的なプロパティファイルの例を次に示します。

```
AddressAndPortsScreen.ManagerAddress=10.xxx.xxx.xxx
AddressAndPortsScreen.NewNode=True
UpgradeVerificationScreen.Overwrite=False
LicenseScreen.License.-1=XY-ABCD-ABCDE-ABCDE-ABCDE-ABCDE-ABCDE
DatabaseScreen.DatabaseType=Microsoft SQL Server
DatabaseScreen.Hostname=10.xxx.xxx.xxx
DatabaseScreen.Transport=TCP
DatabaseScreen.DatabaseName=XE
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
```



```
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SecurityUpdateScreen.Proxy=False
SecurityUpdateScreen.ProxyType=
SecurityUpdateScreen.ProxyAddress=
SecurityUpdateScreen.ProxyPort=
SecurityUpdateScreen.ProxyAuthentication=False
SecurityUpdateScreen.ProxyUsername=
SecurityUpdateScreen.ProxyPassword=
SoftwareUpdateScreen.UpdateSoftware=True
SoftwareUpdateScreen.Proxy=False
SoftwareUpdateScreen.ProxyType=
SoftwareUpdateScreen.ProxyAddress=
SoftwareUpdateScreen.ProxyPort=
SoftwareUpdateScreen.ProxyAuthentication=False
SoftwareUpdateScreen.ProxyUsername=
SoftwareUpdateScreen.ProxyPassword=
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

Deep Security Managerの設定プロパティファイル

ヒント: [Deep Security 12 - Linux - Silent Install](#) (YouTube) を視聴すると、Deep Security ManagerのサイレントインストールプロセスをRed Hat 7サーバで確認できます。

設定プロパティファイルは、Deep Security Managerのコマンドラインインストール (サイレントインストール) で使用できます(「[Deep Security Managerのサイレントインストール](#)」を参照してください)。

設定プロパティファイル内の各エントリは、次の形式になっています。

```
<Screen Name>.<Property Name>=<Property Value>
```

設定プロパティファイルには、必須の値とオプションの値があります。

注意: オプションのプロパティに無効な値を入力した場合は、インストーラによって代わりに初期設定値が使用されます。

必須の設定

LicenseScreen

プロパティ	指定できる値	初期設定値
LicenseScreen.License.-1	<すべてのモジュールのアクティベーションコード>	<なし>

または

プロパティ	指定できる値	初期設定値
LicenseScreen.License.0	<不正プログラム対策のアクティベーションコード>	<なし>
LicenseScreen.License.1	<ファイアウォール/侵入防御のアクティベーションコード>	<なし>
LicenseScreen.License.2	<変更監視のアクティベーションコード>	<なし>
LicenseScreen.License.3	<セキュリティログ監視のアクティベーションコード>	<なし>

CredentialsScreen

プロパティ	指定できる値	初期設定値
CredentialsScreen.Administrator.Username	<マスター管理者のユーザ名>	<なし>
CredentialsScreen.Administrator.Password	<マスター管理者のパスワード>	<なし>

オプションの設定

LanguageScreen

プロパティ	指定できる値	初期設定値	備考
sys.languageId	en_US ja	en_US	<ul style="list-style-type: none"> 「en_US」 = 英語。 「ja」 = 日本語。

UpgradeVerificationScreen

この画面は、既存のインストールが検出された場合の処理を決定します。

注意: 既存のインストールが検出されないかぎり、この設定は参照されません。

プロパティ	指定できる値	初期設定値
UpgradeVerificationScreen.Overwrite	• True	False

プロパティ	指定できる値	初期設定値
	<ul style="list-style-type: none"> False 	

Trueを指定すると、新規インストールが実行され、既存のデータベース内のすべてのデータが破棄されます。False値を指定すると、既存のインストールを修復するオプションが提供されません。

警告: この値をTrueに設定すると、データベース内の既存データがすべて上書きされます。この処理中にプロンプトは表示されません。

OldDataMigrationScreen

この画面では、データを保持する日数を定義します。この設定が0の場合、すべての履歴データが保持されますが、アップグレードにかかるが長くなる可能性があります。データ移行時、サイレントインストールで移行されたレコードの割合が10%単位で表示されます。

注意: データベーススキーマをアップグレードするためにデータ移行が必要な既存のインストールが検出されないかぎり、この設定は参照されません。

プロパティ	指定できる値	初期設定値
OldDataMigrationScreen.HistoricalDays	<整数>	0

DatabaseScreen

この画面ではデータベースタイプを定義したり、オプションとして、特定のデータベースタイプにアクセスする場合に必要なパラメータを定義したりできます。

注意: 対話式インストールでは、[詳細] をクリックしてMicrosoft SQL Serverのインスタンス名およびドメインを定義できます。このフィールドはダイアログに表示されます。無人インストールではダイアログが表示されないため、これらの引数は次に示すDatabaseScreen設定で指定します。

プロパティ	指定できる値	初期設定値	備考
DatabaseScreen.DatabaseType	<ul style="list-style-type: none"> Microsoft SQL Server Oracle PostgreS 	Microsoft SQL Server	なし

プロパティ	指定できる値	初期設定値	備考
	QL		
DatabaseScreen.Hostname	<ul style="list-style-type: none"> • <データベースのホスト名またはIPアドレス> • <現在のホスト名> 	<現在のホスト名>	なし ポート番号は <hostname>:<port>の形式で指定できます。 例: example:123
DatabaseScreen.DatabaseName	<文字列>	dsm	
DatabaseScreen.Transport	<ul style="list-style-type: none"> • Named Pipes • TCP 	Named Pipes	SQL Serverの場合のみ必須
DatabaseScreen.Username	<データベースのユーザー名>	<なし>	Managerがデータベースサーバへの認証に使用するユーザ名。既存のデータベースアカウントと一致する必要があります。Deep Security Managerのデータベース権限は、このユーザの権限に対応することになります。たとえば、読み取り専用権限のデータベースアカウントを選択した場合、Deep Security Managerはデータベースに書き込みできません。Microsoft SQL ServerおよびOracleには必須です。
DatabaseScreen.Password	<データベースのパスワード>	<なし>	Managerがデータベースサーバへの認証に使用するパスワード。Microsoft SQL ServerおよびOracleには必須です。
DatabaseScreen.SQLServer.Instance	<文字列>	<なし>	単一のサーバまたはプロセッサで複数のインスタ

プロパティ	指定できる値	初期設定値	備考
			<p>ンスを使用可能な Microsoft SQL Serverでのみ使用します。初期設定のインスタンスは1つだけで、他のインスタンスはすべて名前付きインスタンスです。Deep Security Managerデータベースインスタンスが初期設定ではない場合、インスタンス名をここに入力します。値は既存のインスタンスに一致する必要があり、空白にすると、初期設定のインスタンスが指定されます。</p>
DatabaseScreen.SQLServer.Domain	<文字列>	<なし>	<p>Microsoft SQL Serverにのみ使用します。SQL Serverへの認証に使用されるWindowsドメインです。前述の DatabaseScreen.UserNameおよび DatabaseScreen.Passwordは、該当するドメイン内でのみ有効です。</p>
DatabaseScreen.SQLServer.UseDefaultCollation	<ul style="list-style-type: none"> • True • False 	False	<p>Microsoft SQL Serverにのみ使用します。照合(順序)は、文字列の並べ替え方法と比較方法を決定します。値が「False」の場合、Deep Securityは、テキスト型の列の照合にLatin1_General_CS_ASを使用します。「True」の場合は、SQL Serverデータベースで指定した照合方法を使用します。照合順序の詳細については、SQL Serverのドキュメントを参照してください。</p>

AddressAndPortsScreen

この画面では、このコンピュータのホスト名、URL、またはIPアドレスと、Managerのポート番号を定義します。

プロパティ	指定できる値	初期設定値	備考
AddressAndPortsScreen.ManagerAddress	<Managerのホスト名、URL、またはIPアドレス>	<現在のホスト名>	なし
AddressAndPortsScreen.ManagerPort	<ポート番号>	4119	"ポート番号、URL、およびIPアドレス" on page 190を参照してください。
AddressAndPortsScreen.HeartbeatPort	<ポート番号>	4120	"ポート番号、URL、およびIPアドレス" on page 190を参照してください。
AddressAndPortsScreen.NewNode	<ul style="list-style-type: none"> • True • False 	False	Trueを指定すると、現在のインストールが新しいノードになります。データベース内に既存データが見つかった場合は、このインストールが新しいノードとして追加されます。マルチノードセットアップは常にサイレントインストールです。注意: 「新規ノード」インストールのための既存のデータベース情報は、DatabaseScreenプロパティで指定します。

CredentialsScreen

プロパティ	指定できる値	初期設定値	備考
CredentialsScreen.UseStrongPasswords	<ul style="list-style-type: none"> • True • False 	False	Trueを指定すると、Deep Security Managerで強固なパスワードの使用が強制されます。

MasterKeyConfigurationScreen

プロパティ	指定できる値	初期設定値	備考
MasterKeyConfigurationScreen.KeyConfigType	<ul style="list-style-type: none"> Do not configure Local Key KMS 	Do not configure	<p>値が設定されている場合、インストーラはKMSまたはローカルの秘密鍵を使用してカスタムのマスターキーを生成します。値が設定されていない場合は、代わりにハードコードされたシードが使用されます。「masterkey」も参照してください。</p> <p>代わりに、インストーラが完了した後でmasterkeyコマンドを実行する必要があります。</p>
MasterKeyConfigurationScreen.ARN	<AWS ARN>	<なし>	<p>KMSキーのAmazon Resource Name (ARN)。</p> <p>MasterKeyConfigurationScreen.KeyConfigType がKMSの場合にのみ使用されます。</p>
MasterKeyConfigurationScreen.LocalKey	<文字列>	<なし>	<p>インストーラがLOCAL_KEY_SECRET ローカル環境変数を設定するとき使用する値。</p> <p>MasterKeyConfigurationScreen.KeyConfigType がLocal Keyの場合にのみ使用されます。</p>

SecurityUpdateScreen

プロパティ	指定できる値	初期設定値	備考
SecurityUpdateScreen.UpdateComponents	<ul style="list-style-type: none"> True False 	True	True の場合は、セキュリティアップデートを自動的にチェックする予約タスクがDeep Security Managerで作成されます。予約タスクは、インストールの完了時に実行されます。
SecurityUpdateScreen.Proxy	<ul style="list-style-type: none"> True False 	False	True を指定すると、Deep Security Managerは、プロキシ経由でインターネット

プロパティ	指定できる値	初期設定値	備考
			に接続して、トレンドマイクロからセキュリティアップデートをダウンロードします。
SecurityUpdateScreen.ProxyType	<ul style="list-style-type: none"> • HTTP • SOCKS4 • SOCKS5 	<なし>	プロキシで使用されるプロトコル。
SecurityUpdateScreen.ProxyAddress	<有効なIPv4またはIPv6のアドレスあるいはホスト名>	<なし>	なし
SecurityUpdateScreen.ProxyPort	<プロキシポート>	<なし>	"ポート番号、URL、およびIPアドレス" on page 190を参照してください。
SecurityUpdateScreen.ProxyAuthentication	<ul style="list-style-type: none"> • True • False 	False	True を指定すると、プロキシに認証資格情報が必要になります。
SecurityUpdateScreen.ProxyUsername	<文字列>	<なし>	なし
SecurityUpdateScreen.ProxyPassword	<文字列>	<なし>	なし

SoftwareUpdateScreen

プロパティ	指定できる値	初期設定値	備考
SoftwareUpdateScreen.UpdateSoftware	<ul style="list-style-type: none"> • True • False 	True	True を指定すると、ソフトウェアアップデートを自動的にチェックする予約タスクがDeep Security Managerで作成されます。予約タスクは、インストールの完了時に実行されます。
SoftwareUpdateScreen.Proxy	<ul style="list-style-type: none"> • True • False 	False	True を指定すると、Deep Security Managerは、プロキシ経由でイン

プロパティ	指定できる値	初期設定値	備考
			ターネットに接続して、トレンドマイクロからソフトウェアアップデートをダウンロードします。
SoftwareUpdateScreen.ProxyType	<ul style="list-style-type: none"> • HTTP • SOCKS4 • SOCKS5 	<なし>	プロキシで使用されるプロトコル。
SoftwareUpdateScreen.ProxyAddress	<有効なIPv4またはIPv6のアドレスあるいはホスト名>	<なし>	なし
SoftwareUpdateScreen.ProxyPort	<整数>	<なし>	"ポート番号、URL、およびIPアドレス" on page 190を参照してください。
SoftwareUpdateScreen.ProxyAuthentication	<ul style="list-style-type: none"> • True • False 	False	True を指定すると、プロキシに認証資格情報が必要になります。
SoftwareUpdateScreen.ProxyUsername	<文字列>	<なし>	なし
SoftwareUpdateScreen.ProxyPassword	<文字列>	<なし>	なし

SmartProtectionNetworkScreen

この画面では、トレンドマイクロスマートフィードバックを有効にするかどうかを定義します。オプションとして業種を定義することもできます。

プロパティ	指定できる値	初期設定値	備考
SmartProtectionNetworkScreen.EnableFeedback	<ul style="list-style-type: none"> • True • False 	False	True を指定すると、トレンドマイクロスマート

プロパティ	指定できる値	初期設定値	備考
			フィードバックが有効になります。
SmartProtectionNetworkScreen.IndustryType	<ul style="list-style-type: none"> • Not specified • Banking • Communications and media • Education • Energy • Fast-moving consumer goods (FMCG) • Financial • Food and beverage • Government • Healthcare • Insurance • Manufacturing • Materials • Media • Oil and gas • Real estate • Retail • Technology • Telecommunications • Transportation • Utilities • Other 	<なし>	値が入力されていない場合は、Not specifiedと同じ結果になります。

RelayScreen

この画面では、Deep Security RelayをDeep Security Managerと同じコンピュータにインストールするかどうかを定義します。

プロパティ	指定できる値	初期設定値	備考
RelayScreen.Install	<ul style="list-style-type: none"> • True • False 	False	<p>True を指定すると、Deep Security RelayがDeep Security Managerコンピュータにインストールされます。</p> <p>False を指定すると、Deep Security RelayがDeep Security Managerにインストールされません (サイレントインストールの場合)。または、Relayをインストールするかどうか尋ねる画面が表示されます (通常インストールの場合)。</p>

プロパティファイルの例

一般的なプロパティファイルの例を次に示します。

```
AddressAndPortsScreen.ManagerAddress=10.xxx.xxx.xxx
AddressAndPortsScreen.NewNode=True
UpgradeVerificationScreen.Overwrite=False
LicenseScreen.License.-1=XY-ABCD-ABCDE-ABCDE-ABCDE-ABCDE-ABCDE
OldDataMigrationScreen.HistoricalDays=30
DatabaseScreen.DatabaseType=Microsoft SQL Server
DatabaseScreen.Hostname=10.xxx.xxx.xxx
DatabaseScreen.Transport=TCP
DatabaseScreen.DatabaseName=XE
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SecurityUpdateScreen.Proxy=False
```

```
SecurityUpdateScreen.ProxyType=  
SecurityUpdateScreen.ProxyAddress=  
SecurityUpdateScreen.ProxyPort=  
SecurityUpdateScreen.ProxyAuthentication=False  
SecurityUpdateScreen.ProxyUsername=  
SecurityUpdateScreen.ProxyPassword=  
SoftwareUpdateScreen.UpdateSoftware=True  
SoftwareUpdateScreen.Proxy=False  
SoftwareUpdateScreen.ProxyType=  
SoftwareUpdateScreen.ProxyAddress=  
SoftwareUpdateScreen.ProxyPort=  
SoftwareUpdateScreen.ProxyAuthentication=False  
SoftwareUpdateScreen.ProxyUsername=  
SoftwareUpdateScreen.ProxyPassword=  
RelayScreen.Install=True  
SmartProtectionNetworkScreen.EnableFeedback=False
```

インストール時の出力

ここでは、インストールに成功した場合の出力例を示し、その次にインストールに失敗した場合(ライセンスが無効な場合)の出力例を示します。トレース内の [Error] タグは、エラーであることを示します。

インストールに成功した場合

```
Stopping Trend Micro Deep Security Manager Service...  
Checking for previous versions of Trend Micro Deep Security Manager...  
Upgrade Verification Screen settings accepted...  
The installation directory has been set to C:\Program Files\Trend  
Micro\Deep Security Manager.  
Database Screen settings accepted...  
License Screen settings accepted...  
Address And Ports Screen settings accepted...  
Credentials Screen settings accepted...  
Security Update Screen settings accepted...  
Software Update Screen settings accepted...  
Smart Protection Network Screen settings accepted...  
All settings accepted, ready to execute...  
Extracting files ...  
Setting Up...  
Connecting to the Database...  
Creating the Database Schema...
```

```
Creating MasterAdmin Account...
Recording Settings...
Creating Temporary Directory...
Installing Reports...
Installing Modules and Plug-ins...
Creating Help System...
Validating and Applying Activation Codes...
Configure Localizable Settings...
Setting Default Password Policy...
Creating Scheduled Tasks...
Creating Asset Importance Entries...
Creating Auditor Role...
Optimizing...
Importing Software Packages...
Configuring Relay For Install...
Importing Performance Profiles...
Recording Installation...
Clearing Sessions...
Creating Properties File...
Creating Shortcut...
Configuring SSL...
Configuring Service...
Configuring Java Security...
Configuring Java Logging...
Cleaning Up...
Starting Deep Security Manager...
Finishing installation ...
```

インストールに失敗した場合

この例では、プロパティファイルに無効なライセンス文字列が含まれていた場合に生成される出力を示します。

```
Stopping Trend Micro Deep Security Manager Service...
Detecting previous versions of Trend Micro Deep Security Manager...
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
Database Options Screen settings accepted...
[ERROR] The license code you have entered is invalid.
[ERROR] License Screen settings rejected...
Rolling back changes...
```

複数のノードでのDeep Security Managerの実行

Deep Security Managerを1台のサーバで実行する代わりに、Deep Security Managerを複数のサーバ(「ノード」)にインストールし、これらを1つの共有データベースに接続できます。これにより、以下が向上します。

- 信頼性
- 可用性
- スケーラビリティ
- パフォーマンス

任意のノードにログインでき、各ノードは全種類のタスクを実行できます。あるノードが他のノードよりも重要ということはありません。1つのノードでエラーが発生してもサービスのダウンタイムは発生せず、データ損失も生じません。Deep Security Managerは、すべてのオンラインノードによって実行される分散プール内で、複数の同時アクティビティを処理します。ユーザ入力によって発生するものでないアクティビティはすべてジョブとしてパッケージされ、利用可能な任意のManager上で実行されます。ただし、キャッシュのクリアなど、各ノードで実行される一部の「ローカル」ジョブは例外です。

各ノードでは同じバージョンのDeep Security Managerソフトウェアを実行する必要があります。アップグレードするときは、アップグレードする最初のManagerがすべてのタスクを一時的に引き継ぎ、他のノードをシャットダウンします。[管理]→[システム情報]にある[システムのアクティビティ]エリアの[アクティビティグラフ付きネットワークマップ]では、その他のノードのステータスが「オフライン」になり、アップグレードが必要であることが示されます。アップグレードするとノードは自動的にオンラインに戻り、処理を再開します。

ノードを追加する

1つのサーバノードにDeep Security Managerをインストールしたら、別のサーバで再びインストーラを実行します。プロンプトが表示されたら、最初のノードと同じデータベースに接続します。

警告: インストーラのインスタンスを複数同時に実行しないでください。データベースの破損など、予期しない結果につながる可能性があります。

注意: 同じタイムゾーンを使用するように各Managerノードのシステム時計を設定します。データベースも同じタイムゾーンを使用する必要があります。タイムゾーンが異なる場合は、Manager Time Out of Syncエラーが発生します。

ノードを削除する

サーバを削除したり置き換えたりするには、最初にDeep Security Managerノードのプールから削除する必要があります。

1. 削除するノードでサービスを停止するか、Deep Security Managerをアンインストールします。

ステータスが「オフライン」になる必要があります。

2. 別のノードでDeep Security Managerにログインします。
3. [管理]→[Managerノード] に移動します。
4. 削除するノードをダブルクリックします。

ノードの [プロパティ] 画面が表示されます。

5. [オプション] エリアで [廃止] をクリックします。

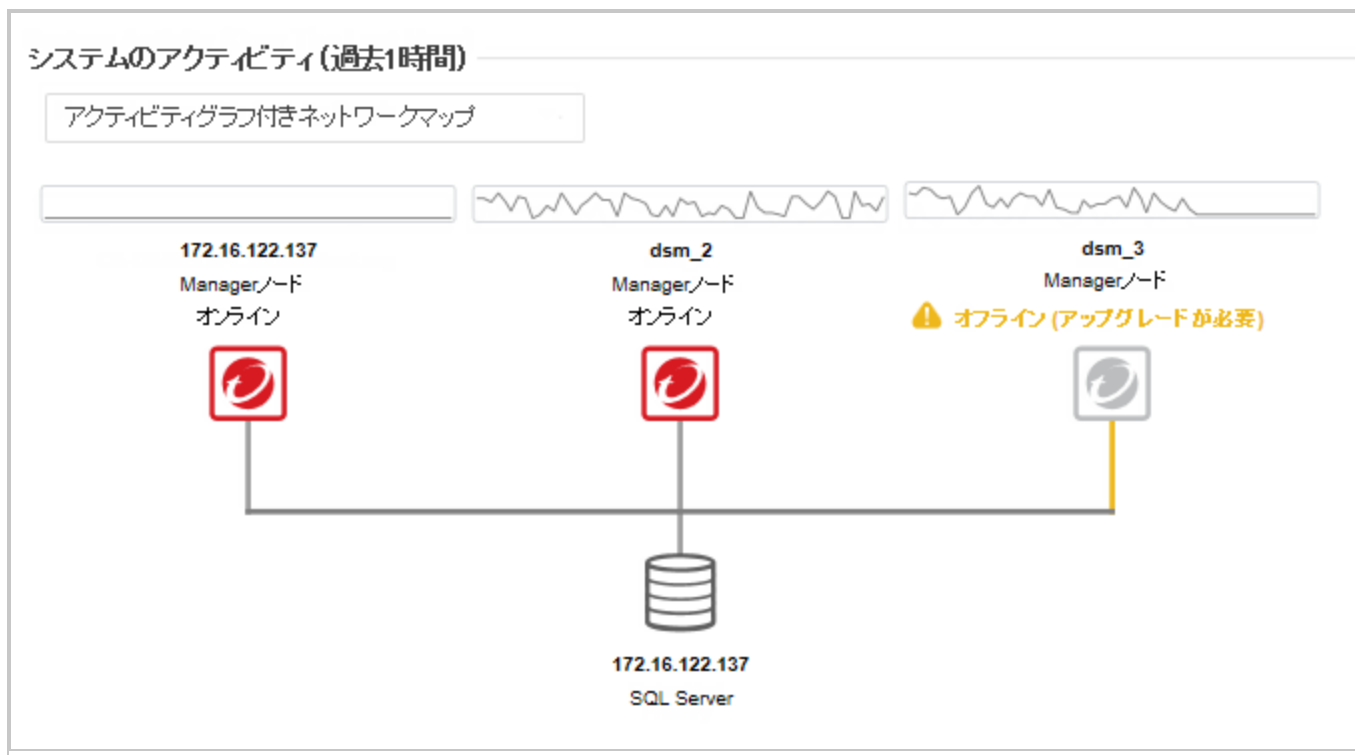
ノードのステータスを表示する

すべてのDeep Security Managerノードとそのステータスを処理中のアクティビティおよびジョブと組み合わせて表示するには、[管理]→[システム情報] に移動します。ドロップダウンメニューから、表示するグラフを選択します。

アクティビティグラフ付きネットワークマップ

[システムのアクティビティ] エリアの [アクティビティグラフ付きネットワークマップ] には、インストール済みのすべてのManagerノードとその現在のステータスのマップ、および過去1時間以内の関連アクティビティが表示されます。ノードには、次の状態があります。

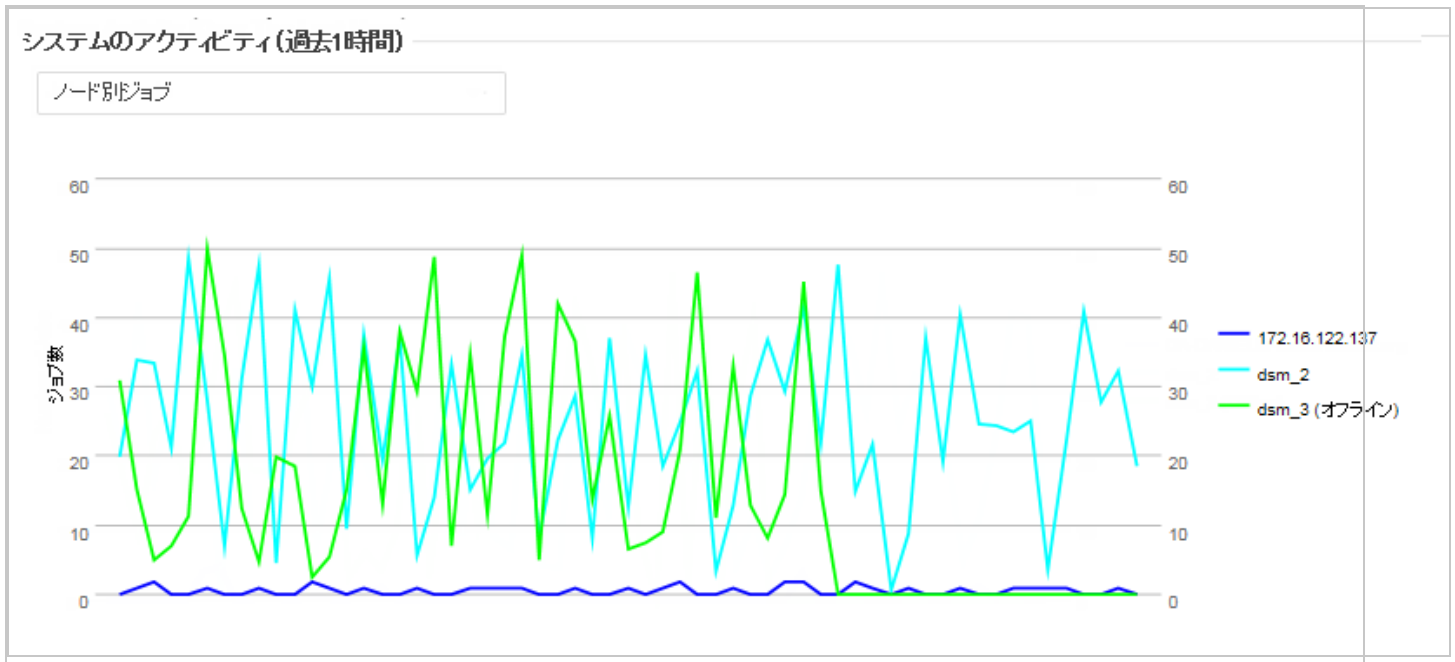
- オンライン
- オフライン
- オフライン (アップグレードが必要)



注意: すべてのDeep Security Managerノードが、他のすべてのノードの状態を定期的に確認します。Managerノードはネットワーク接続が3分を超えて失われているとオフラインと判断されます。このノードのタスクは残りのノードが引き受けます。

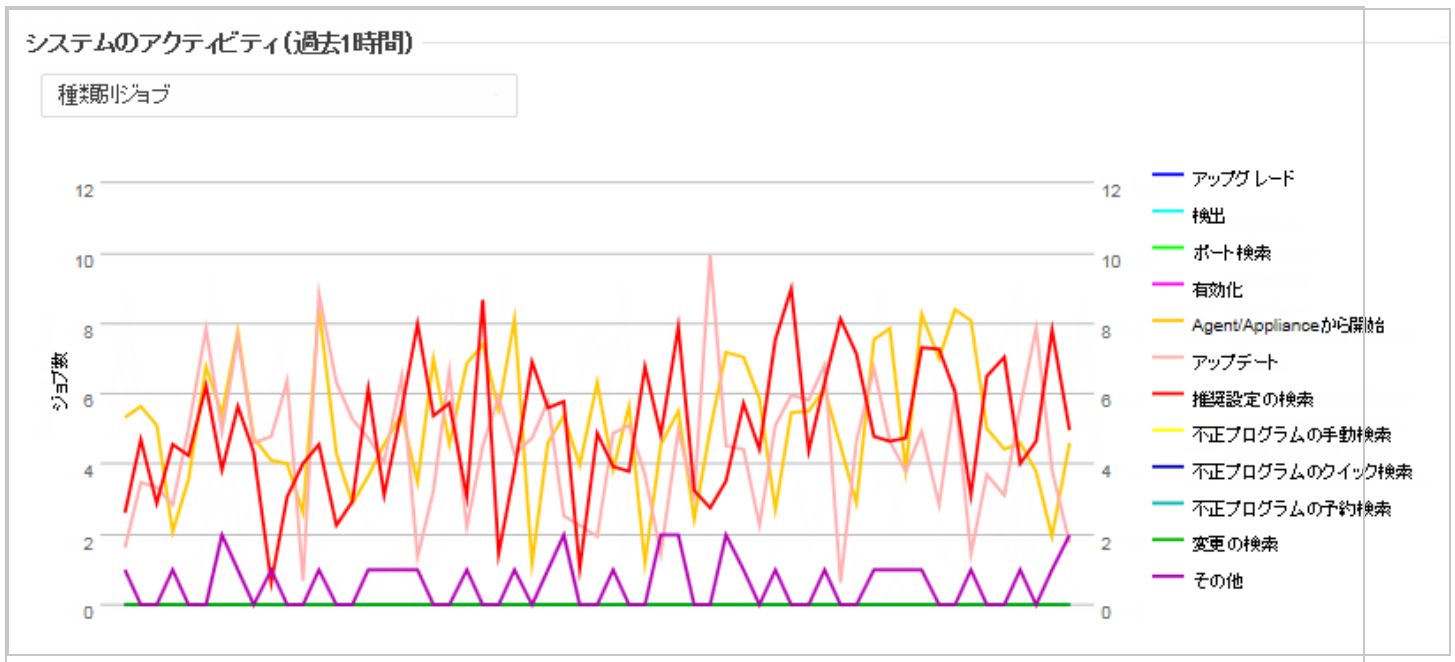
ノード別ジョブ

このグラフは、過去1時間以内に実行されたジョブの数をノード別に表示します。



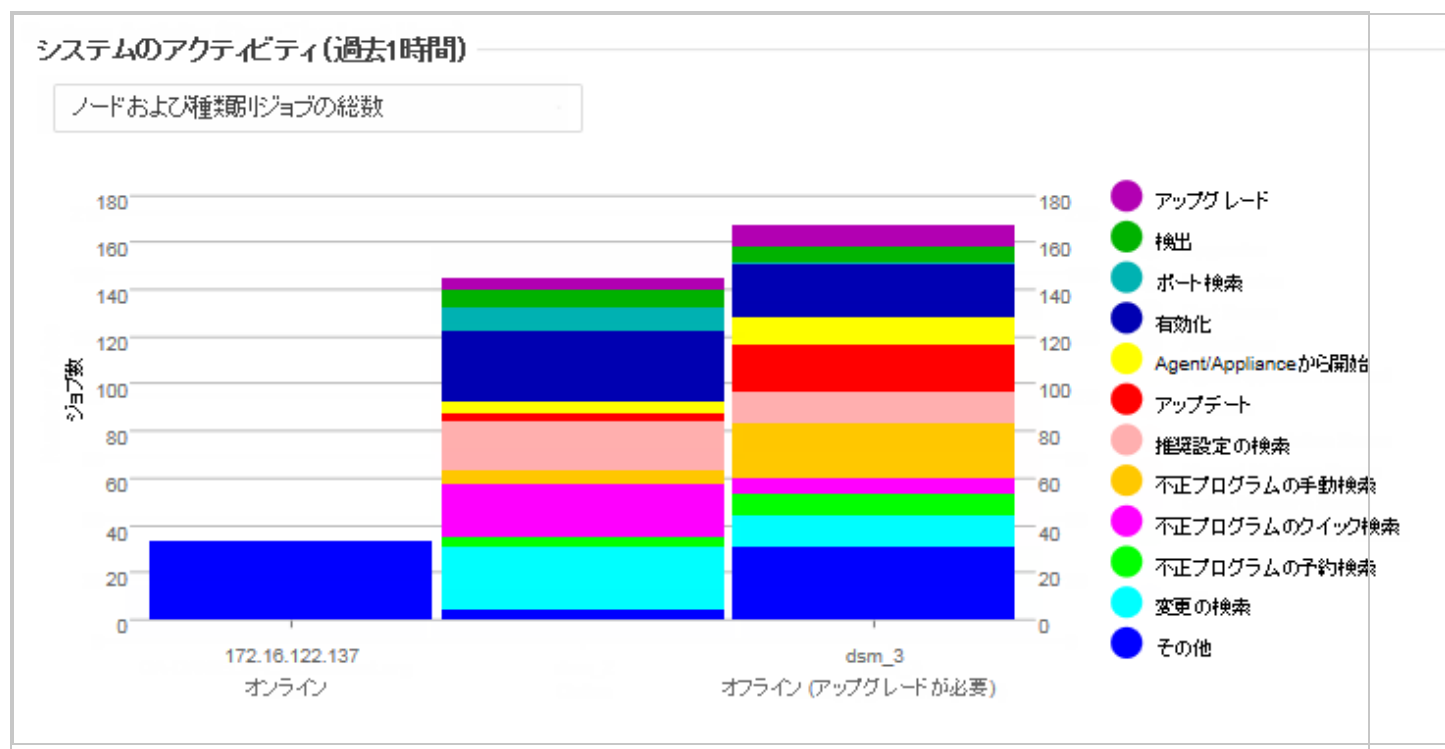
種類別ジョブ

このグラフは、過去1時間以内に実行されたジョブの種類別に表示します。



ノードおよび種類別ジョブの総数

このグラフは、過去1時間以内に実行されたジョブをノードごとの種類別に表示します。



アクティベーションコードを追加

ライセンス契約 (BYOL) を使用している場合、インストール時にライセンス認証コードを入力していない場合は、管理者に1つ以上のアクティベーションコードを入力する必要があります。課金課金を使用している場合は、アクティベーションコードが入力されていないため、アクティベーションコードを入力する必要はありません。

注意: アクティベーションコードはライセンスとも呼ばれます。

アクティベーションコードを入力するには

1. Deep Security Managerにログインします。
2. 上部にある[Administration]をクリックします。
3. 左側の[Licenses]をクリックします。
4. メイン画面で、[Enter New Activation Code]をクリックします。
5. 販売店から取得したアクティベーションコードを入力します。
6. [次へ][]の順にクリックし、終了したらウィザードを閉じます。

Deep Security Managerのメモリ使用量の設定

インストーラの最大メモリ使用量を設定する

初期設定で、インストーラは連続する1GBのメモリを使用するように設定されています。インストーラの実行に失敗する場合は、インストーラで使用するメモリを少なく設定することもできます。

1. インストーラのあるディレクトリに移動します。
2. インストールプラットフォームに応じて、「Manager-Windows-xx.x.xxxx.x64.exe.vmoptions」または「Manager-Linux-xx.x.xxxx.x64.sh.vmoptions」という新しいテキストファイルを作成します（「xx」 .x.xxxx "はインストーラのビルド番号です）。
3. ファイルに「-Xmx800m」という行を追加します（この例では、インストーラで使用可能なメモリが800MBに設定されます）。
4. ファイルを保存して、インストーラを起動します。

Deep Security Managerの最大メモリ使用量を設定する

Deep Security ManagerのManager JVMプロセスに割り当てられるメモリの初期設定は4GBです。この設定は変更することができます。

1. Deep Security Managerのインストールディレクトリに移動します (Deep Security Managerの実行可能ファイルと同じディレクトリです)。
2. 新しいファイルを作成します。プラットフォームに応じて、次のように名前を付けます。
 - Windows: Deep Security Manager.vmoptions
 - Linux: dsm_s.vmoptions
3. ファイルに「-Xmx10g 」という行を追加します (この例では「10g」を指定することにより、Deep Security Managerで10GBのメモリを使用できるようになります)。
4. ファイルを保存し、Deep Security Managerを再起動します。
5. 新しい設定内容を確認するには、[管理]→[システム情報]に進み、[システムの詳細] エリアで、[Managerノード]→[メモリ]を展開します。[最大メモリ]に新しい設定内容が表示されます。

Deep Security Managerのパフォーマンス機能

パフォーマンスプロファイル

Deep Security Managerでは、CPU、データベース、およびAgent/Applianceにおける各ジョブの影響を考慮する、最適化された同時スケジューラを使用します。初期設定では、新しいインストールは、専用のManager向けに最適化された「アグレッシブ」パフォーマンスプロファイルを使用します。多くのリソースを消費する他のソフトウェアがインストールされているシステムにDeep Security Managerがインストールされている場合は、「標準」パフォーマンスプロファイルを使用した方がよいこともあります。パフォーマンスプロファイルを変更するには、[管理]→[Managerノード]に移動します。この画面で、Managerノードを選択し、[プロパティ]画面を開きます。この画面から、メニューを使用してパフォーマンスプロファイルを変更できます。

パフォーマンスプロファイルは、Agent/Applianceから開始された接続のうち、Managerが受け入れる接続数も制御します。各パフォーマンスプロファイルの初期設定は、受け入れ、遅延、および拒否されるハートビートの量を、効率的に平均化します。

ディスク容量不足のアラート

データベースのディスク容量不足

Deep Security Managerはデータベースから「disk full」のエラーメッセージを受け取ると、自身のハードドライブにイベントを書き込み、状況を知らせるメールメッセージをすべてのユーザに送信します。この動作は変更できません。

複数のManagerノードを実行している場合、イベントを処理しているすべてのノードのディスクにイベントが書き込まれます(複数のノードで実行する方法については、"[複数のノードでのDeep Security Managerの実行](#)" on page 270を参照してください)。

データベースのディスク容量の問題が解決されると、Managerは、ローカルに保存されたデータをデータベースに書き込みます。

Managerのディスク容量不足

Deep Security Managerがインストールされたコンピュータで利用可能なディスク容量が10%未満になると、Managerは「ディスク容量不足」アラートを生成します。このアラートは標準のアラートシステムの一部で、他のアラートと同様に設定することができます(詳細については、"[アラートの設定](#)" on page 1091を参照してください)。

複数のManagerノードを実行している場合、アラートには対象ノードが記載されます。

Managerで利用可能なディスク容量が5 MB未満になると、Managerはすべてのユーザにメールメッセージを送信してシャットダウンします。利用可能なディスク容量が5 MBを超えるまで、Managerを再起動することはできません。


Managerは手動で再起動する必要があります。

複数のノードを実行している場合、ディスク容量不足のノードだけがシャットダウンします。それ以外のManagerノードは継続して動作します。

ロードバランサの証明書のアップデート

通常、自己署名証明書を使用してサーバに接続しようとする時、証明書の検証エラーを示す警告がブラウザに表示されます。これは、自己署名証明書の場合、信頼できるサードパーティの認証局 (CA) に対して証明書の署名をブラウザが自動的に検証できず、この証明書が攻撃者によって送信されたものかどうかを判別できないためです。インストール時、Deep Security ManagerはHTTPS接続 (SSLまたはTLS) に自己署名証明書を使用するように設定されているため、この接続の保護に使用されているサーバ証明書フィンガープリントがお使いのDeep Securityサーバに属していることを手動で確認する必要があります。これは、自己署名証明書をCAによって署名された証明書に置き換えるまで続きます。

AWS Elasticロードバランサ (ELB) または他のロードバランサを使用した場合も同じエラーが発生し、ブラウザに自己署名証明書が表示されます。



Your connection is not private

Attackers might be trying to steal your information from **deepsecurity.example.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

[Automatically report](#) details of possible security incidents to Google. [Privacy policy](#)

HIDE ADVANCED Back to safety

This server could not prove that it is **deepsecurity.example.com**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. [Learn more](#).

Proceed to **deepsecurity.example.com** (unsafe)

警告を無視し続けても、Deep Security Managerにアクセスすることはできます (ブラウザごとに方法が異なります)。ただし、次の操作を行わない限り、接続のたびにこのエラーが発生しません。

- コンピュータの信頼された証明書のストアに証明書を追加します (非推奨)。
 - ロードバランサの証明書を、信頼できるCAによって署名された証明書に置き換えます (強く推奨)。
1. すべてのHTTPSクライアントに信頼されるCAに、管理者、Relay、およびAgentがDeep Security Managerへの接続に使用する完全修飾ドメイン名 (IPアドレスではない) を

登録します。

Deep Security Managerを一意に識別するサブドメインを指定します (deepsecurity.example.comなど)。SSLターミネータロードバランサの背後にあるノードの場合、この証明書は、Deep Security Managerのノードごとではなく、そのロードバランサでブラウザおよび他のHTTPSクライアントに表示されます。

CAが証明書に署名したら、証明書 (公開鍵) と秘密鍵の両方をダウンロードします。

警告: 秘密鍵をセキュアな方法で保存および送信します。ファイル権限または暗号化されていない接続により、第三者による秘密鍵へのアクセスが許可される場合、この証明書と鍵で保護されるすべての接続が危険にさらされます。この証明書を無効にして、鍵を削除し、新しい証明書と鍵を取得する必要があります。

2. [証明書を証明書ストアに追加します](#) (証明書に署名したCAをコンピュータが信頼する場合は任意)。
3. [新規ドメイン名を使用するようにロードバランサのDNS設定をアップデートします](#)。
4. [ロードバランサのSSL証明書を置き換えます](#)。

マルチテナント環境の設定

Deep Securityのマルチテナント機能では、1つのDeep Security Manager内に複数の独立した管理環境を作成できます。各テナントでは、独自の設定とポリシーを適用でき、そのテナントのイベントを監視できます。この機能は、準備環境と実稼働環境を別々に作成する場合や、組織の事業単位ごとに環境を作成する必要がある場合に役立ちます。また、サービスモデルの顧客にDeep Securityをプロビジョニングする場合にも、マルチテナント機能を利用できます。

マルチテナントを有効にすると、「プライマリテナント」ではDeep Security Managerの通常のインストール環境の機能がすべて維持されます。ただし、プライマリテナントがその後作成するテナントについては、システムの構成に基づいて、利用できるDeep Securityの機能を制限できます。

注意: マルチテナント環境では、FIPSモードはサポートされていません。"[FIPS 140-2のサポート](#)" on page 1457を参照してください。

このトピックの内容:

- ["マルチテナントの要件" on the next page](#)
- ["マルチテナントを有効にする" on page 281](#)

- ["テナントを作成する" on the next page](#)
- ["スケーラビリティのガイドライン" on page 284](#)
- ["マルチテナントに関するヒント" on page 284](#)
- ["テナントを管理する" on page 285](#)
- ["マルチテナント環境の設定" on the previous page](#)
- ["使用状況の監視" on page 289](#)
- ["データベースのユーザアカウントを設定する" on page 291](#)
- ["API" on page 300](#)
- ["アップグレード" on page 301](#)
- ["テナントをサポートする" on page 301](#)
- ["ロードバランサ" on page 302](#)
- ["Deep Security Virtual Appliance環境のマルチテナント" on page 303](#)

マルチテナントの要件

次の製品ではマルチテナントを設定できません。

- Deep Security Manager VM for Azure Marketplace
- Azure SQLデータベース
- Azure SQLまたはオンプレミス常時可用性グループ

マルチテナントにはアクティベーションコードが必要です。マルチテナントには追加のデータベース要件もあります。詳細については、["Deep Security Managerで使用するデータベースの準備" on page 206](#)、["データベースのユーザアカウントを設定する" on page 291](#)を参照してください。

スケーラビリティを最大化するために、複数ノードのDeep Security Managerを使用することをお勧めします (["複数のノードでのDeep Security Managerの実行" on page 270](#)を参照)。すべてのManagerノードが、任意のテナントのGUI、ハートビート、またはジョブの要求を処理します。バックグラウンド処理については、各テナントに、ジョブの処理待ち、メンテナンス、およびその他のバックグラウンドタスクを処理するManagerノードが割り当てられます。タスクは、Managerノードが追加またはオフラインにされたときに、残りのノードに再調整されます。

マルチテナントを有効にすると、Deep Security Managerの現在のインストール環境がプライマリテナント (t0) になり、他のテナントの作成などの特別な権限を付与されます。他のテナントは特定の機能の使用を制限されており、Deep Security Managerでそれらの機能のUIを表示

する権限を持っていません。たとえば、プライマリ以外のテナントが他のテナントを作成することはできません。詳細については、"[マルチテナント環境の設定](#)" on page 279を参照してください。

マルチテナントを有効にする

注意: マルチテナントは、いったん有効にすると無効にすることができず、プライマリテナントを削除することもできません。

1. Deep Security Managerで、[管理]→[システム設定]→[詳細] の順に選択します。[マルチテナントのオプション] エリアで [マルチテナントモードの有効化] をクリックします。
2. マルチテナント設定ウィザードが表示されます。マルチテナントのアクティベーションコードを入力し、[次へ] をクリックします。
3. 使用するライセンスモードを選択します。
 - プライマリテナントからライセンスを継承: すべてのテナントにプライマリテナントと同じライセンスを使用します。準備環境でマルチテナントを使用する場合や、同じ組織内の部門ごとにテナントを設定する場合は、このオプションが推奨されます。
 - テナント単位のライセンス: この設定では、テナント作成時にDeep Security APIを使用してライセンスを提供するか、またはテナントがDeep Security Managerに初めてログオンするときにライセンスを入力できます。

4. [次へ] をクリックします。

ウィザードが終了したら、[管理]→[システム設定]→[テナント] の順に選択して、そこでマルチテナントのオプションを設定できます。この画面のオプションについては、Deep Security Managerの右上にある [ヘルプ] をクリックしてください。

テナントを作成する

ヒント: Deep Security APIを使用してテナントの作成と設定を自動化できます。例については、Deep Security Automation Centerで、[Configure database user accounts](#)を参照してください。

マルチテナントモードが有効になったら、[管理]→[テナント] からテナントを管理できます。

テナントの追加に必要なデータベースのユーザアカウントの権限の詳細については、"[データベースのユーザアカウントを設定する](#)" on page 291を参照してください。

1. Deep Security Managerで、[管理]→[テナント]の順に選択し、[新規]をクリックします。
2. 新規テナントウィザードが表示されます。テナントのアカウント名を入力します。アカウント名には、プライマリテナント用に予約されている「プライマリ」以外の任意の名前を使用できます。
3. テナントへの連絡に使用されるメールアドレスを入力してください。
4. ロケールを選択します。ロケールによって、テナントでのDeep Security Managerのユーザインタフェースの言語が決まります。
5. タイムゾーンを選択します。イベントの時間は、イベントが発生したシステムのタイムゾーンではなく、このタイムゾーンを基準にして表示されます。
6. 複数のデータベースを使用するDeep Securityインストール環境では、新しいテナントアカウントを格納するデータベースサーバを Deep Securityで自動的に選択するオプションを選択するか ([自動 - 設定なし])、または特定のサーバを指定できます。

新しいテナントを受け入れていないデータベースサーバは、リストに表示されません。

7. 新しいテナントアカウントの最初のユーザのユーザ名を入力します。
8. 次の3つのパスワードオプションのうち1つを選択します。
 - メールなし: テナントの最初のユーザのユーザ名とパスワードを設定します。メールは送信されません。
 - 確認リンクをメール: テナントの最初のユーザのパスワードを設定します。ただし、ユーザが確認メールのリンクをクリックするまでアカウントは有効になりません。メール確認によって、ユーザがアカウントにアクセスする前に、指定されたメールアドレスがユーザのものであることを確認できます。
 - 生成したパスワードをメール: パスワードを指定せずにテナントを生成できます。

ヒント:

3つのオプションはすべて、APIにより利用可能となります。メール確認オプションは、一般ユーザが登録するのに適しています。テナントの作成者がプログラムではなく人であることを確認する方法として、CAPTCHAが推奨されています。

9. [次へ]をクリックしてウィザードを終了し、テナントを作成します。

テナントの作成には、スキーマの作成と、初期データの登録が必要なので、最大4分程度かかることがあります。この方法で、新しいテナントは最新の設定になり、またデータベーステンプレートを管理する負担、特に複数のデータベースサーバを管理する負担が軽減されます。

各テナントデータベースには約100 MBのディスク容量のオーバーヘッドがあります (初期設定でシステムに入力されるルール、ポリシー、およびイベントに起因)。

テナントに送信されるメッセージの例

確認リンクをメール: アカウント確認要求

```
Welcome to Deep Security! To begin using your account, click the following confirmation URL. You can then access the console using your chosen password.
```

```
Account Name: ExampleCorp
```

```
User name: admin
```

```
Click the following URL to activate your account:
```

```
https://managerIP:portnumber/SignIn.screen?confirmation=1A16EC7A-D84F-D451-05F6-706095B6F646&tenantAccount=ExampleCorp&username=admin
```

生成したパスワードをメール

1通目のメール: アカウントとユーザ名の通知

```
Welcome to Deep Security! A new account has been created for you. Your password will be generated and provided in a separate email.
```

```
Account Name: ExampleCorp
```

```
Username: admin
```

```
You can access Deep Security using the following URL:
```

```
https://managerIP:portnumber/SignIn.screen?tenantAccount=ExampleCorp&username=admin
```

2通目のメール: パスワード通知

```
This is the automatically generated password for your Deep Security account. Your Account Name, Username, and a link to access Deep Security will follow in a separate email.
```

```
Password: z3IgrUQ@jaFi
```

スケーラビリティのガイドライン

テナント数が50~100、またはこれを超える環境では、スケーラビリティの問題を避けるために次のガイドラインに従う必要があります。

- Deep Security Managerノードセット1つにつき作成するテナント数は最大2000です。
- 1つのデータベースサーバで作成するテナント数は最大300です。
- プライマリテナントには別のデータベースサーバを使用し、他のテナントは含めません。
- 1テナントあたりのエージェント数は3000に制限します。
- エージェントの総数は20000に制限します。
- 使用するDeep Security Managerノードは最大2つです。
- Relayを同じ場所に配置して使用しません。

マルチテナントでは、複数のデータベース (Microsoft SQLを使用する場合) または複数のユーザ (Oracleを使用する場合) が使用されます。規模を拡大する場合は、Deep Security Managerを複数のデータベースサーバに接続し、使用可能な一連のデータベースサーバに新しいテナントを自動的に分散させることができます。["データベースのユーザアカウントを設定する" on page 291](#)を参照してください。

マルチテナントに関するヒント

攻撃の予兆IPリスト

マルチテナント環境では、テナントがDeep Security ManagerのIPアドレスを「攻撃の予兆を無視」IPリスト ([ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト]) の順に選択) に追加することが必要になる場合があります。これは、「攻撃の予兆の検出: ネットワークまたはポートの検索」警告が表示されないようにするためです。

複数のデータベースサーバを使用する

マルチテナントでは、複数のデータベース (Microsoft SQLを使用する場合) または複数のユーザ (Oracleを使用する場合) が使用されます。規模を拡大する場合は、Deep Security Managerを複数のデータベースサーバに接続し、使用可能な一連のデータベースサーバに新しいテナントを自動的に分散させることができます。["データベースのユーザアカウントを設定する" on page 291](#)を参照してください。

テナントの「削除の保留中」状態

テナントは削除できますが、処理はすぐに実行されません。Deep Securityでは、レコードを削除する前に、テナント関連のすべてのジョブが完了している必要があります。最も頻度の低いジョブは毎週実行されるため、テナントは最大で約7日間、「削除の保留中」状態のままになる可能性があります。

[システム設定] のマルチテナントオプション

[管理]→[システム設定]→[テナント] では、次のオプションを設定できます。

「初期設定のRelayグループ」内のRelayの使用をテナントに許可(割り当てられていないRelay): プライマリテナントで設定されているRelay有効化済みAgentにテナントが自動的にアクセスできるようにします。これにより、セキュリティアップデート用に専用のRelay有効化済みAgentをテナント側で設定する必要がなくなります。

予約タスク「スクリプトの実行」の使用をテナントに許可: スクリプトは、システムへのアクセスを潜在的な危険にさらす可能性があります。ただし、スクリプトはファイルシステムのアクセス権を使用してDeep Security Managerにインストールする必要があるため、リスクを軽減できます。

テナントを管理する

[管理]→[テナント] には、全テナントのリストが表示されます。テナントのステータスは次のいずれかです。

- 作成: 作成済みですが、アクティベーションのメールがテナントのユーザに送信されていません。
- 設定が必要: 作成済みですが、テナントのユーザに送信された確認メールのアクティベーションリンクがクリックされていません(このステータスは手動で変更できます)。
- 有効: 完全にオンラインで管理されている状態です。
- 一時停止: ログオンが許可されていません。
- 削除の保留中: テナントは削除できますが、すぐにではありません。保留中のジョブが終了するまで、テナントは最大で7日間、「削除の保留中」状態になることがあります。
- データベースアップグレード失敗: アップグレードに失敗したテナントです。[データベースアップグレード] ボタンで、この問題を解決できます。

テナントのプロパティ

テナントをダブルクリックすると、テナントの [プロパティ] 画面が表示されます。

一般

ロケール、タイムゾーン、およびステータスを変更できます。変更は既存のテナントユーザには影響しません (新しいユーザ、およびユーザ固有ではないUIの一部にのみ変更が反映されません)。

データベース名は、このテナントに使用されているデータベースの名前です。ハイパーリンクを介して、テナントデータベースのプロパティにアクセスできます。

モジュール

[モジュール] タブには、保護モジュールの表示に関するオプションがあります。表示オプションを選択することで、各テナントに表示されるモジュールを調整できます。初期設定では、ライセンス許可されていないモジュールはすべて非表示になります。この設定は、[ライセンス許可されていないモジュールを常に非表示] をオフにすることで変更できます。選択したモジュールをテナント単位で表示することもできます。

初期設定では、「テナント単位」のライセンスを使用している場合、各テナントにはライセンスを許可されているモジュールしか表示されません。

[プライマリテナントからライセンスを継承] を選択すると、すべてのテナントに、自分 (プライマリテナント) がライセンスを許可されているすべての機能が表示されます。

注意: このオプションを選択すると、プライマリテナントのライセンス許可されていないすべてのモジュールが他のテナントで非表示になります。他のテナントのオプション [ライセンス許可されていないモジュールを常に非表示] の選択を解除した場合でも、非表示になります。

テスト環境でDeep Securityを評価し、完全なマルチテナント環境がどのようなものかを確認する場合は、マルチテナントのデモモードを有効にできます。デモモードの場合、Managerは、シミュレートされたテナント、コンピュータ、イベント、アラート、およびその他のデータをデータベースに入力します。最初に7日分のデータが生成されますが、その後も、Managerの [ダッシュボード]、[レポート]、および [イベント] の各画面にデータを入力するために新しいデータが継続的に生成されます。

警告: 実稼働環境ではデモモードを使用しないでください。デモンストレーションデータが実際のデータと混ざるため、実際の攻撃または不正プログラムが存在するかどうかの判断が困難になる場合があります。

機能

管理者は、特定のテナントの特定の機能を有効または無効にすることができます。これらの使用可能な機能は、時間とともに変化する場合があります。

[イベント転送の詳細な説明] を有効にした場合、Deep Securityによって、Amazon SNSまたはSIEMに転送されるイベントの完全な説明が含まれます。そうしなかった場合、説明は省略されます。初期設定では、[\[SAMLアイデンティティプロバイダの統合\]](#)、[\[Amazon WorkSpacesを含める\]](#)、[\[アプリケーション\]](#) (アプリケーションコントロール)、および (Automation Centerの) [API Rate Limiter](#)が有効になっています。

統計

[統計] タブには、データベースのサイズ、処理済みジョブ、ログオン、セキュリティイベント、システムイベントなど、現在のテナントに関する情報が表示されます。グラフは、過去24時間のデータを示します。

Deep Security Agentの有効化

[Agentの有効化] タブには、コンピュータ上のAgentを有効にするために実行できるコマンドが表示されます。コマンドは、このテナントのコンピュータのAgentインストールディレクトリを基準にしています。Deep Security Managerが安全に接続できるようにし、テナントがDeep Security Managerからポリシーを割り当てたり、他の設定手順を実行したりできるようにするには、有効化が必要です。

テナントに表示される内容

マルチテナントが有効になっている場合は、ログオンページに追加の [アカウント名] テキストフィールドが表示されます。

テナントは、ユーザ名とパスワードに加えてアカウント名を入力する必要があります。アカウント名があるので、ユーザ名が重複していてもかまいません。たとえば、複数のテナントが同じActive Directoryサーバと同期する場合があります。

注意: プライマリテナントとしてログインするときは、アカウント名を空白のままにするか、「プライマリ」と入力します。

テナントユーザは、Deep Security Manager UIの一部の機能を使用できません。以下の項目は、テナントには表示されません。

- Managerノードのウィジェット
- マルチテナントのウィジェット
- [管理]→[システム情報]
- [管理]→[ライセンス] (継承オプションが選択されている場合)
- [管理]→[Managerノード]
- [管理]→[テナント]

- [管理]→[システム設定]
 - [テナント] タブ
 - [セキュリティ] タブ→[ログオンページのメッセージ]
 - [アップデート] タブ→プライマリテナントのRelayの使用をテナントに許可する設定
 - [詳細] タブ→[ロードバランサ]
 - [詳細] タブ→[プラグイン] セクション
- テナントに関係がないヘルプの内容
- テナントに関係がない一部のレポート
- マルチテナントオプションに基づくその他の機能

- 一部のアラートも非表示になります。
 - ハートビートサーバの失敗
 - Managerのディスク容量不足
 - Managerがオフライン
 - Managerの時刻が非同期
 - 新しいバージョンの Deep Security Managerが利用可能
 - コンピュータ数がデータベースの上限を超過
 - ライセンスの継承が有効になっている場合、ライセンス関連の アラート

テナントからは、プライマリテナントのマルチテナント機能や、他のテナントのデータは確認できません。また、プライマリテナントの権限が必要な一部のAPIも制限されます (他のテナントの作成など)。

テナントユーザが使用できる機能と使用できない機能の詳細については、"[マルチテナント設定](#)" on page 304を参照してください。

すべてのテナントは、複数のユーザアカウントで役割に基づいたアクセス制御 (RBAC) を使用して、アクセスをさらに分割することもできます。また、ユーザのActive Directory統合を使用して、認証をドメインに委任することもできます。この場合も、テナントの認証にテナントのアカウント名が必要です。

Agentからのリモート有効化

Agentからのリモート有効化は、すべてのテナントで初期設定で有効になっています。

注意: プライマリテナントにおけるAgentからのリモート有効化とは異なり、他のテナントユーザが有効化を実行するには、パスワードとテナントIDが必要です。

Agentからのリモート有効化に必要なこれらの情報を確認するには、[管理]→[アップデート]→[ソフトウェア]→[ローカル]の順に移動し、Agentソフトウェアを選択して、[インストールスクリプトの生成]をクリックします。WindowsコンピュータにおけるAgentからのリモート有効化のスクリプトの例を次に示します。

```
dsa_control -a dsm://<host or IP>:4120/ "tenantID:XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" "token:XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
```

テナントの診断

Managerの診断パッケージに含まれるデータは機密性が高いので、テナントからこのパッケージにアクセスすることはできません。ただし、テナントは、コンピュータエディタを開き、[概要]→[処理]の順に移動して [診断パッケージの作成] を選択することで、Agentの診断情報を生成することができます。

使用状況の監視

Deep Security Managerでは、テナントの使用状況に関するデータが記録されます。確認するには、ダッシュボードの [テナントの保護アクティビティ] ウィジェット、テナントの [プロパティ] 画面の [統計] タブ、およびレポートに移動します。この情報は、従来のREST APIのステータス監視からもアクセスできます。このAPIは、[管理]→[システム設定]→[詳細]→[ステータス監視API]の順に移動して、有効または無効にすることができます。

環境に応じて、表示するテナント情報の種類をカスタマイズするには、従来のREST APIのステータス監視を使用します。企業では、事業単位ごとの使用状況を確認する場合に便利です。また、この情報を使用してDeep Securityシステム全体の使用状況を監視し、異常の兆候を検出することができます。たとえば、1つのテナントでセキュリティイベントアクティビティが急増している場合は、攻撃を受けている可能性があります。

マルチテナントのダッシュボード

マルチテナントが有効になっているとき、プライマリテナントのユーザには、テナントの使用状況を監視できる次のダッシュボードウィジェットが追加されます。

- テナントのデータベース使用状況
- テナントのジョブアクティビティ
- テナントの保護アクティビティ
- テナントのセキュリティイベントアクティビティ
- テナントのログオンアクティビティ
- テナントのシステムイベントアクティビティ
- テナント

同じ情報を、[管理]→[テナント] (一部はオプションの列) と、テナントの [プロパティ] 画面の [統計] タブで確認できます。

この情報によって、システム全体の使用状況を監視し、異常の兆候を検出することができます。たとえば、1つのテナントでセキュリティイベントアクティビティが急増している場合は、攻撃を受けている可能性があります。

マルチテナントのレポート

必要な情報が含まれているレポートを生成するには、[イベントとレポート]→[レポートの生成]の順に移動して、ドロップダウンメニューから生成するレポートを選択します。マルチテナント環境のレポートと含まれる情報は次のとおりです。

セキュリティモジュールの累積使用状況レポート

- テナント
- ホスト名
- ID
- 不正プログラム対策
- ネットワーク時間
- システムセキュリティ
- SAPシステム
- 企業時間

セキュリティモジュールの使用状況レポート

- テナント
- ID
- ホスト名
- 表示名
- コンピュータグループ
- インスタンスの種類
- 開始日
- 開始時刻
- 停止時刻
- 期間 (秒)
- 不正プログラム対策
- Webレピュテーション
- ファイアウォール
- 侵入防御
- 変更監視
- セキュリティログ監視
- アプリケーションコントロール
- SAP

テナントレポート

- テナント名
- データベースサイズ
- ピーク時のホスト数
- 保護時間
- 保護されている時間の割合

データベースのユーザアカウントを設定する

各テナントのデータの大部分は別個のデータベースに保存されます。このデータベースは、他のテナントと同じデータベースサーバに共存させることも、専用のデータベースサーバに分離することもできます。いずれの場合も、一部のデータはプライマリデータベース (Deep

Security Managerとともにインストールされたデータベース) だけに保存されます。複数のデータベースサーバが利用可能な場合、テナントは、負荷が最も低いデータベースに作成されます。

データベースへの各テナントのデータの分割には、次のメリットがあります。

- **データ削除:** テナントを削除すると、製品でサポートされているテナントのデータがすべて削除されます。
- **バックアップ:** 各テナントのデータに、それぞれ異なるバックアップポリシーを適用できます。これは、準備環境と実稼働環境でテナントを使用し、準備環境のバックアップ要件が厳しくない場合に便利です (バックアップは、Deep Security Managerを設定した管理者が実行します)。
- **調整:** 将来、すべてのデータベースサーバで負荷を均等に分散するための再調整が可能です。

データベースのユーザアカウントを設定する

注意:

Microsoft SQL Server、Oracle、およびPostgreSQLでは、データベースの概念を表す用語が、次のように異なります。

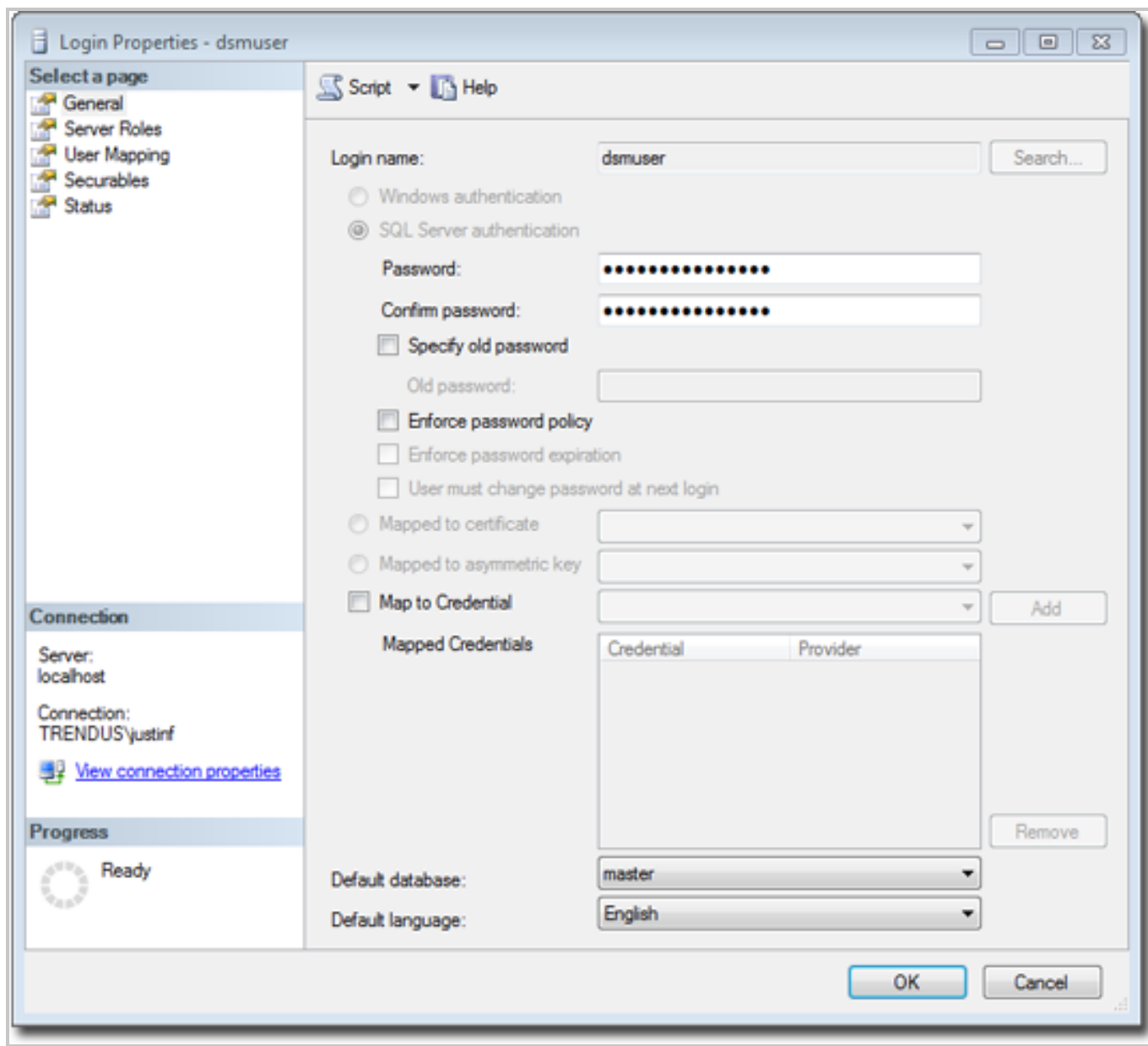
概念	SQL Serverの用語	Oracleの用語	PostgreSQLの用語
複数のテナントが実行されるプロセス	データベースサーバ	データベース	データベースサーバ
単一のテナントのデータ	データベース	表領域/ユーザ	データベース

次のセクションでは、SQL ServerとOracleの両方にMicrosoft SQL Serverの用語を使用します。

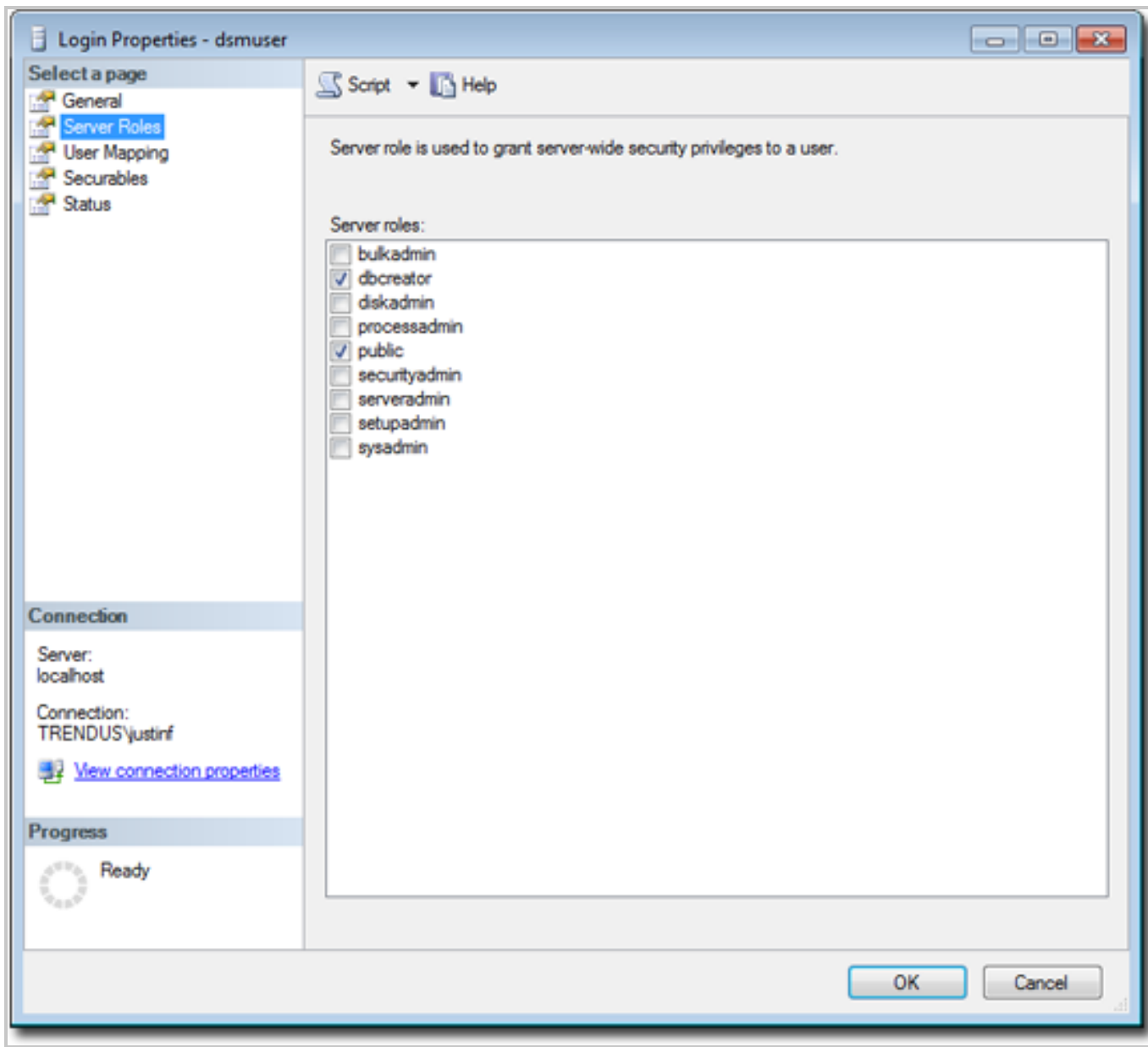
"データベースのユーザアカウントを設定する" [on the previous page](#)も参照してください。

SQL Server

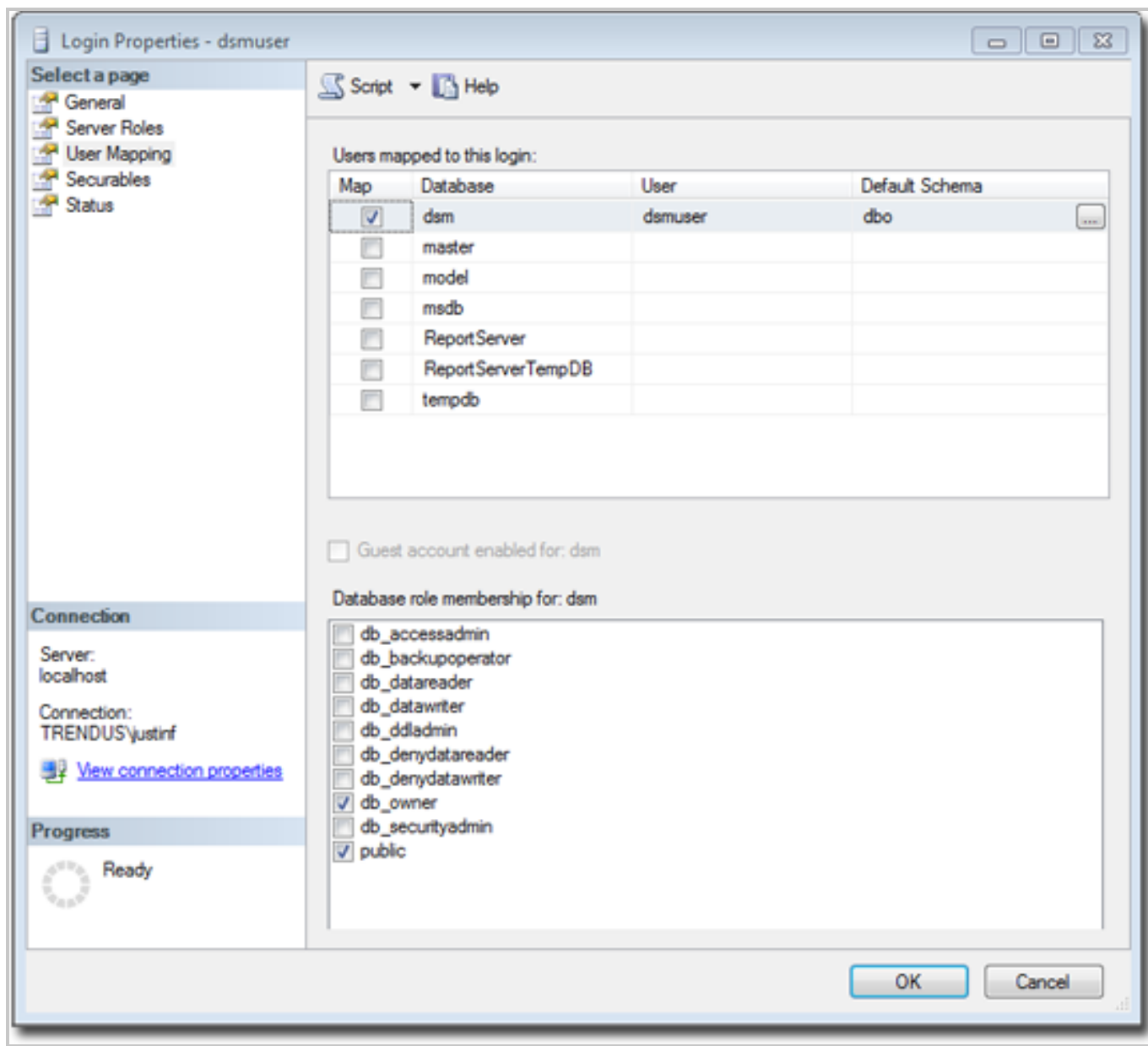
マルチテナントでは、新しいテナントを作成するときにDeep Securityがデータベースを作成できることが必要であるため、そのSQL Serverデータベースユーザには「dbcreator」ロールが必要です。



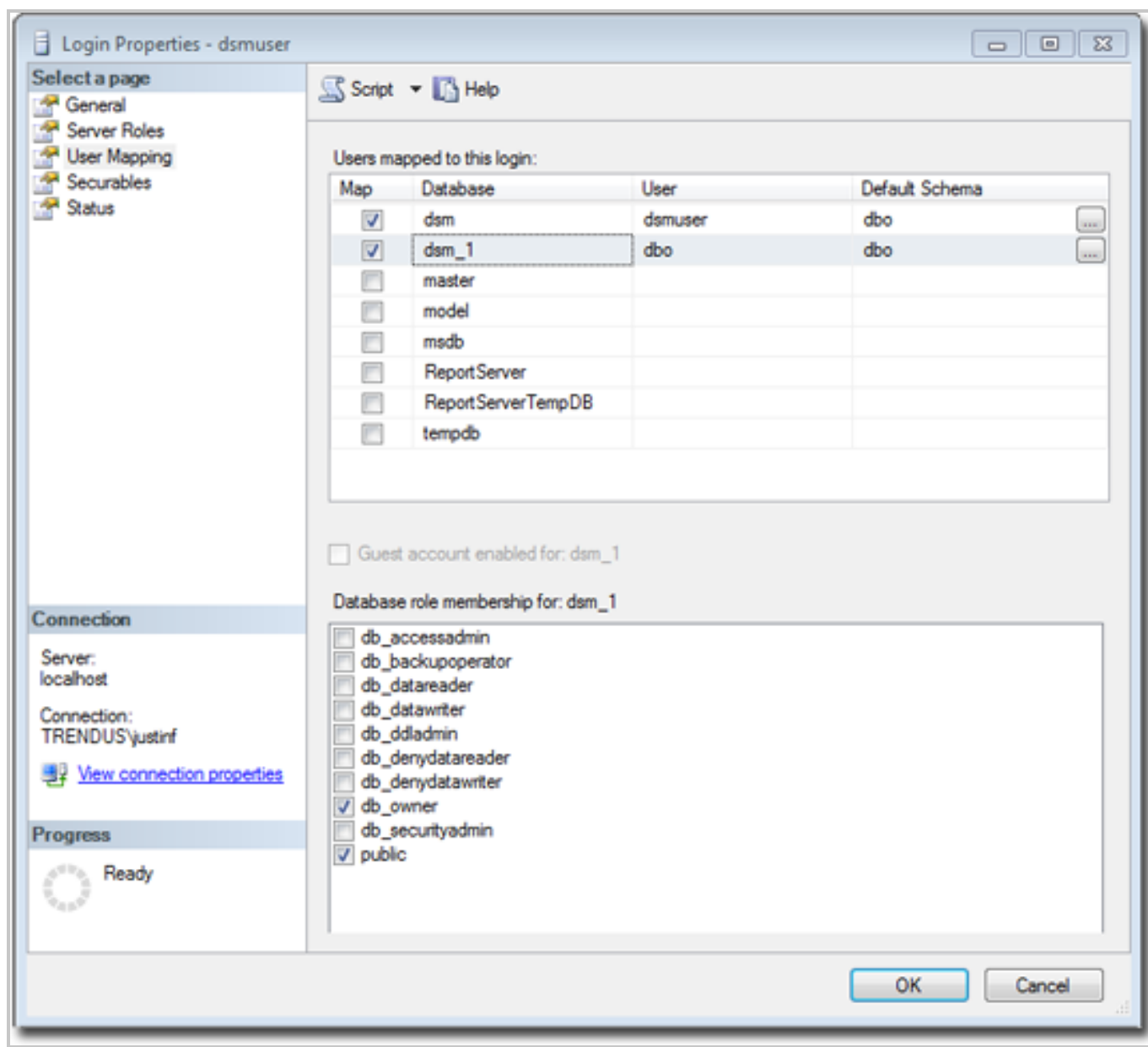
プライマリテナントのユーザのロールについては、メインデータベースのDB所有者を割り当てます。



権限を制限して、スキーマの変更とデータのアクセスのみを許可することもできます。



「dbcreator」ロールを持つアカウントが作成したデータベースは、自動的にそのユーザの所有になります。たとえば、最初のテナント作成後のユーザプロパティは次のとおりです。



セカンダリデータベースサーバの最初のアカウントを作成するには、「dbcreator」サーバロールのみが必要です。ユーザマッピングは必要ありません。

Oracle

Oracleにおけるマルチテナントは、Microsoft SQL Serverの場合と似ていますが、重要な違いがいくつかあります。SQL Serverでは、データベースサーバごとにユーザアカウントが1つですが、Oracleではテナントごとにユーザアカウントが1つです。Deep Securityをインストールしたユーザがプライマリテナントに対応付けられます。このユーザには、追加のユーザやテーブルスペースを割り当てる権限を付与できます。

注意: Oracleでは、引用符で囲めば特殊文字をデータベースオブジェクト名に使用できますが、Deep Securityでは、データベースオブジェクト名内の特殊文字がサポートされていません。引用符を使わずに名前で使用できる文字については、次のOracleのサイトを参照してください。 https://docs.oracle.com/cd/B28359_01/server.111/b28286/sql_elements008.htm#SQLRF00223#SQLRF00223

ヒント: テナントのデータベース名を読みやすくするために、メインデータベース名には短い名前を使用してください。Deep Securityのテナントのデータベース名は、Oracleのメイン(プライマリテナント)データベース名から派生します。たとえば、メインデータベースの名前が「MAINDB」の場合、最初のテナントのデータベース名は「MAINDB_1」、2番目のテナントのデータベース名は「MAINDB_2」になります(以下同様)。

マルチテナントが有効になっている場合は、以下のOracle権限を割り当てる必要があります。

役割

役割	管理オプション	初期設定
CONNECT	N	Y
RESOURCE	N	Y

システム権限

システム権限	管理オプション
ALTER USER	N
CREATE SEQUENCE	N
CREATE TABLE	N
CREATE TRIGGER	N
CREATE USER	N
DROP USER	N
GRANT ANY PRIVILEGE	N
GRANT ANY ROLE	N
UNLIMITED TABLESPACE	N

オブジェクト権限

オブジェクト権限	スキーマ	オブジェクト	付与オプション
アイテムが見つかりません			

テナントは、長いランダムパスワードを持つユーザとして作成され、次の権限が付与されま
す。

役割

役割	管理オプション	初期設定
CONNECT	N	Y
RESOURCE	N	Y

システム権限

システム権限	管理オプション
CREATE SEQUENCE	N
CREATE TABLE	N
CREATE TRIGGER	N
UNLIMITED TABLESPACE	N

オブジェクト権限

オブジェクト権限	スキーマ	オブジェクト	付与オプション
アイテムが見つかりません			

Oracleのセカンダリサーバ用に、最初のユーザアカウント (ブートストラップユーザアカウント) を作成する必要があります。このユーザは、ほとんどの場合、テーブルスペースを持ちます。設定は、プライマリユーザアカウントと同じです。

PostgreSQL

ユーザは、新しいデータベースとロールを作成する権限を持つ必要があります。

```
ALTER ROLE [username] CREATEDB CREATEROLE;
```

セカンダリデータベースサーバでは、ホスト名、ユーザ名、およびパスワードが必要です。ユーザ名には、追加のユーザ (役割) とデータベースを作成する権限が必要です。

複数のデータベースサーバを設定する

初期設定では、すべてのテナントがDeep Security Managerと同じデータベースサーバ上に作成されます。スケーラビリティを高めるために、Deep Security Managerではデータベースサーバを追加できます (追加データベースサーバはセカンダリデータベースと呼ばれることが

あります)。テナントを追加するときに、新しいテナントアカウントを格納するデータベースサーバをDeep Securityで自動的に選択するオプションを選択するか、または特定のサーバを指定できます。

より多くのデータベースを設定するには、[管理]→[システム設定]→[テナント]の順に移動します。[データベースサーバ]セクションで、[データベースサーバの表示]をクリックし、[新規]をクリックします。

Microsoft SQL Serverの場合、セカンダリデータベースサーバにはホスト名、ユーザ名、およびパスワードが必要です(名前付きインスタンスとドメイン)。Deep Security Managerのデータベースユーザは、以下の権限を持つ必要があります。

- データベースの作成
- データベースの削除
- スキーマの定義

このアカウントは、データベースの作成だけでなく、作成されたデータベースに対する認証にも使用されます。

Oracleのマルチテナント環境では、異なるモデルが使用されます。新しいデータベース定義で、表領域にバインドされるユーザが定義されます。このユーザを使用して、Oracleにおける追加ユーザの作成が自動化されます。

セカンダリデータベースを削除または変更する

サーバにテナントが存在しない場合、プライマリデータベース以外のデータベースサーバを削除できます。

セカンダリサーバのホスト名、ユーザ名、パスワード、またはその他の情報が変わった場合は、Deep Security Managerコンソールでこれらの値を変更できます。プライマリデータベースの値を変更するには、Deep Security Managerのすべてのノードをシャットダウンし、dsm.propertiesファイルを編集して新しい情報を追加する必要があります。

API

Deep Security Managerには、次の処理を実行するための多くのAPIが含まれています。

1. マルチテナントの有効化
2. テナントの管理
3. 監視データのアクセス

4. チャージバックデータ (保護の利用状況) のアクセス
5. セカンダリデータベースサーバの管理

また、従来のSOAP APIには、3つ目のパラメータとしてテナントアカウント名を受け取る新しい認証メソッドがあります。

APIの詳細については、「["Deep Security APIを使用したタスクの自動化" on page 478](#)」を参照してください。

アップグレード

Deep Security Managerインストーラを実行すると、既存のインストールが検出されます。新たにインストールを行うか、既存のインストールをアップグレードするかを選択できます。アップグレードすると、インストーラは最初に他のノードをシャットダウンしようとし、その後、アップグレードを開始します。

プライマリテナントが最初にアップグレードされ、その後、他のテナントが並行して処理されます (5テナントずつ)。インストーラが終了したら、他のManagerノードで同じインストーラを実行します。

テナントのデータベースのアップグレード中に問題が発生した場合、[管理]→[テナント]でのテナントの[ステータス]は[データベースアップグレード失敗 (オフライン)]です。テナントのインターフェースを使用して、強制的にアップグレードを実行できます。強制的にアップグレードができない場合は、サポートにお問い合わせください。

テナントをサポートする

特に、テナントに対する最上位サポート担当者であるMSSPの場合、プライマリテナントは他のテナントのユーザインタフェースにログインする必要があるかもしれません。

そうするには、[管理]→[テナント]に移動します。テナントの名前を右クリックし、[テナントとしてログオン]を選択します。テナントのアクセスが無効になっている場合、このオプションを使用できないことがあります。この機能により、そのテナント内に「フルアクセス」ロールを持つ一時的なユーザアカウントが作成され、すぐにそのアカウントへのログインが行われます。一時的なアカウント名は、「support_」で始まり、その後にプライマリテナント内のユーザ名が続きます。

たとえば、プライマリテナントのユーザ名が「user」で、一時アカウントをテナント「T1」の内部に作成した場合、すぐに「support_user」として「T1」へのログインが行われます。

一時的なサポートアカウントは、ログアウトするかセッションがタイムアウトすると削除されます。テナントは、一時的なサポートアカウントの作成、ログイン、ログアウト、および削除に関するシステムイベントを確認できます。

プライマリテナントのユーザは、より多くの診断ツールや情報にアクセスできます。

1. [管理]→[システム情報]には、テナントのメモリ使用量とスレッドの状態に関するより多くの情報が表示されます。
2. 各Managerノードのディスク上のserver#.logログファイル (server0.logなど)には、各イベントに関連するテナントの名前と、該当する場合にはユーザの名前が表示されます。

場合によっては、処理を行ったり、GUIで使用できないテナントの設定を変更したりする必要があります。これは通常、トレンドマイクロのサポートからの要望に応じて行います。[コマンドライン](#)で、次の引数を追加します。

```
-tenantname <tenant-name>
```

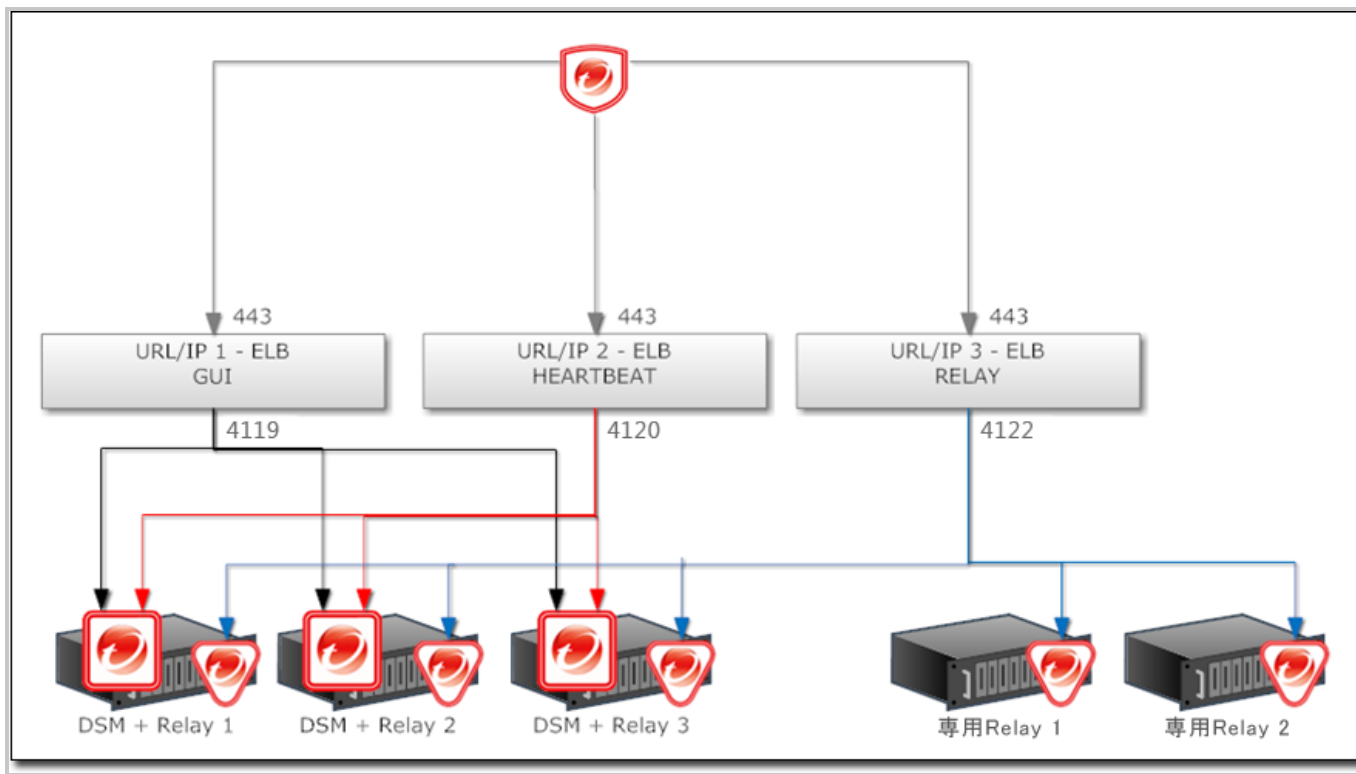
このようにして、設定の変更や処理をそのテナントに適用します。引数を省略すると、コマンドはプライマリテナントに適用されます。

ロードバランサ

初期設定では、複数ノードのManagerから、すべてのノードのアドレスが、すべてのAgentとVirtual Applianceに提供されます。AgentとVirtual Applianceは、接続しようとするときに、リストのノードをランダムに選択します。接続できない場合は、リストにある別のノードを試し、接続が成功するか、ノードがなくなるまでこのプロセスを続けます。接続できるノードがなかった場合は、次のハートビートまで待ってから再度実行します。

ノードが追加または削除されるたびに、アップデートされたリストがすべてのエージェントおよび仮想アプライアンスに送信されます。それまでは、古いノードへの接続は失敗する可能性があります。新しいノードは使用されません。そのため、通信が遅くなり、ネットワークトラフィックが増加します。これを避けるために、代わりに、[ロードバランサのアドレスを介して接続するようにAgentとVirtual Applianceを設定](#)します。

ロードバランサは、トラフィックの種類ごとに異なるポート番号を使用するように設定できます。また、ロードバランサでポートのリダイレクトがサポートされている場合は、3つのロードバランサを使用して、必要なすべてのプロトコルをポート443を経由して公開できます。



TCP接続に基づいて負荷を分散します。SSL終端は使用しません。これにより、接続全体が同じManagerノード内で確実に行われます。次の接続は、別のノードに分散される可能性があります。

詳細なDeep Security Managerの配信推奨事項については、"[Deep Securityのベストプラクティスガイド](#)" on page 988 (英語) を参照してください。

Deep Security Virtual Appliance環境のマルチテナント

VMware環境にDeep Securityを導入する場合、vCenterとそのコネクタをプライマリテナント内に設定し、vCloud Connectorをその他のテナント内に設定することができます。正しく設定された場合、プライマリテナントでは、ESXiサーバ、Deep Security Virtual Appliance、およびその他のインフラストラクチャを確認でき、他のテナントでは、vCloud環境でテナントが所有するAgentレスに保護された仮想マシンのみを確認できます。

このような環境を有効にするには、[管理]→[システム設定]→[Agent] の順に移動し、[ApplianceによるvCloud仮想マシンの保護を許可] チェックボックスをオンにします。

vCloudとの統合の詳細については、"[VMware vCloudへのAgentのインストール](#)" on page 383 を参照してください。

マルチテナント設定

[テナント] タブは、マルチテナントモードを有効にしている場合のみ表示されます。

- マルチテナントライセンスモード: マルチテナントのライセンスモードは、マルチテナントの設定後に変更できます。ただし、このモードを継承からテナント単位に切り替えると、ライセンス許可されているモジュールが既存のテナントで使用できなくなるので注意が必要です。
- 予約タスク「スクリプトの実行」の使用をテナントに許可: スクリプトは、システムへのアクセスを潜在的な危険にさらす可能性があります。ただし、スクリプトはファイルシステムのアクセス権を使用してManagerにインストールされるため、リスクを軽減できます。
- 「コンピュータの検索」の実行をテナントに許可 (直接および予約タスクとして): 検出を許可するかどうかを指定します。ネットワーク検出が禁止されているサービスプロバイダ環境での実行には適していない場合があります。
- 「ポートの検索」の実行をテナントに許可 (直接および予約タスクとして): ポートの検索を実行できるかどうかを指定します。ネットワーク検索が禁止されているサービスプロバイダ環境での実行には適していない場合があります。
- VMware vCenterの追加をテナントに許可: vCenterとの接続を許可するかどうかをテナントごとに指定します。インターネットなどの安全ではないネットワークやパブリックネットワーク経由で接続を行う場合、通常はこのオプションを無効にする必要があります。
- クラウドアカウントの追加をテナントに許可: クラウド同期の設定をテナントに許可するかどうかを指定します。通常、クラウド同期はすべてのセットアップに対し適用されます。
- LDAPディレクトリとの同期をテナントに許可: ユーザとコンピュータの両方をディレクトリ (コンピュータはLDAPまたはActive Directory、ユーザはActive Directoryのみ) と同期することをテナントに許可するかどうかを指定します。インターネットなどの安全ではないネットワークやパブリックネットワーク経由で接続を行う場合、通常はこのオプションを無効にする必要があります。
- イベント転送のSIEMの設定を各テナントに許可: SIEMの設定を [イベントの転送] タブに表示します。
- SNSの設定をテナントに許可: SNSの設定を [イベントの転送] タブに表示します。
- SNMPの設定をテナントに許可: リモートコンピュータへのシステムイベントの転送をテナントに許可します (SNMP経由)。このオプションを選択しない場合は、すべてのテナントが [イベントの転送] タブの設定をすべてのイベントタイプに使用し、SyslogはDeep Security Managerを介して転送されます。

- [パスワードを忘れた場合] オプションを表示:パスワードのリセット画面に進むリンクをログオン画面に表示します。この機能を使用するには、[管理]→[システム設定]→[SMTP] タブでSMTP設定を正しく指定しておく必要があります。
- [アカウント名とユーザ名を記憶] オプションを表示:ユーザのアカウント名とユーザ名を記憶してログオン画面の該当するフィールドに自動的に入力するためのオプションを表示します。
- プライマリテナントからのアクセス管理をテナントに許可: 初期設定では、プライマリテナントは、[管理]→[テナント] 画面の [テナントとしてログオン] オプションを使用してテナントのアカウントにログオンできます。[プライマリテナントからのアクセス管理をテナントに許可] オプションをオンにすると、プライマリテナントからDeep Security環境へのアクセスを許可するか禁止するかをテナントが指定できるようになります ([管理]→[システム設定]→[詳細])。このオプションをオンにした場合、テナント環境の初期設定ではプライマリテナントのアクセスが禁止されます。

注意: プライマリテナントがテナントのアカウントにアクセスするたび、テナントのシステムイベントにアクセスが記録されます。

- プライマリテナントのTrend Micro Apex CentralおよびDeep Discovery Analyzerサーバの設定の使用をテナントに許可: プライマリテナントのConnected Threat Defense設定をテナントと共有できます。詳細については、"[Connected Threat Defenseを使用した脅威の検出](#)" on page 758を参照してください。
- 「初期設定のRelayグループ」のRelayの使用をテナントに許可: テナントは、プライマリテナントに設定されているRelayに自動的にアクセスできます。その結果、テナントはセキュリティアップデート専用のRelayを設定する必要がなくなります。

注意: テナントは、「共有」Relayの使用を拒否できます。拒否するには、[管理]→[システム設定] 画面の [アップデート] タブを選択し、[プライマリテナントのRelayグループを初期設定のRelayグループとして使用 (割り当てられていないRelay)] オプションの選択を解除します。この設定の選択を解除する場合は、専用のRelayを設定する必要があります。

注意: Relayを共有する場合は、プライマリテナントがRelayを最新の状態に保つ必要があります。最新の状態に保つには、すべてのRelayに対して予約タスク「セキュリティアップデートのダウンロード」を作成し、定期的に行います。

- 新規テナントでのセキュリティアップデートの自動ダウンロードを有効化: 新しいテナントアカウントが作成されると同時に、最新のセキュリティアップデートの有無を確認してダウンロードします。
- 次のオプションをロックして非表示 (すべてのテナントがプライマリテナントの設定を使用):
 - [Agent] タブのデータプライバシーオプション: プライマリテナントにデータプライバシーの設定を許可します。この設定は、[管理]→[システム設定]→[Agent] タブの [暗号化されたトラフィック (SSL) のパケットデータの取り込みを許可] にのみ適用されます。
 - [SMTP] タブのすべてのオプション: [SMTP] タブの設定をすべてロックします。
 - [ストレージ] タブのすべてのオプション: [ストレージ] タブの設定をすべてロックします。

データベースサーバ

初期設定では、すべてのテナントがDeep Security Managerと同じデータベースサーバ上に作成されます。スケーラビリティ向上のために、Deep Security Managerではデータベースサーバを追加できます。詳細については、"[マルチテナント環境の設定](#)" on page 279を参照してください。

新しいテナントテンプレート

テナントテンプレート機能では、カスタマイズしたテンプレートから新しいテナントを作成できます。

プロセスは次のとおりです。

1. 新しいテナントを作成します。
2. 作成したテナントでログインします。
3. サンプルポリシーをカスタマイズ (追加、削除、または変更) し、セキュリティアップデートのバージョンを新しいバージョンに変更します。
4. プライマリテナントに戻り、テナントテンプレートウィザードを実行します。
5. 作成したテナントを選択し、スナップショットを作成します。

新しいテンプレートには次のアイテムが含まれます。

- 最新のセキュリティアップデートルール (作成時にテンプレートに適用されていたアップデート。トレンドマイクロによって提供された侵入防御ルール、変更監視ルール、セキュリティログ監視ルールなど)

- ポリシーファイアウォールルール
- IPリスト
- MACリスト
- ディレクトリリスト
- ファイルリスト
- ファイル拡張子リスト
- ポートリスト
- コンテキスト
- スケジュール
- ファイアウォールステートフル設定
- 不正プログラム検索設定

新しいテンプレートには次のアイテムが含まれません。

- カスタム侵入防御ルール
- カスタムのアプリケーションの種類
- カスタム変更監視ルール
- カスタムセキュリティログ監視ルール
- カスタムセキュリティログ監視デコーダ
- ダッシュボード
- アラートの設定
- システム設定
- 予約タスク
- イベントベースタスク
- ユーザ
- 役割
- 連絡先情報

この機能は、一部のサンプルを使用できない、または特殊なサンプルを作成する必要があるサービスプロバイダ環境で便利です。

サンプルポリシーは、テナントで使用するポリシーを作成するための開始ポイントです。テナントごとに、それぞれ固有のニーズに応じたポリシーを作成することを推奨します。

注意: 新しいテンプレートを作成しても、既存のテナントには影響しません。

保護の使用状況の監視

Deep Securityは、保護対象のコンピュータに関する情報を収集します。この情報は、[テナント] ウィジェットと [テナントの保護アクティビティ] ウィジェットのダッシュボードに表示されます。また、テナントレポートでもこの情報を確認でき、従来のREST API経由で取得できます。

注意: 監視機能は、一般的な使用の場合、(レポートまたはAPIを使用して) 保護時間からDeep Security Managerの使用率を判断するのに便利です。一般に「ショーバック」または「チャージバック」と呼ばれるこの情報は、さまざまな形で使用できます。高度な使い方としては、テナントコンピュータのOSなどの特性に基づいたカスタム請求に使用できます。

これらのオプションを使用して、追加で記録するテナントコンピュータの情報を指定します。

メール通知のSMTPの設定

Deep Security Managerでは、選択したアラートがトリガされた場合に、ユーザにメールを送信できます ("[アラートの設定](#)" on page 1091を参照)。メール通知を設定する前に、Deep Security ManagerがSMTPメールサーバにアクセスできるようにする必要があります。

1. [管理]→[システム設定]→[SMTP] の順に選択します。
2. SMTPメールサーバのIPアドレスまたはホスト名を入力します。[初期設定のポート番号](#)以外を使用する場合は、ポート番号を含めてください。

ヒント:

AWSでは、SMTPのIANA標準ポート番号 (ポート25) を経由するメールは調整されます (速度が制限されます)。AWS Marketplaceを使用する場合は、SMTP over STARTTLS (セキュアなSMTP) を代わりに使用すると、アラートを速く配信できる可能性があります。詳細については次を参照してください。

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html>

3. メールを送信元とする「送信元」メールアドレスを入力します。

注意:

Amazon SESを使用している場合は、送信者のメールアドレスを検証する必要があります。Amazon SESでメールアドレスを検証する方法と検証済みのアドレスリストを表示

する方法については、次のページを参照してください。

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-email-addresses.html>

4. オプションで、アラートメールを1人以上のユーザに配信できなかった場合に配信不能通知 (DSN) を送信する「バウンス」メールアドレスを入力します。
5. SMTPサーバで送信認証が必要な場合は、ユーザ名とパスワードの資格情報を入力します。
6. SMTPサーバがSTARTTLSプロトコルをサポートする場合は、そのプロトコルを選択します。(STARTTLSはFIPSモードでサポートされていません。["FIPS 140-2のサポート" on page 1457](#)を参照してください。)
7. 必要な情報を入力したら、[SMTP設定のテスト] をクリックして接続をテストします。

Applianceのインストール

VMware環境の保護

Trend Micro Deep SecurityはVMwareと緊密に連携し、Agentレスによるセキュリティをハイパーバイザレベルで提供します。このセキュリティを提供するのがDeep Security Virtual Applianceです。Applianceは、NSX Managerを使用してクラスタレベルで配置され、同じESXiホスト上の仮想マシンを保護します。

このページのトピック:

- ["Deep Security Virtual Applianceの機能" below](#)
- ["Virtual ApplianceおよびNSXを使用するVMware環境" on the next page](#)
- ["エージェントのみを使用したVMwareの配置" on page 315](#)
- ["追加情報" on page 315](#)

Deep Security Virtual Applianceの機能

検索キャッシュ

検索キャッシュを使用すると、不正プログラム対策 検索の結果を、複数のコンピュータで同じファイルを検索するときに使用できます。元のゲスト仮想マシンを検索する際、Applianceは検索対象ファイルの属性を追跡します。他の仮想マシンを検索する際には、各ファイルの追跡した属性を比較します。属性が同じ後続のファイルを再び完全に検索する必要がないため、全体的な検索時間が短縮されます。ほぼ同じイメージの仮想デスクトップインフラストラクチャ

(VDI) などでは、検索キャッシュを使用することでパフォーマンスに与える影響を大幅に削減できます。

検索ストームの最適化

同時に多数の検索が実行されると、「検索ストーム」が発生し、パフォーマンスが低下します。通常、検索ストームは、大規模なVDI環境で発生します。不正プログラム対策 検索を実行すると、アプライアンスは [検索キャッシュ](#) の機能を使用して、スキャンの嵐の最中にリソースの使用を最適化できます。

管理の簡素化

一般に、Deep Security Virtual Applianceを各ESXiホストに1つずつ配置することは、複数のVMにDeep Security Agentを配置するより簡単です。NSXを使用している場合は、新しいESXiホストがクラスタに追加されると、NSX Managerによって自動的にDeep Securityサービスが配信されるため、さらに管理の手間を節約できます。

また、Virtual Applianceを使用するとネットワークの柔軟性も向上します。Deep Security Agentは、それぞれがネットワークに接続してDeep Security ManagerとRelayを解決する必要があります。Deep Security Virtual Applianceを使用した場合、このネットワーク接続が必要なのはVirtual Applianceのみで、各仮想マシンへの接続は必要ありません。

インフラストラクチャと仮想マシンが別々のチームによって管理される場合があります。Virtual Applianceを使用すると、ハイパーバイザレベルで保護を実施して各仮想マシンを保護できるため、インフラストラクチャチームは保護を追加するために仮想マシンにアクセスする必要がありません。

Virtual ApplianceおよびNSXを使用するVMware環境

Deep Security Virtual Applianceを使用してゲスト仮想マシンを保護する場合は、VMware NSX Data Center for vSphere (NSX-V) またはNSX-T Data Centerを使用する必要があります。NSX-VおよびNSX-Tのライセンスには、いくつかのタイプがあります。次の表には、これらのライセンスタイプと各タイプでサポートされるDeep Security機能を示します。

注意: Deep Security Virtual Applianceでサポートされるサポート対象の機能およびサブ機能の詳細なリストについては、"[各プラットフォームでサポートされている機能](#)" on page 183 を参照してください。

Deep Security Virtual Appliance環境														
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x					
	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	
不正プログラム対策	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1
変更監視とアプリケーションシミュレーション	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	X2	X2	X2	X2	X2	X2

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
ロニル													
ファイアウォール	X2	✓	✓	X2	X2	✓	✓	✓	X2	X2	X2	X2	X2
侵入防御	X2	✓	✓	X2	X2	✓	✓	✓	X2	X2	X2	X2	X2
Webレピュテーション	X2	✓	✓	X2	X2	✓	✓	✓	X2	X2	X2	X2	X2

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x							NSX-T 2.4.x、2.5.x				
標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	
モニ													
セキュリティログ監視	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2
アプリケーションシミュレーション	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2	X2

Deep Security Virtual Appliance環境												
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x					
標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center Remote Office Branch Office
二												

1 Windowsゲスト仮想マシンでのみ使用可

2 各ゲスト仮想マシンにAgentをインストールした場合にのみ使用可 ([コンバインモード](#))

Virtual Applianceの機能を補うためにAgentをインストールすることを、[コンバインモード](#)と呼びます。

コンバインモードを検討する場合、以下が主要なポイントとなります。

- 管理: Deep Securityには、さまざまなオーケストレーションツール (Chef、Puppetなど) を使用してDeep Security Agentのインストールをスクリプト化できる、インストールスクリプトが用意されています。[インストールスクリプト](#)を使用するとAgentを簡単にインストールでき、Agentの有効化およびポリシーの割り当ても可能です。インストールスクリプトを使用することで、VMware環境にAgentをインストールする際の手動操作や管理コストを減らすことができます。
- ["検索キャッシュ" on page 309](#) のパフォーマンスが向上し、["検索ストームの最適化" on page 310](#) : 複合モードでは、仮想アプライアンスは不正プログラム対策 検索の検索キャッシュと検索の嵐の最適化を実行します。これにより、インストールが必要なのは

ネットワークドライバのみとなるため、各仮想マシンでAgentが占有するスペースを抑えることができます。

Deep Security Virtual Appliance環境の設定方法の詳細については、「[NSX-VへのDeep Security Virtual Applianceのインストール](#)」または"[Applianceのインストール \(NSX-T\)](#)" on [page 320](#)を参照してください。

エージェントのみを使用したVMwareの配置

仮想アプライアンスまたはNSXなしでVMware環境を保護するには、Deep Security Agentを各VMに配信する必要があります。このシナリオでは、Agentがすべての保護を提供するため、Deep Security Virtual Applianceは必要ありません。Deep Security Agentを使用することで、Deep Securityの主な機能をすべて利用できます。つまり、[不正プログラム対策](#)、[変更監視](#)、[ファイアウォール](#)、[侵入防御](#)、[Webレピュテーション](#)、[セキュリティログ監視](#)と[アプリケーションコントロール](#)の3つの機能を使用できます。加えて、Agentには次の特性があります。

- 軽量 (Smart Agent)。指定した保護モジュール（不正プログラム対策 および 変更監視など）のみが、マネージャで設定したポリシーに従ってインストールされます。さらに、Deep Securityには「推奨設定の検索」と呼ばれる機能があり、これを使用すると、保護している特定のワークロードに必要なルールだけを割り当てることができます。
- Windowsクライアントには、不正プログラム対策 検索キャッシュが含まれています。このキャッシュには、頻繁にアクセスされる以前に検索されたファイルのハッシュが格納されているため、再スキャンする必要はありません。

Agentをインストールするため、トレンドマイクロではさまざまなオーケストレーションツール (Chef、Puppetなど) で使用できる[インストールスクリプト](#)を提供しています。[手動でAgentをインストール](#)することもできます。

追加情報

- Deep Security Webサイト:https://www.trendmicro.com/ja_jp/business/products/hybrid-cloud/deep-security-data-center.html

Agentレスによる保護またはコンバインモードの保護の選択

仮想マシン (VM) を保護する場合は、他のコンピュータと同様にDeep Security Agentをインストールできます。ただし、Deep Security 9.6以降では、仮想マシンを保護する方法がこの他に2つあります。

- Agentレスによる保護 (Virtual Applianceを使用)
- AgentベースとAgentレスを組み合わせる保護 (コンバインモード)

Agentレスによる保護

Deep Securityエージェントのインストールを **が実行せずに、不正プログラム対策および変更監視の保護を**に提供できます。代わりに、仮想マシンにインストールされたVMware Toolsドライバを使用してセキュリティ処理をDeep Security Virtual Applianceにオフロードできます。

注意: Linux仮想マシンでは、Deep Security Virtual ApplianceではなくDeep Security Agentが不正プログラム対策保護を実行します。

注意: Deep Security9.5以前では、Deep Security Agentをインストールせずに仮想マシンを保護するには、Deep Security Virtual ApplianceとFilter Driverを使用します。従来、Filter DriverはESXiサーバにインストールされ、ハイパーバイザでネットワークトラフィックをインターセプトしてApplianceに送信するために使用されていました。VMwareによるvShield (VMsafe-NET APIドライバ) のサポートは終了しました。古いドライバはDeep Security 12.0でサポートされないため、削除する必要があります。

Agentレスによる保護ではApplianceと保護するコンピュータとの間の高速接続が必要なため、コンピュータとApplianceの距離が離れている (リモートESXiサーバまたは別のデータセンターにある) 場合はAgentレスを使用しないでください。

"vCloud環境でのAgentレスによる保護の実施" on page 354も参照してください。

コンバインモード

ヒント: YouTubeで [Deep Security 12 - Agentless to Agent Based Migration](#) を監視することで、エージェントレス保護環境からエージェントベース保護に移行するために必要ないくつかの手順を確認できます。

Deep SecurityVirtual Applianceでサポートされないその他の保護機能が必要な場合は、各仮想マシンにDeep Security Agentをインストールする必要がありますが、引き続きDeep Security Virtual Applianceを使用して一部の保護を提供することができます。これにより、パフォーマンスが向上します。ApplianceとAgentの両方を使用する方法は「コンバインモード」と呼ばれます。

コンバインモードでは、Applianceが不正プログラム対策と変更監視を提供し、Deep Security Agentがその他の機能を提供します。

協調的保護からコンバインモードへの変換

- 協調的保護: Deep Security 9.5では、仮想マシン上のAgentがオフラインの場合、代わりにDeep Security Virtual Applianceから保護機能が提供されます。ただし、各機能についてどちらを使用するかを個別に設定することはできません。
- コンバインモード: Deep Security 9.6では、それぞれの保護機能について、AgentまたはApplianceのどちらを使用するかを個別に設定できます。ただし、優先する保護ソースがオフラインの場合、もう一方の保護ソースが代わりに使用されることはありません。

Deep Security 10.0以降では、「保護ソース」の設定で両方の動作を設定できます。

- 各機能をAgentとApplianceのどちらから提供するか
- 優先する保護 (AgentまたはAppliance) を利用できない場合にもう一方を代わりに使用するかどうか

そのため、以前の協調的保護と同様の動作が必要な場合、Deep Security 9.6にアップグレードするのではなく、Deep Security 9.5からDeep Security 10.0にアップグレードしてから12.0にアップグレードすることをお勧めします。

各保護機能をAgentとApplianceのどちらから提供するかを選択

コンピュータをApplianceまたはAgentで保護できる場合は、各保護機能をどちらが提供するかを選択できます。

注意: セキュリティログ監視とアプリケーションコントロールには、この設定はありません。VMwareの最新の統合テクノロジーでは、これらの機能をDeep Security Virtual Applianceから提供することはできません。

保護ソースを設定するには、VMware vCenterをDeep Security Managerにインポートしてから、**コンピュータエディタまたはポリシーエディタ**¹で、[設定]→[一般]の順に移動します。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

コンバインモードの場合の保護ソース

AgentとApplianceの両方が存在する場合に保護を提供するコンポーネントを選択してください。

不正プログラム対策:	継承 (Appliance優先) ▼
Webレピュテーション / ファイアウォール / 侵入防御:	継承 (Agent優先) ▼
変更監視:	継承 (Appliance優先) ▼

ここに表示されていない保護モジュールでは、コンバインモードの設定はサポートされません。

各保護モジュールまたはモジュールグループに対して、次のいずれかを選択します。

- **Applianceのみ:** 仮想マシンにAgentがあり、Deep Security Virtual Applianceが無効化または削除されている場合でも、Applianceからのみ保護を提供します。

警告: Scanner (SAP) が必要な場合、Applianceは使用しないでください。ScannerにはDeep Security Agentの不正プログラム対策が必要です。

ヒント: Agentで不正プログラム対策が有効になっている場合、Anti-malware Solution Platform (AMSP) がダウンロードされてサービスとして起動されます。このサービスが不要な場合は、**[不正プログラム対策]** で **[Applianceのみ]** を選択してください。これにより、Applianceが無効化されている場合でも、AMSPサービスが起動されることはありません。

- **Appliance優先:** ESXiサーバに有効化されたApplianceがある場合は、そのApplianceが保護を提供します。ただし、Applianceが無効化または削除された場合は、Agentが代わりに保護を提供します。
- **Agentのみ:** 有効化されたApplianceがある場合でも、Agentからのみ保護を提供します。
- **Agent優先:** 仮想マシンに有効化されたAgentがある場合は、そのAgentが保護を提供します。しかし、有効化されたAgentがない場合は、Applianceが代わりに保護を提供します。

vCloud Director環境で、エージェント起動の有効化を使用して複合モードを有効にする

vCloud Directorの仮想マシンのホスト名がDeep Security Managerから解決できない場合は、エージェント起動のアクティベーションを使用して複合モードを有効にしてください。vCloud Directorの仮想マシンで複合モードを有効にするには

1. コンピュータに移動し、対象のvCloud Directorコンピュータを右クリックして、[アクティベーション]を選択します。
2. 対象のvCloud Directorコンピュータをダブルクリックし、ポップアップウィンドウで[設定>全般]を選択します。コミュニケーションの方向をAgent/Appliance 開始に変更します。

Communication Direction

Direction of Deep Security Manager to Agent/Appliance communication:

Agent/Appliance Initiated

3. 対象のvCloud DirectorコンピュータにDeep Security Agentをインストールし、[エージェントを有効にします](#)。

アプライアンスを配信する前に

Deep Security Virtual Applianceを配信する前に、次の手順を実行します。

- [この表](#)で、サポートされているNSXのライセンスとバージョンを確認します。
- [システム要件](#)を確認します。
- 必要な機能をAgentレスで利用できない場合は、「[コンバインモード](#)」を使用します。
- 高可用性のためにVMware DRS (Distributed Resource Scheduler) を使用する場合は (HA), [DRSの設定](#))。
- ゲスト仮想マシンがネットワークカードに直接アクセスできるように設定した場合は、それらの仮想マシンにAgentをインストールしてください。この場合は、パケットをインターセプトすることができないため、ゲスト内にAgentをインストールすることをお勧めします。詳細については、"[Agentレスによる保護またはコンバインモードの保護の選択](#)" [on page 315](#)を参照してください。
- VMwareの用語で「サービスVM」と呼ばれる仮想アプライアンスが、管理ネットワークレベルでパートナーのService Manager (コンソール) と通信できることを確認します。詳細については、NSX-Tを使用している場合はこの[NSX-Tヘルプページ](#)、この[NSX-Vヘルプページ](#)を参照してくださいifあなたはNSX-Vを使用しています。

これで、アプライアンスを配信する準備ができました。VMware環境に応じて、次のいずれかのページに進んでください。

- Applianceのインストール (NSX-T)
- Deep Security Virtual Applianceの配信

- "vCloud環境でのAgentレスによる保護の実施" on page 354

Applianceのインストール (NSX-T)

"アプライアンスを配信する前に" on the previous pageのタスクを完了したら、NSX-T Data Centerにアプライアンスを配信する準備が整いました。以下の手順に従ってください。

注意: NSX Data Center for vSphere (NSX-V) へのインストールについては、「Applianceのインストール (NSX-V)」を参照してください。

- "手順1: Deep Security ManagerにApplianceパッケージをインポートする" below
- "手順2: ファブリック設定を準備する" on the next page
- "手順3: Deep Security ManagerにvCenterを追加する" on page 327
- "手順4: Deep Security Virtual ApplianceをNSX-Tにインストールする" on page 327
- "手順5: エンドポイント保護を設定する" on page 331
- "手順6: NSX-Tで有効化を準備する" on page 334
- "手順7: 有効化とポリシーの割り当てを開始する" on page 353
- "手順8: 仮想マシンが有効化されて、ポリシーが割り当てられていることを確認する" on page 354
- "次の手順 (新しい仮想マシンを追加する方法)" on page 354

新しいOSの脆弱性から保護するために"Deep Security Virtual Applianceのアップグレード" on page 1006することもできます。

手順1: Deep Security ManagerにApplianceパッケージをインポートする

次の手順を実行し、Deep Security Virtual ApplianceをダウンロードしてDeep Security Managerにインポートします。

1. Deep Security Managerコンピュータで、<https://help.deepsecurity.trendmicro.com/ja-jp/software.html>のソフトウェアページに移動します。
2. 最新のDeep Security Virtual Applianceパッケージをコンピュータにダウンロードします。
3. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に進みます。
4. [インポート]をクリックして、パッケージをDeep Security Managerにアップロードします。

Applianceのパッケージをインポートすると、Applianceの仮想マシンのOSと互換性のあるDeep Security Agentソフトウェアを、Deep Security Managerが自動的にダウンロードします。このAgentソフトウェアは、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に表示されます。Applianceをインストールすると、組み込みのAgentソフトウェアは、初期設定で [ローカルソフトウェア] 内の最新の互換バージョンに自動的にアップグレードされます。[管理]→[システム設定]→[アップデート]タブ→[Virtual Applianceの配置]をクリックすると、自動アップグレードのバージョンを変更できます。

注意: Deep Security Virtual Applianceのパッケージのバージョンを [ローカルソフトウェア] に複数表示することも可能です。新しいDeep Security Virtual Applianceをインストールした場合は、常に最新バージョンが選択されます。

5. オプションで、Microsoft Windowsを実行するゲスト仮想マシンの場合は、Deep Security Notifierをダウンロードすることもできます。Notifierは、Deep Securityシステムイベントのメッセージをシステムトレイに表示するコンポーネントです。詳細については、"[Deep Security Notifierのインストール](#)" on page 437を参照してください。

手順2: ファブリック設定を準備する

最初に、NSX-T Managerを使用してvCenterを追加します。

1. vCenterとESXiサーバが管理用に設定されていることを確認します。
2. NSX-T Managerで、上部にある [System] をクリックしてから、左側で [Fabric]→[Compute Managers] の順にクリックします。
3. [+ADD] をクリックします。
4. [New Compute Manager] ダイアログボックスが表示されます。

5. vCenterの情報をフィールドに入力します。次に例を示します。

New Compute Manager

Name* 10.201.111.111

Description vCenter-10.201.111.111

Domain Name/IP Address* 10.201.111.111

Type* vCenter

Username* administrator@vsphere.local

Password*

SHA-256 Thumbprint

CANCEL ADD

6. [ADD] をクリックします。vCenterが追加されます。

Compute M	ID	Domain Name/IP Ac	Type	Registration Status	Version	Connection Status	Last Inventory Upd
<input type="checkbox"/>	10.201.1...	8bd3...9...	vCenter	Registered	6.7.0	Up	Apr 1, 2019 1:32...

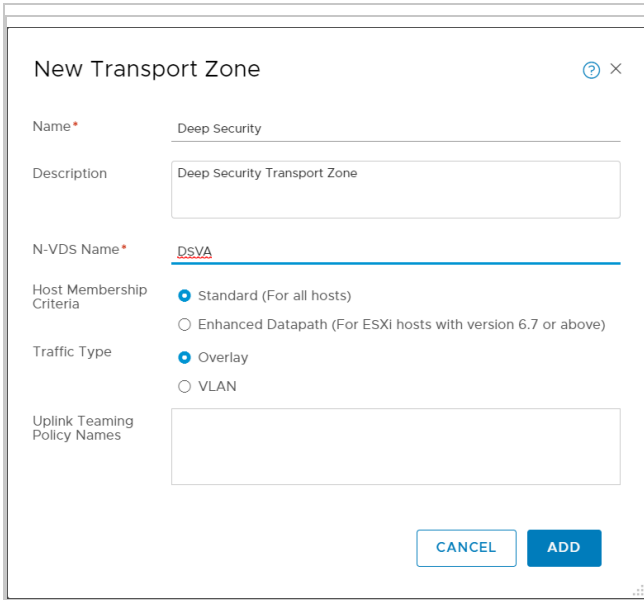
7. vCenterの [Registration Status] が [Registered] で、[Connection Status] が [Up] であることを確認します。

これで、vCenterの追加が完了しました。

次に、Deep Security転送ゾーンを設定します（まだ設定していない場合）。

1. NSX-T Managerで、[Fabric]→[Transport Zones] の順に進み、[+ADD] をクリックして、Virtual Appliance用のトランスポートゾーンを作成します。

2. [New Transport Zone] ダイアログボックスが表示されます。



The screenshot shows a dialog box titled "New Transport Zone". It contains the following fields and options:

- Name:** Deep Security
- Description:** Deep Security Transport Zone
- N-VDS Name:** DSVA
- Host Membership Criteria:** Standard (For all hosts), Enhanced Datapath (For ESXi hosts with version 6.7 or above)
- Traffic Type:** Overlay, VLAN
- Uplink Teaming Policy Names:** (Empty text box)

Buttons at the bottom: CANCEL, ADD

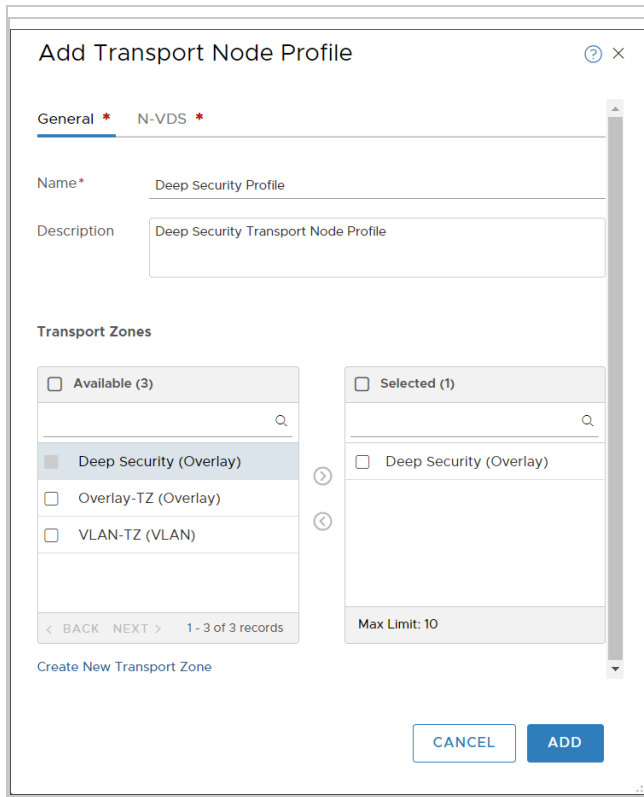
3. フィールドに入力します。[Host Membership Criteria] および [Traffic Type] には任意の値を設定してください。上記の例では、[Standard (For all hosts)] および [Overlay] が選択されています。
4. [ADD] をクリックします。

トランスポートゾーンが作成されます。

次に、Deep Securityトランスポートノードプロファイルを作成します（まだ作成していない場合）。

1. NSX-T Managerで、左側にある [Profiles] をクリックしてから、メイン画面で、[Transport Node Profiles] をクリックします。

[Add Transport Node Profile] ダイアログボックスが表示されます。



2. 上記の画像に示されているように、フィールドに入力します。Deep Securityのトランスポートゾーンが [Selected] 列に移動していることを確認します。
3. ダイアログボックスの上部で [N-VDS] をクリックし、次のようにフィールドに入力します。
 - [N-VDS Name] には、[DSVA] またはDeep Securityトランスポートゾーンを作成したときに指定した名前を選択します。
 - [NIOC Profile] には、[nsx-default-nioc-hostswitch-profile] を選択します。
 - [Uplink Profile] には、[nsx-default-uplink-hostswitch-profile] を選択します。
 - [LLDP Profile] には、[LLDP [Send Packet Enabled]] を選択します。
 - [IP Assignment] には、[Use IP Pool] または [Use DHCP] を選択します。必要な方を使用します。
 - [IP Pool] が表示されている場合は、[OR Create and Use a new IP Pool] をクリックし、名前が `dsva-ip-pool` のIPプールを作成して、それを [IP Pool] の値として使用します。
 - [Physical NICs] が表示されている場合は、物理NICを追加します。たとえば、[uplink-1] に `vmnic2` を使用します。

それぞれの値の詳細を確認するには、ダイアログボックスの上部にある
②
をクリックします。

ダイアログボックスは次のようになります。

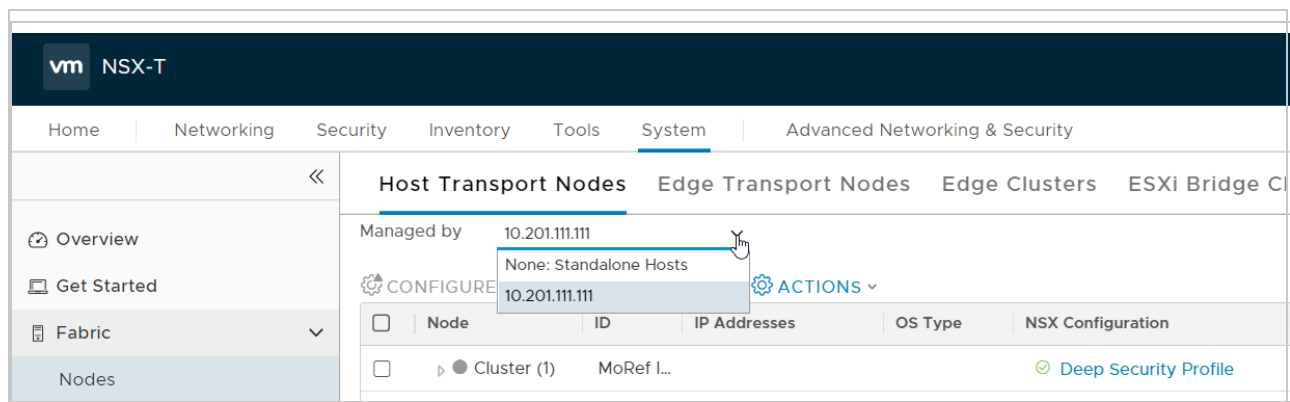
The screenshot shows a dialog box titled "Add Transport Node Profile". It has two tabs: "General" and "N-VDS". The "N-VDS" tab is selected. Under "N-VDS Creation", there are two radio buttons: "NSX Created" (selected) and "Preconfigured". Below this is a section titled "New Node Switch" with several dropdown menus: "N-VDS Name" (DsVA), "Associated Transport Zones" (Deep Security), "NIOC Profile" (nsx-default-nioc-hostswitch-profile), "Uplink Profile" (nsx-default-uplink-hostswitch-profile), "LLDP Profile" (LLDP [Send Packet Enabled]), "IP Assignment" (Use IP Pool), and "IP Pool" (dsva-ip-pool). There are "CANCEL" and "ADD" buttons at the bottom.

4. [General] タブおよび [N-VDS] タブに入力した後、[ADD] をクリックします。

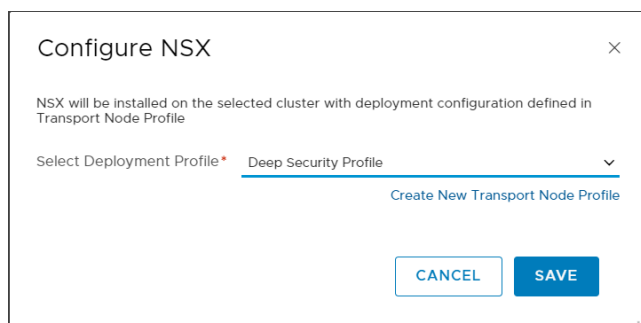
Deep Security Transport Node Profileという名前のトランスポートノードプロファイルが作成されます。

次に、Deep Security転送ノードプロファイルをクラスタに適用します（まだ実行していない場合）。

1. [Fabric]→[Nodes] の順にクリックし、メイン画面で [Host Transport Nodes] をクリックします。
2. [Managed by] ドロップダウンリストで、先ほど追加したvCenterを選択します。この例では、vCenterは10.201.111.111です。



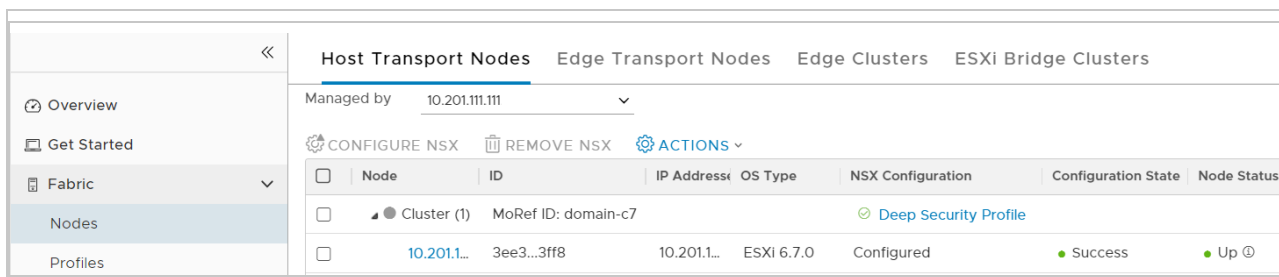
3. Deep Security Virtual Applianceで保護する仮想マシンが含まれているクラスタを選択します。クラスタが2つ以上ある場合は、Deep Security Virtual Applianceで保護するクラスタをすべて選択します。
4. [CONFIGURE NSX] をクリックします。
5. [Select Deployment Profile] ドロップダウンリストから、[Deep Security Profile] または Deep Securityトランスポートノードプロファイルに該当するものを選択します。



6. [SAVE] をクリックします。

次の処理が行われます。

- Deep Securityトランスポートノードプロファイルがクラスタに適用されます。
- プロファイルの適用中に、「NSX Install in Progress」というメッセージが表示される場合があります。
- 操作が完了すると、各ノードの [Configuration Status] が [Success] に変更され、[Node Status] が [Up] に変更されます。ESXiサーバが複数ある場合は、そのすべてが [Success] および [Up] としてマークされる必要があります。



これで、NSX-T Managerでファブリック設定の準備ができました。

手順3: Deep Security ManagerにvCenterを追加する

"VMware vCenterの追加" on page 512に記載されている手順に従って、Deep Security ManagerにvCenterを追加します。

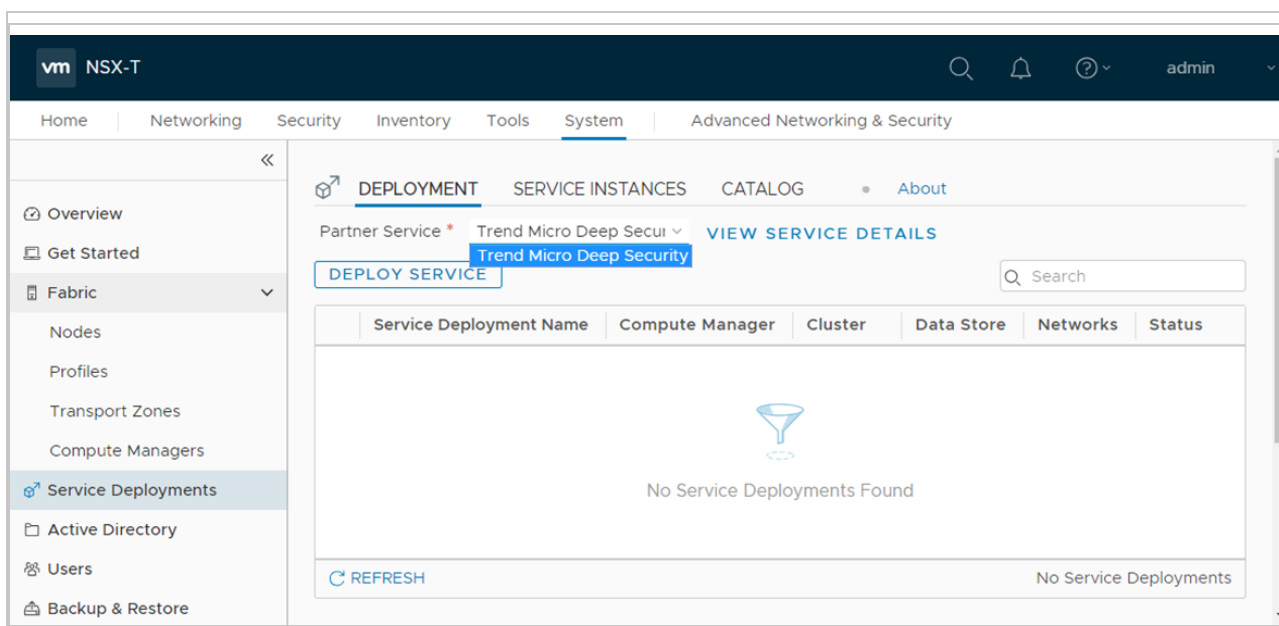
完了後:

- ゲスト仮想マシンがDeep Security Managerに表示されます。
- Trend Micro Deep SecurityサービスがNSX-Tに登録されます。

手順4: Deep Security Virtual ApplianceをNSX-Tにインストールする

Deep Security Virtual Applianceはクラスタごとにインストールする必要があります。

1. NSX-T Managerで、[System] をクリックしてから、[Service Deployments] を選択します。

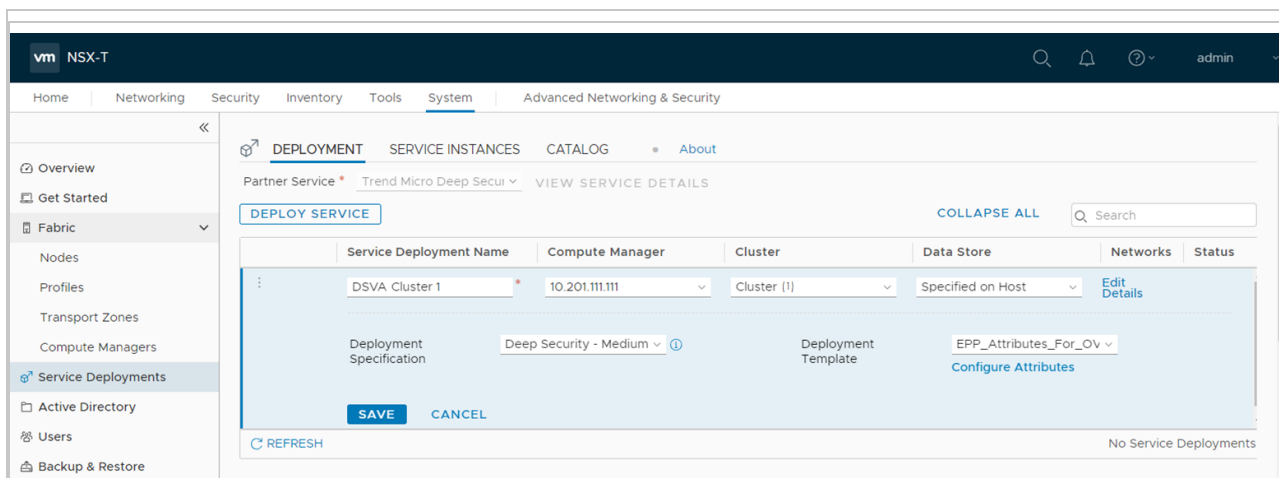


2. [Partner Service] ドロップダウンリストから、[Trend Micro Deep Security] を選択します。Trend Micro Deep Securityサービスは、Deep Security ManagerでvCenterを追加したときに登録されています。
3. [DEPLOY SERVICE] をクリックします。
4. 以下のようにフィールドに入力します。
 - [Service Deployment Name] に、名前を入力します。クラスタが複数ある場合は、インストール先となるクラスタの名前が含まれた名前にすることを検討してください。インストール先となるクラスタは、同じページの [Cluster] 見出しの下のリストに表示されます。例: `DSVA Cluster 1`。
 - [Compute Manager] には、先ほど追加したvCenterを選択します。この例では、vCenterは`10.201.111.111`です。
 - [Cluster] には、先ほど設定したクラスタを選択します。Trend Micro Deep Security サービスが、このクラスタのすべてのESXiサーバにインストールされます。クラスタが複数ある場合、ここでは1つだけ選択します。別のクラスタを選択するために後でこの手順に戻ることもできます。
 - [Data Store] には、お使いの環境に適したオプションを選択します。この例では、[Specified on Host] を選択しています。
 - [Networks] では、[Set] と [Edit Details] のいずれかを使用できる方をクリックし、[ens0 - MANAGEMENT] を設定します。ネットワークをホストまたはDVPGに指定し、ネットワークタイプ→DHCPまたは静的IP プールを選択します。[SAVE] をクリックします。

注意: ホストまたは DVPG で Specifiedが表示または選択できない場合は、この knowledge baseページを参照して回避策を参照してください。

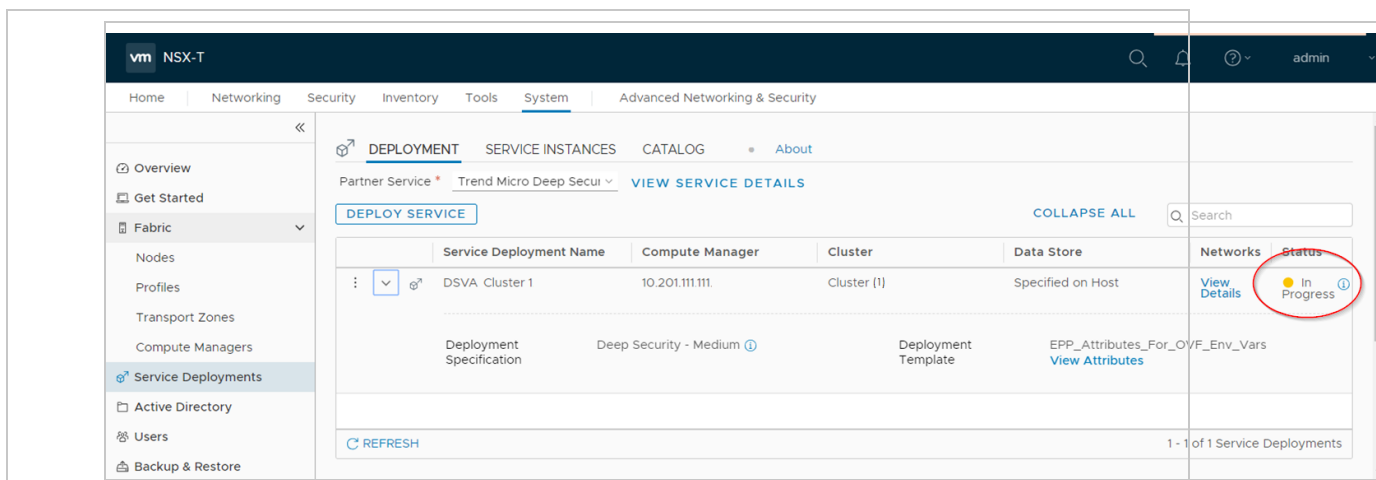
- [Deployment Specification] には、[Deep Security - Medium] を選択します。
- [Deployment Template] には、[EPP_Attributes_For_OVF_Env_Vars] を選択します。

サービスのインストールの詳細は次のようになります。



5. [SAVE] をクリックします。

サービスのインストールが開始されます。



NSX-T Managerの [Status] 列に、[In Progress] と表示されます。

6. 完了するまで待ちます。インストールが完了すると、[Status] が [Up] に変更されます。

割り当てたクラスタにESXiサーバが複数ある場合は、Trend Micro Deep Securityサービスが各ESXiサーバにインストールされます。サービスには区別できるように次のようなラベルが付けられます。

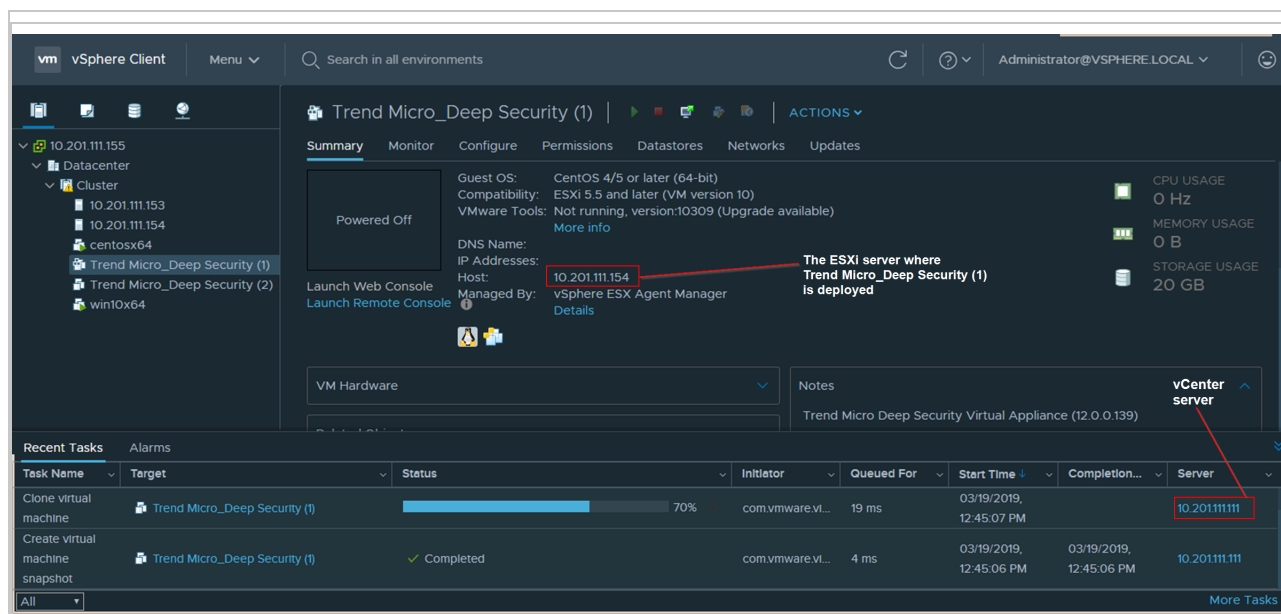
- Trend Micro_Deep Security (1) (1つ目のESXiサーバの場合)
- Trend Micro_Deep Security (2) (2つ目のESXiサーバの場合)

などです。

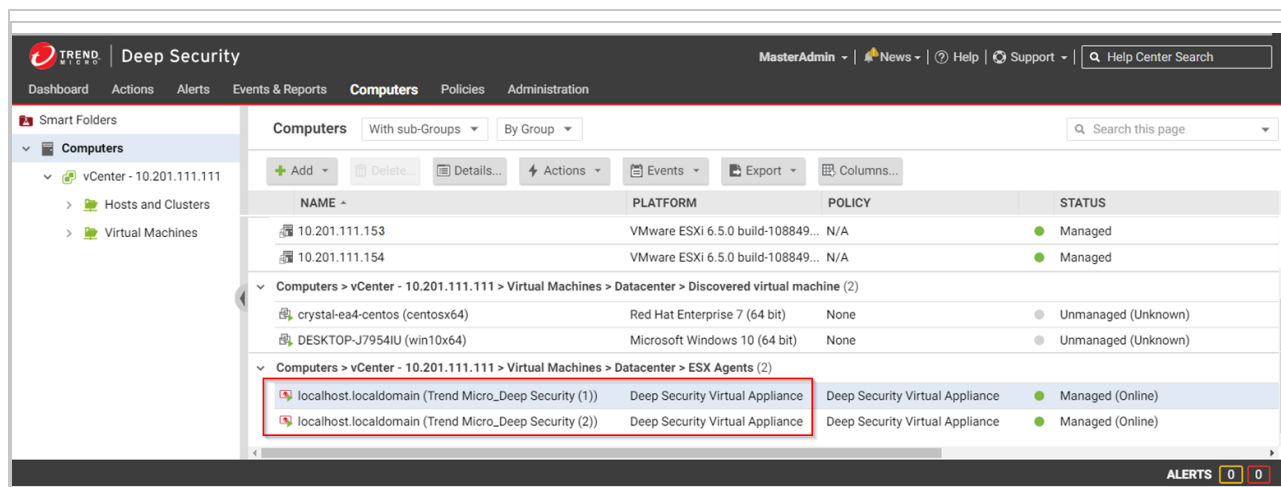
Trend Micro Deep Security(オンプレミス) 12.0

- (オプション) vSphere ClientからvCenterにアクセスしてインストールのステータスを確認します。vSphere Clientにはさらに詳しく進行状況が表示されます。[Status] が [Complete] に変更されるまで待ちます。

注意: 下の画像で、Trend Micro Deep Securityサービスが2つ、左側にリスト表示されているのがわかります。クラスタにESXiサーバが2つあるため、サービスが2つインストールされました。



- 上部にある [Computers] をクリックし、Trend Micro Deep SecurityサービスがインストールされたvCenterを左側で展開して、配置が完了していることをDeep Security Managerで確認します。



[Virtual Machines]→[Datacenter]→[ESX Agents] の下に、Deep Security Virtual Applianceというプラットフォームと共にTrend Micro_Deep Security (1) が表示されます。クラスタ内のESXiサーバごとにVirtual Applianceが1つあるのを確認できます。

9. クラスタごとに、"[手順4: Deep Security Virtual ApplianceをNSX-Tにインストールする](#) on page 327のすべての手順を繰り返します。

Deep Security Managerに仮想マシンが表示されますが、仮想マシンはこの時点では保護されていません。

手順5: エンドポイント保護を設定する

エンドポイント保護の設定は、Deep Security Virtual Applianceで既存の仮想マシンを保護するために必要です。

まず、Deep Security Virtual Applianceで保護する仮想マシンが含まれるグループを作成します。

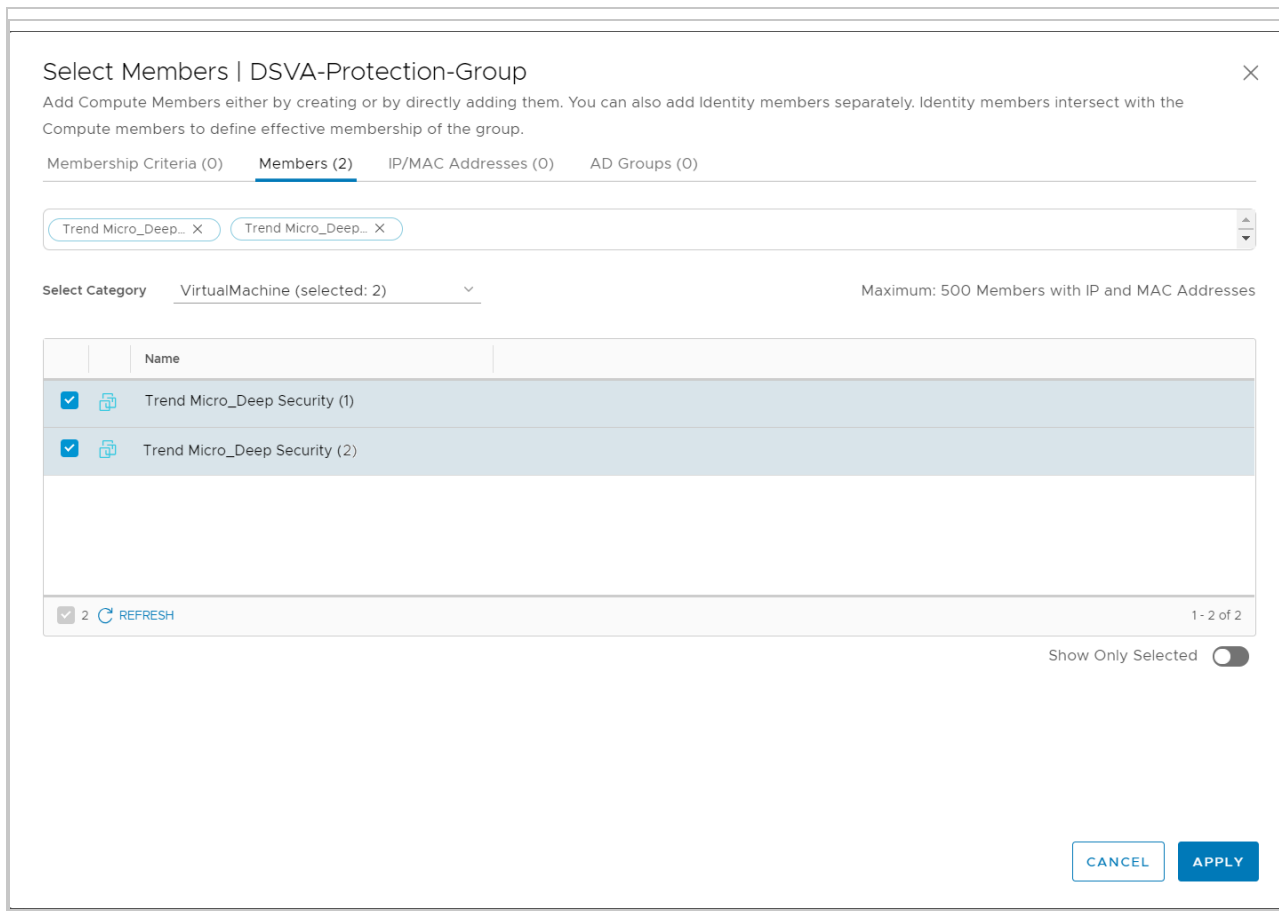
1. NSX-T Managerで、上部にある [Inventory] をクリックし、左側で [Groups] をクリックします。
2. [ADD GROUP] をクリックして、Deep Security Virtual Applianceで保護される仮想マシンが含まれるグループを作成します。以下のようにフィールドに入力します。
 - [Name] には、グループの名前を入力します。例: DSVA-Protection-Group。
 - [Domain] では、[default] を選択するか、[Inventory]→[Domains] の下に新しいドメインを作成します。
 - [Compute Members] では、[Set Members] をクリックしてグループに含める仮想マシンを選択します。

注意: 以下の手順では、メンバーを追加する最も簡単な方法を説明します。

[Membership Criteria] などを使用する、より複雑な方法については、NSX-Tのドキュメントを参照してください。

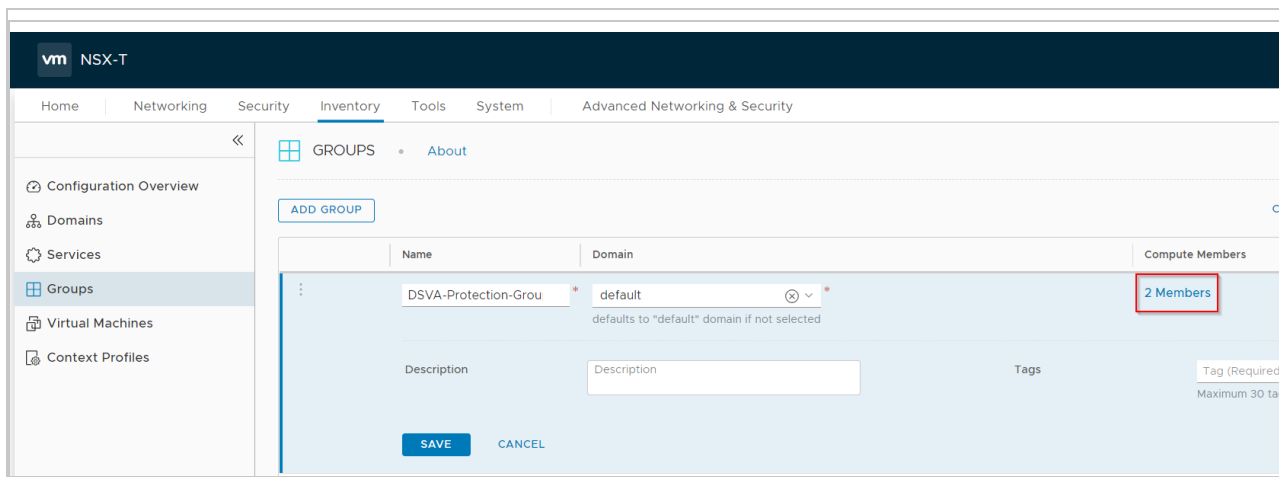
3. 上部にある [Members (0)] をクリックし、[VirtualMachine (selected: 0)] を選択します。
4. 仮想マシンが表示されていない場合は、下部の [Refresh] をクリックします。
5. グループに追加するゲストVMを選択します。選択した仮想マシンは、Deep Security Virtual Applianceによって保護されます。

[メンバーの選択] ダイアログボックスが次のようになり、ゲストVMが選択され、Trend Micro_Deep Securityの が選択解除されました。仮想アプライアンスを保護する必要がないためです。



6. 上部付近にある [Members] タブで仮想マシンの数を確認します。上記の例では、仮想マシンの数は1つです。
7. [APPLY] をクリックします。

[ADD GROUP] ページには、更新された数が表示されます。



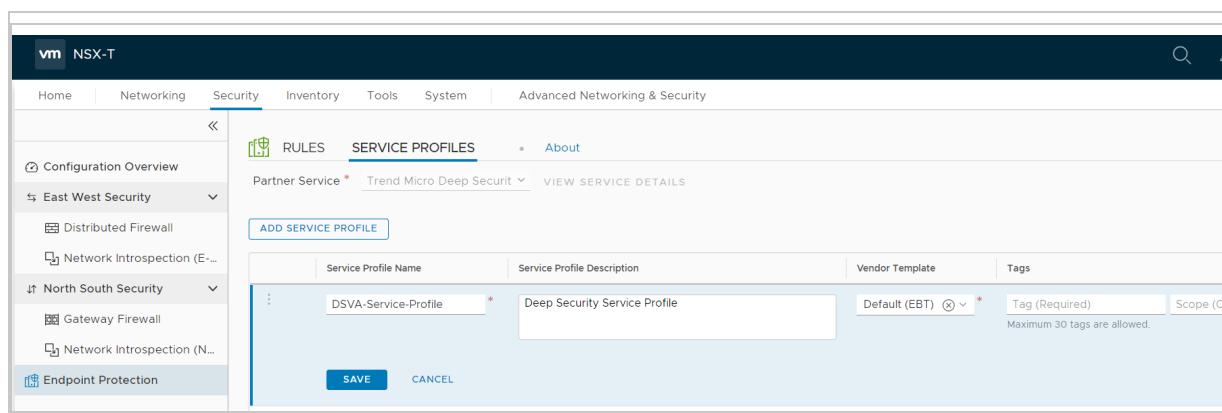
8. [SAVE] をクリックします。

これでメンバーが含まれたグループを追加することができました。

次に、Deep Security Virtual Applianceのサービスプロファイルを設定します。

1. NSX-T Managerで、上部にある [Security] をクリックし、左側の [Endpoint Protection] をクリックします。
2. メイン画面で、[SERVICE PROFILES] をクリックします。
3. [Partner Service] ドロップダウンリストから、[Trend Micro Deep Security] を選択します (選択されていない場合)。
4. [ADD SERVICE PROFILE] をクリックし、次のようにフィールドに入力します。
 - [Service Profile Name] フィールドでは、名前を指定します。例: `DSVA-Service-Profile`
 - [Service Profile Description] では、説明を入力します。例: `Deep Security Service Profile`
 - [Vendor Template] では、[Default (EBT)] を選択します。このテンプレートは、Trend Micro Deep Securityサービスと同時にロードされました。

[ADD SERVICE PROFILE] ページの表示内容は、次のようになります。

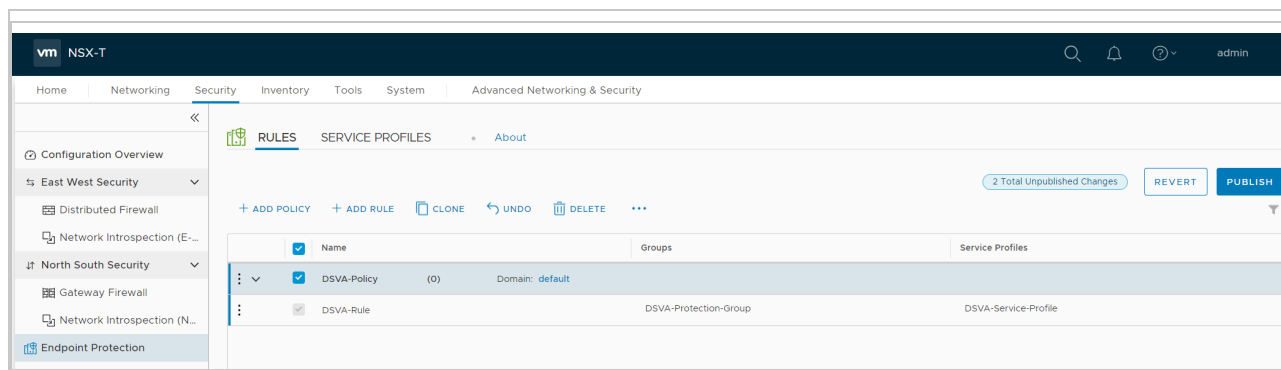


Service Profile Name	Service Profile Description	Vendor Template	Tags
DSVA-Service-Profile *	Deep Security Service Profile	Default (EBT) ⌵ *	Tag (Required) Scope (Optional) Maximum 30 tags are allowed.

5. [SAVE] をクリックします。
6. [RULES] に切り替えて、[+ ADD POLICY] をクリックします。
7. [Name] 列で、[New Policy] セル内をクリックして名前を変更します。名前の例: `DSVA-Policy`
8. [DSVA-Policy] の横にあるチェックボックスをオンにし、[+ ADD RULE] をクリックします。[DSVA-Policy] の下にルールが表示されます。
9. ルールに名前を付けて、対応するグループとサービスプロファイルを選択します。たとえば、ルールに `DSVA-Rule` という名前を付け、[DSVA-Protection-Group] と [DSVA-

Service-Profile] を選択します。これで、DSVA-Protection-Groupの仮想マシンとDSVA-Service-Profileで指定したDefault (EBT) テンプレートとのマッピングが完了しました。

ポリシーは次のようになります。



10. [PUBLISH] をクリックして、ポリシーとルールを作成を完了します。

これで、NSX-Tでエンドポイント保護の設定が完了しました。仮想マシンは現時点では保護されていません。

手順6: NSX-Tで有効化を準備する

次のステップでは、Deep Securityで既存のVMをアクティベートします。アクティベーション方法の詳細については、次の表を参照してください。次の表を参照して、"[方法1: 「コンピュータの作成」 イベントベースタスクを作成する](#)" on page 352のプロセスを確認してください。"[方法1: 「コンピュータの作成」 イベントベースタスクを作成する](#)" on page 352 を作成します（これは、NSX-Tの配置でサポートされる唯一のメソッドです）。

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
方法1: 「コンピュータの作成」	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
イベントベースタスクを作成する													

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
	または NSX for vShield Endpoint (無料)												
詳細を表示	この方法では												

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
	、 が新しく作成する が												

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
	、自動的に有効化され、ポリシー												

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
	が割り当てられます。												
方	X	✓ ₁	✓ ₁	X	X	✓ ₁	✓ ₁	✓ ₁	X	X	X	X	X

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
法2: 「NSXセキュリティグループ													

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
変更イベントベースタスクを													

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
詳細を表示													

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
——	また、既存の仮想マシンが												

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
い 有 交 作 し た り 、 ホ ス ト シ ス ー が 害													

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
—													
方法 3: Deep Security ポリシ	X	✓ ₁	✓ ₁	X	X	✓ ₁	✓ ₁	✓ ₁	X	X	X	X	X

Deep Security Virtual Appliance環境													
	NSX for vSphere (NSX-V) 6.3.x~6.4.x			NSX for vSphere (NSX-V) 6.4.x					NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
一とNSXを同期する。 詳細を表示													

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x						NSX-T 2.4.x、2.5.x					
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
	この方法												

Deep Security Virtual Appliance環境													
NSX for vSphere (NSX-V) 6.3.x~6.4.x		NSX for vSphere (NSX-V) 6.4.x							NSX-T 2.4.x、2.5.x				
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
—													

¹ VMwareのNetwork Introspection Serviceが必要です。

方法1: 「コンピュータの作成」 イベントベースタスクを作成する

次の手順はタスクベースです。イベントベースタスクに関する詳細については、"[NSX環境での自動ポリシー管理](#)" on page 359を参照してください。

1. Deep Security Managerで、上部の [管理] をクリックします。
2. 左側で、[イベントベースタスク] をクリックします。
3. メイン画面で、[新規] をクリックします。
4. [イベント] ドロップダウンリストから [コンピュータの作成 (システムによる)] を選択します。[コンピュータの作成 (システムによる)] イベントタイプは、新しい仮想マシンを作成するとトリガされます。

[次へ] をクリックします。

5. [コンピュータの有効化] を選択して5分に設定します。
6. [ポリシーの割り当て] を選択し、Windows Server 2016など、ドロップダウンリストからポリシーを選択します。矢印をクリックすると、子ポリシーを表示できます。[次へ] をクリックします。
7. イベントベースタスクがトリガされたときに制限する条件を指定します。次の条件を追加します。

[vCenter名] が <ご使用のvCenter名> と一致する

8. イベントベースタスクがトリガされたときにさらに制限する条件を追加します。たとえば、すべてのWindows仮想マシンに接頭語「Windows」を含めるという命名規則を仮想マシンに使用している場合は、次のように設定します。

[コンピュータ名] が Windows* と一致する

[次へ] をクリックします。

9. [名前] フィールドで、Activate Windows Server 2016 など、割り当てたポリシーを反映させるタスクの名前を入力します。
10. [タスクの有効化] を選択して [完了] をクリックします。
11. 割り当て時に計画したDeep Securityポリシーごとに追加のイベントベースタスクを作成します。イベントベースタスクのイベントタイプには [コンピュータの作成 (システムによる)] を指定し、コンピュータを有効化してポリシーの割り当てを実行できるように設定する必要があります。

新しく作成した仮想マシンを有効化してポリシーを割り当てられるようにイベントベースタスクを設定しました。仮想マシンが作成されるとすぐに、[コンピュータの作成 (システムによる)] イベントベースタスクのすべてがレビューされます。タスクの条件が一致すると、タスクがトリガされます。また、仮想マシンが有効化され、関連するポリシーが割り当てられます。

手順7: 有効化とポリシーの割り当てを開始する

次に、ポリシーを手動で有効化して既存の仮想マシンに割り当てる必要があります。

1. Deep Security Managerに移動して、上部の [コンピュータ] をクリックし、左側でvCenterをクリックします。ゲスト仮想マシンが右側に表示されます。
2. <Shift> キーを押しながら仮想マシンのセットをクリックし、そのセットを右クリックして [Actions] → [Assign Policy] の順に選択します。ポリシーを選択して [OK] をクリックします。Deep Securityのポリシーが仮想マシンに割り当てられます。

3. <Shift> キーを押しながら同じ仮想マシンのセットをクリックし、そのセットを右クリックして [Actions]→[Activate/Reactivate] の順に選択します。仮想マシンがDeep Security Managerで有効化されます。これで、仮想マシンが保護された状態になりました。
4. 既存の仮想マシンをさらに保護する場合は、このセクションの手順を繰り返して、ポリシーを割り当てて仮想マシンを有効化します。

手順8: 仮想マシンが有効化されて、ポリシーが割り当てられていることを確認する

Deep Security Managerの仮想マシンが有効化され、ポリシーが割り当てられていることを確認します。

1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. 左側で、[コンピュータ]→[<ご使用のvCenter>]→[仮想マシン] を選択します。
3. [タスク] 列および [ステータス] 列を確認します。(列が表示されていない場合は、上部で [列] をクリックして追加します)。[タスク] 列に [有効化中] と表示され、仮想マシンのステータスが [非管理対象 (不明)] から [非管理対象 (Agentなし)] や [管理対象 (オンライン)] に変わります。仮想マシンのステータスが [VMware Toolsがインストールされていない] になることがありますが、これは一時的です。
4. [ポリシー] 列をチェックして、Deep Securityポリシーが正しく割り当てられていることを確認します。

これで、Deep Security Virtual Applianceがインストールされ、仮想マシンが保護されます。

次の手順 (新しい仮想マシンを追加する方法)

新しい仮想マシンをシステムに追加してDeep Securityで保護するには、新しい仮想マシンをvCenterに作成します。これにより、[コンピュータの作成 (システムによる)] イベントベースタスクが開始し、新しい仮想マシンの有効化およびポリシーの割り当てが行われます。これで、新しい仮想マシンがDeep Securityで保護されるようになります。

vCloud環境でのAgentレスによる保護の実施

VMware vCloudとの統合により、マルチテナントインストールのプライマリテナントは、Deep Security ManagerにvCenterを追加し、コネクタを設定し、Deep Security Virtual Applianceを配信および管理できます。その後、テナントはvCloud Organizationsをクラウドアカウントとしてインポートし、エージェントレスDeep Securityの保護を適用できます。

このトピックの内容:

- ["開始前の準備" below](#)
- ["vCloud仮想マシンのAgentレスによる保護を有効にする" below](#)
- ["マルチテナント環境を作成する" below](#)
- ["vCenterを追加してDeep Security Virtual Applianceを配置する" below](#)
- ["Deep SecurityでVMware vCloudリソースを使用できるように設定する" on the next page](#)
- ["仮想マシンでVirtual Appliance保護を有効にする" on page 357](#)

開始前の準備

開始前の準備:

- [この表](#)で、サポートされているNSXのライセンスとバージョンを確認します。
- [システム要件](#)を確認します。
- 必要な機能をAgentレスで利用できない場合は、「[コンバインモード](#)」を使用します。
- ゲスト仮想マシンがネットワークカードに直接アクセスできるように設定した場合は、それらの仮想マシンにAgentをインストールしてください。この場合は、パケットをインターセプトすることができないため、ゲスト内にAgentをインストールすることをお勧めします。詳細については、「[Agentレスによる保護またはコンバインモードの保護の選択](#) on page 315」を参照してください。

vCloud仮想マシンのAgentレスによる保護を有効にする

1. Deep Security Managerコンソールで、[管理]→[システム設定]→[Agent] の順に選択します。
2. [vCloud VMsの アプライアンスの許可を有効にする]チェックボックスをオンにします。
3. [保存] をクリックします。

マルチテナント環境を作成する

マルチテナント環境を作成するために必要なタスクは、主に2つあります。マルチテナントの有効化とテナントの作成です。これらのタスクの実施方法に関する詳細な手順、マルチテナント環境の要件と推奨事項については、「[マルチテナント環境の設定](#) on page 279」を参照してください。

vCenterを追加してDeep Security Virtual Applianceを配置する

プライマリテナントでvCenterを追加し、Deep Security Virtual Applianceを配置する必要があります。手順については、「[Applianceのインストール \(NSX-V\)](#)」または「[Applianceのインス](#)

[ツール \(NSX-T\)" on page 320](#)を参照してください。

Deep SecurityでVMware vCloudリソースを使用できるように設定する

Deep Securityとの統合のためのVMware vCloudリソースを設定するには

- ["vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する" below](#)
- ["新しい仮想マシンに一意的UUIDを割り当てる" on the next page](#)
- ["ゲスト仮想マシンでVMware Toolsの \[OVF Environment Transport\] を有効にする" on the next page](#)

vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する

vCloud Directorで作成した、Deep SecurityのテナントがDeep Security Managerにクラウドアカウントを追加するために使用するユーザアカウントには、の[すべての権限]→[一般]→[管理者ビュー 権限]の権限のみが必要です。

1. vCloud Directorにログインします。
2. [System] タブで [Administration] をクリックします。
3. 左側のナビゲーションパネルで [Roles] をクリックします。
4. 「プラス」記号 (+) をクリックして新しいロール (「DS_User」 など) を作成します。
5. [All Rights]→[General] フォルダの [Administrator View] 権限を選択します。
6. [OK] をクリックします。

これで、Deep Security ManagerにvCloudリソースをインポートするユーザアカウントにこの役割を割り当てることができます。

注意: Deep Securityのユーザにこの資格情報を提供する際は、vCloud OrganizationのIPアドレスも通知してください。また、vCloudのリソースをDeep Security Managerにインポートする際は、ユーザ名に「@orgName」を含めるように指示してください。たとえば、vCloudアカウントのユーザ名がuserで、アカウントのアクセス権を付与されたvCloud OrganizationがCloudOrgOneである場合、Deep Securityのユーザは、vCloudのリソースをインポートするときにユーザ名として「user@CloudOrgOne」と入力する必要があります。(vCloud管理者の場合、@systemを使用します)。

注意: クラウドアカウントで保護されているインスタンスへの接続にプロキシサーバを使用するよう、Deep Security Managerを設定できます。プロキシ設定は、[管理]→[システム設定]→[プロキシ]→[プロキシサーバの使用]→[Deep Security Manager (クラウドアカウント)]で行います。

新しい仮想マシンに一意的UUIDを割り当てる

Deep Securityでは、保護対象のすべての仮想マシンに一意的UUIDを割り当てる必要があります。vAppテンプレートから作成した仮想マシンにはUUIDを重複して割り当てることができるため、問題が発生する場合があります。一意的UUIDを割り当てるようにvCloudデータベースを設定するには、[VMwareナレッジベースの記事2002506](#)に従って、CloneBiosUuidOnVmCopy プロパティをゼロ (0) に設定します。

ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする

ゲストVM上のVMware ToolsのOVF Environment Transportを有効にすると、guestInfo.ovfEnv 環境変数が公開され、エージェントはVMをDeep Security Managerに対して一意に識別できるようになります。これにより、仮想マシンの誤認リスクが低減されます。

1. vCloud Directorで、VMの[Properties] []画面を開き、[Guest OS Customization]タブに移動し、の[Guest customization を有効にする]チェックボックスをオンにします。[OK] をクリックします。
2. vCenterで同じ仮想マシンを選択し、[Properties] 画面を開いて [Options] タブに進みます。
3. [vApp Options] をクリックし、[Enabled] オプションを選択します。これで [OVF Settings] が公開されます。
4. OVF Settingsで、OVF Environment Transport 領域の VMware Tools チェックボックスをオンにします。[OK] をクリックします。

仮想マシンが実行中の場合は、変更を有効にするために再起動する必要があります。

Deep Securityで使用されるデータは、プロパティvmware.guestinfo.ovfenv.vcenteridおよびvmware.guestinfo.ovfenv.vcloud.computernameから取得されます。

仮想マシンでVirtual Appliance保護を有効にする

仮想アプライアンスの保護を有効にするには、テナントがvCloud Organizationアカウントをインポートし、エージェントレスDeep Security保護を適用する必要があります。

注意: vCloud組織アカウントはテナント別に追加する必要があります (プライマリテナントではない)。

VMware vCloud Organizationアカウントからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで[コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。

2. [名前] に表示名を、[説明] に追加メモを入力します。
3. [アドレス] にvCloud Directorのホスト名を入力します。
4. ユーザ名とパスワードを入力します。

注意: ユーザ名は、username@vcloudorganizationの形式にします。

5. [次へ] をクリックします。
6. Deep Security Managerは、クラウドリソースへの接続を確認し、インポート処理の概要を表示します。[完了] をクリックします。

VMware vCloudのリソースが、Deep Security Managerのナビゲーションパネル内の [コンピュータ] の下に、それぞれ別個の項目として表示されます。

VMware vCloud Air仮想データセンターからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで [コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するVMware vCloud Air仮想データセンターの名前と説明を入力します(Deep Security Managerでの表示に使用されます)。
3. VMware vCloud Air仮想データセンターのアドレスを入力します。

VMware vCloud Air仮想データセンターのアドレスを確認するには、次の手順を実行します。

- a. VMware vCloud Airポータルにログインします。
 - b. [Dashboard] タブで、Deep Securityにインポートするデータセンターをクリックします。[Virtual Data Center Details] 情報画面が表示されます。
 - c. [Virtual Data Center Details] 画面の [Related Links] セクションで、[vCloud Director API URL] をクリックします。vCloud Director APIの完全なURLが表示されます。
 - d. Deep SecurityにインポートするVMware vCloud Air仮想データセンターのアドレスとして、完全なURLのうちホスト名の部分だけを使用します。
4. ユーザ名とパスワードを入力します。

注意: ユーザ名は、username@virtualdatacenteridの形式にします。

5. [次へ] をクリックします。
6. Deep Security Managerによって仮想データセンターへの接続が確認され、インポート処理の概要が表示されます。[完了] をクリックします。

VMware vCloud Airのデータセンターが、Deep Security Managerのナビゲーションパネル内の [コンピュータ] の下に、それぞれ別個の項目として表示されます。

仮想マシンでVirtual Appliance保護を有効にする

Virtual Appliance保護を有効にするには、[コンピュータ] リストで仮想マシンを右クリックし、[処理]→[有効化] をクリックします。

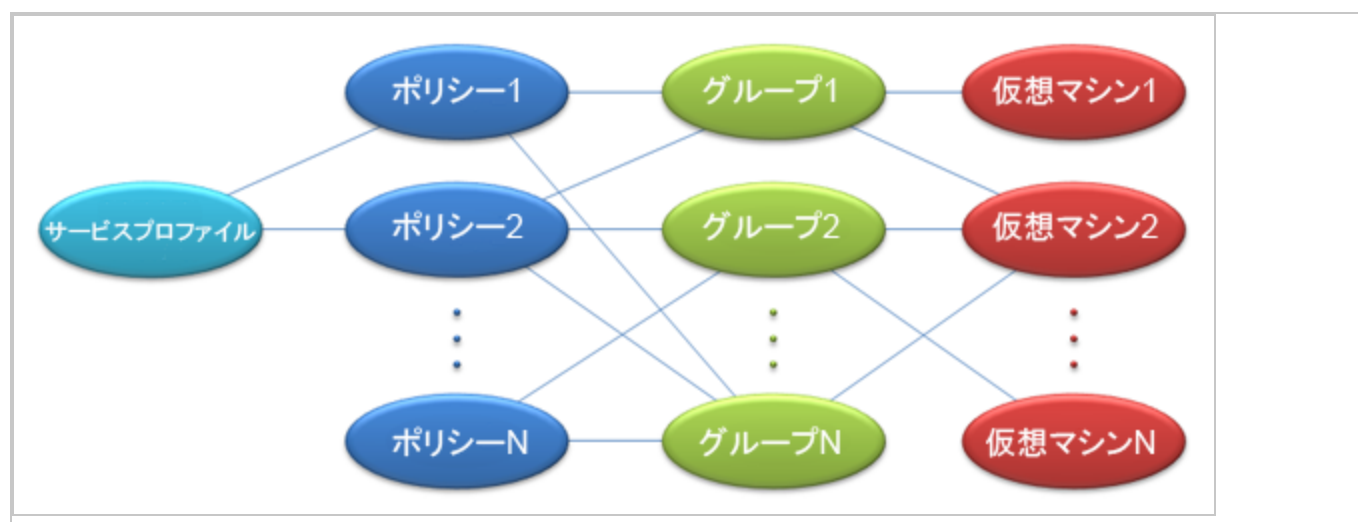
NSX環境での自動ポリシー管理

注意: このトピックは、NSX-T Data Center環境には適用されません。

注意: NSXへのDeep Securityポリシーの同期を有効にしている場合は、NSXセキュリティグループの変更イベントベースタスクを使用する必要はありません。ポリシー同期の詳細については、"[Deep SecurityポリシーのNSXとの同期](#)" on page 364を参照してください。

NSX環境内のVMのセキュリティ設定は、VMのNSXセキュリティグループの変更に基づいて自動的に変更できます。セキュリティ設定の自動化は、NSXセキュリティグループの変更イベントベースタスクを使用して設定します。

仮想マシンはNSXセキュリティグループ、NSXセキュリティグループはNSXセキュリティポリシー、NSXセキュリティポリシーはNSXサービスプロファイルに、それぞれ関連付けられます。



「NSXセキュリティグループの変更」 イベントベースタスク

Deep Securityには、特定の条件で特定のイベントが検出されたときに処理を実行するように設定できるイベントベースタスク (EBT) があります。NSXセキュリティグループの変更EBTを使

用すると、仮想マシンが属しているNSXセキュリティグループへの変更が検出されたときに、その仮想マシンの保護設定を変更できます。

注意: NSXセキュリティグループの変更EBTは、Default (EBT) NSXサービスプロファイルに関連付けられたNSXセキュリティグループへの変更のみを検出します。同様に、1つの仮想マシンが複数のグループ/ポリシーに関連付けられている場合でも、Deep SecurityはDefault (EBT) NSXサービスプロファイルに関連付けられたグループとポリシーに関連する変更のみを監視およびレポートします。

このタスクを変更するには、Deep Security Managerで [管理]→[イベントベースタスク] に進みます。

NSXセキュリティグループの変更EBTは、次のいずれかのイベントが発生した場合に開始されます。

- Default (EBT) NSXサービスプロファイルに間接的に関連付けられたNSXグループに仮想マシンが追加された場合。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXグループから仮想マシンが削除された場合。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXポリシーがNSXグループに適用された場合。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXポリシーがNSXグループから削除された場合。
- NSXポリシーがDefault (EBT) NSXサービスプロファイルに関連付けられます。
- NSXポリシーがDefault (EBT) NSXサービスプロファイルから削除されます。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXグループの名前が変更された場合。

変更によって影響を受ける仮想マシンごとにイベントがトリガされます。

タスクを実行する条件

次の条件を「NSXセキュリティグループの変更」イベントベースタスクに適用して、処理を実行する前にテストすることができます。

- コンピュータ名: ゲスト仮想マシンのホスト名。
- ESXi名: ゲスト仮想マシンが実行されているESXiのホスト名。
- フォルダ名: ESXiフォルダ構造にあるゲスト仮想マシンのフォルダ名。

- NSXセキュリティグループ名: 変更されたNSXセキュリティグループの名前。
- プラットフォーム: ゲスト仮想マシンのOS。
- vCenter名: ゲスト仮想マシンが属するvCenterの名前。
- Appliance保護が利用可能: 仮想マシンがホストされているESXi上にDeep Security Virtual Applianceがあり、仮想マシンを保護できる。仮想マシンの状態が有効化済みになっているかどうかは問いません。
- Appliance保護が有効化済み: Deep Security Virtual Applianceを使用して、有効化されている仮想マシンをホストしているESXi上の仮想マシンを保護できます。
- 最後に使用されたIPアドレス: 仮想マシンコンピュータの現在の、または最後に確認されたIPアドレス。

これらの条件およびイベントベースタスクの概要については、"[コンピュータの追加または変更時のタスクの自動実行](#)" on page 482を参照してください。

NSXセキュリティグループ名条件は、NSXセキュリティグループの変更イベントベースタスクへの変更に対するものです。

プロパティが変更された、仮想マシンが属しているNSXセキュリティグループに一致するJava正規表現を受け付けます。次の2つの特殊なケースがあります。

- いずれかのグループのメンバーシップに対する一致。この場合に推奨される正規表現は「+」です。
- グループのメンバーシップに対する不一致。この場合に推奨される正規表現は「^\$」です。

他の正規表現としては、特定のグループ名または部分名 (複数のグループに一致) などがあります。

注意: この条件に適合する可能性のあるグループのリストには、Default (EBT) NSXサービスプロファイルのポリシーに関連付けられたグループのみが含まれます。

実行可能な処理

仮想マシンが属しているNSXセキュリティグループへの変更を検出したときに、仮想マシンに対して次の処理を実行できます。

- コンピュータの有効化: Deep Security Virtual Applianceによる保護を有効化します。この処理は、Deep Securityで保護されたNSXセキュリティグループに仮想マシンを移動した場合に使用します。

- コンピュータの無効化: Deep Security Virtual Applianceによる保護を無効化します。この処理は、Deep Securityで保護されたNSXセキュリティグループから仮想マシンを移動した場合に使用します。仮想マシンが保護されなくなるため、Deep Securityで保護されたNSXセキュリティグループから仮想マシンを移動したときにこの処理が実行されない場合は、アラートが発生します。
- ポリシーの割り当て: Deep Securityポリシーを仮想マシンに割り当てます。
- Relayグループの割り当て: Relayグループを仮想マシンに割り当てます。

vCenterがDeep Security Managerに追加されたときに作成されるイベントベースタスク

NSX Managerと連携したvCenterをDSMに追加したときに、2つのイベントベースタスクを作成できます。vCenterの追加ウィザードの最後の画面にチェックボックスが表示されます。オンにした場合、2つのイベントベースタスクが作成されます。1つは、保護が追加されたときに仮想マシンを有効化し、もう1つは、保護が削除されたときに仮想マシンを無効化します。

最初のイベントベースタスクは、次のように設定されます。

- 名前: <vCenter名>を有効化します。この<vCenter名>は、vCenterプロパティの [名前] フィールドに表示される値です。
- イベント: NSXセキュリティグループの変更
- タスクの有効化: True
- 処理: 5分間の遅延後にコンピュータを有効化します
- 条件:
 - vCenter名: EBTはvCenter固有のため、<vCenter名>が一致している必要があります。
 - Appliance保護が利用可能: True。有効化されたDeep Security Virtual Applianceが同じESXi上に配置されている必要があります。
 - Appliance保護が有効化済み: False。無効化されている仮想マシンにのみ適用されません。
 - NSXセキュリティグループ: 「.+」 。1つ以上のDeep Securityグループのメンバーである必要があります。

たとえばDeep Security保護ポリシーを適用したり、別のRelayグループを割り当てたりして、このイベントベースタスクに関連付けられた処理を変更できます。既存のイベントベースタスクの処理 (およびその他のプロパティ) は、Deep Security Managerの [管理]→[イベントベースタスク] 画面で編集できます。

2つ目のイベントベースタスクは、次のように設定されます。

- 名前: <vCenter名>を無効化します。この<vCenter名>は、vCenterプロパティの [名前] フィールドに表示される値です。
- イベント: NSXセキュリティグループの変更
- タスクの有効化: False
- 処理: コンピュータを無効化します
- 条件:
 - vCenter名: <vCenter名>。イベントベースタスクはvCenter固有のため、一致する必要があります。
 - Appliance保護が有効化済み: True。有効化されている仮想マシンにのみ適用されません。
 - NSXセキュリティグループ: 「^\$」。グループのメンバーではありません。

注意: イベントベースタスクは初期設定で無効化されています。vCenterのインストールの完了後に、必要に応じて有効化したりカスタマイズしたりできます。

注意: 複数のイベントベースタスクが同一条件で開始される場合、タスクはタスク名のアルファベット順に実行されます。

Deep Security ManagerからvCenterを削除する

vCenterをDeep Security Managerから削除すると、次の条件を満たすすべてのイベントベースタスクが無効化されます。

1. vCenter名の条件は、削除するvCenterの名前に一致します。

注意: これは完全一致である必要があります。複数のvCenter名に一致するイベントベースタスクは、無効化されません。

2. イベントベースタスク「イベントタイプ」は、「NSXセキュリティグループの変更」です。他のタイプのイベントベースタスクは、無効化されません。

Deep Security ManagerからvCenterを削除するには、最初にNSXからDeep Securityを削除する必要があります。NSXからDeep Securityを削除する手順と、Deep Security ManagerからvCenterを削除する手順については、"[NSX環境からのDeep Securityのアンインストール](#)" on [page 1507](#)を参照してください。

Deep SecurityポリシーのNSXとの同期

注意: このトピックは、NSX-T Data Center環境には適用されません。

Deep Securityで仮想マシンを保護する方法は2種類あります。

- イベントベースタスクを使用して仮想マシンを有効化および無効化し、初期設定のポリシーを適用または削除します。詳細については、"[NSX環境での自動ポリシー管理](#)" on [page 359](#)の「vCenterがDeep Security Managerに追加されたときに作成されるイベントベースタスク」を参照してください。
- Deep SecurityポリシーをNSXと同期します。この方法については、この後の説明を参照してください。

保護する各仮想マシンは、NSXセキュリティポリシーが割り当てられたNSXセキュリティグループに属している必要があります。NSXセキュリティポリシーの設定時には、NSXサービスプロファイルを選択します。Deep Security 9.6までは、Deep Securityで使用するNSXサービスプロファイルは1つだけでした。Deep Security 9.6 SP1以降では、すべてのDeep SecurityポリシーをNSXと同期することが可能になり、それぞれのDeep Securityポリシーに対応するNSXサービスプロファイルが作成されるようになりました。Deep Securityでは、このサービスプロファイルのことを「マッピングされたサービスプロファイル」と呼びます。

ポリシーの同期を有効にする

注意: Deep Security ポリシーをNSXと同期するには、すべてのポリシーの名前が一意である必要があります。

1. Deep Security Managerで、[コンピュータ] 画面に移動し、同期を有効にするvCenterを右クリックします。
2. [プロパティ] をクリックします。
3. [NSX設定] タブで、[Deep SecurityポリシーとNSXサービスプロファイルの同期] を選択します。[OK] をクリックします。

次の手順

1. Deep Security Virtual Applianceで仮想マシンを保護するには複数の手順があり、特定の順番で完了する必要があります。手順の完全なリストについては、「[Applianceのインストール \(NSX-V\)](#)」または"[Applianceのインストール \(NSX-T\)](#)" on [page 320](#)を参照してください。

仮想マシンに割り当てられたポリシーを変更または削除する

マッピングされたサービスプロファイルで仮想マシンを保護する場合、ポリシーの割り当てを Deep Security Manager で変更することはできません。仮想マシンの保護に使用するプロファイルを変更するには、vSphere Web Client で NSX セキュリティポリシーまたは NSX セキュリティグループを変更する必要があります。

グループに対する NSX セキュリティポリシーの割り当てを解除すると、そのグループに属する仮想マシンが Deep Security Manager で無効化されます。

ポリシーの名前を変更する

Deep Security Manager でポリシーの名前を変更すると、NSX サービスプロファイルの名前も変更されます。

ポリシーを削除する

Deep Security Manager でポリシーを削除すると、対応する NSX サービスプロファイルも使用中でなければ削除されます。対応する NSX サービスプロファイルが使用中の場合は、Deep Security Manager と同期されなくなり、無効になったことがわかるように名前が変更されます。この NSX サービスプロファイルは、後で使用されなくなると自動的に削除されます。

VMware vRealize

VMware vRealize でブループリントを設定する場合、ブループリントに NSX セキュリティグループまたは NSX セキュリティポリシーのどちらかを割り当てることができます。セキュリティグループとセキュリティポリシーのどちらも、マッピングされたサービスプロファイルを使用できます。

NSX セキュリティタグの設定

Agentレスによる保護を使用している場合、不正プログラム対策または侵入防御 (IPS) モジュールが脅威を検出したときに保護対象の仮想マシンに NSX セキュリティタグを適用するように Deep Security Virtual Appliance を設定できます。NSX セキュリティタグを NSX Service Composer で使用することで、感染した仮想マシンの隔離など、特定のタスクを自動化することができます。NSX のタグ付けおよび動的な NSX セキュリティグループの割り当ての詳細については、VMware のドキュメントを参照してください。

注意: VMware NSX セキュリティタグは、Deep Security のイベントタグとは異なります。NSX のタグ付けは、VMware vSphere 環境で実行されます。つまり、Deep Security のイベントタグは、Deep Security データベース内で使用されます。

このページのトピック:

- "NSXセキュリティタグを適用するように不正プログラム対策を設定する" below
- "NSXセキュリティタグを適用するように侵入防御を設定する" on the next page

NSXセキュリティタグを適用するように不正プログラム対策を設定する

不正プログラムが検出されたときにNSXセキュリティタグを適用するように不正プログラム対策モジュールを設定するには、次の手順に従います。

1. **コンピュータエディタまたはポリシーエディタ**で、¹[不正プログラム対策]→[詳細]→[NSXセキュリティのタグ付け]に移動します。
2. [オン]を選択してこの機能を有効にします。
3. [NSXセキュリティタグ]ドロップダウンリストで、不正プログラムが検出されたときにNSXで割り当てるNSXセキュリティタグの名前を選択します。オプションは次のとおりです。
 - ANTI_VIRUS.VirusFound.threat=low
 - ANTI_VIRUS.VirusFound.threat=medium
 - ANTI_VIRUS.VirusFound.threat=high

たとえば、[ANTI_VIRUS.VirusFound.threat=low]を選択した場合は、仮想マシンで不正プログラムが検出されたときに、ANTI_VIRUS.VirusFound.threat=lowという名前のNSXセキュリティタグが仮想マシンに割り当てられます。タグの名前は不正プログラムの脅威レベルには関連付けられていないため、不正プログラムの脅威レベルが高い場合でも「low」タグが適用されます(逆の場合も同様です)。

4. オプションとして、[修復処理に失敗した場合にのみ、NSXセキュリティタグを適用する]を選択すると、不正プログラム対策モジュールによる修復処理が失敗したときにのみ、NSXセキュリティタグを適用できます(実行される修復処理は、有効になっている不正プログラム検索設定によって異なります。どの不正プログラム検索設定が有効になっているかを確認するには、**コンピュータエディタまたはポリシーエディタ**²で、[不正プログラム対策]→[一般]タブに移動し、[リアルタイム検索]、[手動検索]、および[予約検索]の各エリアを確認します)。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

- オプションで、[この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用されたNSXセキュリティタグを削除]を選択することもできます。このオプションを選択すると、その後の不正プログラム検索で不正プログラムが検出されなかった場合に、セキュリティタグが削除されます。この設定は、すべての不正プログラム検索の種類が同じ場合にのみ使用してください。
- [保存] をクリックします。

NSXセキュリティタグを適用するように侵入防御を設定する

NSXセキュリティタグを適用するように侵入防御モジュールを設定するには、**コンピュータエディタまたはポリシーエディタ**¹で、[侵入防御]→[詳細]→[NSXセキュリティのタグ付け] に移動します。

侵入防御イベントには、イベントを引き起こした侵入防御ルールの重要度によって決定される重要度があります。侵入防御ルールの重要度を設定するには、**コンピュータエディタまたはポリシーエディタ**²で、[侵入防御]→[一般]→[現在割り当てられている侵入防御ルール] の順に選択し、ルールをダブルクリックします。必要に応じて、[重要度] フィールドを変更します。

侵入防御ルールの重要度とNSXタグは次のように対応します。

IPSルールの重要度	NSXセキュリティタグ
重大	IDS_IPS.threat=high
高	IDS_IPS.threat=high
中	IDS_IPS.threat=medium
低	IDS_IPS.threat=low

タグ付けの重要度は、仮想マシンにNSXセキュリティタグが適用される侵入防御ルールの最小重要度を指定することで設定できます。

[NSXセキュリティタグの適用を開始するルール重要度] 設定のオプションは次のとおりです。

- 初期設定 (タグを適用しない):NSXタグは適用されません。
- 重大:重要度が「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- 高:重要度が「高」または「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。
- 中:重要度が「中」、「高」、または「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。
- 低:重要度が「低」、「中」、「高」、または「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。

防御モードと検出のみモードでは、ルールに別々の設定が適用されます。動作モードの詳細については、"[動作モードを使用してルールをテストする](#)" on page 791を参照してください。

アプライアンスのOVFの場所を設定する

初期設定では、Deep Security Virtual Appliance OVFファイルはDeep Security Managerコンピュータの `https://<deep_security_manager_host>:4119/dsva/dsva.ovf` にあります。必要に応じて、OVFを別の場所（別のWebサーバなど）に配置してから、マネージャにそのOVFを指すことができます。次のようにします。

- 信頼性を向上させ、アプライアンスOVFのダウンロード速度を向上させます。
- 接続の問題によりNSXで配信エラーが修正されました。 インストールユニットのインストールに失敗しました。 `ovf/vib URL`が正しい形式でアクセス可能であること、および `ovf` 環境のすべてのプロパティがサービス属性で設定されていることを確認してください。ログで詳細を確認してください。

アプライアンスOVFの場所を設定するには

まず、アプライアンスのZIPパッケージ（OVFファイル):が含まれています) を取得します。

1. Deep Security Managerで、上部にある[Administration]をクリックします。
2. 左側の[Updates]→[Software]→[Local]の順に展開します（仮想アプライアンスの), または Updates→Software→Download Center ().を使用していない場合) を展開します。
3. 仮想アプライアンスのZIPファイルを検索します。 `Appliance-ESX-<appliance_version>.x86_64.zip` という名前です。
4. [エクスポート]→[パッケージのエクスポート] []の順にクリックします。ZIPがローカルコンピュータにダウンロードされます。

次に、アプライアンスファイルをWebサーバに配置します。

1. ZIPファイルを解凍します。
2. ZIPファイルのルートで、`dsva.ovf` および `system.vmdk` ファイルを探します。

注意: ZIPファイルのバージョンが12 Update 3 (12.0.682) 以上の場合は、代わりに `*.ovf`、`*.vmdk`、`*.mf`、および`*.cert`ファイルを参照してください。

3. これらのファイルは、ESXiおよびマネージャサーバからアクセス可能なWebサーバに配置します。
4. Webサーバで、コピーした各ファイルタイプのMIMEタイプを追加します。MIMEタイプについては、次の表で説明します。MIMEタイプをWebサーバに追加する方法の詳細については、Webサーバのドキュメントを参照してください。

ファイル拡張子	MIMEタイプ
ovf	application/vmware
vmdk	application/octet-stream
mf	text/cache-manifest
証明書	application/x-x509-user-cert

最後に、新しいOVFの場所を参照するようにマネージャを設定します。

1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. 左側で、Computersを展開し、vCenterを右クリックして、[Properties]を選択します。
3. [NSX設定] []タブをクリックします。
4. Deep Security Manager データベースではなく、ローカル Web サーバで Deep Security Virtual Appliance ソフトウェアパッケージをホストすることを選択します。
5. [URL to Virtual Appliance OVF]の下に、OVFのURLの場所を入力します。
例:`https://my.webserver.com/dsva/dsva.ovf`。

警告: NSX 2.5.xを使用している場合は、HTTPSではなくHTTPを使用してください。詳細については、[ナレッジベースの記事157039](#)を参照してください。

6. [OK] をクリックします。

これで、アプライアンスOVFにマネージャおよびESXiサーバからアクセスできるようになります。アプライアンスを新しい場所から配置できるようになりました。アプライアンスの配信またはバージョンアップの手順については、"[Applianceのインストール \(NSX-T\)](#)" on page 320, [アプライアンスを配信する \(NSX-V\)](#)、および "[Deep Security Virtual Applianceのアップグレード](#)" on page 1006をアップグレードします。

Deep Security Virtual Applianceのメモリ割り当て

Deep Security Virtual Applianceの初期設定では、4GBのRAMを使用します。初期設定の4GBよりもメモリが必要になることが予測される場合は、Applianceの設定を変更する必要があります。設定を変更するには、2通りの方法があります。

- アプライアンスの設定をvCenterにインポートする前に変更することで、そのvCenter内のすべてのアプライアンスサービスの初期設定を設定します。
- vCenterにインポートし、ESXiに配置してから、Applianceのメモリ割り当てを個別に変更します。

Applianceに割り当てるRAMのサイズについては、"[Deep Security Virtual Applianceのサイジング](#)" on page 189を参照してください。

vCenterに配置する前にApplianceのメモリ割り当てを設定する

注意: このトピックは、NSX-T 2.5.xデータセンター環境には適用されません。詳細については、[ナレッジベースの記事157039](#)を参照してください。

Applianceの初期設定のメモリ割り当てを変更するには、vCenterにインポートする前にApplianceのOVFファイルで割り当ての設定を編集する必要があります。

1. ApplianceのZIPをDeep Security Managerにインポートして、Applianceのパッケージフォルダが、`<DSM_Install>\temp\Appliance-ESX-<appliance_version>`に完全にダウンロードされるのを待ちます。

警告: ApplianceのZIPは、OVFでメモリ割り当て設定を変更する前にインポートする必要があります。これらのタスクを逆の順番で実行すると、変更したOVFファイルが原因となってデジタル署名の確認でエラーが発生し、その結果インポートが失敗します。

2. テキストエディタで、`<DSM_install>\temp\Appliance-ESX-<appliance_version>`にある`dsva.ovf`を開きます。
3. ご使用の環境に合わせて、初期設定のメモリ割り当て (4096MB) を編集します。詳細については、"[Deep Security Virtual Applianceのサイジング](#)" on page 189を参照してください。

```
<Item>
<rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
<rasd:Description>Memory Size</rasd:Description>
<rasd:ElementName
xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_
```

```
ResourceAllocationSettingData">4096 MB of memory</rasd:ElementName>  
<rasd:InstanceID xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-  
schema/2/CIM_ResourceAllocationSettingData">2</rasd:InstanceID>  
<rasd:Reservation>4096</rasd:Reservation>  
<rasd:ResourceType>4</rasd:ResourceType>  
<rasd:VirtualQuantity>4096</rasd:VirtualQuantity>  
</Item>
```

4. OVFファイルを保存します。
5. 複数のApplianceパッケージをDeep Security Managerにインポートした場合は、それぞれの\Appliance-ESX-`<appliance_version>`フォルダにあるdsva.ovfを変更します。

これで、Virtual Appliance OVFファイルをvCenterにインストールできるようになりました。

「[Applianceのインストール \(NSX-V\)](#)」または「[Applianceのインストール \(NSX-T\) on page 320](#)」を参照してください。

配置済みのApplianceのメモリ割り当てを設定する

警告: Applianceのメモリ割り当て設定を変更するには、Applianceの仮想マシンをパワーオフする必要があります。Applianceによって保護される仮想マシンは、再びパワーオン状態になるまで保護されません。回避策として、可能な場合はAgentベースの保護を一時的に設定します。

1. VMware vSphere Web ClientでApplianceを右クリックし、[Power]→[Shut Down Guest]の順に選択します。
2. 再度Applianceを右クリックし、[Edit Settings]を選択します。仮想マシンの[Properties]画面が表示されます。
3. [Hardware] タブで、[Memory]を選択してメモリ割り当ての値を変更します。
4. [OK] をクリックします。
5. 再度Applianceを右クリックし、[Power]→[Power On]の順に選択します。

アプライアンスを起動または停止する

Deep Security Virtual Applianceを開始または停止するには、Deep Security Agentを起動または停止する必要があります。これは、ホストコンピュータでのみローカルで実行できます。

LinuxでAgentを起動または停止するには

SysV initスクリプトの使用：

- 開始： `/etc/init.d/ds_agent start`
- 停止： `/etc/init.d/ds_agent stop`

systemdコマンドの使用：

- 開始： `systemctl start ds_agent`
- 停止： `systemctl stop ds_agent`

Agentのインストール

Deep Security Agentソフトウェアの入手

Deep Security Agentをインストールするには、Agentのインストーラをダウンロードし、Agentの保護モジュール用のパッケージをDeep Security Managerにロードする必要があります。Deep Security Managerにインポートされたソフトウェアのリストを表示するには、[管理]→[アップデート]→[ソフトウェア]→[ローカル] に移動します。

Deep Securityはモジュール形式です。Deep Security Agentには、最初はコア機能だけが含まれています。保護モジュールを有効にすると、Agentがそのプラグインをダウンロードしてインストールします。そのため、Agentを有効化する前に、AgentソフトウェアパッケージをDeep Security Managerのデータベースにダウンロード（「インポート」）して、それらのパッケージをAgentおよびRelayで使用できるようにします。

警告: サードパーティの配信システムを使用する場合でも、インストールされているすべてのDeep Security AgentソフトウェアをDeep Security Managerのデータベースにインポートする必要があります。Deep Security Agentを初めて有効化する際には、セキュリティポリシーで現在有効になっている保護モジュールだけがインストールされます。新しい保護モジュールを後から有効にすると、Deep Security AgentはDeep Security Managerからプラグインをダウンロードしようとします。そのソフトウェアが見つからない場合、Agentは保護モジュールをインストールできないことがあります。

Deep Security ManagerにAgentソフトウェアパッケージをダウンロードする

Agentのアップデートの配信にDeep Security Managerを使用しない場合でも、Deep Security Managerのデータベースにソフトウェアをインポートする必要があります。これは、手動または自動で行うことができます。

ソフトウェアアップデートを自動的にインポートする

Deep Securityにインポート済みのソフトウェアに対するアップデートをすべて自動的にダウンロードするようにDeep Security Managerを設定できます。この機能を有効にするには、[管理]→[システム設定]→[アップデート]に移動し、ローカルにダウンロードしたソフトウェアの最新版を自動的にダウンロードセンターから取得を選択します。

注意: ソフトウェアはDeep Securityにダウンロードされますが、AgentまたはApplianceソフトウェアが自動的にアップデートされるわけではありません。"[Deep Security Agentのアップグレード](#)" on page 998に進んでください。

ソフトウェアアップデートを手動でインポートする

ダウンロードセンターで利用可能になったソフトウェアアップデートは手動でインポートできます。

1. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]に進みます。

トレンドマイクロのダウンロードセンターには、最新バージョンのAgentソフトウェアが表示されます。

2. ManagerのローカルストレージにAgentソフトウェアパッケージをダウンロードするために、リストからインストーラを選択し、[インポート]をクリックします。

Deep Security Managerがインターネットに接続してトレンドマイクロからソフトウェアをダウンロードします。Managerがダウンロードを完了すると、そのAgentの [インポート済み] 列に緑色のチェックマークが表示されます。ソフトウェアパッケージは、[管理]→[アップデート]→[ソフトウェア]→[ローカル] に表示されます。

パッケージを直接インポートできない場合、その旨を示すポップアップ通知が表示されません。これらのパッケージについては、トレンドマイクロのダウンロードセンターWebサイトからローカルフォルダにダウンロードし、[管理]→[アップデート]→[ソフトウェア]→[ローカル] に移動して手動でインポートします。

ヒント: また、Deep Security Managerをエアギャップ環境で使用している (インターネットに接続されていない) ためにダウンロードセンターに直接接続できない場合は、ソフトウェアパッケージを間接的にロードできます。最初にzipパッケージを管理コンピュータにダウンロードし、次にDeep Security Managerにログインしてそれらをアップロードします。

Agentのインストーラをエクスポートする

AgentのインストーラをDeep Security Managerからダウンロードできます。

1. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に進みます。
2. リストからAgentを選択します。
3. [エクスポート]→[インストーラのエクスポート]をクリックします。

古いバージョンがある場合、最新バージョンのソフトウェアの [最新版] 列に緑色のチェックマークが表示されます。

4. Agentのインストーラを保存します。Agentを手動でインストールする場合は、Deep Security Agentをインストールするコンピュータにインストーラを保存します。

ヒント: Deep Security エージェントをインストールするには、エクスポートされたエージェントインストーラ (.msi, .rpm, .pkg, .p5pまたはプラットフォームに応じて.bffファイルのみ) を使用してください。 *not full* ZIPパッケージ。Agentの他のコンポーネントのzipファイルも格納されているフォルダからAgentのインストーラを実行すると、コンピュータで有効になっていない保護モジュールも含めて、すべての保護モジュールがインストールされます。その結果、ディスク容量が追加で消費されます (比較のため、.msi, .rpm, .pkg, .p5pまたは.bffファイルを使用する場合は、保護モジュールのみをダウンロードしてインストールし *ず* (設定に.)が必要な場合のみ)。

ヒント: Agentのインストール、有効化、セキュリティポリシーによる保護の適用は、コマンドラインスクリプトを使用して実行できます。詳細については、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498を参照してください。

ヒント: Deep Security APIを使用して、Agentのインストールを自動化するためのインストールスクリプトを生成できます。詳細については、"[Generate an agent deployment script](#)"を参照してください。

Deep Securityデータベースからソフトウェアパッケージを削除する

ディスク容量を節約するために、使われていないパッケージはDeep Securityのデータベースから定期的に削除されます。保管する古いパッケージの最大数を設定するには、[システム設定]→[ストレージ]に移動します。

注意: Deep Security Virtual Applianceは、64ビット版のRed Hat Enterprise Linux用Agentソフトウェアパッケージに含まれる保護モジュールプラグインを使用します。そのため、Deep Security Virtual Applianceが有効化されている場合に、64ビット版のRed Hat Enterprise Linux用Agentソフトウェアパッケージをデータベースから削除しようとする、ソフトウェアが使用中であるというエラーメッセージが表示されます。

削除できるパッケージは次のとおりです。

- agent
- カーネルサポート

シングルテナントモードでAgentパッケージを削除する

シングルテナントモードでは、現在Agentによって使用されていないAgentパッケージ (Agent-プラットフォーム-バージョン番号.zip) が自動的に削除されます。また、使われていないAgentパッケージを手動で削除することもできます。削除できるのは、使われていないソフトウェアパッケージのみです。

注意: Windows版とLinux版のAgentパッケージについては、使用中のパッケージ (Agentインストーラと同じバージョンのパッケージ) のみ削除できません。

マルチテナントモードでAgentパッケージを削除する

マルチテナントモードでは、使用されていないAgentパッケージ (Agent-プラットフォーム-バージョン番号.zip) が自動的に削除されることはありません。プライバシー上の理由から、Deep Securityのデータベースにあるソフトウェアリポジトリをテナントと共有している場合でも、ソフトウェアが現在テナントによって使用されているかどうかをDeep Securityで確認することはできません。プライマリテナントであるDeep Securityでは、現在アカウント内のどのコンピュータでも実行されていないソフトウェアを削除することが可能ですが、そのソフトウェアを使用しているテナントがないことを削除する前に必ず確認してください。

カーネルサポートパッケージを削除する

シングルテナントモードとマルチテナントモードのどちらの場合でも、Deep Securityは、使用されていないカーネルサポートパッケージ (KernelSupport-プラットフォーム-バージョン番号.zip) を自動的に削除します。カーネルサポートパッケージは、次の条件を両方満たす場合に削除できます。

- グループIDが同じAgentパッケージがない。
- 同じグループIDでビルド番号がより新しいカーネルサポートパッケージが別にある。

また、使用されていないカーネルサポートパッケージを手動で削除することもできます。Linux版のカーネルサポートパッケージについては、最新版のパッケージのみ削除できません。

Deep Security Agentの手動インストール

ヒント: Agentを簡単にインストールおよび有効化するには、代わりにインストールスクリプトを使用します。詳細については、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498を参照してください。

Deep Security Agentをインストールする前に、次の作業を行う必要があります。

- エージェントのシステム要件を確認してください。"[システム要件](#)" on page 184を参照してください。
- エージェントソフトウェアをDeep Security Managerにインポートし、インストーラをエクスポートします。"[Deep Security Agentソフトウェアの入手](#)" on page 372を参照してください。

インストール後は、コンピュータの保護やRelayへの変換を実行する前に、Agentを有効にする必要があります。"[Agentの有効化](#)" on page 430を参照してください。

このトピックの内容:

- "[WindowsにAgentをインストールする](#)" below
- "[Red Hat、SUSE、Oracle Linux、またはCloudLinuxにAgentをインストールする](#)" on page 378
- "[UbuntuまたはDebianにAgentをインストールする](#)" on page 378
- "[SolarisにAgentをインストールする](#)" on page 379
- "[AIXにAgentをインストールする](#)" on page 381
- "[Microsoft Azure Virtual MachineへのAgentのインストール](#)" on page 382

WindowsにAgentをインストールする

1. インストーラファイルをコンピュータにコピーします。
2. インストールファイル (.MSIファイル) をダブルクリックして、インストーラパッケージ

を実行します。

注意: Windows Server 2012 R2 Server Coreの場合は、次のコマンドを使用してインストーラを起動します。 `msiexec /i Agent-Core-Windows-12.0.x-xxxx.x86_64.msi`

3. 最初の画面で [次へ] をクリックしてインストールを開始します。
4. 使用許諾契約書: 使用許諾契約書の内容をご確認いただき同意できる場合は、使用許諾内容に同意し、[次へ] をクリックします。
5. インストール先フォルダ: Deep Security Agentのインストール先を選択し、[次へ] をクリックします。
6. Trend Micro Deep Security Agentのインストール準備完了: [インストール] をクリックしてインストールを続行します。
7. 完了: インストールが正常に完了したら、[完了] をクリックします。

これで、Deep Security Agentはコンピュータにインストールされ、稼働しています。コンピュータを起動するたびに、Deep Security Agentが起動します。

注意: AgentをWindows Server 2012 Server Coreにインストールする場合は、Notifierは含まれません。

注意: インストール中、ネットワークインタフェースが停止し、復旧までに数秒間かかります。DHCPを使用している場合、新しい要求が生成されるため、復旧した接続に対して別のIPアドレスが割り当てられる可能性があります。

Amazon WorkSpacesでのインストール

- エラーコード「2503」でDeep Security Agentの.msiファイルをインストールできない場合は、次のいずれかを実行する必要があります。
 - C:\Windows\Tempフォルダを編集して、ユーザの書き込み権限を許可します。
または
 - コマンドプロンプトを管理者として開いて、.msiファイルを実行します。

注意: Amazonは、新しく導入されたAmazon WorkSpacesのこの問題を修正しています。

Windows 2012 Server Coreでのインストール

- Deep Securityでは、Deep Security Agentのインストール後に、Windows Server 2012のサーバモードをServer Coreモードとフル (GUI) モードの間で切り替えることはできません。

- Hyper-V環境でServer Coreモードを使用している場合、Server Coreコンピュータを別のコンピュータからリモートで管理するにはHyper-Vマネージャを使用する必要があります。Server CoreコンピュータにDeep Security Agentをインストールしてファイアウォールを有効にしている場合は、リモート管理接続がファイアウォールでブロックされます。Server Coreコンピュータをリモートで管理するには、ファイアウォール機能をオフにしてください。
- Hyper-Vには、ゲスト仮想マシンをHyper-Vサーバ間で移動するための移行機能があります。Hyper-Vサーバ間の接続はDeep Securityのファイアウォールでブロックされるため、この移行機能を使用する場合はファイアウォール機能をオフにする必要があります。

Red Hat、SUSE、Oracle Linux、またはCloudLinuxにAgentをインストールする

1. インストーラファイルをコンピュータにコピーします。
2. Agentをインストールします。

```
# sudo rpm -i <package name>
Preparing... ##### [100%]
1:ds_agent ##### [100%]
Loading ds_filter_im module version ELx.x [ OK ]
Starting ds_agent: [ OK ]
```

以前のインストールからアップグレードするには、代わりに「rpm -U」を使用します。この場合、現在のプロファイル設定が保持されます。

インストールが完了すると、Deep Security Agentは自動的に起動します。

UbuntuまたはDebianにAgentをインストールする

1. [管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]の順に選択します。
2. Deep Security ManagerにAgentパッケージをインポートします。
3. インストーラ(.debファイル)をエクスポートします。
4. インストーラファイルをコンピュータにコピーします。
5. Agentをインストールします。

```
sudo dpkg -i <installer file>
```

Agentを起動、停止、リセットするには:

SysV initスクリプトの使用:

Trend Micro Deep Security(オンプレミス) 12.0

- 開始: `/etc/init.d/ds_agent start`
- 停止: `/etc/init.d/ds_agent stop`
- リセット: `/etc/init.d/ds_agent reset`
- 再起動: `/etc/init.d/ds_agent restart`
- ステータスの表示: `svcs -a | grep ds_agent`

systemdコマンドの使用:

- 開始: `systemctl start ds_agent`
- 停止: `systemctl stop ds_agent`
- 再起動: `systemctl restart ds_agent`
- ステータスの表示: `systemctl status ds_agent`

SolarisにAgentをインストールする

注意: Deep Security Agentのインストールは、グローバルゾーンでのみサポートされています。グローバル以外のゾーンはサポートされていません。

Solarisでは、Deep Security Agentをサポートするために次のライブラリをインストールする必要があります。

- Solaris 10: SUNWgccruntime
- Solaris 11.0 - 11.3: gcc-45-runtime
- Solaris 11.4: なし; gcc-c-runtimeバージョン7.3が初期設定でインストールされていません

1. [エージェントインストーラパッケージ](#) をマネージャにインポートし、次に [で](#) をエクスポートします。ご使用のプラットフォームで複数のエージェントが使用可能な場合は、最新のものを選択してください。選択するエージェントパッケージが不明な場合は、次のマッピングテーブルを確認してください。
3. ZIPファイルを解凍します。
4. GZファイルを解凍します:

```
gunzip <agent_GZ_file>
```

エージェントインストーラファイル (P5PまたはPKG) を使用できるようになりました。

5. Agentをインストールします。方法はバージョンとゾーンによって異なります。ファイル名はSPARCとx86で異なります。

- Solaris 11、1つのゾーン (グローバルゾーンで実行):

```
x86: pkg install -g file:///mnt/Agent-Solaris_5.11-xx.x.x-xxx.x86_64/Agent-Core-Solaris_5.11-xx.x.x-xxx.x86_64.p5p pkg:/security/ds-agent
```

```
SPARC: pkg install -g file:///mnt/Agent-Solaris_5.11-xx.x.x-xxx.sparc/Agent-Core-Solaris_5.11-xx.x.x-xxx.sparc.p5p pkg:/security/ds-agent
```

- Solaris 11、複数のゾーン (グローバルゾーンで実行):

```
mkdir <path>
```

```
pkgrepo create <path>
```

```
pkgrecv -s file:///<path_to_agent_p5p_file> -d <path> '*'
```

```
pkg set-publisher -g <path> trendmicro
```

```
pkg install pkg://trendmicro/security/ds-agent
```

```
pkg unset-publisher trendmicro
```

```
rm -rf <path>
```

- Solaris 10:

```
x86: pkgadd -G -d Agent-Core-Solaris_5.10_Ux-xx.x.x-xxx.x86_64.pkg
```

```
SPARC: pkgadd -G -d Agent-Core-Solaris_5.10_Ux-xx.x.x-xxx.sparc.pkg
```

Solaris版のエージェント間パッケージマッピングテーブル

エージェントをインストールしている場合は...	このエージェントパッケージを使用しています...	ヘルプセンターオプション
Solaris 10 Updates 4-6 (64ビット、SPARCまたはx86)	エージェント - Solaris_5.10_U5-xx.xx-xxx。 <sparc .x86_64> .zip	Solaris_5.10_U5
Solaris 10 Updates 7-11 (64ビット、SPARCまたはx86)	エージェント - Solaris_5.10_U7-xx.xx-xxx。 <sparc .x86_64> .zip	Solaris_5.10_U7

エージェントをインストールしている場合は...	このエージェントパッケージを使用しています...	ヘルプセンターオプション
Solaris 11.0 (1111)-11.3 (64ビット、SPARCまたはx86)	エージェント-solaris_5.11-xx.xx-xxx。 <sparc .x86_64> .zip	Solaris_5.11
Solaris 11.4 (64ビット、SPARCまたはx86)	エージェント-solaris_5.11_U4-xx.xx-xxx。 <sparc .x86_64> .zip	Solaris_5.11_U4

※日本語版では削除：※

- ヘルプセンターの[]列には、 [ヘルプセンターの\[Deep Security Software\]の](#) ページにある エージェントの ドロップダウンリストから選択するオプションが表示されます（その場合は、パッケージの取得方法を選択します）。
- xx.x.x.xxx はエージェントのビルド番号です。次に例を示します。12.0.0-682
- <sparc | .x86_64> は、 sparc または .x86_64のいずれかで、Solarisプロセッサによって異なります。

Agentを起動、停止、リセットするには:

- 開始: `svcadm enable ds_agent`
- 停止: `svcadm disable ds_agent`
- リセット: `/opt/ds_agent/dsa_control -r`
- 再起動: `svcadm restart ds_agent`
- ステータスの表示: `svcs -a | grep ds_agent`

Solaris 11でAgentをアンインストールするには:

```
pkg uninstall pkg:/security/ds-agent
```

Solaris 10でAgentをアンインストールするには:

```
pkgrm -v ds-agent
```

AIXにAgentをインストールする

- [管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター] の順に選択します。
- Deep Security Agent for AIXパッケージ (ZIPファイル) をDeep Security Managerにインポートします。エージェントパッケージの命名形式は次のとおりです。

- AIX版Deep Security Agent 12 : Agent-AIX-<agent_release>-<build>.powerpc.zip。例:Agent-AIX-12.0.0-1234.powerpc.zip
- AIX用Deep Security Agent 9.0 : Agent-AIX_<AIX_version>-<agent_release>-<build>.powerpc.bff.gz.zip。例 : Agent-AIX_5.3-9.0.0-5625.powerpc.bff.gz.zip。

使用しているAIXバージョンに必要なエージェントの詳細については、"[Deep Security Agentのプラットフォーム](#)" on page 182を参照してください。

3. ZIPファイルを解凍します。GZファイルが使用可能になります。
4. GZファイルを別の場所に移動します。
5. gunzipを使用してGZファイルを展開します。BFFファイルが使用可能になります。インストーラファイルです。
6. BFFファイルをAIXコンピュータにコピーします。
7. BFFファイルを /tmpなどの一時フォルダに配置します。
8. Agentをインストールします。

```
/tmp> installp -a -d /tmp/<agent_BFF_file_name> ds_agent
```

ここで、<agent_BFF_file_name> は、抽出したBFFインストーラファイルの名前に置き換えられます。

Agentのドライバを開始、停止、ロード、アンロードするには:

- 開始: `startsrc -s ds_agent`
- 停止: `stopsrc -s ds_agent`
- ドライバのロード: `/opt/ds_agent/ds_fctrl load`
- ドライバのアンロード: `/opt/ds_agent/ds_fctrl unload`

Microsoft Azure Virtual MachineへのAgentのインストール

Microsoft Azureクラウドで実行されている仮想マシンインスタンスにAgentをインストールするには、それらの仮想マシンインスタンスにDeep Security Agentをインストールする必要があります。これには複数の方法があります。

- "[インストールスクリプトを生成して実行する](#)" on the next page
- "[カスタムスクリプト拡張機能を既存の仮想マシンに追加する](#)" on the next page

インストールスクリプトを生成して実行する

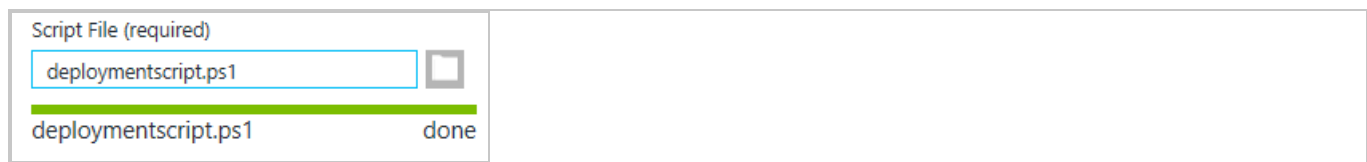
RightScale、Chef、Puppet、SSHなどの配信ツールを使用して自動的にAgentをインストールするDeep Securityインストールスクリプトを生成できます。

詳しい手順については、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on [page 498](#)を参照してください。

カスタムスクリプト拡張機能を既存の仮想マシンに追加する

既存の仮想マシンにカスタムスクリプト拡張機能を追加して、Deep Security Agentをインストールおよび有効化することもできます。そのためには、Azure管理ポータルで既存の仮想マシンに移動し、次の手順に従ってインストールスクリプトをAzure仮想マシンにアップロードして実行します。

1. Azureポータルにログインします。
2. プレビューポータルに切り替えて、カスタムスクリプトを追加する仮想マシンをクリックします。
3. [Settings] ブレードで [Extensions]、[Extensions] ブレードで [Add extension] をクリックし、[New Resource] ブレードで [Custom Script] を選択して、[Create] をクリックします。
4. [Script File (required)] の [Add Extension] ブレードで、[upload] をクリックし、保存した.ps1インストールスクリプトを選択して、[OK] をクリックします。



VMware vCloudへのAgentのインストール

vCloudとの統合を可能にするには、テナントがvCloudの「クラウドアカウント」のインポートに使用するユーザアカウントに、最小限の権限セットを割り当てる必要があります。また、新しい仮想マシンに一意的UUIDを割り当てるようにvCenterデータベースを設定する必要があります。

注意: vCloud環境にDeep Securityセキュリティ保護をエージェントなしで配置するには、代わりに "[vCloud環境でのAgentレスによる保護の実施](#)" on [page 354](#)でエージェントレス保護を配信するを参照してください。

vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する

vCloud Directorで作成した、Deep SecurityのテナントがDeep Security Managerにクラウドアカウントを追加するために使用するユーザアカウントには、の[すべての権限]→[一般]→[管理者ビュー 権限]の権限のみが必要です。

1. vCloud Directorにログインします。
2. [System] タブで [Administration] をクリックします。
3. 左側のナビゲーションパネルで [Roles] をクリックします。
4. 「プラス」記号 (+) をクリックして新しいロール (「DS_User」 など) を作成します。
5. [All Rights]→[General] フォルダの [Administrator View] 権限を選択します。
6. [OK] をクリックします。

これで、Deep Security ManagerにvCloudリソースをインポートするユーザアカウントにこの役割を割り当てることができます。

注意: Deep Securityのユーザにこの資格情報を提供する際は、vCloud OrganizationのIPアドレスも通知してください。また、vCloudのリソースをDeep Security Managerにインポートする際は、ユーザ名に「@orgName」を含めるように指示してください。たとえば、vCloudアカウントのユーザ名がuserで、アカウントのアクセス権を付与されたvCloud OrganizationがCloudOrgOneである場合、Deep Securityのユーザは、vCloudのリソースをインポートするときにユーザ名として「user@CloudOrgOne」と入力する必要があります。(vCloud管理者の場合、@systemを使用します)。

注意: クラウドアカウントで保護されているインスタンスへの接続にプロキシサーバを使用するよう、Deep Security Managerを設定できます。プロキシ設定は、[管理]→[システム設定]→[プロキシ]→[プロキシサーバの使用]→[Deep Security Manager (クラウドアカウント)]で行います。

新しい仮想マシンに一意的UUIDを割り当てる

Deep Securityでは、保護対象のすべての仮想マシンに一意的UUIDを割り当てる必要があります。vAppテンプレートから作成した仮想マシンにはUUIDを重複して割り当てることができるため、問題が発生する場合があります。一意的UUIDを割り当てるようにvCloudデータベースを設定するには、[VMwareナレッジベースの記事2002506](#)に従って、CloneBiosUuidOnVmCopy プロパティをゼロ (0) に設定します。

ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする

ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にすると、guestInfo.ovfEnv環境変数がDeep Security Managerに公開され、Agentで仮想マシンを一意に識別することが容易になります。これにより、仮想マシンの誤認リスクが低減されます。

1. vCloud Directorで仮想マシンの [Properties] 画面を開き、[Guest OS Customization] タブに進んで [Enable guest customization] チェックボックスをオンにします。[OK] をクリックします。
2. vCenterで同じ仮想マシンを選択し、[Properties] 画面を開いて [Options] タブに進みます。
3. [vApp Options] をクリックし、[Enabled] オプションを選択します。これで [OVF Settings] が公開されます。
4. [OVF Settings] で、[OVF Environment Transport] エリアの [VMware Tools] チェックボックスをオンにします。[OK] をクリックします。

仮想マシンが実行中の場合は、変更を有効にするために再起動する必要があります。

Deep Securityで使用されるデータは、プロパティvmware.guestinfo.ovfenv.vcenteridおよびvmware.guestinfo.ovfenv.vcloud.computernameから取得されます。

VMware vCloud Organizationアカウントからのコンピュータのインポート

注意: vCloud組織アカウントはテナント別に追加する必要があります (プライマリテナントではない)。

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで [コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するリソースの名前と説明を入力します(Deep Security Managerでの表示に使用されます)。
3. vCloudのアドレスを入力します(vCloud Directorホストコンピュータのホスト名です)。
4. ユーザ名とパスワードを入力します。

注意: ユーザ名は、username@vcloudorganizationの形式にします。

5. [次へ] をクリックします。
6. Deep Security Managerによってクラウドリソースへの接続が確認され、インポート処理の概要が表示されます。[完了] をクリックします。

VMware vCloudのリソースが、Deep Security Managerのナビゲーションパネル内の [コンピュータ] の下に、それぞれ別個の項目として表示されます。

クラウドプロバイダのリソースを追加したら、コンピュータにAgentをインストールして有効化し、ポリシーを割り当てる必要があります ("[Deep Security Agentの手動インストール](#)" on page 376または"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498と"[Agentの有効化](#)" on page 430を参照してください)。

VMware vCloud Air仮想データセンターからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで [コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するVMware vCloud Air仮想データセンターの名前と説明を入力します(Deep Security Managerでの表示に使用されます)。
3. VMware vCloud Air仮想データセンターのアドレスを入力します。

注意: VMware vCloud Air仮想データセンターのアドレスを確認するには、次の手順を実行します。

- a. VMware vCloud Airポータルにログインします。
- b. [Dashboard] タブで、Deep Securityにインポートするデータセンターをクリックします。[Virtual Data Center Details] 情報画面が表示されます。
- c. [Virtual Data Center Details] 画面の [Related Links] セクションで、[vCloud Director API URL] をクリックします。vCloud Director APIの完全なURLが表示されます。
- d. Deep SecurityにインポートするVMware vCloud Air仮想データセンターのアドレスとして、完全なURLのうちホスト名の部分だけを使用します。

4. ユーザ名とパスワードを入力します。

注意: ユーザ名は、username@virtualdatacenteridの形式にします。

5. [次へ] をクリックします。
6. Deep Security Managerによって仮想データセンターへの接続が確認され、インポート処理の概要が表示されます。[完了] をクリックします。

VMware vCloud Airのデータセンターが、Deep Security Managerのナビゲーションパネル内の [コンピュータ] の下に、それぞれ別個の項目として表示されます。

クラウドプロバイダのリソースを追加したら、コンピュータにAgentをインストールして有効化し、ポリシーを割り当てる必要があります ("[Deep Security Agentの手動インストール](#)" on

page 376または"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498と"[Agentの有効化](#)" on page 430を参照してください。

Amazon EC2およびWorkSpacesへのAgentのインストール

注意: Deep Security Agentは、WindowsデスクトップでのみAmazon WorkSpacesをサポートします。Linuxデスクトップではサポートされません。

Deep Securityで既存のAmazon EC2インスタンスおよびAmazon WorkSpacesを保護する場合はこのページを確認してください。

ただし、次の場合にはそれぞれの手順に従ってください。

- Agentが「統合」されている新しいAmazon EC2インスタンスおよびAmazon WorkSpacesを起動する場合は、"[AgentのAMIまたはWorkSpaceバンドルへの統合](#)" on page 393を参照してください。
- Amazon EC2インスタンスを保護した後にAmazon WorkSpacesを保護する場合は、"[Amazon WorkSpacesを保護する \(AWSアカウントをすでに追加している場合\)](#)" on page 536を参照してください。

Deep Securityで既存のAmazon EC2インスタンスおよびAmazon WorkSpacesを保護するには、次の手順に従います。

1. "[AWSアカウントをDeep Security Managerに追加する](#)" below
2. "[通信方向を設定する](#)" on the next page
3. "[有効化の種類を設定する](#)" on the next page
4. "[ポートを開く](#)" on page 389
5. "[AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする](#)" on page 390
6. "[Agentが適切にインストールされ有効化されたことを確認する](#)" on page 391
7. "[ポリシーを割り当てる](#)" on page 392

AWSアカウントをDeep Security Managerに追加する

1つまたは複数のAWSアカウントをDeep Security Managerに追加する必要があります。これらのAWSアカウントには、Deep Securityで保護するAmazon EC2インスタンスおよびAmazon WorkSpacesが含まれます。

AWSアカウントを追加するには、"[AWSクラウドアカウントの追加](#)" on page 516の手順に従ってください。

AWSアカウントを追加すると、次のようになります。

- 既存のAmazon EC2インスタンスおよびAmazon WorkSpacesがDeep Security Managerに表示されます。Agentがインストールされていない場合は、ステータスは [非管理対象 (不明)] になり、灰色のドットが表示されます。Agentがすでにインストールされている場合は、[ステータス] が [管理対象 (オンライン)] になり、緑色のドットが表示されます。
- このAWSアカウントでAWSを介して起動する新しいAmazon EC2インスタンスまたはAmazon WorkSpacesは、Deep Security Managerによって自動的に保護され、コンピュータのリストに表示されます。

通信方向を設定する

通信方向は、[Agent/Applianceから開始]、[Managerから開始]、または [双方向] のいずれかに設定する必要があります。

1. Deep Security Managerにログインします。
2. "[通信方向を設定する](#)" on page 401の手順に従って通信方向を設定します。次のガイドラインに従います。
 - [Agent/Applianceから開始] では、Amazon EC2インスタンスまたはAmazon WorkSpacesで受信ポートを開く必要はありません。ただし、双方向 および [Managerから開始] では開く必要があります。
 - Agent/Applianceから開始 は、Amazon EC2インスタンスまたはAmazon WorkSpaceで受信ポートを開く必要がないため、最も安全なオプションです。
3. Amazon WorkSpacesを使用し、通信方向を [双方向] または [Managerから開始] に設定する場合は、このページの以降の手順を続行する前に、[Elastic IPアドレスを各WorkSpaceに手動で割り当てます](#)。これにより、Deep Security Managerで接続可能なパブリックIPがWorkSpaceに付与されます。EC2インスタンスはパブリックIPアドレスをすでに使用しているため、この操作は必要ありません。WorkSpacesはプライベートIPアドレスを使用します。

有効化の種類を設定する

「有効化」は、AgentをManagerに登録するプロセスです。Agentからのリモート有効化を許可するかどうかを示す必要があります。許可しない場合は、Managerからの有効化のみが許可されます。

1. Deep Security Managerにログインします。
2. 上部の [管理] をクリックします。
3. 左側で [システム設定] をクリックします。
4. メイン画面で [Agent] タブが選択されていることを確認します。

5. [Agentからのリモート有効化を許可] をオンまたはオフにし、次の点に注意します。
 - Agentからのリモート有効化では、Amazon EC2インスタンスまたはAmazon WorkSpacesに対する受信ポートを開く必要はありません。ただし、Managerからのリモート有効化では開く必要があります。
 - Agentからのリモート有効化を有効にしても、Managerからのリモート有効化は引き続き機能します。
 - 通信方向を [Managerから開始] に設定しても、Agentからのリモート有効化は機能します。
6. [Agentからのリモート有効化を許可] を選択した場合は、[クローンAgentの再有効化] および [不明なAgentの再有効化] を選択します。詳細については、"[Agentの設定](#)" on [page 434](#)を参照してください。
7. [保存] をクリックします。
8. Amazon WorkSpacesを使用し、[Agentからのリモート有効化]を許可しなかった場合は、このページの以降の手順を続行する前に、[Elastic IPアドレスを各WorkSpaceに手動で割り当てます](#)。これにより、他のコンピュータで接続可能なパブリックIPが各Amazon WorkSpaceに付与されます。EC2インスタンスはパブリックIPアドレスをすでに使用しているため、この操作は必要ありません。



ポートを開く

Amazon EC2インスタンスまたはAmazon WorkSpacesで必要なポートが開いていることを確認する必要があります。

ポートを開くには:

1. Amazon EC2に対するポートを次のように開きます。
 - a. [AWSマネジメントコンソール](#)にログインします。
 - b. [EC2]→[Network & Security]→[Security Groups] の順に選択します。
 - c. EC2インスタンスに関連付けられたセキュリティグループを選択し、[Actions]→[Edit outbound rules] の順に選択します。
 - d. 必要なポートを開きます。次の"[開くポート](#)" [below](#)を参照してください。
2. Amazon WorkSpacesに対するポートを次のように開きます。
 - a. Amazon WorkSpacesを保護するファイアウォールソフトウェアに移動して、上記のポートを開きます。

これで、Deep Security AgentおよびDeep Security Managerが通信できるように、必要なポートが開きました。

開くポート

一般:

- AgentからManagerへの通信では、送信TCPポート (初期設定で443または80) を開く必要があります。
- ManagerからAgentへの通信では、受信TCPポート (4118) を開く必要があります。

詳細:

- 通信方向を [Agent/Applianceから開始] に設定した場合は、送信TCPポート (初期設定で443または80) を開く必要があります。
- 通信方向を [Managerから開始] に設定した場合は、受信TCPポート4118を開く必要があります。
- 通信方向を 双方向 に設定した場合は、送信TCPポート (初期設定で、443または80) と受信TCPポート4118の両方を開く必要があります。
- [Agentからのリモート有効化を許可] を有効にした場合は、通信方向を設定する方法に関係なく、送信TCPポート (初期設定で443または80) を開く必要があります。
- [Agentからのリモート有効化を許可] を無効にした場合は、通信方向を設定する方法に関係なく、受信TCPポート4118を開く必要があります。

AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする

AgentをAmazon EC2インスタンスおよびAmazon WorkSpacesにインストールする必要があります。オプションは次のとおりです。

- オプション1: インストールスクリプトを使用して、ポリシーをインストール、有効化、および割り当てる

Agentを多数のAmazon EC2インスタンスおよびAmazon WorkSpacesにインストールする必要がある場合は、オプション1を使用します。

このオプションでは、Amazon EC2インスタンスまたはAmazon WorkSpacesでインストールスクリプトを実行する必要があります。このスクリプトはAgentをインストールして有効化し、ポリシーを割り当てます。詳細については、["インストールスクリプトを使用したコンピュータの追加と保護" on page 498](#)を参照してください。

または

- オプション2: 手動でインストールして有効化する

AgentをインストールするEC2インスタンスおよびAmazon WorkSpacesが少ない場合は、オプション2を使用します。

- a. Deep Security Agentソフトウェアを入手して、Amazon EC2インスタンスまたはAmazon WorkSpacesにコピーし、インストールします。詳細については、["Deep Security Agentソフトウェアの入手" on page 372](#)と["Deep Security Agentの手動インストール" on page 376](#)を参照してください。
- b. Agentを有効化します。Agent ([Agentからのリモート有効化] を有効にした場合) またはDeep Security Managerで有効化します。詳細については、["Agentの有効化" on page 430](#)を参照してください。

これで、Deep Security AgentがAmazon EC2インスタンスまたはAmazon WorkSpaceにインストールされ、有効化されました。ポリシーは、選択するオプションに応じて割り当てられるかどうか異なります。オプション1 (インストールスクリプトを使用) を選択した場合、ポリシーは有効化中にAgentに割り当てられます。オプション2 (Agentを手動でインストールして有効化) を選択した場合、ポリシーは割り当てられません。このページの以降の手順に従ってポリシーを割り当てる必要があります。

Agentが適切にインストールされ有効化されたことを確認する

Agentが適切にインストールされ有効化されたことを確認する必要があります。

1. Deep SecurityManagerにログインします。
2. 上部の [コンピュータ] をクリックします。

3. 左側のナビゲーション画面で、[コンピュータ]→[<ご使用のAWSアカウント>]→[<ご使用のリージョン>]の下にAmazon> EC2インスタンスまたはAmazon WorkSpaceが表示されることを確認します ([WorkSpaces] サブノードでWorkSpacesを探します)。
4. メイン画面で、Amazon EC2インスタンスまたはAmazon WorkSpacesの [ステータス] が [管理対象 (オンライン)] で、緑色のドットが横に表示されていることを確認します。

ポリシーを割り当てる

インストールスクリプトを実行して、Agentをインストールして有効化した場合は、次の手順を省略します。スクリプトがポリシーをすでに割り当てているため、これ以上の処理は必要ありません。

Agentを手動でインストールして有効化した場合は、Agentにポリシーを割り当てる必要があります。ポリシーを割り当てると、コンピュータが保護されるように必要な保護モジュールがAgentに送信されます。

ポリシーを割り当てるには、"[ポリシーをコンピュータに割り当てる](#)" on page 585を参照してください。

ポリシーを割り当てると、Amazon EC2インスタンスまたはAmazon WorkSpaceが保護されます。

AgentのAMIまたはWorkSpaceバンドルへの統合

Agentが「統合」されている新しいAmazon EC2インスタンスとAmazon WorkSpacesを起動する場合は、このページを参照してください。

ただし、次の場合にはそれぞれの手順に従ってください。

- Deep Securityを使用して既存のAmazon EC2インスタンスとAmazon WorkSpacesを保護する場合は、"[Amazon EC2およびWorkSpacesへのAgentのインストール](#)" on [page 387](#)を参照してください。
- Amazon EC2インスタンスを保護した後にAmazon WorkSpacesを保護する場合は、"[Amazon WorkSpacesを保護する \(AWSアカウントをすでに追加している場合\)](#)" on [page 536](#)を参照してください。

「Agentの統合」はパブリックAMIをベースにしてEC2インスタンスを起動するプロセスで、AgentをEC2インスタンスにインストールした後にこのカスタムEC2イメージをAMIとして保存します。このAMI (Agentが「統合」されている) を新しいAmazon EC2インスタンスの起動時に選択できます。

同様に、Deep Security Agentを複数のAmazon WorkSpacesにインストールする場合は、Agentが統合されたカスタム「WorkSpaceバンドル」を作成します。カスタムバンドルを新しいAmazon WorkSpacesの起動時に選択できます。

AMIを統合し、事前にインストールされ、有効化されたAgentを使用してカスタムWorkSpaceバンドルを作成するには、次の手順に従います。

1. "[AWSアカウントをDeep Security Managerに追加する](#)" on the next page
2. "[通信方向を設定する](#)" on the next page
3. "[有効化の種類を設定する](#)" on the next page
4. "[「マスター」 Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する](#)" on the next page
5. "[Agentをマスターにインストールする](#)" on the next page
6. "[Agentが適切にインストールされ有効化されたことを確認する](#)" on page 395
7. "[\(推奨\) 自動ポリシー割り当てを設定する](#)" on page 395
8. "[マスターに基づいてAMIまたはカスタムWorkSpaceバンドルを作成する](#)" on page 396
9. "[AMIを使用する](#)" on page 397

AWSアカウントをDeep Security Managerに追加する

AWSアカウントをDeep Security Managerに追加する必要があります。これらは、保護するAmazon EC2インスタンスおよびAmazon WorkSpacesを含むAWSアカウントです。

手順については、"[AWSクラウドアカウントの追加](#)" on page 516を参照してください。

通信方向を設定する

通信方向は、[Agent/Applianceから開始]、[Managerから開始]、または[双方向]のいずれかに設定する必要があります。

手順については、"[Amazon EC2およびWorkSpacesへのAgentのインストール](#)" on page 387の"[通信方向を設定する](#)" on page 388を参照してください。

有効化の種類を設定する

Agentからのリモート有効化を許可するかどうかを示す必要があります。

手順については、"[Amazon EC2およびWorkSpacesへのAgentのインストール](#)" on page 387の"[有効化の種類を設定する](#)" on page 388を参照してください。

「マスター」 Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する

「マスター」 Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する必要があります。マスターインスタンスは、これから作成するEC2 AMIまたはWorkSpaceバンドルの基になります。

1. AWSで、Amazon EC2インスタンスまたはAmazon WorkSpacesを起動します。詳細については[Amazon EC2ドキュメント](#)と[Amazon WorkSpacesドキュメント](#)を参照してください。
2. このインスタンスを「マスター」とします。

Agentをマスターにインストールする

マスターにAgentをインストールして有効にする必要があります。このプロセスでは、オプションでポリシーをインストールできます。

手順については、"[Amazon EC2およびWorkSpacesへのAgentのインストール](#)" on page 387の"[AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする](#)" on page 390を参照してください。

ヒント: AgentをAMIまたはWorkSpaceバンドルに統合し、後から新しいAgentを使用する場合は、バンドルをアップデートして新しいAgentを追加するのが理想的です。ただし、これが不可能な場合は、[Agentを有効化するとき自動的にアップグレードする]設定を使用できます。その結果、AMIまたはバンドル内のAgentが自動的に有効化されたときに、Deep Security ManagerはそのAgentを自動的に最新バージョンにアップグレードできるようになります。詳細については、"[Agentを有効化するとき自動的にアップグレードする](#)" on [page 397](#)を参照してください。

Agentが適切にインストールされ有効化されたことを確認する

続行する前に、マスターにAgentが適切にインストールされ、有効化されていることを確認する必要があります。

手順については、"[Amazon EC2およびWorkSpacesへのAgentのインストール](#)" on [page 387](#)の"[Agentが適切にインストールされ有効化されたことを確認する](#)" on [page 391](#)を参照してください。

(推奨) 自動ポリシー割り当てを設定する

マスターにAgentをどのようにインストールしたかによって、自動ポリシー割り当てを設定する必要があります。

- インストールスクリプトを使用した場合、ポリシーはすでに割り当てられており、追加の処理は必要ありません。
- Agentを手動でインストールして有効にした場合は、Agentにポリシーが割り当てられていないため、ポリシーを割り当ててマスターを保護する必要があります。マスターに基づいて起動されるAmazon EC2インスタンスおよびAmazon WorkSpacesも保護されます。

マスターにポリシーを割り当て、マスターを使用して今後EC2インスタンスまたはWorkSpaceにポリシーを自動割り当てする場合は、次の手順に従います。

1. Deep Security Managerで、イベントベースタスクを次のパラメータを設定して作成します。
 - [イベント] を [Agentからのリモート有効化] に設定します。
 - [ポリシーの割り当て] を割り当てるポリシーに設定します。
 - (オプション) 条件を [クラウドインスタンスのメタデータ] に設定して、
 - [tagKey] を [EC2] に[tagValue.*]を[True]にします (EC2インスタンスの場合)。または

- [tagKey]を [WorkSpaces] に、[tagValue.*]を [True] にします (WorkSpacesの場合)

上記のイベントベースタスクは次のように設定されます。

EC2=true またはor WorkSpaces=trueがAmazon EC2インスタンスまたはWorkSpaceに存在する場合は、Agentが有効化されると、指定されたポリシーを割り当てます。

このキー/値ペアがAmazon EC2インスタンスまたはWorkSpaceに存在しない場合、ポリシーは割り当てられません (Agentの有効化は維持されます)。条件を設定しないと、有効化時に無条件でポリシーが割り当てられます。

イベントベースタスクの作成の詳細については、"[AWSインスタンスタグに基づくポリシーの自動割り当て](#)" on page 502を参照してください。

2. 前述の手順でDeep Security Managerにキー/値ペアを追加した場合は、次の手順を実行します。

- a. AWSにログインします。
- b. マスターEC2インスタンスまたはWorkSpaceを特定します。
- c. タグに [Key] は [EC2] または [WorkSpaces] を、[Value] は [True] を設定して、マスターに追加します。

詳細については、[タグ付けに関するAmazon EC2のドキュメント](#)と[タグ付けに関するAmazon WorkSpaceのドキュメント](#)を参照してください。

これで、自動ポリシー割り当てが設定されました。マスターを使用して起動した新しいAmazon EC2インスタンスおよびAmazon WorkSpaceは、自動的に有効化され (Agentはマスターで事前に有効化されるため)、イベントベースタスクでポリシーが自動的に割り当てられます。

3. マスターEC2インスタンスまたはWorkSpaceで、Agentに対して有効化コマンドを再実行するか、Deep Security Managerの [再有効化] ボタンをクリックしてAgentを再有効化します。詳細については、"[Agentの有効化](#)" on page 430を参照してください。再有効化を実行すると、イベントベースタスクがポリシーをマスターに割り当てます。これでマスターは保護されます。

AMIまたはカスタムWorkSpaceバンドルを作成する準備ができました。

マスターに基づいてAMIまたはカスタムWorkSpaceバンドルを作成する

- LinuxでAMIを作成する場合は、[このAmazonドキュメント](#)を参照してください。
- WindowsでAMIを作成する場合は、[このAmazonドキュメント](#)を参照してください。

- カスタムWorkSpaceバンドルを作成するには、[このAmazonドキュメント](#)を参照してください。

Agentが事前にインストールされ、有効化されたAMIまたはWorkSpaceバンドルが作成されました。

AMIを使用する

カスタムAMIまたはWorkSpaceバンドルを作成すると、今後のAmazon EC2インスタンスおよびAmazon WorkSpacesのベースとして使用できます。カスタムAMIまたはバンドルを使用すると、Deep Security Agentは自動的に起動および有効化し、割り当て済みの保護ポリシーを適用します。これはDeep Security Managerに表示されます。[ステータス] は [管理対象] で、その横に緑色のドットが表示されます。

Agentを有効化するとき自動的にアップグレードする

Deep Security AgentがインストールされたLinuxコンピュータが環境に含まれている場合は、Agentが有効化または再有効化されたときに、[管理]→[アップデート]→[ソフトウェア]→[ローカル]で入手可能な最新バージョンのソフトウェアにそれらのAgentを自動的にアップグレードすることもできます。

注意: 現在、この機能は、Linuxコンピュータのみで利用できます。WindowsおよびUnixについては、今後のリリースでサポートされる予定です。

"AgentのAMIまたはWorkSpaceバンドルへの統合" on page 393を行い、新しいAgentを使用する場合は、バンドルをアップデートして新しいAgentを追加するのが理想的です。ただし、これが不可能な場合は、[Agentを有効化するとき自動的にアップグレードする]設定を使用できます。その結果、AMIまたはバンドル内のAgentが自動的に有効化されたときに、Deep Security ManagerはそのAgentを自動的に最新バージョンにアップグレードできるようになります。

この機能は次のOSで利用できます。

- Red Hat Enterprise Linux
- Ubuntu
- CentOS
- Debian
- Amazon Linux

- Oracle Linux
- SUSE Linux Enterprise Server
- Cloud Linux

Agentの自動アップグレードを有効にする

1. Deep Security Managerで最新のAgentソフトウェアとカーネルサポートパッケージが利用できることを確認します。ソフトウェアアップデートを自動的にダウンロードするか手動でインポートするようにDeep Security Managerを設定できます。詳細については、"[Deep Security Agentソフトウェアの入手](#)" on page 372を参照してください。
2. [管理]→[システム設定]→[Agent] の順に選択します。
3. [Agentのアップグレード] で、[Agentを有効化するとき自動的にアップグレードする] を選択します。
4. [保存] をクリックします。

Agentが正常にアップグレードされたことを確認する

[コンピュータ] 画面の [バージョン] 列には、各コンピュータにインストールされたDeep Security Agentのバージョンが表示されます。

さらに、Agentの自動アップグレードが開始されると、アップグレードのステータスの追跡に使用できる"[システムイベント](#)" on page 1271が生成されます。次のシステムイベントを確認できます。

ID	イベント	Description
264	Agentソフトウェアのアップグレード要求	手動かAgentの自動アップグレードによって、Agentソフトウェアのアップグレードが開始されました。
277	Agentソフトウェアの自動アップグレードがスキップされました	<p>Agentは自動アップグレードの対象でしたが、アップグレードは発生しませんでした。</p> <p>このイベント詳細には、Agentの現行のバージョン、アップグレードが試行されたバージョン、アップグレードが失敗した理由が表示されます。次の理由が考えられます。</p> <ul style="list-style-type: none"> • アップグレードを完了するにはAgentの再起動が必要なため、Agentは自動アップグレードされませんでした。Agentを手動で

ID	イベント	Description
		<p>アップグレードしてシステムを再起動できます。"Deep Security Agentのアップグレード" on page 998を参照してください。</p> <ul style="list-style-type: none"> 必要なLinuxカーネルサポートファイルが見つからないため、Agentが自動アップグレードされませんでした。Deep Security Managerでは、通常、必要なLinuxカーネルサポートパッケージが自動的にダウンロードされますが、パッケージを手動でダウンロードしてDeep Security Managerにインポートすることにより、Agentをアップグレードすることもできます。"Deep Security Agentソフトウェアの入手" on page 372を参照してください。 現在インストールされているOSは自動アップグレード機能でサポートされていないため、Agentが自動アップグレードされませんでした。Agentを手動でアップグレードできる場合があります。"Deep Security Agentの手動インストール" on page 376を参照してください。
706	ソフトウェアアップデート: Agentソフトウェアのアップグレード	アップグレードが成功しました。
707	ソフトウェアアップデート: Agentソフトウェアのアップグレードの失敗	アップグレードに失敗しました。アップグレードに失敗した理由については、イベントの詳細を確認してください。

コンポーネント間の通信の設定

通常、通信関連の設定は1回設定したら、変更の必要はほとんどありません。

- ["AgentとManagerの通信" below](#)
- ["Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 408](#)
- ["プロキシの背後に配置されたAgentの接続" on page 410](#)
- ["Deep Securityでサポートされるプロキシプロトコル" on page 421](#)
- ["プロキシ設定" on page 422](#)
- ["メール通知のSMTPの設定" on page 308](#)
- ["Deep SecurityのURL" on page 196](#)
- ["信頼された証明書の管理" on page 424](#)

AgentとManagerの通信

Deep Security ManagerとAgentまたはApplianceの通信では、相互にサポートされている最新バージョンのTLSが使用されます。

この記事のトピック:

- ["ハートビートを設定する" below](#)
- ["通信方向を設定する" on the next page](#)
- ["AgentとManagerの通信でサポートされている暗号化スイート" on page 404](#)

ハートビートを設定する

「ハートビート」とは、Deep Security ManagerとAgent (またはAppliance)の間の定期的な通信です。Managerは、ハートビート中に次の情報を収集します。

- ドライバのステータス (オンラインまたはオフライン)
- AgentまたはApplianceのステータス (時刻を含む)
- 前回のハートビート以後のAgentまたはApplianceのログ
- カウンタをアップデートするデータ
- AgentまたはApplianceのセキュリティ設定のフィンガープリント (設定が最新のものがどうか判断するために使用)

ハートビートは、ベースまたは親ポリシー、サブポリシー、あるいは個々のコンピュータで設定できます。

ハートビートは次のプロパティを設定できます。

- ハートビート間隔: ハートビートの送信間隔。
- 次の数を超えるハートビートが失われた場合にアラートを発令: アラートをトリガする、連続して失われるハートビートの数(たとえば3に設定すると、ハートビートが4回失われた時点でアラートをトリガします)。

注意: コンピュータがサーバの場合に、連続して大量のハートビートが失われたときは、Agent/Applianceまたはコンピュータ自体に問題がある可能性があります。ただしノートパソコンなど、継続的にネットワークから切断されることの多いシステムの場合、この設定は「無制限」にしてください。

- ハートビート間でコンピュータのローカルシステム時間が次の時間を超えて変更された場合にアラートを発令: Agentがシステム時計への変更を検出できる場合は (Windows Agentのみ)、そのイベントがAgentイベント5004としてManagerに報告されます。時計の変更がここに示された時間を超えた場合は、アラートがトリガされます。この機能をサポートしないAgentの場合は、Managerがハートビート処理のたびにAgentから報告されるシステム時間を監視し、設定で指定された最大変更値よりも大きい場合にアラートをトリガします。

注意: 「コンピュータの時計の変更」アラートがトリガされたら、アラートを手動で消去する必要があります。

- 非アクティブな仮想マシンに対してオフラインエラーを発令: 仮想マシンが停止した場合にオフラインエラーを発生させるかどうかを設定します。
1. 設定するポリシーまたはコンピュータの**ポリシーエディタ**¹または**コンピュータエディタ**²を開きます。
 2. [設定]→[一般]→[ハートビート]に移動します。
 3. 必要に応じてプロパティを変更します。
 4. [保存]をクリックします。

通信方向を設定する

注意: 双方向通信は、初期設定で有効になっています。

¹ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。

²コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

Agent/ApplianceまたはManagerのどちらから通信を開始するかを設定します。「通信」には、ハートビートとその他すべての通信が含まれます。次のオプションを使用できます。

双方向: 通常はAgent/Applianceからハートビートを送信し、Deep Security Managerからの接続もAgentの待機ポート番号で待機します ("[Deep Securityのポート番号](#)" on [page 191](#)を参照)。Managerは必要な処理を実行するためにAgentまたはApplianceに接続できます。ManagerはAgentまたはApplianceのセキュリティ設定に変更内容を適用することもできます。

注意: Deep Security Virtual Applianceは双方向モードでのみ動作します。Virtual Applianceの設定を他のモードに変更すると、機能が中断します。

- Managerから開始: AgentまたはApplianceとの通信をすべてManagerから開始します。この通信には、セキュリティ設定のアップデート、ハートビートの処理、およびイベントログの要求が含まれます。このオプションを選択した場合は、既知のDeep Security Managerからの接続のみが許可されるように "[Deep Security Agentの保護](#)" on [page 1055](#)を行うことを強くお勧めします。
- Agent/Applianceから開始: AgentまたはApplianceはManagerからの接続を待機しません。代わりに、ManagerがAgentのハートビートを待機しているポート番号でManagerに接続します ("[Deep Securityのポート番号](#)" on [page 191](#)を参照)。AgentまたはApplianceからManagerへのTCP接続が確立されると、各種処理が実行されます。Managerは最初にAgentまたはApplianceにステータスとイベントを問い合わせます (これはハートビートの処理です)。コンピュータで実行する必要のある未解決処理がある場合 (ポリシーのアップデートが必要など) は、接続が終了する前にその処理が実行されます。ハートビートごとにManagerとAgentまたはAppliance間の通信が発生します。AgentまたはApplianceのセキュリティ設定が変更された場合は、次のハートビートまでアップデートされません。

注意: Agentからのリモート有効化を設定し、インストールスクリプトを使用してAgentを有効化する方法については、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on [page 408](#)を参照してください。

注意: ManagerとAgent/Appliance間の通信を可能にするために、Managerは、Agent/Applianceのハートビートの待機ポート番号で受信TCP/IPトラフィックを許可する (非表示の) ファイアウォールルール (優先度4、バイパス) を自動的に実装します。このルールは、初期設定ではすべてのIPアドレスおよびMACアドレスからの接続を許可するようになっています。特定のIPまたはMACアドレスまたはその両方から受信TCP/IPトラフィックのみを許可する新しい優先度4 (強制的に許可またはファイアウォールルールをバイパス) を作成する

ことで、このポートの受信トラフィックを制限できます。非表示のファイアウォールルールに置き換えるには、次の設定で新しいルールを作成します。

処理: 強制的に許可またはバイパス

優先度: 4 - 最高

パケットの方向: 受信

フレームの種類: IP

プロトコル: TCP

パケットの送信先ポート: AgentがManagerからのハートビート接続を待機するポート番号、またはそのポート番号を含むリスト ([Agentの待機ポート番号](#)を参照)。

これらの設定が有効な場合、新しいルールで非表示のルールが置き換えられます。その後、IPまたはMACアドレス、またはその両方のパケットソース情報を入力して、コンピュータへのトラフィックを制限できます。

1. 設定するポリシーまたはコンピュータの**ポリシーエディタ**¹または**コンピュータエディタ**²を開きます。
2. [設定]→[一般]→[通信方向] に移動します。
3. [Deep Security ManagerとAgent/Applianceの通信方向] メニューで、[Managerから開始]、[Agent/Applianceから開始]、[双方向] の3つのオプションのいずれかを選択するか、[継承] を選択します。[継承] を選択した場合、ポリシーまたはコンピュータには、親ポリシーの設定が継承されます。その他のオプションのいずれかを選択すると、継承された設定がオーバーライドされます。
4. [保存] をクリックして変更を適用します。

注意: AgentとApplianceは、Managerのホスト名によってネットワーク上のDeep Security Managerを検索します。このため、AgentまたはApplianceによる開始または双方向の通信を使用する場合は、Managerのホスト名が必ずローカルDNS内にある必要があります。

¹ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

²コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

AgentとManagerの通信でサポートされている暗号化スイート

Deep Security ManagerとAgentまたはApplianceの通信では、相互にサポートされている最新バージョンのTLSが使用されます。

Deep Security Agentは、Managerとの通信で次の暗号化スイートをサポートしています。Deep Security Managerでサポートされている暗号化スイートを調べる必要がある場合は、トレンドマイクロにお問い合わせください。Deep Security Virtual Applianceでサポートされている暗号化スイートを調べる必要がある場合は、Applianceに組み込まれているAgentのバージョンを確認し、以下のリストでそのAgentを探してください。

暗号化スイートは、鍵交換非対称アルゴリズム、対称データ暗号化アルゴリズム、およびハッシュ関数で構成されます。

- ["Deep Security Agent 9.5の暗号化スイート" below](#)
- ["Deep Security Agent 9.6の暗号化スイート" on the next page](#)
- ["Deep Security Agent 10.0の暗号化スイート" on the next page](#)
- ["Deep Security Agent 11.0の暗号化スイート" on page 406](#)
- ["Deep Security Agent 12.0の暗号化スイート" on page 407](#)

Deep Security Agent 9.5の暗号化スイート

Deep Security Agent 9.5 (SP、パッチ、またはアップデート適用なし) では、以下のTLS 1.0暗号化スイートがサポートされています。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.5 SP1～9.5 SP1 Patch 3 Update 2では、以下の暗号化スイートがサポートされています。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.5 SP1 Patch 3 Update 3～8では、以下の暗号化スイートがサポートされています。

Trend Micro Deep Security(オンプレミス) 12.0

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.6の暗号化スイート

Deep Security Agent 9.6 (SP、パッチ、またはアップデート適用なし) ~9.6 Patch 1では、以下のTLS 1.0暗号化スイートがサポートされています。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.6 Patch 2~9.6 SP1 Patch 1 Update 4では、以下の暗号化スイートがサポートされています。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.6 SP1 Patch 1 Update 5~21では、以下の暗号化スイートがサポートされています。

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 10.0の暗号化スイート

Deep Security Agent 10.0のUpdate 15まででは、以下のTLS 1.2暗号化スイートがサポートされています。

Trend Micro Deep Security(オンプレミス) 12.0

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 10.0のUpdate 16以降のアップデートでは、以下のTLS 1.2暗号化スイートがそのままの形でサポートされています。

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 10.0 Update 16以降のアップデートでは、以下のTLS 1.2暗号化スイートがサポートされています。また、[強力な暗号化スイートが有効になっている](#)場合は、サポートされるのは以下のスイートのみです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 11.0の暗号化スイート

Deep Security Agent 11.0のUpdate 4まででは、以下の暗号化スイートがサポートされていません。

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 11.0 Update 6以降のアップデートでは、以下のTLS 1.2暗号化スイートがサポートされています。

[FIPSモード](#)の場合は、以下のTLS 1.2スイートがサポートされています。

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

FIPS以外のモードの場合は、以下のTLS 1.2スイートがサポートされています。サポートされているのはこれらのスイートだけです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 12.0の暗号化スイート

FIPSモードの場合は、以下のTLS 1.2スイートがサポートされています。

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

FIPS以外のモードの場合、以下のTLS 1.2スイートがサポートされています。サポートされているのはこれらのスイートだけです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

SSLの実装と資格情報のプロビジョニング

Deep Security Agentが双方向モードで動作するように設定されていれば、AgentがDeep Security Managerへの通信を開始したり、Managerからの通信を受信したりできます。Deep Security Managerでは、AgentおよびApplianceへの接続をすべて同じように扱います。Agentが有効化されていない場合、相互作用は限られたものになりますが、管理者による有効化またはAgentからのリモート有効化機能によってAgentが有効化されていれば、すべての相互作用が有効になります。Deep Security Managerは、TCP接続を確立するときにクライアントであったかどうかにかかわらず、すべての場合でHTTPクライアントとして機能します。AgentおよびApplianceからは、データの要求や処理の開始を直接実行することはできません。イベントやステータスなどの情報の要求、処理の開始、Agentへの設定の適用は、いずれもManagerを通じて行います。AgentおよびApplianceからはDeep Security Managerやそれを実行しているコンピュータにアクセスできないように高度に制御されています。

AgentとManagerの両方で異なる2つのセキュリティコンテンツを使用して、HTTP要求の安全なチャネルを確立します。

1. 有効化の前に、Agentはまずブートストラップ証明書を受け入れてSSLまたはTLSチャネルを確立します。
2. その認証が完了すると、今度は、接続を開始するための相互認証が必要になります。この相互認証を行うために、Managerの証明書がAgentに送信され、Agentの証明書がManagerに送信されます。Agentでそれらの証明書の認証局が同じ (Deep Security Manager) であることが確認されると、特権アクセスがAgentに付与されます。

安全なチャネルの確立後は、AgentはHTTP通信のサーバとして機能します。Managerへのアクセスは制限され、要求に対する応答のみが可能です。この安全なチャネルにより、認証性、暗号化による機密性、および整合性が確保されます。相互認証を使用することで、第三者によるSSL通信チャネルの不正なプロキシを防ぎ、中間者 (MitM) 攻撃から保護することができます。ストリーム内の内部コンテンツにはGZIPが使用され、設定はPKCS #7でさらに暗号化されます。

Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する

Agentに直接接続するDeep Security Managerではなく、Agentからのリモート有効化 (AIA) を有効にすると、AgentはManagerとの通信を開始し、Managerのハートビート[ポート](#) (初期設定は4120) を介して、暗号化されたTCP接続を確立します。

AIAを有効にすると、ManagerとAgent間の通信の問題を防ぐことができます。また、インストールスクリプトと共に使用すると、Agentのインストールを簡略化できます。Trend Microでは、次のような場合にAIAを使用することをお勧めしています。

- ネットワーク環境により、ManagerからAgentへの接続を開始できない場合。
- 複数のAgentを一度にインストールする必要がある場合。
- クラウドアカウントでコンピュータを保護している場合。

注意: AIAを有効にする前に、AgentがManagerのURLとハートビートのポートに接続できることを確認してください。ManagerのURLとハートビートのポートは、[管理]→[システム情報]→[システムの詳細]→[Managerノード] で確認できます。

Agentからのリモート有効化およびAgentからの通信を有効にする

次の手順を続行します。

1. "Agentからの通信を有効にしたポリシーを作成または変更する" below。
2. "Agentからのリモート有効化を有効にする" below。
3. "Agentにポリシーを割り当てる" below。
4. "インストールスクリプトを使用してAgentを有効にする" on the next page。

Agentからの通信を有効にしたポリシーを作成または変更する

Agentの有効化後に、Managerとの通信を引き続きAgentから開始するには、Agentが使用するポリシーでAgentからの通信を有効にする必要があります。これを行うには、既存のポリシーを変更するか、新しいポリシーを作成してAgentに割り当てます。

ヒント: 既存のポリシーを右クリックして [複製] を選択すると、既存のポリシーから新しいポリシーを簡単に作成できます。

1. [ポリシー] 画面でポリシーをダブルクリックします。
2. [設定]→[一般] に移動します。
3. [通信方向] で [Agent/Applianceから開始] を選択します。
4. [保存] をクリックします。

Agentからのリモート有効化を有効にする

1. [管理]→[システム設定]→[Agent] の順に選択します。
2. [Agentからのリモート有効化を許可] を選択します。
3. [Agentによるホスト名指定を許可] を選択します。
4. [同じ名前のコンピュータがすでに存在する場合] リストで、[既存のコンピュータの再有効化] を選択します。
5. [保存] をクリックします。

注意: AIAの各設定の詳細な説明については、"[Agentの設定](#)" on page 434の「[Agentからのリモート有効化](#)」セクションを参照してください。

Agentにポリシーを割り当てる

インストールスクリプトの設定時にポリシーをAgentに割り当てることも、インストールスクリプトの実行後にイベントベースタスクを使用してポリシーをAgentに割り当てることも可能です。

すべてのAgentで同じポリシーを使用する場合は、次の手順の一環としてインストールスクリプトでポリシーを割り当てることができます。Agentのグループごとに異なるポリシーを使用する必要がある場合は、次の手順に進む前に、[ポリシーを割り当てるためにイベントベースタスクを作成](#)してください。

インストールスクリプトを使用してAgentを有効にする

インストールスクリプトを使用してAgentを有効にする方法については、"[インストールスクリプトを生成する](#)" on page 499の「[インストールスクリプトを生成する](#)」セクションを参照してください。インストールスクリプトの設定時にポリシーを割り当てる場合は、[セキュリティポリシー] リストから選択します。

プロキシの背後に配置されたAgentの接続

ヒント: YouTubeで [Deep Security 12 - Scoping Environment Pt2 - Network Communication](#) を視聴すると、さまざまなDeep Securityコンポーネントに関連するネットワーク通信を確認できます。

インターネット、Deep Security Manager、またはRelayにアクセスするためにプロキシを必要とするコンピュータを保護するには、Deep Security Managerにプロキシのアドレスを設定する必要があります。この設定により、Agentにこの情報が提供されます(また、[CLIを使用してAgentでローカルにプロキシを設定する](#)こともできます)。

このトピックの内容:

- "要件" below
- "Deep Security Managerでプロキシを登録する" on the next page
- "プロキシを経由してAgent、Appliance、Relayをセキュリティアップデートに接続する" on the next page
- "プロキシを経由してAgentをセキュリティサービスに接続する" on the next page
- "プロキシを経由してAgentをRelayに接続する" on page 412
- "プロキシ設定を削除する" on page 413
- "以降のAgentのインストール" on page 413

要件

プロキシを経由してAgentをRelayまたはManagerに接続する場合 (特にアプリケーションコントロールルールセットの場合) は、Deep Security Agent 10.0以降が必要です。

Deep Security Managerでプロキシを登録する

1. Deep Security Managerで、[管理]→[システム設定]→[プロキシ]の順に選択します。
2. [プロキシサーバ] エリアで、メニューバーの [新規] をクリックして新しいHTTPプロキシを作成します。
3. プロトコル、IPアドレス、ポート番号、ユーザ名、パスワードを入力します。

プロキシを経由してAgent、Appliance、Relayをセキュリティアップデートに接続する

また、代わりに[コマンドラインを使用してプロキシの使用を設定する](#)こともできます。

1. [プロキシ] タブの [プロキシサーバの使用] エリアで、[Agent、Appliance、およびRelayで使用するセキュリティアップデート用のプライマリプロキシサーバ] 設定を新しいプロキシに変更します。
2. [保存] をクリックします。

プロキシを経由してAgentをセキュリティサービスに接続する

1. Deep Security Managerで、上部の [ポリシー] をクリックします。
2. 左側で [ポリシー] をクリックします。
3. メイン画面で、プロキシの背後にあるコンピュータの保護に使用するポリシーをダブルクリックします。
4. 次の手順に従って、Census、Good File Reputationサービス、機械学習型検索にプロキシを設定します。
 - a. 左側にある [設定] をクリックします。
 - b. メイン画面で [一般] タブをクリックします。
 - c. メイン画面で [Census、Good File Reputationサービスおよび機械学習型検索向けのネットワーク設定] セクションを探します。
 - d. [継承] チェックボックスがオンになっている場合、プロキシ設定は親ポリシーから継承されます。このポリシーまたはコンピュータでこの設定を変更する場合は、チェックボックスをオフにします。
 - e. [グローバルサーバへのアクセス時にプロキシを使用する] を選択し、リストでプロキシを選択するか、[新規] を選択して別のプロキシを指定します。
 - f. 設定を保存します。
5. 不正プログラム対策で使用するSmart Protection Networkにプロキシを設定します。
 - a. 左側にある [不正プログラム対策] をクリックします。
 - b. メイン画面で、[Smart Protection] タブをクリックします。
 - c. [ファイルレピュテーションサービス用のSmart Protection Server] の [継承] チェックボックスがオンになっている場合、プロキシ設定は親ポリシーから継承されます。このポリシーまたはコンピュータでこの設定を変更する場合は、チェックボックスをオフにします。

- d. [Global Smart Protectionサービスへの直接接続] を選択します。
 - e. [Global Smart Protectionサービスへのアクセス時にプロキシを使用する] を選択し、リストでプロキシを選択するか、[新規] を選択して別のプロキシを指定します。
 - f. プロキシ設定を指定し、[OK] をクリックします。
 - g. 設定を保存します。
6. Webレピュテーションで使用するSmart Protection Networkにプロキシを設定します。
- a. 左側にある [Webレピュテーション] をクリックします。
 - b. メイン画面で、[Smart Protection] タブをクリックします。
 - c. 前の手順の [不正プログラム対策] と同じ方法で、[Webレピュテーションサービス用のSmart Protection Server] でプロキシを設定します。
 - d. 左側にある [Webレピュテーション] を選択したまま、[詳細] タブをクリックします。
 - e. [ポート] で、使用しているプロキシの待機ポート番号を含むポートグループを選択し、[保存] をクリックします。たとえば、Squidプロキシサーバを使用している場合は、[Squid Web Server] を選択します。該当するポートグループがない場合は、[ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順に選択し、[新規] をクリックして、ポートを設定します。
 - f. 設定を保存します。

Agentからプロキシを使用してインターネット経由でトレンドマイクロのセキュリティサービスに接続できるようになりました。

プロキシを経由してAgentをRelayに接続する

1. Deep Security Managerの画面右上で、[サポート]→[インストールスクリプト] の順にクリックします。
2. [Relayへの接続に使用するプロキシ] からプロキシを選択します。
3. スクリプトをコピーするか保存します。
4. コンピュータでスクリプトを実行します。

AgentをRelayのプライベートIPアドレスに接続する

RelayにElastic IPアドレスがある場合、AWS VPC内のAgentはそのIPアドレス経由でRelayにアクセスできない場合があります。その代わりに、RelayグループのプライベートIPアドレスを使用する必要があります。

1. [管理]→[システム設定] の順に選択します。
2. [システム設定] エリアで [アップデート] タブをクリックします。
3. [ソフトウェアアップデート] の [Deep Security Relayの代わりとなるソフトウェアアップデート配信サーバ] で、次のように入力します。

`https://<IP>:<ポート>/`

<IP> にはRelayのプライベートネットワークIPアドレス、<ポート>には[Relayのポート番号](#)を指定します。

4. [追加] をクリックします。
5. [保存] をクリックします。

注意: RelayグループのプライベートIPが変わった場合は、この設定を手動で更新する必要があります。この設定は自動的に更新されません。

プロキシ設定を削除する

不要になったプロキシ設定を追加するインストールスクリプトを使用してAgentをインストールした場合は、コマンドラインで次のコマンドを入力して設定を削除できます。

Windows

```
>C:\Program Files\Trend Micro\Deep Security\dsa_control -x ""
```

```
C:\Program Files\Trend Micro\Deep Security\dsa_control -y ""
```

Linux

```
/opt/ds_agent/dsa_control -x ""
```

```
/opt/ds_agent/dsa_control -y ""
```

以降のAgentのインストール

初期インストール後にAgentを追加する場合は、インストールスクリプトジェネレータでプロキシを使用するようにインストールスクリプトを変更します。

インターネットにアクセスできない エージェントを設定する

エージェントまたはリレーがインターネットへのアクセス権を持っていない場合（「エアギャップAgent」とも呼ばれます）、Trend Micro Smart Protection Networkが提供するセキュリティサービスのいくつかにアクセスすることはできません。これらのセキュリティサービスは、Deep Security不正プログラム対策 および Webレピュテーションの機能を正常に実行するために必要です。

Trend Micro Smart Protection Network のセキュリティサービスは次のとおりです。

サービス名	対象機能
スマートスキャンサービス	スマートスキャン
Webレピュテーションサービス	Webレピュテーション
Global Censusサービス	挙動監視 、 機械学習型検索
Good File Reputationサービス	挙動監視 、 機械学習型検索 、 プロセスメモリ検索
機械学習型検索サービス	機械学習型検索

上記のサービスに加えて、エージェントおよびリレー対応エージェントは、トレンドマイクロのアップデートサーバ（Smart Protection Networkの一部ではないアクティブなアップデート）、とも呼ばれますが、Trendによってホストされるコンポーネントです）にもアクセスする必要があります。マイクロソフトは、インターネットを介してアクセスします。

エージェントまたはリレー対応エージェントのいずれかが上記のサービスにアクセスできない場合は、いくつかの解決方法があります（後述）。

解決策

- 解決策1:"[プロキシを使用する](#)" below
- 解決策2:"[Smart Protection Serverをローカルにインストールする](#)" on the next page
- 解決策3: "[隔離されたネットワークでアップデートを取得する](#)" on page 416
- 解決策4:"[トレンドマイクロのセキュリティサービスを使用する機能を無効にする](#)" on page 419

プロキシを使用する

エージェントまたはリレー対応エージェントがインターネットに接続できない場合は、できるプロキシをインストールできます。Deep Security AgentおよびRelayがプロキシに接続すると、このプロキシはSmart Protection Network内のトレンドマイクロのセキュリティサービスに送信接続します。

注意: プロキシを使用すると、各スマートスキャンまたはWebレピュテーション要求がSmart Protection Networkにインターネット経由で送信されます。代わりに[LAN内のSmart Protection Serverを使用](#)して、これらの要求をネットワーク内に保持し、エクストラネットの帯域幅の使用を削減することを検討してください。

プロキシを使用するには、"[プロキシの背後に配置されたAgentの接続](#)" on page 410を参照してください。

Smart Protection Serverをローカルにインストールする

エージェントとリレー対応エージェントがインターネットに接続できない場合は、[が](#)に接続できるローカルエリアネットワーク（LAN）に Smart Protection Server をインストールできます。ローカル Smart Protection Server は定期的にインターネット経由で Smart Protection ネットワークに接続し、最新のスマートスキャン不正プログラム対策 パターンファイルと Webレピュテーション 情報を取得します。この情報は、Smart Protection Server にキャッチされ、クライアントおよびリレー対応エージェントによって照会されます。Smart Protection Server では、エージェントまたはリレー対応エージェントにアップデートを適用しません。

この解決策を使用する場合は、次のことに覚えておいてください。

- 機能は制限されています。ローカルの Smart Protection Serverでは、[スマートスキャン](#) および [Webレピュテーション](#) 機能のみがサポートされます。
- [挙動監視](#)、[機械学習型検索](#)、および [プロセスメモリ検索](#) 機能が必要な場合は、プロキシソリューションを使用してください。詳細については、前述の"[プロキシを使用する](#)" on the previous pageを参照してください。これらの機能を使用しない場合は、クエリの失敗を防止して、パフォーマンスを向上させるために、これらの機能を無効にする必要があります。これらの機能を無効にする手順については、"[トレンドマイクロのセキュリティサービスを使用する機能を無効にする](#)" on page 419を参照してください。

Smart Protection Serverの配置:

- 手動でインストールします。詳細については、[Smart Protection Serverドキュメント](#)を参照してください。
OR
- AgentまたはRelay有効化済みAgentがAWS内にある場合は、トレンドマイクロによって作成されたAWS CloudFormationテンプレートを使用してインストールします。詳細については、「[AWSでのSmart Protection Serverの配置](#)」を参照してください。

上記のシナリオは、Deep Security Agentとリレー対応エージェントがエアギャップされている場合にのみ適用されますが、Deep Security Managerには"[ポート番号、URL、およびIPアドレス](#)" on page 190で説明されているように、インターネットアクセスまたはプロキシアクセスがあります。Deep Security Managerも空白にされている場合は、Trend Micro Active Update Serverからセキュリティアップデートを受信するためにプロキシを使用する必要があります。

ります。または、ソリューション3: "[隔離されたネットワークでアップデートを取得する](#)" [below](#)でアップデートを取得します。

隔離されたネットワークでアップデートを取得する

Deep Security Managerがインターネットに接続されていない隔離されたネットワーク内にあり、エージェントまたはリレー対応エージェントもインターネットに接続できない場合は、スタンドアロンのDeep Security Managerにデータベースとリレーを有効にすることができます。非武装地帯 (DMZ) 内のクライアントまたはインターネットアクセスが利用可能なその他のエリア

すべてのコンポーネントをインストールしたら、DMZでリレー対応エージェントを設定して、インターネット上のアップデートサーバから最新の不正プログラム検索アップデートを自動的に取得できます。これらのアップデートは、.zipファイルに解凍してから手動でAir-Gappedリレーにコピーする必要があります。(詳細な手順は以下を参照)。

この解決策を使用する場合は、次のことに覚えておいてください。

- .zipファイルには、伝統的な (大規模な) 不正プログラムパターンファイルが含まれており、不正プログラム対策 機能を利用できます。
- .zipファイルには、[侵入防御](#)、[変更監視](#)および [セキュリティログ監視](#)に使用されるディープセキュリティルールの更新も含まれています。これらの更新を個別に取得することもできます ("隔離されたネットワークでルールのアップデートを取得する" on page 418でルール更新を取得するを参照)。
- 次の高度な不正プログラム対策機能は使用できません。[スマートスキャン](#)、[挙動監視](#)、[機械学習型検索](#)、[プロセスメモリ検索](#)、Webレピュテーション。これらの機能はすべて、トレンドマイクロのセキュリティサービスにアクセスする必要があります。
- [では、高度な不正プログラム対策の機能](#) (ソリューション4) を無効にする必要があります。この機能は使用できません。
- エアギャップRelayで.zipファイルを定期的にアップデートして、常に最新の不正プログラムパターンファイルを維持するよう計画する必要があります。

この解決策を導入するには、次の手順に従います (アップグレードの手順については、下記を参照してください)。

1. Deep Security Managerと関連するデータベースをDMZにインストールします。これらのインターネット接続コンポーネントは、「DMZ Manager」および「DMZデータベース」と呼ばれます。
2. Deep Security AgentをDMZにインストールして、Relayとして設定します。このAgentのことを「DMZ Relay」と呼びます。Relayの設定方法については、"[Relayによるセキュリ](#)

ティとソフトウェアのアップデートの配布" on page 438を参照してください。

Deep Security次のアイテムがインストールされました。

- DMZ Manager
- DMZデータベース
- DMZ Relay
- エアギャップManager
- エアギャップデータベース
- エアギャップRelay
- 複数のエアギャップAgent

3. DMZ Relayで、次のコマンドを実行して最新の不正プログラムパターンファイルが含まれる.zipファイルを作成します。

```
dsa_control -b
```

コマンドラインの出力に、生成された.zipファイルの名前と場所が表示されます。

4. .zipファイルをair-gapped relayにコピーします。ファイルをリレーのインストールディレクトリに配置します。
 - 初期設定のディレクトリは、Windowsの場合は「C:\Program Files\Trend Micro\Deep Security Agent」、
 - Linuxの場合は、「/opt/ds_agent」です。

注意: .zipファイルの名前は変更しないでください。

5. エアギャップManagerで、セキュリティアップデートのダウンロードを開始します。
 - a. 上部の [コンピュータ] をクリックします。
 - b. コンピュータのリストで、.zipファイルをコピーしたAir-gappedリレーを探して右クリックし、[セキュリティアップデートのダウンロード]を選択します。

エアギャップ型リレーは、設定されたアップデート元（通常はインターネット上のアップデートサーバ）.）をチェックします。このサーバに接続できないため、インストールディレクトリ内の.zipファイルを確認します。.zipファイルを見つけたら、そのファイルを解凍してアップデートをインポートします。アップデートは、リレーに接続するように設定されたエアギャップのあるエージェントに配信されます。
 - c. エアギャップリレーにアップデートをインポートした後に、.zipファイルを削除します。
6. 空のギャップのあるリレーを、アップデートサーバではなく自身に接続するように設定します（接続エラーのアラートを防ぐために):
 - a. エアギャップManagerにログインします。
 - b. 上部の [管理] をクリックします。

- c. 左側で [システム設定] をクリックします。
 - d. メイン画面で [アップデート] タブをクリックします。
 - e. [セキュリティアップデート元] で [その他のアップデート元] を選択し、
`https://localhost:[port]` と入力します。 [port] は [セキュリティデータベース用に設定したポート番号](#) で、初期設定は4122です。
 - f. [OK] をクリックします。
エアギャップのあるリレーは、インターネット上のアップデートサーバに接続しようとしなくなりました。
7. 任意の要件 (推奨): パフォーマンスを向上するには、"[トレンドマイクロのセキュリティサービスを使用する機能を無効にする](#)" on the next page。
 8. 定期的に最新のアップデートをDMZリレーにダウンロードし、解凍して空中中継リレーにコピーし、リレーでセキュリティアップデートのダウンロードを開始してください。

これで、不正プログラム検索アップデートの取得元であるDMZに、Deep Security Manager、関連するデータベース、およびRelayが配置されました。

この解決策をアップグレードするには、次の順序で実行します。

1. DMZ Manager (データベースソフトウェアのアップグレードも必要な場合はそのデータベースを含む)
2. DMZ Relay
3. エアギャップManager (データベースソフトウェアのアップグレードも必要な場合はそのデータベースを含む)
4. エアギャップRelay
5. エアギャップAgent

警告: リレーを最初にアップグレードしない場合、セキュリティコンポーネントのアップグレードとソフトウェアのアップグレードにより がに失敗することがあります。

アップグレードの詳細については、"[Deep Securityのインストールまたはアップグレード](#)" on page 223(Managerのアップグレード手順)、"[Deep Security Relayのアップグレード](#)" on page 997、"[Deep Security Agentのアップグレード](#)" on page 998を参照してください。

隔離されたネットワークでルールのアップデートを取得する

前のセクションで作成した.zipファイルには、侵入防御, 変更監視およびセキュリティログ監視に使用されるディープセキュリティルールの更新が含まれています。ただし、これらの更新を個別に取得する場合は、次のようにします。

1. DMZ Managerで、[[管理]→[アップデート]→[セキュリティ]→[ルール]]の順に選択します。
2. ルールアップデート (.dsruファイル) をクリックし、[エクスポート]をクリックします。ファイルはローカルにダウンロードされます。
3. Air-Gapped Managerに適用する.dsruファイルごとにエクスポートを繰り返します。
4. .dsruファイルをAir-Gapped Managerにコピーします。
5. Air-Gapped Managerで、[[管理]→[アップデート]→[セキュリティ]→[ルール]]の順に選択します。
6. インポートをクリックし、.dsruファイルを選択して、[次へ]をクリックします。
7. マネージャはファイルを検証し、ファイルに含まれるルールの概要を表示します。次へをクリックします。
8. ルールのアップデートが正常にインポートされたことを示すメッセージが表示されます。閉じる をクリックします。
9. Air-Gapped Managerに適用する.dsruファイルごとにインポートを繰り返します。

トレンドマイクロのセキュリティサービスを使用する機能を無効にする

トレンドマイクロのセキュリティサービスを使用する機能を無効にできます。無効にすると、エアギャップAgentはサービスを照会しなくなるため (失敗するため) パフォーマンスが向上します。

注意:トレンドマイクロのセキュリティサービスを使用しない場合は、不正プログラム検出が大幅にダウングレードされ、ランサムウェアがまったく検出されず、プロセスメモリ検索にも影響を与えます。そのため、トレンドマイクロのセキュリティサービスにアクセスできるように他の解決策のいずれかを使用することを強くお勧めします。これが不可能な場合は、パフォーマンスを向上するために機能を無効にする必要があります。

- スマートスキャンを無効にするには、次の手順に従います。
 - a. **コンピュータまたはポリシーエディタ**¹を開きます。
 - b. 左側で [不正プログラム対策] をクリックします。
 - c. メイン画面で [Smart Protection] をクリックします。
 - d. [スマートスキャン] で [継承] (選択されている場合) を選択解除し、[オフ] を選択します。
 - e. [保存] をクリックします。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- Webレピュテーションを無効にするには、次の手順に従います。
 - a. **コンピュータまたはポリシーエディタ¹**を開きます。
 - b. 左側で [Webレピュテーション] をクリックします。
 - c. メイン画面で [一般] タブが選択されていることを確認します。
 - d. [設定] ドロップダウンリストから [オフ] を選択します。
 - e. [保存] をクリックします。
- スマートフィードバックを無効にするには、次の手順に従います。
 - a. Deep Security Managerで、上部の [管理] をクリックします。
 - b. 左側にある [システム設定] をクリックします。
 - c. メイン画面で [スマートフィードバック] タブをクリックします。
 - d. [トレンドマイクロスマートフィードバックを有効にする (推奨)] を選択解除します。
 - e. [保存] をクリックします。
- プロセスメモリ検索を無効にするには、次の手順に従います。
 - a. Deep Security Managerで、上部の [ポリシー] をクリックします。
 - b. 左側で [共通オブジェクト]→[その他] を展開し、[不正プログラム検索設定] をクリックします。
 - c. [リアルタイム] の [検索の種類] で不正プログラム検索設定をダブルクリックします。
 - d. [一般] タブの [プロセスメモリ検索] で、[プロセスメモリ内の不正プログラムを検索する] を選択解除します。
 - e. [OK] をクリックします。
- 機械学習型検索を無効にするには、次の手順に従います。
 - a. 不正プログラムリアルタイム検索設定がまだ開いていることを確認します。
 - b. [一般] タブの [機械学習型検索] で、[機械学習型検索の有効化] を選択解除します。
 - c. [OK] をクリックします。
- 挙動監視を無効にするには、次の手順に従います。
 - a. 不正プログラムリアルタイム検索設定がまだ開いていることを確認します。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- b. [一般] タブの [挙動監視] で、[不審なアクティビティ/不正な変更 (ランサムウェアを含む) を検出する] と [ランサムウェアによって暗号化されたファイルをバックアップおよび復元する] の両方のオプションを選択解除します。
- c. [OK] をクリックします。

また、パフォーマンスの向上が必要な場合は、Deep Security Managerで国勢調査およびグリッドクエリを無効にします。有効にしたままにすると、多くの不要なバックグラウンド処理が実行されます。これらのクエリを無効にするには、次の手順に従います。

1. Censusクエリを無効にします。

```
dsm_c -action changesetting -name settings.configuration.enableCensusQuery -value false
```

2. GRIDクエリを無効にします。

```
dsm_c -action changesetting -name settings.configuration.enableGridQuery -value false
```

Deep Securityでサポートされるプロキシプロトコル

この表にはDeep Securityによって[サポートされるプロキシプロトコル](#)が表示されます。

トラフィックの発信元	対象サービス	HTTP	SOCKS4	SOCKS5
Manager	ソフトウェアアップデート、CSS、ニュースアップデート、製品登録とライセンス管理	○	×	×
Manager	スマートフィードバック	○	×	○
Manager	クラウドアカウント	○	×	×
Manager	Apex Central	○	×	×
Manager	Deep Discovery Analyzer	○	×	×
AgentまたはRelay	Manager (有効化およびハートビート)	○	×	×
Agentまたは	Relay (ソフトウェアアップデートとセキュリティ	○	○	○

トラフィックの発信元	対象サービス	HTTP	SOCKS4	SOCKS5
はRelay	アップデート)			
Agent	Census、Good File Reputationおよび機械学習型検索向けのネットワーク設定	○	×	×
Agent	Global Smart Protection Server	○	×	×

プロキシ設定

ヒント: YouTubeで [Deep Security 12 - Scoping Environment Pt2 - Network Communication](#) を視聴すると、さまざまなDeep Securityコンポーネントに関連するネットワーク通信を確認できます。

ネットワークでプロキシを使用する場合、[初期設定のポート番号](#)の代わりにプロキシを使用するようにDeep Securityを設定できます。プロキシ設定はいくつかの場所にあります。

プロキシサーバの使用

使用可能なプロキシの一覧を表示して編集するには、[管理]→[システム設定]→[プロキシ]の順に選択します。

- Agent、Appliance、およびRelayで使用するセキュリティアップデート用のプロキシサーバ: Deep Security Relayが [アップデート] タブの [Relay] エリアで指定したアップデート元への接続に使用するプロキシサーバを選択します ([トレンドマイクロのアップデートサーバ] または [その他のアップデート元])。

注意: 初期設定では、**AgentおよびAppliance¹**はDeep Security Relayから不正プログラム対策コンポーネントのセキュリティアップデートをダウンロードします。ただし、AgentまたはApplianceが、割り当てられたRelayに接続できず、[Deep Security Relayが使用できない場合、Agent/Applianceにセキュリティアップデートのダウンロードを許可] オプションが選択されている場合、AgentおよびApplianceもこのプロキシを使用します。

¹Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

警告: バージョン 10よりも前のDeep Security Agentでは、プロキシからRelayへの接続はサポートされていませんでした。プロキシが原因で[ルールセットダウンロードに失敗した場合](#)、およびAgentが[RelayまたはManagerにアクセスするためのプロキシを必要とする場合は](#)、次のいずれかを実行する必要があります。

- Agentsのソフトウェアをアップデートして ("Deep Security Agentソフトウェアの入手" on page 372を参照)、[プロキシを設定する](#)。インターネットにアクセスするためのプロキシを必要とする
 - プロキシをバイパスする。
 - 回避策として[アプリケーションコントロールルールセットのRelay設定を変更する](#)
- Deep Security Manager (ソフトウェアアップデート、CSSS、ニュースアップデート、製品登録、ライセンス):トレンドマイクロへの接続にDeep Security Managerが使用するプロキシを選択してDeep Securityのライセンスを有効にし、Certified Safe Software Serviceに接続します Amazon Web Services (AWS) およびVMware vCloudクラウドアカウントに接続し、Deep Securityの匿名の製品使用状況データ収集サービスに接続します。

注意: CSSS用のプロキシ設定に対する変更は、Deep Security ManagerおよびすべてのManagerノードを再起動すると有効になります(サービスは手動で再起動する必要があります)。

- Deep Security Manager (クラウドアカウント - HTTPプロトコルのみ):Deep Security Managerが、[クラウドアカウントの追加] を使用してDeep Security Managerに追加したクラウドベースのインスタンスへの接続に使用するプロキシを選択します。

注意: プロキシの選択後、そのプロキシを使用するAgentを再起動します。

プロキシサーバ

Deep Securityの各クライアントおよびサービスで使用できるプロキシサーバを定義します。たとえば、**コンピュータエディタまたはポリシーエディタ**¹の [不正プログラム対策]→[Smart Protection] で、Smart Protection用のプロキシサーバを定義します。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

次の表は、Deep Securityの各サービスおよびクライアントでサポートされているプロキシプロトコルの一覧です。

サービス	接続元	HTTP	SOCKS4	SOCKS5
ソフトウェアアップデート、ソフトウェア安全性評価サービス、ニュースアップデート、製品登録とライセンス管理	Manager	○	×	×
匿名製品使用状況データ収集	Manager	○	×	×
スマートフィードバック	Manager	○	×	○
クラウドアカウント (AWS、VMware vCloud、Microsoft Azure)	Manager	○	×	×
Apex Central	Manager	○	×	×
Deep Discovery Analyzer	Manager	○	×	×
Manager (有効化およびハートビート)	Agent/Relay	○	×	×
Relay (ソフトウェアアップデートとセキュリティアップデート)	Agent/Relay	○	○	○
Census、Good File Reputationおよび機械学習型検索向けのネットワーク設定	Agent	○	×	×
Global Smart Protection Server	Agent	○	×	×

信頼された証明書の管理

信頼された証明書は、コード署名と、Microsoft Active DirectoryやVMware vCenterなどの外部サービスへのSSL接続に使用されます。

信頼された証明書をインポートする

注意: 信頼された証明書をインポートして、Amazon Web Servicesのリージョンと信頼を確立する場合は、`dsm_c`コマンドラインツールを使用する必要があります。

Deep Security Managerを使用して信頼された証明書をインポートするには

1. Deep Security Managerで、[管理]→[システム設定]→[セキュリティ]の順に選択します。
2. [信頼された証明書]で[証明書リストの表示]をクリックします。Deep Security Managerで受け入れられたすべてのセキュリティ証明書のリストが表示されます。
3. [ファイルからインポート]をクリックして証明書のインポートウィザードを起動します。

`dsm_c`を使用して信頼された証明書をインポートするには

1. Deep Security Managerサーバで、次のコマンドを実行します。

```
dsm_c -action addcert -purpose PURPOSE -cert CERTFILE
```

パラメータは次のとおりです。

パラメータ	説明	値のサンプル
PURPOSE	証明書を使用する接続の種類。右のいずれかの値を選択する必要があります。	AWS - Amazon Web Services
		DSA - コード署名
		SSL - SSL接続
CERTFILE	インポートする証明書を含むファイルのユーザ定義の名前。	/path/to/cacert.pem

注意: Linux環境でDeep Security Managerを実行している場合、rootユーザとしてdsm_cコマンドを実行する必要があります。

信頼された証明書を表示する

注意: Amazon Web Services接続に使用する信頼された証明書を表示する場合は、dsm_cコマンドラインツールを使用する必要があります。

Deep Security Managerを使用して信頼された証明書を表示するには

1. Deep Security Managerで、[管理]→[システム設定]→[セキュリティ]の順に選択します。
2. [信頼された証明書]で[証明書リストの表示]をクリックします。

dsm_cを使用して信頼された証明書を表示するには

1. Deep Security Managerサーバで、次のコマンドを実行します。

```
dsm_c -action listcerts [-purpose 目的]
```

「-purpose PURPOSE」はオプションのパラメータで、すべての証明書のリストを表示する場合は省略できます。「PURPOSE」に値を指定した場合は、その目的に使用する証明書だけが表示されます。

パラメータ	説明	値のサンプル
PURPOSE	証明書を使用する接続の種類。	AWS - Amazon Web Services
		DSA - コード署名

パラメータ	説明	値のサンプル
		SSL - SSL接続

注意: Linux環境でDeep Security Managerを実行している場合、rootユーザとしてdsm_cコマンドを実行する必要があります。

信頼された証明書を削除する

注意: Amazon Web Services接続に使用する信頼された証明書を削除する場合は、dsm_cコマンドラインツールを使用する必要があります。

Deep Security Managerを使用して信頼された証明書を削除するには

1. Deep Security Managerで、[管理]→[システム設定]→[セキュリティ]の順に選択します。
2. [信頼された証明書]で[証明書リストの表示]をクリックします。
3. 削除する証明書を選択し、[削除]をクリックします。

dsm_cを使用して信頼された証明書を削除するには

1. Deep Security Managerにログインします。
2. 次のコマンドを実行します。

```
dsm_c -action listcerts [-purpose 目的]
```

「-purpose PURPOSE」はオプションのパラメータで、すべての証明書のリストを表示する場合は省略できます。「PURPOSE」に値を指定した場合は、その目的に使用する証明書だけが表示されます。

パラメータ	説明	値のサンプル
PURPOSE	証明書を使用する接続の種類。	AWS - Amazon Web Services
		DSA - コード署名
		SSL - SSL接続

3. 削除する証明書のIDをリストから探します。
4. 次のコマンドを実行します。

```
dsm_c -action removecert -id ID
```

「ID」パラメータは必須です。

パラメータ	説明	値のサンプル
ID	削除する証明書に、Deep Security Managerによって割り当てられているIDの値。	3

注意: Linux環境でDeep Security Managerを実行している場合、rootユーザとしてdsm_cコマンドを実行する必要があります。

Smart Protection Networkの接続を無効にした場合のトレンドマイクロへの情報の送信について

Smart Protection Networkが無効になっている場合、Deep Security Agentからトレンドマイクロに脅威情報が送信されることはありません。

Agent向けのLinux Secure Bootのサポート

Deep Security AgentコンピュータでLinuxセキュアブートが有効になっている場合、Linuxカーネルはカーネルモジュールがインストールされる前に、署名確認を実行します。次のDeep Securityの機能でカーネルモジュールがインストールされます。

- 不正プログラム対策
- Webレピュテーション
- ファイアウォール
- 変更監視
- 侵入防御
- アプリケーションコントロール

注意: Deep Security AgentはRHEL 7でのセキュアブートのみに対応しています。

セキュアブートが有効なLinuxコンピュータでこれらのモジュールのいずれかを使用する場合は、RHEL7のTrendMicro公開鍵（[Trend Micro公開鍵のダウンロード](#)を参照）をLinuxコンピュータのファームウェアに登録して、認識できるようにする必要があります。Trend Microカーネルモジュールの署名が認識されるようにする必要があります。この操作を実行しない場合、カーネルモジュールをインストールできません。

注意: Deep Securityはメジャーリリース (10.0、11.0など) ごとにカーネルモジュールの署名鍵を更新します。Deep Security Agentを新しいメジャーリリースにアップグレードするとき

にセキュリティ機能が動作し続けるようにするには、セキュアブートが有効なLinuxコンピュータに新しい公開鍵を登録する必要があります。公開鍵を登録するまでアップグレードしたカーネルモジュールがOSに読み込まれないために、「エンジンがオフライン」というエラーメッセージがDeep Security Managerコンソールに表示される場合があります。

VMware仮想マシンを保護する場合、セキュアブート機能はVMware vSphere 6.5以降で使用できます。この機能を有効にする方法については、VMware Docsサイトで「[Enable or Disable UEFI Secure Boot for a Virtual Machine](#)」を参照してください。

注意: AWSインスタンスとAzure VMでは、セキュアブート機能は使用できません。

トレンドマイクロの公開鍵をダウンロードする

トレンドマイクロの公開鍵は、次のリストからダウンロードできます。

ヒント: 次のファイルのダウンロードで問題が発生した場合は、右クリックして[リンクに名前を付けて保存として保存]を選択します。

- [DS12.der](#)
- [DS11.der](#)

注意: このDeep Security Agent 11の公開鍵の有効期限は2022年12月5日です。この日以降もエージェントを使用するには、新しい [DS11_2022.der](#) Secure Bootキーを0d 0b 3b ff ee 28 fa df 30 80 e9 bb 88 63 d0 57 fe 07 47 afのSHA1ハッシュで登録する必要があります。

Shim MOK Managerの鍵データベースを使用して鍵を登録する

トレンドマイクロの公開鍵を登録するには、次の操作を実行します。

1. 保護するRHEL 7コンピュータにDeep Security Agentがまだインストールされていない場合はインストールします。
2. MOK (Machine Owner Key) がまだインストールされていない場合はインストールします。

```
yum install mokutil
```

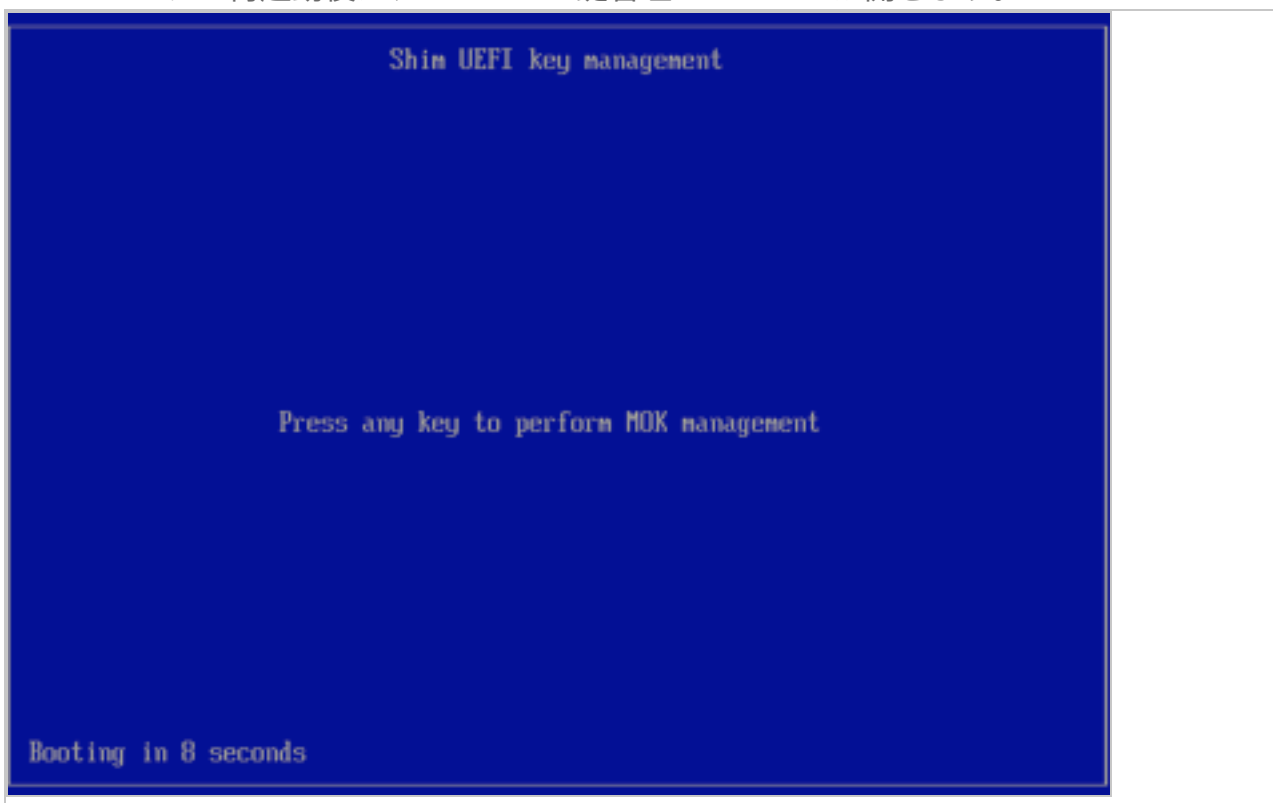
3. 公開鍵をMOKリストに追加します。

```
mokutil --import /opt/ds_agent/DS12.der /opt/ds_agent/DS11.der
```

注意: mokutil --import コマンドが機能するには、そのパスがキーの場所と一致している必要があります。上記のコマンドは、 /opt/ds_agent/ からキーを追加しています。

ヒント: 公開鍵をMOKリストに手動で追加する方法の詳細については、Linuxのマニュアルを参照してください。

4. プロンプトが表示されたら、この手順で後に使用するパスワードを入力します。
5. システムを再起動します。
6. コンピュータの再起動後に、Shim UEFI鍵管理コンソールが開きます。



7. 開始するには、いずれかのキーを押します。
8. [Perform MOK management]画面で、[Enroll MOK]を選択します。
9. [Enroll MOK]画面で、[View key 0]を選択します。
10. [Enroll the key(s)?]画面で[Yes]を選択してから、上記の手順4で設定したパスワードを入力します。
11. [The system must now be rebooted]画面で[OK]を選択して変更を確認し、再起動します。

12. `mokutil` ユーティリティを使用して、キーが正常に登録されているかどうかを確認します。

```
mokutil --test-key /opt/ds_agent/DS12.der
```

```
mokutil --test-key /opt/ds_agent/DS11.der
```

注意: `mokutil --test-key` コマンドが機能するには、そのパスがキーの場所と一致している必要があります。上記のコマンドは、`/opt/ds_agent/`のキーをテストしていません。

13. `keyctl` ユーティリティがインストールされていない場合は、インストールします。

```
yum install keyutils
```

14. `keyctl` ユーティリティを使用して、システムの鍵リングにある鍵を一覧表示します。

```
keyctl list %:.system_keyring
```

表示されたTrend Micro署名鍵を確認します。

Agentの有効化

ヒント: Agentをまだインストールしていない場合は、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498または"[Deep Security Agentの手動インストール](#)" on page 376を参照してAgentをインストールしてください。

インストールされたエージェントがコンピュータを保護したり、リレーに変換される前に、Deep Security Managerを使用してエージェントをアクティベートする必要があります。有効化により、最初の通信時にManagerにAgentが登録されます。

そのためには、次のいずれかの方法があります。

- ManagerからAgentを有効化します。[コンピュータ]に移動し、AgentまたはApplianceを有効化または再有効化するコンピュータを右クリックして、[処理]→[有効化/再有効化]の順に選択します(または、コンピュータの[詳細]画面で[有効化]または[再有効化]をクリックします)。
- インストールスクリプトを使用してAgentを有効化します。詳細については、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498を参照してください。
- AgentがインストールされているコンピュータからAgentを有効化します。次のコマンドを実行します。

```
dsa_control -a dsm://<dsm_host_or_IP>:<port>/
```

指定する項目は次のとおりです。

<dsm_host_or_IP>はDeep Security Managerのホスト名またはIPアドレスに置き換え、<port>はDeep Security Managerのハートビートポート (初期設定は4120) に置き換えます。

その他のパラメータなど、このコマンドの詳細については、"[コマンドラインの基本](#)" on page 447を参照してください。

- イベントベースタスク (「コンピュータの作成 (システムによる)」 イベント) を使用して Agentを有効化して、コンピュータがManagerに接続したとき、またはManagerがLDAPディレクトリ、クラウドアカウント、vCenterと同期したときに自動的にコンピュータを有効化します。詳細については、"[コンピュータの追加または変更時のタスクの自動実行](#)" on page 482を参照してください。

有効化の前は、AgentまたはApplianceは次のいずれかの[ステータス](#)になっています。

- Agent/Applianceなし: 次のいずれかの状況を示しています。
 - 初期設定のポートでAgentまたはApplianceが実行されていないか、待機中ではありません。
 - AgentまたはApplianceはインストールされ実行中ですが、別のManagerと連携しており、通信がAgent/Applianceから開始されるように設定されています。この場合、AgentまたはApplianceはこのManagerを待機していません。この問題を解決するには、コンピュータからAgentを無効化します。
- 有効化が必要: AgentまたはApplianceはインストールされ待機中で、Managerによる有効化の準備ができています。
- 再有効化が必要: AgentまたはApplianceはインストールされ待機中で、Managerによる再有効化を待機しています。
- 無効化が必要: AgentまたはApplianceはインストールされ待機中ですが、別のManagerによってすでに有効化されています。
- 不明: 状態情報のないコンピュータが、インポート済みのコンピュータリストの一部としてインポートされました。または、LDAPディレクトリ検出プロセスによって、コンピュータが追加されました。

有効化が正常に実行されると、AgentまたはApplianceの状態はオンラインになります。有効化に失敗すると、コンピュータは有効化の失敗ステータスになり、カッコ内に失敗の理由が表示されます。このリンクをクリックすると、有効化の失敗理由の詳細を示すシステムイベントが表示されます。

注意: IPv6トラフィックは、Deep Security 8.0以前のAgentとApplianceでサポートされていますが、初期設定ではブロックされています。Deep Security 8.0のAgentとApplianceでIPv6トラフィックを許可するには、**コンピュータエディタまたはポリシーエディタ**¹を開いて、[設定]→[詳細]→[ネットワークエンジンの詳細設定]の順に移動します。[バージョン8以降のAgentとApplianceでIPv6をブロック] オプションを [いいえ] に設定します。

Agentを無効化する

別々にインストールされたDeep Security Manager間で管理するコンピュータを移動する場合は、現在のManagerでAgentまたはApplianceを無効化してから、新しいManagerで再有効化する必要があります。

通常は、現在AgentまたはApplianceを管理しているDeep Security Managerから、AgentまたはApplianceを無効化できます。Deep Security ManagerがAgentまたはApplianceと通信できない場合は、無効化を手動で実行する必要があります。以下のコマンドを実行するには、ローカルのコンピュータに対する管理者権限が必要です。

WindowsでAgentを無効にするには

1. コマンドラインから、Agentのディレクトリ (初期設定ではC:\Program Files\Trend Micro\Deep Security Agent) に移動します。
2. 次のコマンドを実行します。dsa_control -r

LinuxでAgentを無効にするには

1. 次のコマンドを実行します。/opt/ds_agent/dsa_control -r

エージェントの起動または停止

WindowsでAgentを起動または停止するには

- 開始： `sc start ds_agent`
- 停止： `sc stop ds_agent`

LinuxでAgentを起動または停止するには

SysV initスクリプトの使用：

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Trend Micro Deep Security(オンプレミス) 12.0

- 開始： `/etc/init.d/ds_agent start`
- 停止： `/etc/init.d/ds_agent stop`

systemdコマンドの使用：

- 開始： `systemctl start ds_agent`
- 停止： `systemctl stop ds_agent`

Deep Security Virtual Applianceに組み込まれているエージェントを開始または停止するには、「["アプライアンスを起動または停止する"](#) on page 371。

Agent配信での問題の診断 (Windows)

WindowsでDeep Security Agentのインストールまたは有効化に失敗した場合、配信ログを確認し原因を検索して、トラブルシューティングします。

1. Agentのインストールを試行したコンピュータにログインします。
2. `%appdata%\Trend Micro\Deep Security Agent\installer`に移動します。
3. 下記のファイルを確認します。
 - `dsa_deploy.txt` - PowerShellスクリプトのログ。Agentの有効化の問題についての記録が含まれています。
 - `dsa_install.txt` - MSIインストーラのログ。Agentのインストールの問題についての記録が含まれています。

NICチームングの設定

「NICチームング」または「リンク集約」とは、複数のネットワークインタフェースカード (NIC) を使ってコンピュータ上のネットワークリンクを作成することです。総ネットワーク帯域幅を増やしたり、リンクの冗長性を提供する場合に役立ちます。

WindowsでNICチームングを設定して、Deep Security Agentと互換性を持たせることができます。

Windowsでは、NICのチームに参加すると、新しい仮想インタフェースが作成されます。この仮想インタフェースでは、最初にチーム化された物理インタフェースのMACアドレスが使用されます。

初期設定では、Windows Agentはインストール時またはアップグレード時にすべての仮想および物理インタフェースとバインドされます。これには、NICチームングによって作成された仮

想インタフェースが含まれます。しかし、複数のインタフェースのMACアドレスが同じ場合、Deep Security Agentは正しく機能しません。この問題は、WindowsでのNICチーミングで発生します。

この問題を回避するには、Agentを物理インタフェースではなく、チーミングした仮想インタフェースにのみバインドします。

警告: インストーラを実行する直前を除き、チーミングしたNICからネットワークインタフェースを追加または削除しないでください。そのような変更を加えると、ネットワーク接続に失敗したり、コンピュータがDeep Security Managerによって正しく検出されなくなったりすることがあります。Agentのネットワークドライバはインストール時またはアップグレード時にネットワークインタフェースにバインドされ、Agentは以後の変更を継続的に監視することはありません。

Agentの設定

Agentを設定するには、[管理]→[システム設定]→[Agent] の順に選択します。

ヒント: Agentに関連するシステム設定の変更は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド [「Configure Policy, Computer, and System Settings」](#) を参照してください。

ホスト名

コンピュータをIPで登録していてIPの変更が検出された場合、コンピュータの [ホスト名] を自動的に更新: IPの変更が検出された場合に、コンピュータの [ホスト名] フィールドに表示されるIPアドレスをアップデートします。

注意: Deep Security Managerは、IPアドレスやホスト名ではなく一意のフィンガープリントによってコンピュータを特定します。

Agentからのリモート有効化

注意: Agentからのリモート有効化の設定の詳細については、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on page 408を参照してください。

Agentからのリモート有効化を許可

- 任意のコンピュータ: Deep Security Managerの [コンピュータ] 画面に表示されているかどうかに関係なく、すべてのコンピュータを対象とします。
- 既存のコンピュータ: [コンピュータ] 画面に表示されているコンピュータのみを対象とします。
- 次のIPリストにあるコンピュータ: 指定したIPリストとIPアドレスが一致するコンピュータのみを対象とします。

割り当てるポリシー (有効化スクリプトによってポリシーが割り当てられていない場合): 有効化スクリプトによってポリシーが割り当てられていない場合に、コンピュータに割り当てるセキュリティポリシーです。

注意: Agentによる有効化が許可されているコンピュータに対して、ポリシーを割り当てるイベントベースタスクがある場合、イベントベースタスクで指定されたポリシーは、割り当てられているポリシーまたは有効化スクリプトによるポリシーをオーバーライドします。

Agentによるホスト名指定を許可: このオプションを選択すると、Agentの有効化プロセスでDeep Security Managerに指定することでAgentがホスト名を指定できるようになります。

同じ名前のコンピュータがすでに存在する場合: Agent GUIDまたは証明書が同じでコンピュータ、VMware仮想マシン、AWSインスタンス、またはAzure仮想マシンがすでに [コンピュータ] 画面に表示されている場合は、Deep Security Managerで次の処理を行うように設定できません。

- 有効化を許可しない: コンピュータオブジェクトは有効化されません。
- 同じ名前で新規コンピュータを有効化: Deep Security Managerは新しい名前で新しいコンピュータオブジェクトを作成します。
- 既存のコンピュータの再有効化: 既存のコンピュータオブジェクトが再有効化されます。

クローンAgentの再有効化:すでに有効化されているDeep Security Agentを実行中の新しいコンピュータ (コンピュータ、VMware仮想マシン、AWSインスタンス、またはAzure仮想マシン) がDeep Security Managerにハートビートを送信すると、Deep Security Managerはそれをクローンと認識します。クローンとして認識されたコンピュータは新しいコンピュータとして再有効化され、元のコンピュータのポリシーやルールは引き継がれません。

不明なAgentの再有効化:この設定を選択すると、一度有効化されたコンピュータがDeep Security Managerから削除され、そのコンピュータが再接続したときに再有効化することができます。

通常、この設定は、特定のコンピュータが削除された場合でも再接続できるようにするために、[非アクティブなAgentのクリーンナップ](#)と組み合わせて使用されます。詳細については、"[非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化](#)" on page 1523を参照してください。

注意: 削除されたコンピュータが再接続した場合、ポリシーは割り当てられず、新しいコンピュータとして追加されます。そのコンピュータへの直接リンクは、Deep Security Manager イベントデータからすべて削除されます。

Agent有効化トークン: この値が指定されている場合、Agentによる有効化の実行時に同じ値を指定する必要があります。Agentからのリモート有効化のパスワードは、Agentの有効化スクリプトのtokenパラメータで指定できます。LinuxコンピュータにおけるAgentからのリモート有効化のスクリプトの例を次に示します。

```
/opt/ds_agent/dsa_control -a dsm://172.31.2.247:4120/ "token:secret"
```

注意: マルチテナント環境の場合、[Agent有効化トークン] 設定はプライマリテナントにのみ適用されます。

Agentのアップグレード

Deep Security AgentがインストールされたLinuxコンピュータが環境に含まれている場合は、Agentを有効化するときに自動的にアップグレードするを選択できます。Linuxコンピュータ上でこのオプションが選択され、エージェントがアクティブ（または再アクティブ化）されている場合、エージェントは、あなたのDeep Security Managerと互換性のある最新のソフトウェアバージョンにアップグレードされます。

詳細については、"[Agentを有効化するときに自動的にアップグレードする](#)" on page 397を参照してください。

非アクティブなAgentのクリーンナップ

Deep Security Managerと通信しておらず、管理が不要となったオフラインコンピュータがDeep Security環境内に多数ある場合は、非アクティブなAgentのクリーンナップを使用して、それらのコンピュータを自動的に削除できます。

次の期間を超過した非アクティブなAgentを削除する:非アクティブな期間がどのくらい続いているコンピュータを削除するかを指定します。

非アクティブなAgentのクリーンアップ設定の詳細については、"[非アクティブなAgentのクリーンアップによるオフラインコンピュータの削除の自動化](#)" on page 1523を参照してください。

データプライバシー

暗号化されたトラフィック (SSL) のパケットデータの取り込みを許可: 侵入防御モジュールを使用すると、侵入防御ルールをトリガするパケットデータを記録できます。この設定をオンにすると、暗号化されたトラフィックに侵入防御ルールが適用された場合のデータの取り込みが有効になります。

AgentレスによるvCloud保護

ApplianceによるvCloud仮想マシンの保護を許可: Deep Security Virtual ApplianceによるvCloud環境内の仮想マシンの保護を許可し、マルチテナントのDeep Security環境内のテナントによってこれらの仮想マシンのセキュリティが管理されるようにします。

Deep Security Notifierのインストール

Deep Security Notifierは、Windowsの物理マシンまたは仮想マシン用のユーティリティです。不正プログラムが検出された場合や、不正なURLがブロックされた場合にローカル通知を送信します。Deep Security Notifierは、Deep Security AgentをWindowsコンピュータにインストールするときに自動的にインストールされます。ここで説明するスタンドアロンのインストール環境は、Deep Security Virtual Applianceで保護されている、AgentレスによるWindows仮想マシンで使用することを想定しています。詳細については、"[Deep Security Notifier](#)" on page 578を参照してください。

インストールパッケージをコピーする

インストールファイルをコンピュータにコピーします。

Windows版Deep Security Notifierをインストールする

注意: WindowsコンピュータにDeep Security Notifierをインストールして実行するには、管理者権限が必要です。

1. インストールファイルをダブルクリックして、インストーラパッケージを実行します。
[次へ] をクリックして、インストールを開始します。

2. 使用許諾契約書の内容をご確認いただき同意できる場合は、使用許諾内容に同意し、[次へ]をクリックします。
3. [インストール]をクリックして、インストールを続行します。
4. [完了]をクリックして、インストールを完了します。

Deep Security Notifierがこのコンピュータにインストールされ、稼働しています。Windows システムトレイにNotifierのアイコンが表示されます。不正プログラムが検出されたり、URLがブロックされたりすると、Notifierによってポップアップ通知が表示されます。通知を手動で無効にするには、トレイのアイコンをダブルクリックして、Notifierステータスおよび設定画面を開きます。

注意: Deep Security Notifierに情報が表示されるためには、Virtual Applianceで保護されている仮想マシンに不正プログラム対策モジュールのライセンスがあり、モジュールが有効になっている必要があります。

Relayによるセキュリティとソフトウェアのアップデートの配布

Deep Security環境の最大限の保護を実現するには、次の2つのコンポーネントを定期的にアップデートする必要があります。ソフトウェアのアップデートでは、Deep Security エージェントに新機能と改善点が追加されました。セキュリティアップデートでは、新しい脅威に対してすぐに保護機能が提供されます。

Deep Security リレーは、これらのアップデートの配信を最適化するのに役立ちます。リレーは、ソフトウェアとセキュリティのアップデートを他のDeep Security AgentおよびVirtual Applianceに配信できるエージェントです。Relayには次の機能があります。

- アップデートトラフィックを形成することにより、WAN帯域幅のコストを削減します。
- アップデート配布のための冗長性を提供します。

注意: リレーは Deep Security 配置の必須部分です。環境内には、Relayが1つ以上存在している必要があります。

まず["Relayの仕組み" on the next page](#)について学び、次に["使用するRelayの数を決定する" on the next page](#)方法について学び、最後に["1つ以上のRelayを設定する" on page 441](#)方法について学びます。

必要に応じて、["AgentからRelay機能を削除する" on page 445](#)こともできます。

Relayの仕組み

Relayは、WAN接続を介して直接トレンドマイクロのアップデートサーバからセキュリティアップデートをダウンロードし、Deep Security Managerからソフトウェアアップデートをダウンロードします。Relayを使用する場合、セキュリティアップデートとソフトウェアアップデートは、WAN接続を介して一度だけダウンロードする必要があります。リレーは、アップデート配信センターとして機能し、セキュリティおよびソフトウェアのアップデートは、マネージャによって指示されると、他のクライアントによってダウンロードされます。

注意: Deep Security Managerに接続してアップデートをダウンロードできない場合、RelayはDeep Securityダウンロードセンターから直接アップデートをダウンロードします。

セキュリティアップデートと、Relayによるセキュリティアップデートの配布方法の詳細については、"[セキュリティアップデートの取得と配布](#)" on page 1039を参照してください。

RelayはRelayグループにまとめられます。Relayをグループにまとめることで、アップデートの負荷が複数のRelayに分散され、Deep Security環境に冗長性が追加されます。

Relayグループは、配布階層の一部にすることもできます。Relayグループの配布階層を作成することで、以下の項目を指定してパフォーマンスと帯域幅の使用をさらに改善できます。

- AgentがセキュリティアップデートとソフトウェアアップデートをダウンロードするRelayグループ
- Relayグループがセキュリティアップデートとソフトウェアアップデートを互いにダウンロードする順序

使用するRelayの数を決定する

Deep Security環境には少なくとも1つのRelayが必要ですが、Trend Microでは、ベースラインとして、環境に少なくとも2つのRelayを使用することをお勧めします。ただし、次の項目に応じて追加のRelayを使用する必要がある場合もあります。

- "[Agentの地域](#)" on the next page
- "[ネットワーク設定](#)" on the next page
- "[ネットワーク帯域幅の使用](#)" on the next page

Agentの地域

Agentは、同じ地域のRelayグループからアップデートをダウンロードすることをお勧めします。複数の地域にAgentがある場合、各地域には少なくとも1つのRelayがある独自のRelayグループが必要です。

ネットワーク設定

ネットワーク設定では、AgentのネットワークセグメントとリモートDeep Security Managerまたはトレンドマイクロのアップデートサーバの間に、帯域幅の低いWAN接続、ルータ、ファイアウォール、またはプロキシが含まれる場合があります。これらの設定が原因で、ソフトウェアアップデートとセキュリティアップデートの配布が遅くなるボトルネックが発生する可能性があります。これらの設定の影響を軽減するには、各ネットワークセグメント内にRelayを配置する必要があります。

ネットワーク帯域幅の使用

Agentへのセキュリティアップデートとソフトウェアアップデートのダウンロードにより、ネットワークが集中的に使用される可能性があります。Relayを使用することで、どのようにネットワーク帯域幅を使用してアップデートを配布するかを決定できます。Relayをネットワークセグメント内に配置することで、Relayがそのセグメントのセキュリティアップデートとソフトウェアアップデートの単一のダウンロード元になります。その後、AgentはローカルRelayからアップデートするため、WAN接続からローカル内部接続にアップデートをダウンロードするために必要となる全体の帯域幅が削減されます。

サイジングの推奨設定

注意: より多くのRelayを有効にする前に、Relayとして有効にするコンピュータが"[Deep Security AgentおよびRelayのサイジング](#)" on page 188要件を満たしていることを確認してください。また、ご利用のエージェントでRelay機能がサポートされていることも確認してください ("[各プラットフォームでサポートされている機能](#)" on page 183を参照してください)。

ほとんどの環境では、冗長性のために少なくとも2つのRelayを配置することをお勧めします。RelayはDeep Security Managerと同じ場所に配置できます。ただし、前述のように、配置するRelayの数を決定する際には、地理的な位置、ネットワーク設定、およびネットワーク帯域幅などの要素も考慮する必要があります。環境内に (10,000を超える) 多数のAgentがある場合は、Relayを専用のシステムに配置する必要があります。

次の場合も、Relayを追加できます。

- 環境のネットワーク設定が変更された場合。
- アップデートの配布に追加の冗長性を提供する必要がある場合。

警告: ネットワーク上に不要なRelayを配置すると実際にはパフォーマンスが低下するため、必要な数のRelayのみを使用する必要があります。Relayには通常のAgentよりも多くのシステムリソースが必要です。

1つ以上のRelayを設定する

Relayを設定するには、次の手順を実行する必要があります。

1. ["1つ以上のRelayグループを作成する" below](#)。
2. ["1つ以上のRelayを有効にする" on page 443](#)。
3. ["AgentをRelayグループに割り当てる" on page 444](#)。
4. ["セキュリティアップデートとソフトウェアアップデートのためのRelay設定を指定する" on page 444](#)。

1つ以上のRelayグループを作成する

すべてのRelayは、Relayグループに属する必要があります。Deep Security Managerのインストール中にDeep Security Relayをインストールした場合は、初期設定のRelayグループが自動的に作成されています。追加のRelayグループを作成することもできます。

注意: 各Agentは、割り当てられたグループ内のRelayがランダムに並べられたリストから、アップデートのダウンロードを試みます。特定のRelayからの応答がない場合、Agentはアップデートを正常にダウンロードできるまでリストから別のRelayを試みます。このリストはAgentごとにランダムなため、アップデートの負荷はグループ内のRelayで均等に共有されません。

1. [管理]→[アップデート]→[Relayの管理]に進みます。
2. [Relayの管理] ウィンドウで、[新規Relayグループ...] をクリックします。表示された [Relayグループのプロパティ] 画面で、Relayグループの設定を指定します。
 - Relayグループの [名前] を入力します。
 - [アップデート元] を選択します。このアップデート元により、Relayグループがセキュリティアップデートをどこからダウンロードして配布するかが決まります。アップデート元には、次のいずれかを使用できます。
 - セキュリティアップデート元
初期設定では、セキュリティアップデート元はトレンドマイクロのアップデート

サーバですが、代わりにローカルミラーに設定できます。初期設定のRelayグループは、常にセキュリティアップデート元を使用します。詳細については、"[セキュリティアップデート元および設定を指定する](#)" on page 1042を参照してください。

- 親Relayグループ

すでに他のRelayグループを作成している場合は、そのいずれかをアップデート元として使用するようRelayグループを設定できます。

ヒント: Relayグループのアップデートダウンロード元を選択する際には、コストと速度の要件に最も適したダウンロード元を選択する必要があります。Relayグループが配布階層の一部である場合でも、セキュリティアップデート元からアップデートをダウンロードする方が安価または高速である場合は、必ずしも親グループのRelayからアップデートをダウンロードする必要はありません。

ヒント: 非常に大規模な環境でのパフォーマンスを向上させるには、複数のRelayグループを作成し、階層内にRelayを配置します。1つ以上の第1レベルのRelayグループがトレンドマイクロのアップデートサーバからアップデートを直接ダウンロードしてから、第2レベルのRelayグループが第1レベルのグループからアップデートをダウンロードします。以降のレベルも同様です。ただし、各グループレベルで待ち時間が追加されるため、Relayグループのレベルが多すぎると、Relayによる帯域幅の最適化よりも合計待ち時間の影響が大きくなり、パフォーマンスが低下する可能性があります。

- セキュリティアップデート元にアクセスするためにRelayが使用する必要がある、[アップデート元のプロキシ] (ある場合) を選択します。

初期設定のRelayグループを除くすべてのRelayグループを、プロキシサーバ経由でセキュリティアップデートをダウンロードするように設定できます。初期設定のRelayグループは、Deep Security Managerと同じプロキシを使用します。"[プロキシの背後に配置されたAgentの接続](#)" on page 410 および "[不正プログラム対策およびルールアップデート用にプロキシを設定する](#)" on page 461 (CLI) のプロキシを設定します。

Relayグループがセキュリティアップデート元を使用するように設定されている場合、Relayはこのプロキシを使用します。または、このRelayグループが別のRelayグループからセキュリティアップデートをダウンロードするように設定されている場

合、Relayは親Relayグループに接続できない場合を除いてプロキシを使用しないため、セキュリティアップデート元への接続を試みます。


警告: Deep Security Agentバージョン10.0以前では、プロキシ経由でのRelayへの接続はサポートされていません。アプリケーションコントロール[ルールセットのダウンロード](#)でプロキシ経由で失敗し、クライアントがリレーまたはマネージャにアクセスするためにプロキシを必要とする場合は、次のいずれかを実行する必要があります。

- Agentのソフトウェアをアップデートして("Deep Security Agentソフトウェアの入手" on page 372を参照)、[プロキシを設定します](#)。
- プロキシをバイパスする。
- [アプリケーションコントロールルールセット](#)が回避する回避策を設定する

3. Relayグループをさらに作成する必要がある場合は、上記の手順を繰り返します。

1つ以上のRelayを有効にする

1. [管理]→[アップデート]→[Relayの管理]に進みます。
2. Relayグループをクリックして選択します。
3. [Relayの追加...] をクリックします。
4. [使用可能なAgent] リストからコンピュータを選択し、[Relayを有効にしてグループに追加] をクリックします。検索フィールドを使用してコンピュータのリストをフィルタできます。

コンピュータがRelayグループに追加され、Relayアイコン () が表示されます。

5. コンピュータでWindowsファイアウォールまたはiptablesが有効になっている場合は、[Relayの待機ポート番号](#)への受信接続を許可するファイアウォールルールも追加します。
6. Relayをプロキシ経由で接続する必要がある場合は、"[プロキシを経由してAgent、Appliance、Relayをセキュリティアップデートに接続する](#)" on page 411を参照してください。

注意: 新しくアクティブにされたリレーは、マネージャによってセキュリティアップデートの内容をアップデートするように自動的に通知されます。

AgentをRelayグループに割り当てる

Relayグループには手動でAgentを割り当てることや、[イベントベースタスク](#)を設定して自動的にAgentを割り当てることができます。

1. Deep SecurityManagerで、[コンピュータ]に進みます。
2. コンピュータを右クリックして、[処理]→[Relayグループの割り当て]の順に選択します。
複数のコンピュータを割り当てるには、リスト内のコンピュータをShiftキーまたはCtrlキーを押しながらクリックし、[処理]→[Relayグループの割り当て]の順に選択します。
3. 使用するRelayグループをリストから選択するか、[コンピュータの詳細]画面の[アップデートのダウンロード元]を使用してRelayグループを選択します。

セキュリティアップデートとソフトウェアアップデートのためのRelay設定を指定する

Deep Security Managerは、[管理]→[システム設定]→[アップデート]画面で、セキュリティアップデートとソフトウェアアップデートを実行するためにRelayが使用される方法に影響を与える追加の設定を提供しています。

セキュリティアップデート

- サポート対象の8.0および9.0エージェントのアップデートを許可： Deep Security Agent 8.0または9.0のセキュリティアップデートが必要な場合は、このオプションを選択します。初期設定では、Deep Security ManagerはDeep Security Agent 9.0以前のアップデートをダウンロードしません。

注意: 8.0および9.0エージェントの使用期限が終了しました。これにより、トレンドマイクロからは、セキュリティアップデート、ソフトウェアアップデート、およびサポートサービスが提供されなくなります。サポートされている8.0および9.0のエージェントの詳細については、)ではなく [Deep Security LTSのライフサイクル日](#)を参照してください。

- すべての地域のパターンファイルをダウンロード: マルチテナントモードで稼働していて、いずれかのテナントが他のリージョンにある場合は、このオプションを選択します。このオプションの選択を解除すると、RelayはDeep Security Managerがインストールされたリージョン (ロケール) のパターンファイルのみをダウンロードして配布します。

- プライマリテナント Relay グループを初期 Relay グループとして使用します (割り当てられていないリレー): の場合は、プライマリテナント Relay グループを使用します。初期設定では、他のテナントは、プライマリテナントのRelayにアクセスできます。この場合、テナントに独自のRelayを設定する必要はありません。他のテナントがプライマリテナントのRelayを共有しないようにするには、このオプションの選択を解除し、他のテナント用の別のRelayを作成します。

注意: このオプションの選択が解除されている場合、[管理]→[アップデート]→[Relayグループ]の順にクリックすると、Relayグループ名は「プライマリテナントのRelayグループ」ではなく「初期設定のRelayグループ」になります。

注意: この設定は、マルチテナントモードを有効にしている場合のみ表示されます。

その他のセキュリティアップデートの設定の詳細については、"[セキュリティアップデートの取得と配布](#)" on page 1039を参照してください。

ソフトウェアアップデート

- Deep Security Managerにアクセスできない場合、トレンドマイクロのダウンロードセンターからのソフトウェアアップデートのダウンロードをRelayに許可 オプションは、Deep Security Managerをエンタープライズ環境に展開し、クラウド環境でコンピュータを管理している場合に役立ちます。このオプションを有効にしてクラウド内にRelayを設定すると、そのRelayはダウンロードセンターから直接ソフトウェアアップデートを入手できるようになります。ソフトウェアを手動でアップグレードしたり、クラウドからエンタープライズ環境への[ポート番号](#)を開いたりする必要はありません。

その他のソフトウェアアップデートの設定の詳細については、"[アップグレードについて](#)" on page 994を参照してください。

AgentからRelay機能を削除する

次の場合に、Relay有効化済みAgentからRelay機能を削除できます。

- 環境内にRelay有効化済みAgentが多すぎるため、通信速度が遅くなった場合。
- AgentがインストールされているコンピュータがRelay機能のための最小システム要件を満たしていない場合。

注意: Deep Securityは、Deep Security Virtual Applianceで保護された仮想マシンをvMotionにより移行する際に、Relayを使用してデータを保存します。環境内でvMotionを使

用して仮想マシンを移行している場合、特定のAgentからRelay機能を削除すると、移行対象の仮想マシンに対する保護が失われ、Virtual Applianceのセキュリティイベントも失われる可能性があります。

1. [管理]→[アップデート]→[Relayの管理]に進みます。
2. Relay機能を削除するコンピュータがあるRelayグループの横の矢印をクリックします。
3. コンピュータをクリックし、[Relayの削除]をクリックします。

Agentのステータスが「無効化しています」に変わり、Relay機能がAgentから削除されます。

注意: Relay機能がAgentから削除されるまでに、最大で15分かかる場合があります。Agentがこれよりも大幅に長く「無効化しています」状態になっている場合は、Agentを無効化してから再有効化し、AgentからのRelay機能の削除を完了します。

開発、自動化、およびAPI

管理開発ワークフローをサポートするために、Deep Securityは、リリースのライフサイクル全体にわたってセキュリティを自動化、監視、および管理するためのAPIを提供します("Deep Security APIを使用したタスクの自動化" on page 478を参照してください)。

[Deep SecurityのGitHub](#)リポジトリには、次の役に立つスクリプトが含まれています。

注意: GitHubに公開されているリソースについてのお問い合わせはサポート対象外となります。

- [AWSにDeep Security Managerを配置するためのCloudFormationテンプレート。](#)
- [解析ロジック、保存された検索、Splunkを使用したDeep Security監視のためのダッシュボードを含む設定ファイル。](#)
- [さまざまなAgentおよびManagerのタスクを自動化する、BashとPowershellのスクリプト。](#)

このAPIの使用を開始するには、Deep Security Automation Centerにあるガイド「[First Steps Toward Deep Security Automation](#)」を参照してください。オートメーションセンターには、[APIレファレンス/参照情報](#)も含まれています。

Deep Securityはコンピュータとその他のリソースの保護の速度を向上するための方法もたくさん提供しています。

- ["Deep Security予約タスクの設定" on page 479](#)
- ["コンピュータの追加または変更時のタスクの自動実行" on page 482](#)
- ["AWSオートスケーリングとDeep Security" on page 488](#)
- ["インストールスクリプトを使用したコンピュータの追加と保護" on page 498](#)
- ["AWSインスタンスタグに基づくポリシーの自動割り当て" on page 502](#)
- ["コマンドラインの基本" below](#)

また、Deep Securityは、Splunk、QRadar、ArcSight、Amazon SNSなどのSIEMにイベントを転送することもできます。詳細については、次のセクションを参照してください。

- ["Deep SecurityイベントをSyslogまたはSIEMサーバに転送する" on page 1141](#)
- ["Amazon SNSでのイベントへのアクセス" on page 1200](#)

コマンドラインの基本

ローカルのコマンドラインインタフェース (CLI) から、Deep Security AgentとDeep Security Managerに対して数々の処理を実行するように指示できます。CLIではいくつかの設定を行い、システムリソースの使用量を表示することもできます。

ヒント: また、以下のCLIコマンドの多くは、Deep Security APIを使用して自動化することが可能です。このAPIの使用を開始するには、Deep Security Automation Centerにあるガイド「[First Steps Toward Deep Security Automation](#)」を参照してください。

次にコマンドの構文と例を示します。

- [Deep Security Agent](#)
- [Deep Security Manager](#)

Deep Security Agent

注意: Windowsで[セルフプロテクションが有効になっている](#)場合、ローカルユーザはAgentの管理、たとえばアンインストール、アップデート、停止などを行うことができません。また、CLIコマンドの実行時には、認証パスワードが必要となります。

dsa_control

注意: Dsa_control は、英語の文字列のみをサポートします。Unicodeはサポートされていません。

dsa_controlを使用してAgentの設定を行い、有効化、不正プログラム検索、またはベースライン再構築などの処理を手動で開始できます。

Windowsの場合:

- 管理者権限でコマンドプロンプトを開きます。
- `cd C:\Program Files\Trend Micro\Deep Security Agent\`
- `dsa_control -m "AntiMalwareManualScan:true"`

Linuxの場合:

- `sudo /opt/ds_agent/dsa_control -m "AntiMalwareManualScan:true"`

使用方法

```
dsa_control [-a <str>] [-b] [-c <str>] [-d] [-g <str>] [-s <num>] [-m] [-p <str>] [-r] [-R <str>] [-t <num>] [-u <str>:<str>] [-w <str>:<str>] [-x dsm_proxy://<str>] [-y relay_proxy://<str>] [--buildBaseline] [--scanForChanges] [Additional keyword:value data to send to manager during activation or heartbeat...]
```

パラメータ	Description
<code>-a <str>, --activate=<str></code>	<p>次の形式で指定されたURLのManagerに対して、Agentを有効化します。</p> <pre>dsm://<host>:<port>/</pre> <p>指定する項目は次のとおりです。</p> <ul style="list-style-type: none"> • <code><host></code> にはManagerの完全修飾ドメイン名 (FQDN)、IPv4アドレス、またはIPv6アドレスを入力します。 • <code><ポート></code> にはManagerの待機ポート番号を入力します。 <p>必要に応じて、有効化中に送信する設定 (説明など) を、この引数に続けて指定することもできます。詳しくは、"Agentからの</p>

パラメータ	Description
	<p>ハートビート有効化コマンド (「<code>dsa_control -m</code>」) " on page 453を参照してください。パラメータはキー:値のペアとして入力する必要があります (セパレータにはコロンを使用します)。入力可能なキー:値のペアの数に制限はありませんが、キー:値のそれぞれのペアをスペースで区切る必要があります。キー:値のペアにスペースや特殊文字が含まれている場合は、キー:値のペアを引用符で囲む必要があります。</p>
<code>-b, --bundle</code>	アップデートバンドルを作成します。
<code>-c <str>, --cert=<str></code>	証明書ファイルを特定します。
<code>-d, --diag</code>	Agentパッケージを生成します。詳細な手順については、" 保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する " " on page 1576 を参照してください。
<code>-g <str>, --agent=<str></code>	AgentのURLです。初期設定: <code>https://localhost:<port>/</code> にはManagerの待機 ポート番号 を入力します。
<code>-m, --heartbeat</code>	Agentを今すぐ強制的にManagerに接続します。
<code>-p <str>, --passwd=<str></code>	<p>認証パスワードです。Deep Security Managerで以前に設定されている可能性があります。詳細については、"Deep Security Managerを介してセルフプロテクションを設定する" " on page 576を参照してください。設定されている場合は、<code>dsa_control -a</code>、<code>dsa_control -x</code>、および<code>dsa_control -y</code>を除く<code>dsa_control</code>コマンドすべてにパスワードを含める必要があります。</p> <p>例: <code>dsa_control -m -p MyPa\$\$w0rd</code></p> <p>パスワードは、コマンドラインに直接入力した場合、画面上に表示されます。入力中のパスワードをアスタリスク (*) にして非表示にする場合は、対話形式のコマンド <code>-p *</code> を入力します。この場合、パスワードの入力を求めるプロンプトが表示されま</p>

パラメータ	Description
	<p>す。</p> <p>例:</p> <pre>dsa_control -m -p *</pre>
<code>-r, --reset</code>	Agentの設定をリセットします。このコマンドにより、Agentから有効化情報が削除され、無効化されます。
<code>-R <str>, --restore=<str></code>	隔離ファイルを復元します。Windows版では、駆除したファイルや削除したファイルも復元できます。
<code>-s <num>, --selfprotect=<num></code>	<p>Agentセルフプロテクションを有効にします (1: 有効、0: 無効)。セルフプロテクションにより、ローカルのエンドユーザはAgentに対してアンインストールや停止などの制御ができなくなります。詳細については、"Agentセルフプロテクションの有効化または無効化" on page 576を参照してください。この機能はWindows版でのみ使用できます。</p> <p>注意: セルフプロテクションはdsa_controlコマンドで有効化できますが、関連付けられた認証パスワードの設定にはDeep Security Managerを使用する必要があります。詳細については、"Deep Security Managerを介してセルフプロテクションを設定する" on page 576を参照してください。パスワードは、設定後は-pまたは--passwd=オプションを使用してコマンドラインに入力する必要があります。</p> <p>注意: Deep Security 9.0以前では、このオプションは、-H <num>, --harden=<num>でした。</p>
<code>-t <num>, --retries=<num></code>	Agentサービスに接続してdsa_controlコマンドの指示を実行できない場合に、dsa_controlを再試行する回数 (<num>) を設定します。再試行は、1秒おきに実行されます。
<code>-u <user>:<password></code>	プロキシが認証を要求する場合は、-x オプションと組み合わせてプロキシのユーザ名とパスワードを指定します。ユーザ名とパスワードは、コロン(:)で区切ります。例: # ./dsa_control

パラメータ	Description
	<p><code>-x dsm_proxy://<str> -u <new username>:<new password></code>。</p> <p>ユーザ名とパスワードを削除するには、空の文字列（""）を入力します。例：<code># ./dsa_control -x dsm_proxy://<str> -u <existing username>:""</code>。</p> <p>プロキシのユーザ名のみを変更せずにプロキシのパスワードのみをアップデートする場合は、<code>-x</code>なしで <code>-u</code> オプションを使用できます。例：<code># ./dsa_control -u <existing username>:<new password></code>。</p> <p>基本認証のみ。Digest認証とNTLM認証はサポートされていません。</p> <p>注意: <code>dsa_control -u</code> の使用は、エージェントのローカル設定にのみ適用されます。このコマンドを実行した結果、マネージャ上でセキュリティポリシーが変更されません。</p>
<p><code>-w <user>:<password></code></p>	<p>プロキシが認証を要求する場合は、<code>-y</code> オプションと組み合わせてプロキシのユーザ名とパスワードを指定します。ユーザ名とパスワードは、コロン(:)で区切ります。例：<code># ./dsa_control -y relay_proxy://<str> -w <new username>:<new password></code>。</p> <p>ユーザ名とパスワードを削除するには、空の文字列（""）を入力します。例：<code># ./dsa_control -y relay_proxy://<str> -w <existing username>:""</code>。</p> <p>プロキシのユーザ名のみを変更せずにプロキシのパスワードのみをアップデートする場合は、<code>-y</code>なしで <code>-w</code> オプションを使用できます。例：<code># ./dsa_control -w <existing username>:<new password></code>。</p> <p>注意: <code>dsa_control -w</code> の使用は、エージェントのローカル設定にのみ適用されます。このコマンドを実行した結果、マネージャ上でセキュリティポリシーが変更されません。</p>
<p><code>-x dsm_</code></p>	<p>Agentがプロキシ経由でManagerに接続する場合は、プロキシのIPv4/IPv6アドレスまたはFQDNと、ポート番号をコロン(:)で区</p>

パラメータ	Description
<code>proxy://<str>:<num></code>	切って入力します。URLではなくアドレスを削除するには、空の文字列 ("") を入力します。IPv6アドレスは角カッコで囲む必要があります。次に例を示します。 <code>dsa_control -x "dsm_proxy://[fe80::340a:7671:64e7:14cc]:808/"</code>
<code>-y relay_</code> <code>proxy://<str>:<num></code>	Agentがセキュリティアップデートやソフトウェアを実行する際にプロキシ経由でRelayに接続する場合は、プロキシのIPアドレスまたはFQDNと、 ポート番号 をコロン(:)で区切って入力します。
<code>--buildBaseline</code>	変更監視のベースラインを構築します。
<code>--scanForChanges</code>	変更監視の変更を検索します。
<code>--max-dsm-retries</code>	有効化を再試行する最大回数。0から100までの値を入力してください。初期設定値は30です。
<code>--dsm-retry-interval</code>	有効化を再試行する間隔(秒)。1から3600までの値を入力してください。初期設定値は300です。

Agentからのリモート有効化 (「dsa_control -a」)

Agentからのリモート有効化 (AIA) を有効にすると、ManagerとAgent間の通信の問題を防ぐことができます。また、インストールスクリプトと共に使用すると、Agentのインストールを簡略化できます。

注意: AIAを設定し、インストールスクリプトを使用してAgentを有効化する方法については、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on page 408を参照してください。

このコマンドには次の形式を使用します。

```
dsa_control -a dsm://<host>:<port>/
```

指定する項目は次のとおりです。

- <host> にはManagerの完全修飾ドメイン名 (FQDN)、IPv4アドレス、またはIPv6アドレスを入力します。
- <port>はAgentからManagerへの通信[ポート番号](#)です (初期設定は4120)。

次に例を示します。

```
dsa_control -a dsm://dsm.example.com:4120/ hostname:www12
"description:Long Description With Spaces"
```

```
dsa_control -a dsm://fe80::ad4a:af37:17cf:8937:4120
```

Agentからのハートビート有効化コマンド (「dsa_control -m」)

AgentからManagerに、ハートビートをただちに強制送信することができます。

有効化コマンドと同様、ハートビート有効化コマンドでも、実行中に設定をManagerに送信することができます。

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
AntiMalwareCancelManualScan	ブール。 コンピュータ上で実行されている手動検索をキャンセルします。	"AntiMalwareCancelManualScan:true"	不可	可
AntiMalwareManualScan	ブール。 コンピュータに対して手動の不正プログラム検索を開始します。	"AntiMalwareManualScan:true"	不可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
description	文字列。 コンピュータの説明を設定します。最大2000文字。	"description:Extra information about the host"	可	可
displayname	文字列。 [コンピュータ]のホスト名の横にカッコで囲んで表示される表示名を設定します。最大2000文字。	"displayname:the_name"	可	可
externalid	整数。 externalid値を設定します。この値を使用して、Agentを一意に識別できます。この値には、従来のSOAP WebサービスAPIを使用してアクセスできます。	"externalid:123"	可	可
group	文字列。	"group:Zone A web servers"	可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	<p>[コンピュータ]画面に表示される、コンピュータの属するグループを設定します。1つの階層レベルの1つのグループ名につき最大254文字。</p> <p>スラッシュ (「/」) はグループの階層を示します。groupパラメータはグループの階層を読み取ったり、作成したりできます。</p> <p>このパラメータは、メインの「コンピュータ」ルートブランチの下位にある標準のグループにコンピュータを追加する場合にのみ使用で</p>			

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	きます。ディレクトリ (Microsoft Active Directory)、VMware vCenter、またはクラウドプロバイダのアカウントに所属するグループにコンピュータを追加する場合には使用できません。			
groupid	整数。	"groupid:33"	可	可
hostname	文字列。 最大254文字。 ManagerがAgentに接続する際に使用するIPアドレス、ホスト名、またはFQDNを指定します。	"hostname:www1"	可	不可
IntegrityScan	ブール。 コンピュータで変更の検索を開	"IntegrityScan:true"	不可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	始します。			
policy	<p>文字列。</p> <p>最大254文字。</p> <p>ポリシー名とポリシーリストの大文字と小文字は区別しません。ポリシーが見つからない場合、ポリシーは割り当てられません。</p> <p>イベントベースタスクによって割り当てられるポリシーは、Agentからのリモート有効化中に割り当てられるポリシーをオーバーライドします。</p>	"policy:Policy Name"	可	可
policyid	整数。	"policyid:12"	可	可
relaygroup	<p>文字列。</p> <p>コンピュータを</p>	"relaygroup:Custom Relay Group"	可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	<p>特定のRelayグループにリンクします。最大254文字。</p> <p>Relayグループ名と既存のRelayグループ名の大文字と小文字は区別しません。Relayグループが見つからない場合は、初期設定のRelayグループが使用されます。</p> <p>これは、イベントベースタスクの際に割り当てられるRelayグループには影響を与えません。このオプションまたはイベントベースタスクのどちらかを使用してください。</p>			

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
relaygroupid	整数。	"relaygroupid:123"	可	可
relayid	整数。	"relayid:123"	可	可
tenantIDと token	文字列。 Agentからのリモート有効化をテナントとして使用する場合は、tenantIDと tokenの両方が必要です。 tenantIDと tokenはインストールスクリプト生成ツールから取得できます。	"tenantID:12651ADC-D4D5" and "token:8601626D-56EE"	可	可
RecommendationScan	ブール。 コンピュータで推奨設定の検索を開始します。	"RecommendationScan:true"	不可	可
UpdateComponent	ブール。 セキュリティアップデートの実行をDeep Security Managerに指示します。	"UpdateComponent:true"	不可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	<p>Deep Security Agent 12.0以降で UpdateComponentパラメータを使用する場合は、Deep Security Relay もバージョン 12.0以降であることを確認してください。詳細を表示。</p>			
RebuildBaseline	<p>ブール。 コンピュータに変更監視ベースラインを再構築します。</p>	"RebuildBaseline:true"	不可	可
UpdateConfiguration	<p>ブール。 「ポリシーの送信」処理を実行するように Deep Security Managerに指示します。</p>	"UpdateConfiguration:true"	不可	可

Trend Micro Deep Security(オンプレミス) 12.0

Agentを有効化する

Agentをコマンドラインから有効化するには、テナントIDとパスワードが必要です。これらの情報はインストールスクリプトで確認できます。

1. Deep Security Managerの画面右上で、[サポート情報]→[インストールスクリプト]の順にクリックします。
2. プラットフォームを選択します。
3. [インストール後にAgentを自動的に有効化]を選択します。
4. インストールスクリプトで、`tenantID`と`token`の文字列を探します。

Windows

PowerShellの場合:

```
& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -a  
<manager URL> <tenant ID> <token>
```

cmd.exeの場合:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_  
control" -a <manager URL> <tenant ID> <token>
```

Linux

```
/opt/ds_agent/dsa_control -a <manager URL> <tenant ID> <token>
```

不正プログラム対策およびルールアップデート用にプロキシを設定する

Agentをプロキシ経由でRelayに接続する必要がある場合は、プロキシ接続を設定する必要があります。

Windows

1. 管理者権限でコマンドプロンプト (cmd.exe) を開きます。
2. 次のコマンドを入力します。

```
cd C:\Program Files\Trend Micro\Deep Security Agent\  
dsa_control -w myUserName:MTPassw0rd  
dsa_control -y relay_proxy://squid.example.com:443
```

Linux

```
/opt/ds_agent/dsa_control -w myUserName:MTPassw0rd
```

```
/opt/ds_agent/dsa_control -y relay_proxy://squid.example.com:443
```

Managerへの接続用にプロキシを設定する

Agentをプロキシ経由でManagerに接続する必要がある場合は、プロキシ接続を設定する必要があります。

Windows

1. 管理者権限でコマンドプロンプト (cmd.exe) を開きます。
2. 次のコマンドを入力します。

```
cd C:\Program Files\Trend Micro\Deep Security Agent\
```

```
dsa_control -u myUserName:MTPassw0rd
```

```
dsa_control -x dsm_proxy://squid.example.com:443
```

Linux

```
/opt/ds_agent/dsa_control -u myUserName:MTPassw0rd
```

```
/opt/ds_agent/dsa_control -x dsm_proxy://squid.example.com:443
```

Agentからのハートビート有効化コマンド

Windows

PowerShellの場合:

```
& "& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -m
```

cmd.exeの場合:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -m
```

Linux

```
/opt/ds_agent/dsa_control -m
```

不正プログラムの手動検索を開始する

Windows

1. 管理者権限でコマンドプロンプト (cmd.exe) を開きます。
2. 次のコマンドを入力します。

```
cd C:\Program Files\Trend Micro\Deep Security Agent\  
dsa_control -m "AntiMalwareManualScan:true"
```

Linux

```
/opt/ds_agent/dsa_control -m "AntiMalwareManualScan:true"
```

診断パッケージを作成する

Deep Security Agentに関する問題のトラブルシューティングを行う必要がある場合に、コンピュータの診断パッケージを作成して送信するよう、サポート担当者から求められることがあります。詳細な手順については、["保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する" on page 1576](#)を参照してください。

注意: Deep Security Agentコンピュータの診断パッケージはDeep Security Managerから作成できますが、Agentコンピュータが[Agent/Applianceによって開始される通信](#)を使用するよう設定されている場合は、Managerは必要なログの一部を収集できません。そのため、テクニカルサポートから診断パッケージを要求された場合は、該当するAgentコンピュータで直接コマンドを実行する必要があります。

Agentをリセットする

このコマンドにより、ターゲットのAgentから有効化情報が削除され、無効化されます。

Windows

PowerShellの場合:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -r
```

cmd.exeの場合:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_  
control" -r
```

Linux

```
/opt/ds_agent/dsa_control -r
```

dsa_query

エージェント情報を表示するには、`dsa_query` コマンドを使用できます。

使用方法

```
dsa_query [-c <str>] [-p <str>] [-r <str>]
```

パラメータ	Description
<code>-p, --passwd <string></code>	<p>オプションのAgentセルフプロテクション機能で使用される認証パスワードです。セルフプロテクションを有効化した際にパスワードを指定した場合は必須となります。</p> <p>注意:一部のクエリコマンドでは認証を直接バイパスできます。このような場合、パスワードは必要ありません。</p>
<code>-c, --cmd <string></code>	<p>Agentに対してクエリコマンドを実行します。次のコマンドがサポートされます。</p> <ul style="list-style-type: none"> "GetHostInfo": ハートビート中にManagerに返されるIDを照会します。 "GetAgentStatus": どの保護モジュールが有効になっているかを検索します。不正プログラム対策 および 変更監視 検索のステータス、その他のその他の情報を照会します。 "GetComponentInfo": 不正プログラム対策のパターンおよびエンジンのバージョン情報を照会します。 "GetPluginVersion": Agentと保護モジュールのバージョン情報を照会します。
<code>-r, --raw <string></code>	<p>"-c"と同じクエリコマンドの情報を返しますが、サードパーティのソフトウェアで解釈できるように未加工のデータ形式で出力します。</p>
<code>pattern</code>	<p>結果をフィルタするためのワイルドカードのパターンです(オプション)。</p> <p>例:</p>

パラメータ	Description
	<code>dsa_query -c "GetComponentInfo" -r "au" "AM*"</code>

CPU使用率とRAM使用量を確認する

Windows

タスクマネージャーまたはprocmonを使用します。

Linux

`top`

ds_agentプロセスまたはサービスが実行されていることを確認する

Windows

タスクマネージャーまたはprocmonを使用します。

Linux

`ps -ef|grep ds_agent`

LinuxでAgentを再起動する

`service ds_agent restart`

または

`/etc/init.d/ds_agent restart`

or

`systemctl restart ds_agent`

一部の処理には`-tenantname`パラメータまたは`-tenantid`パラメータのいずれかが必要です。テナント名を使用すると実行エラーが発生する場合は、関連付けられたテナントIDを使用してコマンドを再度実行します。

Deep Security Manager

コマンドを使用して、Managerでいくつかの設定を行い、ユーザアカウントをロック解除できます。

注意: 一部のコマンドではDeep Security Managerが再起動することがあります。コマンドが実行されたら、Deep Security Managerが再起動したことを確認します。

使用方法

```
dsm_c -action actionname
```

ヒント: コマンドのヘルプを表示するには、`-h`オプションを使用します。 `dsm_c -h`

注意: 次の表のカッコで囲まれたパラメータは、すべて必須パラメータです。

一部の処理には`-tenantname`パラメータまたは`-tenantid`パラメータのいずれかが必要です。テナント名を使用すると実行エラーが発生する場合は、関連付けられたテナントIDを使用してコマンドを再度実行します。

処理名	Description	使用方法
<code>addcert</code>	信頼済み証明書を追加します。	<code>dsm_c -action addcert -purpose PURPOSE -cert CERT</code>
<code>addregion</code>	プライベートクラウドプロバイダのリージョンを追加します。	<code>dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT</code>
<code>changesetting</code>	設定を変更します。 警告: このコマンド	<code>dsm_c -action changesetting -name NAME [-value VALUE -valuefile FILENAME] [-computerid COMPUTERID] [-computername COMPUTERTNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME -tenantid TENANTID]</code>

処理名	Description	使用方法
	<p>の実行前に環境をバックアップしてください。この設定による影響を理解している場合を除いては、このコマンドは使用しないでください。誤った設定により、サービスが利用不可能となったり、データが読み取り不能となったりすることがあります。このコマン</p>	

処理名	Description	使用方法
	<p>ドを使用するのは通常、テクニカルサポートから依頼された場合のみです。この場合、どの設定のNAMEを変更するか指示があります。通常の処理でこのコマンドの使用が必要となることもあります。その場合、設定方法はドキュメント内の該当セクション(masterkeyなど)に</p>	

処理名	Description	使用方法
	記載されていません。	
createinsertstatements	別のデータベースへのエクスポートに使用するinsert文を作成します。	dsm_c -action createinsertstatements [-file FILEPATH] [-generateDDL] [-databaseType sqlserver oracle] [-maxresultfromdb count] [-tenantname TENANTNAME -tenantid TENANTID]
diagnostic	システム用の診断パッケージを作成します。 注意: 必要に応じて、"詳細な診断パッケージのプロセスメモリを増やす" on page 157 8ことができます。	dsm_c -action diagnostic [-verbose 0 1] [-tenantname TENANTNAME -tenantid TENANTID]
fullaccess	管理者に Full Access の役割を与えます。	dsm_c -action fullaccess -username USERNAME [-tenantname TENANTNAME -tenantid TENANTID]
listcerts	信頼済み証	dsm_c -action listcerts [-purpose PURPOSE]

処理名	Description	使用方法
	明書を一覧表示します。	
listregions	プライベートクラウドプロバイダのリージョンを一覧表示します。	<code>dsm_c -action listregions</code>
masterkey	<p>カスタムのマスターキーを生成、インポート、エクスポート、または使用して、以下を暗号化します。</p> <ul style="list-style-type: none"> データベースのパスワード Keystoreパスワード 個人データ <p>注意: カスタムのマスター</p>	<p>新規インストール時にカスタムのマスターキーを設定した場合は、セットアップがすでにインストーラにより行われています。マスターキーの生成をスキップしていて、その設定を今行う必要がある場合は、手順1のコマンドから開始して、順番にすべてのコマンドを入力してください。</p> <p>アップグレード時にマスターキーを設定した場合は、データベースとプロパティファイルをバックアップして、手順4のコマンドから開始してください。</p> <ol style="list-style-type: none"> <code>dsm_c -action masterkey -subaction [generatekmskey -arn AWSARN generatelocalkey]</code> - Key Management System (KMS) キーのAmazon Resource Name (ARN) か、<code>LOCAL_KEY_SECRET</code>ローカル環境変数を使用して、マスターキーを生成します。複数ノードのDeep Security Managerにローカル環境変数を使用する場合は、すべてのノードに対してユーザレベルではなくシステムレベルで、64文字以下で設定する必要があります。 <p>注意: マスターキーの設定時には、Deep Security Managerで権限が必要となります。また、KMSまたは<code>LOCAL_KEY_</code></p>

処理名	Description	使用方法
		<p>SECRETとのネットワーク接続が安定している必要もあります。マスターキーの暗号化と復号化を行う際にこれらが必要となります。一時的に接続が切れた場合は、Deep Security Managerでは必要なデータの復号化ができなくなり、サービスが利用不可能になります。症状としては、再起動の失敗などのエラーに関するイベントログやアラートが断続的に途切れたりします。</p> <p>注意：</p> <p>キー</p>

処理名	Description	使用方法
		<p>をプロビジョニングするには、ローカルファイルに依存しないため、KMSを使用することをお勧めします。ローカル環境変数を使用している場合、LOCAL_KEY_SECRET値は、データベースを暗号化するための実際のマスターキーを生成するためにsalt（キー生成プロセスに提供される一意の追加データ）です。鍵がなければ、データベースを盗む人はそれを復号化できません。塩がなければ、鍵自体は再計算できません。このシークレットのクライアント管理部分は、キー生成プロセスを独自の追加データでカスタマイズするためのオプションとして提供されています。しかし、塩の有無にかかわらず、実際のキーはクリアテキストでは保存されません。また、この文字列は、読み取り専用の権限を持つファイルに保存されます。</p> <p>2. <code>dsm_c -action masterkey -subaction export -file FILEPATH</code> - マスターキーをバックアップのために、パスワードで暗号化されたファイルにエクスポートします。パスワードが要求されます。</p> <p>警告: マスターキーを安全な場所にエクスポートしてバックアップします。バックアップがないと、マスターキーを紛失または破損した場合に暗号化データがすべて読み取り不能となります。その場合、Deep Security Manager、すべてのRelay、およびすべてのAgent/Appliances</p>

処理名	Description	使用方法
		<p>の再インストールが必要となります。マスターキーが盗まれた場合は、Deep Security環境のセキュリティが侵害されます。欧州の一般データ保護規則 (GDPR) などのコンプライアンス規則により、個人データの漏えいから72時間以内に監督機関に通知する義務が生じたり、コンプライアンスに準拠していない場合に罰金が科せられたりする場合があります。詳しくは、弁護士に相談してください。</p> <p>障害復旧を目的にバックアップを検証するには、マスターキーをインポートしてテストします。</p> <pre>dsm_c -action masterkey -subaction [importkmskey -file FILEPATH -arn AWSARN importlocalkey -file FILEPATH] - バックアップしたマスターキーをインポートします。このコマンドは、マスターキーが破損した場合に障害復旧を行う場合や、マスターキーを他のKMSに移行する場合に役立ちます。このコマンドの実行前に、プライマリテナント (T0) のデータベースから既存のマスターキーを削除する必要があります。</pre> <p>たとえば、以下のSQLコマンドを入力します。</p> <pre>delete from systemsettings where uniquekey = 'settings.configuration.keyEncryptingKey'</pre> <p>3. <code>dsm_c -action masterkey -subaction encryptproperties</code> - マスターキーを使用</p>

処理名	Description	使用方法
		<p>して、dsm.propertiesと configuration.propertiesのKeystoreパスワードおよびデータベースのパスワードを暗号化します。この設定を有効にするには、Deep Security Managerを再起動してください。</p> <p>4. <code>dsm_c -action masterkey -subaction encrypttenantkey -tenantid [all TENANTNUM]</code> - マルチテナント環境が構築されている場合に、マスターキーを使用して既存のテナントキーシードを暗号化します。テナントキーシードは、次の手順で使用するサブキーを生成するために必要となります。シードがすでに暗号化されていたとしても、何重にも暗号化されることはないため、複数回実行しても安全です。</p> <p>ヒント: 既存のテナントの暗号化は徐々に行い、今は新しいテナントのみを暗号化する場合は、次のコマンドを最初に入力してください。</p> <pre>dsm_c -action changesetting -name settings.configuration.encryptTenantKeyForNewTenants -value true</pre> <p>5. <code>dsm_c -action masterkey -subaction encryptpii -tenantid [all TENANTNUM]</code> - 各テナントのキーを使用して、データベースに格納されている管理者と連絡先の個人データを暗号化します。</p> <p>6. <code>dsm_c -action masterkey -subaction encryptdsmprivatekey -tenantid [all TENANTNUM]</code> - マスターキーを使用して、有効化など、SSL/TLS経由のAgent</p>

処理名	Description	使用方法
		とManagerの通信で使用される秘密鍵を暗号化します。 7. <code>dsm_c -action masterkey -subaction isconfigured</code> - マスターキーが作成されたかどうかを確認します。
<code>removecert</code>	信頼済み証明書を削除します。	<code>dsm_c -action removecert -id ID</code>
<code>removereigion</code>	プライベートクラウドプロバイダのリージョンを削除します。	<code>dsm_c -action removereigion -region REGION</code>
<code>resetcounters</code>	カウンタテーブルをリセットして空の状態に戻します。	<code>dsm_c -action resetcounters [-tenantname TENANTNAME -tenantid TENANTID]</code>
<code>script</code>	スクリプトファイル内にある <code>dsm_c</code> コマンドのバッチ処理を実行します。	<code>dsm_c -action script -scriptfile FILEPATH [-tenantname TENANTNAME -tenantid TENANTID]</code>
<code>setports</code>	Deep Security Managerの ポート を設定します。	<code>dsm_c -action setports [-managerPort port] [-heartbeatPort port]</code>
<code>trustdirectorycert</code>	ディレクトリの証明書を信頼します。	<code>dsm_c -action trustdirectorycert -directoryaddress DIRECTORYADDRESS -directoryport DIRECTORYPORT [-username USERNAME] [-password PASSWORD] [-tenantname TENANTNAME -tenantid</code>

処理名	Description	使用方法
unlockout	ユーザアカウントのロックを解除します。	<p>TENANTID]</p> <pre>dsm_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD] [-disablemfa] [-tenantname TENANTNAME -tenantid TENANTID]</pre>
upgradetasks	インサービスアップグレードの一環として必要になる場合がある、アップグレードタスク処理を実行します。	<pre>dsm_c -action upgradetasks [-listtasksets] [-listtasks -taskset UPGRADE_TASK_SET [-force]] [-tenantlist] [-tenantsummary] [-run -taskset UPGRADE_TASK_SET [-force] [-filter REGULAR_EXPRESSION]] [-showrollbackinfo -task TASKNAME] [-purgehistory [-task TASKNAME]] [-showhistory [-task TASKNAME]] [-tenantname TENANTNAME -tenantid TENANTID]</pre> <ul style="list-style-type: none"> [-listtasksets]: システム全体またはテナント (-tenantnameで指定) 用の一連のタスクを一覧表示します。 [-listtasks -taskset UPGRADE_TASK_SET [-force]]: 実行する変更内容を一覧表示します。すべてのタスクを表示するには、-forceを指定します。 [-tenantlist]: 指定したテナントの未解決アップグレード処理のバージョンを表示します。 [-tenantsummary]: 最新ではないテナントの概要を表示します。 [-run -taskset UPGRADE_TASK_SET [-force] [-filter REGX]]: 各テナントにアップグレード処理を実行します。実行済みであっても、すべてのタスクを実行する場合は、-forceを含めます。正規表現で処理を制限する場合は、-filterを含めます。

処理名	Description	使用方法
		<ul style="list-style-type: none"> [-showrollbackinfo -task TASKNAME]: 指定したタスクのロールバック情報を表示します。1つのテナントまたはすべてのテナントを表示できます。 [-purgehistory [-task TASKNAME]]: 指定したテナントやタスクの履歴を削除します。テナントやタスクを指定しないと、すべての項目が対象になります。 [-showhistory [-task TASKNAME]]: 指定したテナントやタスクの履歴を表示します。テナントやタスクを指定しないと、すべての項目が対象になります。
versionget	現在のソフトウェアバージョン、データベーススキーマバージョン、またはその両方に関する情報を表示します。	dsm_c -action versionget [-software] [-dbschema]
viewsetting	設定値を表示します。	dsm_c -action viewsetting -name NAME [-computerid COMPUTERID] [-computername COMPUTERTNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME -tenantid TENANTID]

リターンコード

dsm_cコマンドは、コマンドの実行に成功したかどうかを示す整数値を返します。返される値は以下のとおりです。

- 0: 実行に成功
- -1: ソフトウェアのインストールの破損など、原因不明の失敗

- 1: データベースに現在アクセスできないなど、実行中の失敗
- 2: 指定されている引数が無効

Deep Security APIを使用したタスクの自動化

Deep Security 11.1以降には、Deep Securityを使用したセキュリティのプロビジョニングとメンテナンスを自動化できる新しいRESTful APIが追加されています。[Deep Security Automation Center](#)にアクセスし、任意の言語でSDKをダウンロードして、APIの使用方法を次の資料で確認します。

- APIリファレンス
- 豊富なコード例が記載されたタスク中心のガイド
- サポートリソース

このAPIは継続的にアップデートされ、新しい機能や改良が加えられています。新しいAPIが自動化のニーズに合っている場合は、新しい自動化プロジェクトを開始する際に、今後も継続的なサポートとメンテナンスを長期にわたって受けられるこのAPIを使用することをお勧めします。

このAPIの使用を開始するには、Deep Security Automation Centerにあるガイド「[First Steps Toward Deep Security Automation](#)」を参照してください。

従来のREST APIおよびSOAP API

注意: Deep Security 11.1より前に提供されたREST APIおよびSOAP APIは変更されていません。これらはすでに非推奨となっているため、新しい機能は追加されませんが、既存のAPI機能は引き続き通常どおりに機能します。

Deep Securityには引き続き従来のREST APIおよびSOAP APIも含まれています。これらのAPIの使用方法については、Deep Security Automation Centerにある次のガイドを参照してください。

- [Transition from the SOAP API](#)
- [Use the Legacy REST API](#)

以降のセクションでは、SOAP APIおよびREST APIの使用に関連するタスクをDeep Security Managerで完了する方法について説明します。どのような場合にこれらのタスクを実行する必要があるかについては、上記のガイドを参照してください。

ステータス監視APIを有効にする (オプション)

従来のREST APIでステータス監視を使用するには、このAPIを有効にする必要があります。このAPIは認証を必要としないため、初期設定では無効になっています。

1. Deep Security Managerで、[管理]→[システム設定]→[詳細] の順に選択します。
2. [ステータス監視API] セクションで、[有効] を選択し、[保存] をクリックします。

Webサービスユーザアカウントを作成する

Webサービスアクセス専用の役割を作成し、新しいユーザに割り当てます。

1. Deep Security Managerで、[管理]→[ユーザ管理]→[役割] の順に選択します。
2. [新規] をクリックします。
3. [Deep Security Managerユーザインタフェースへのアクセスを許可] チェックボックスをオフにし、[WebサービスAPIへのアクセスを許可] チェックボックスをオンにします。
4. 他の設定がすべて完了したら、[保存] をクリックします。
5. [管理]→[ユーザ管理]→[ユーザ] に進み、[新規] をクリックします。
6. WebサービスAPIでのみ使用する新しいユーザを作成します。先に作成した新しい役割をこのユーザに割り当てます。

新しいユーザアカウントのユーザ名とパスワードを書き留めてください。

Deep Security予約タスクの設定

Deep Securityには、定期的に自動実行すると便利なタスクが多数あります。予約タスクは、お客様の環境にDeep Securityをインストールする時はもちろん、インストール後にシステムを最新の状態に保ち、スムーズに運用するうえでも便利です。特に、オフピーク時の定期的な検索には予約タスクが役立ちます。

ヒント: 予約タスクの作成と設定は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド [「Maintain Protection Using Scheduled Tasks」](#) を参照してください。

予約タスクを作成する

Deep Security Managerで予約タスクをセットアップするには、[管理]→[予約タスク]→[新規] をクリックします。「新規予約タスクウィザード」が表示されます。このウィザードの手順に従って予約タスクを作成できます。

セキュリティアップデートの確認: セキュリティアップデートを定期的を確認し、使用可能なアップデートがある場合、Deep Securityにインポートします。ほとんどの組織にとって、このタスクは毎日1回実行するのが理想的です。

注意: Deep Security 11.0 Update 2以降を使用している場合、[セキュリティアップデートの確認] タスクは、30日以上通信がないオフラインホストを無視します。

ソフトウェアアップデートの確認: Deep Security Agentソフトウェアアップデートを定期的を確認し、使用可能なアップデートがある場合、ダウンロードします。

コンピュータの検出: 検出操作を予約することによって、ネットワーク上の新しいコンピュータを定期的を確認します。確認するIP範囲を入力し、コンピュータの追加先となるコンピュータグループを指定するよう求められます。このタスクは、クラウドコネクタに含まれていないコンピュータを検出するのに便利です。

レポートの生成および送信: レポートを自動生成し、オプションでユーザのリストへ送信します。

コンピュータの変更を検索: Deep Security Managerで変更の検索が実行され、コンピュータの現在の状態とベースラインが比較されます。

コンピュータの不正プログラムを検索: 不正プログラム検索の予定を作成します。検索の設定は、各コンピュータのポリシーエディタまたはコンピュータエディタの [不正プログラム対策] 画面で行います。ほとんどの組織にとって、このタスクは週に1回 (または組織のポリシーに従って) 実行するのが理想的です。このタスクを設定する際に、検索のタイムアウト値を指定できます。タイムアウトオプションは、毎日、毎週、毎月、および1回のみを検索に使用できます。毎時の検索には使用できません。予約された不正プログラム検索が実行されているときにタイムアウト制限に達すると、現在実行中または保留中のタスクがキャンセルされます。

ヒント: [コンピュータの不正プログラムを検索] タスクがタイムアウトすると、次の予約検索は (前回の検索が終了したところから再開されるのではなく) 最初から開始されます。検索を完了することが目的であるため、検索が頻繁にタイムアウト値に達する場合は、設定を変更することをお勧めします。不正プログラム検索設定を変更して、例外を追加したり、タイムアウト値を延長したりできます。

コンピュータのオープンポートを検索: 1つ以上のコンピュータに対して定期的なポート検索を予約します。検索対象には、個別のコンピュータまたは特定のコンピュータグループに所属するすべてのコンピュータを指定できます。Deep Security Managerによって、ポリシーまたはコンピュータエディタの [設定] 画面の [検索] タブで定義したポート番号が検索されます。

コンピュータの推奨設定を検索: Deep Security Managerによって、コンピュータ上の一般的なアプリケーションが検索され、検出結果に基づいた推奨設定が作成されます。定期的に推奨設定の検索を実行すると、関連する最新のルールセットによってコンピュータが保護され、不要になったルールは削除されます。推奨設定の検索をサポートする3つの各保護モジュールに対して「推奨設定を自動的に適用」オプションを設定すると、必要なルールの割り当てと割り当ての解除がDeep Securityによって行われます。特別な注意が必要なルールについては、その内容を通知するアラートが発令されます。ほとんどの組織にとって、このタスクは週に1回実行するのが理想的です。

注意: 推奨設定の検索はCPU負荷が高くなることがあります。このため、推奨設定の検索を予約する場合は、タスクをグループ別に設定し(たとえば、ポリシーごとやコンピュータグループ別、ただしグループあたりのマシン台数が1,000台を超えないようにする)、タスクを各曜日に振り分ける(たとえば、データベースサーバ検索を毎週月曜日に予約し、メールサーバ検索を毎週火曜日に予約するなど)ことが推奨されます。頻繁に変更されるシステムの場合、より頻繁に推奨設定の検索を実行するように設定してください。

未解決アラートの概要の送信: すべての未解決アラートをリストしたメールを生成します。

ポリシーの送信: 更新されたポリシーを定期的に確認し、送信します。予約アップデートでは、既存の変更制御プロセスに準拠することができます。例として、マシンのアップデートをメンテナンス期間中や業務時間外などに実行するよう予約タスクを設定できます。

クラウドアカウントの同期: コンピュータのリストと追加したクラウドアカウントを同期します。クラウドアカウントをDeep Security Managerに追加した場合のみ使用可能です。

ディレクトリの同期: コンピュータのリストと追加のLDAPディレクトリを同期します。LDAPディレクトリをDeep Security Managerに追加した場合のみ使用可能です。

ユーザ/連絡先の同期: ユーザおよび連絡先のリストを、追加されたActive Directoryと同期します。Active DirectoryをDeep Security Managerに追加した場合のみ使用可能です。

VMware vCenterの同期: コンピュータのリストを、追加されたVMware vCenterと同期します。VMware vCenterをDeep Security Managerに追加した場合のみ使用可能です。

予約タスクを有効または無効にする

予約タスクを有効または無効にできます。たとえば、特定の管理作業を実行する間他のアクティビティが発生しないようにするには、予約タスクを一時的に無効にします。予約タスクの有効化または無効化は、該当タスクの [プロパティ] ウィンドウの [一般] タブで設定します。

定期レポートをセットアップする

定期レポートとは、レポートを定期的に生成して、ユーザまたは連絡先宛てに配布する予約タスクのことです。ほとんどのオプションは前述の単独レポートと同じですが、[期間] オプションだけは例外です。

ヒント: 複数のコンピュータグループから特定のコンピュータに関するレポートを生成するには、まず該当するコンピュータのみの閲覧権限があるユーザを作成し、「すべてのコンピュータ」レポートを定期的に生成する予約タスクを作成するか、作成したユーザでログオンして「すべてのコンピュータ」レポートを実行します。レポートには、そのユーザが閲覧できるコンピュータのみが記載されます。

コンピュータの追加または変更時のタスクの自動実行

注意: この記事は、Deep Securityオンプレミスソフトウェアインストールにのみ適用される仮想マシンの保護に関するリファレンスです。

イベントベースタスクを使用して、保護対象のコンピュータの特定のイベントを監視し、特定の条件に基づいてタスクを実行できます。

イベントベースタスクを作成する

Deep Security Managerで、[管理]→[イベントベースタスク]→[新規] をクリックします。表示されるウィザードの手順に従って、新しいタスクを作成します。タスクの種類によって、入力を求められる情報が異なります。

既存のイベントベースタスクを編集または停止する

既存のイベントベースタスクのプロパティを変更するには、[管理]→[イベントベースタスク] をクリックします。リストからイベントベースタスクを選択し、[プロパティ] をクリックします。

監視できるイベント

- コンピュータの作成 (システムによる): Active Directoryやクラウドプロバイダのアカウントとの同期中、またはVirtual Applianceを実行する管理対象ESXiサーバ上への仮想マシン

の作成中における、Managerへのコンピュータの追加。

- コンピュータの移動 (システムによる): 1台のESXi内のvApp間での仮想マシンの移動。またはデータセンター間、あるいはESXi間 (非管理対象ESXiサーバからVirtual Applianceを実行する管理対象ESXiサーバへの移動を含む) でのESXi上の仮想マシンの移動。
- Agentからのリモート有効化: Agentからのリモート有効化によるAgentの有効化。
- IPアドレスの変更: コンピュータが別のIPの使用を開始した場合。
- NSXセキュリティグループの変更: このイベントは下記の状況で発生します (イベントは影響を受ける各仮想マシン側に記録されます)。
 - NSX Deep Securityサービスプロファイルに間接的に関連付けられたグループに仮想マシンが追加された
 - NSX Deep Securityサービスプロファイルに関連付けられたNSXグループから仮想マシンが削除された
 - NSX Deep Securityサービスプロファイルに関連付けられたNSXポリシーがNSXグループに適用された
 - NSX Deep Securityサービスプロファイルに関連付けられたNSXポリシーがNSXグループから削除された
 - NSXポリシーがNSX Deep Securityサービスプロファイルに関連付けられた
 - NSXポリシーがNSX Deep Securityサービスプロファイルから削除された
 - NSX Deep Securityサービスプロファイルに関連付けられたNSXグループの名前が変更された
- コンピュータの電源オン (システムによる): VMware仮想マシンの電源オンイベントによってユーザが有効化をトリガできるようにします。

注意: 「コンピュータの電源オン」 イベントは、VMWareのESX環境でホストされた仮想マシンでのみ使用できます。このイベントを使用する際は、同時に多数のコンピュータの電源がオンになると処理速度が低下する可能性があることに注意してください。

条件

タスクを実行するために満たす必要のある一致条件を指定できます。条件を追加するには、「+」 ボタンを押します。複数の条件を追加した場合、タスクが実行されるためにはすべての条件が満たされる必要があります。つまり、条件は「AND」条件であり、「OR」条件ではありません。

次のフィールドでパターンを一致させるには、Javaの正規表現の構文 (<https://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html>) を使用します。

- クラウドインスタンスのイメージID: AWS クラウドインスタンスAMI ID。

注意: この一致条件は、AWSクラウドインスタンスに対してのみ使用できます。

- クラウドインスタンスのメタデータ: 照合されるメタデータは、Amazon環境のAWS「タグ」に対応します。

注意: この一致条件は、AWSクラウドインスタンスに対してのみ使用できます。コンピュータに現在関連付けられているメタデータが、エディタ画面の [概要] 画面に表示されます。条件を定義するには、2種類の情報 (メタデータタグのキーとその値) を指定する必要があります。たとえば、「AlphaFunction」という名前のメタデータキーの値が「DServer」であるコンピュータに一致させるためには、「AlphaFunction」および「DServer」を入力します (括弧は不要)。複数の候補に一致させる場合、正規表現を使用できます。この例では、「AlphaFunction」と「.*Server」、または「AlphaFunction」と「D.*」というように指定できます。

- クラウドインスタンスのセキュリティグループ名: クラウドインスタンスが適用されるセキュリティグループです。

注意: この一致条件は、AWSクラウドインスタンスに対してのみ使用できます。

- クラウドアカウント名: クラウドアカウントプロパティウィンドウの [表示名] フィールドです。
- コンピュータ名: コンピュータプロパティウィンドウの [ホスト名] フィールドです。
- ESXi名: 仮想マシンコンピュータをホストするESXiサーバの [ホスト名] フィールドです。
- フォルダ名: ローカル環境でコンピュータが配置されているフォルダ名またはディレクトリ名です。

注意: この一致条件は、コンピュータの任意の上位フォルダ (vCenterサーバと統合されている場合はルートデータセンターを含む) の名前を照合します。正規表現の先頭に「*」を追加すると、すべての上位フォルダの名前が条件に一致する必要があります。これは、正規表現の否定構文と組み合わせると特に便利です。たとえば、フォルダ名に「Linux」を含まないフォルダ内のコンピュータを検索するには、「*^((?!Linux).)*\$」という正規表現を使用できます。

- NSXセキュリティグループ名: この条件に適合するグループは、NSX Deep SecurityサービスプロファイルのNSXポリシーに関連付けられたNSXグループのみです。仮想マシンは

他のNSXグループのメンバーである可能性があります、この一致条件では関係ありません。

- プラットフォーム: コンピュータのOSです。
- vCenter名: Deep Security Managerに追加されたコンピュータのvCenterプロパティの [名前] フィールドです。

Java正規表現の例:

一致させる値	正規表現
任意の文字列 (空ではない)	.+
空の文字列 (文字なし)	^\$
Folder Alpha	Folder\ Alpha
FIN-1234	FIN-\d+ または FIN-.*
RD-ABCD	RD-\w+ または RD-.*
AB または ABC または ABCCCCCCCC	ABC*
Microsoft Windows 2003 または Windows XP	.*Windows.*
Red Hat 7 または Some_Linux123	.*Red.* . *Linux.*

次の2つの条件は、TrueまたはFalseと一致させる条件です。

- Appliance保護が利用可能: 仮想マシンがホストされているESXi上にDeep Security Virtual Applianceがあり、仮想マシンを保護できます。仮想マシンの状態が有効化済みになっているかどうかは問いません。
- Appliance保護が有効化済み: Deep Security Virtual Applianceを使用して、有効化されている仮想マシンをホストしているESXi上の仮想マシンを保護できます。

最後の条件オプションは、IPリスト内のIPとの一致を検索します。

- 最後に使用されたIPアドレス: コンピュータの現在または最後に使用された既知のIPアドレスです。

注意: 新しいコンピュータは、そのソースによって使用可能なフィールドが異なります。たとえば、Active Directoryを使用した同期の結果として追加されたコンピュータの場合、「プラットフォーム」は使用できません。

処理

上記のどのイベントが検出されたかに応じて、次の処理が実行されます。

- コンピュータの有効化: コンピュータでDeep Securityの保護が有効化されます。
 - 有効化の遅延 (分): 指定した時間 (分) の経過後に有効化されます。
- **注意:** イベントベースのタスクによって、Deep Security Virtual Applianceで保護されているESXiにvMotionで移動中の仮想マシンに保護が適用される場合、保留になっているVMware管理タスクを完了できるように、有効化を遅らせます。遅らせる時間は環境ごとに異なります。
- コンピュータの無効化: コンピュータでDeep Securityの保護が無効化されます。
- ポリシーの割り当て: 新しいコンピュータにポリシーが自動的に割り当てられます。(最初にコンピュータを有効化する必要があります)。
- Relayグループの割り当て: 新しいコンピュータに、セキュリティアップデートを受信するためのRelayグループが自動的に割り当てられます。
- コンピュータグループへの割り当て: [コンピュータ] 画面のいずれかのコンピュータグループにコンピュータが配置されます。

実行順序

イベントベースのタスクを使用する場合は、各タスクに固有の条件を作成して使用する必要があります。これは、同一の条件に遭遇した場合、Deep Securityはそれらを特定の順序で処理するため、この順序では、タスク内の条件の数を考慮しないため、これらのタスクを相互にランク付けします。

たとえば、Windows Server 2012 プラットフォーム上の `server01.example.com` コンピュータで、次のイベントベースのタスクが発生したとします。

General	Actions	Conditions
General Information		
Name:	Specific EBT	
Event:	Agent-Initiated Activation	
Task Enabled:	<input checked="" type="checkbox"/>	
Summary Information		
Actions: Assign Policy: Windows Server 2012 Conditions: "Computer Name" matches "server.*.example.com" "Platform" matches ".*Windows.*"		
Description:		
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>		

General	Actions	Conditions
General Information		
Name:	catch-All EBT	
Event:	Agent-Initiated Activation	
Task Enabled:	<input checked="" type="checkbox"/>	
Summary Information		
Actions: Assign Policy: Windows Conditions: "Platform" matches ".*Windows.*"		
Description:		
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>		

条件の多いイベントベースのタスクは自動的に実行されません。代わりに、「Platform」条件は2回照合され、イベントベースのタスクはタスクの名前とデータベースの種類に基づいて実行されます。

- PostgreSQL：「a task」、「A task」、「b task」、「B task」
- Oracle：「タスク」、「Bタスク」、「aタスク」、「bタスク」 ([ASCIIbetical](#) の順)
- Microsoft SQL Server：オペレーティングシステムのロケールによって異なります。

ただし、この順序は最初の一致では停止せず、最後に一致した時点で停止します。これは実際には、Oracleを使用している場合、上記の例では「catch-All EBT」によってポリシーが割り当てられることとなります。というのも、ASCIIbetical orderを使用すると、「catch」の「c」が「S」の後に来るからです。「特定」

予期しない結果を回避するには、イベントベースのタスク（CamelCaseなど）に固有の命名規則を使用してください。

注意: タスク名の順序は実際には、データベース内のテーブル「scheduledtasks」の列「name」に使用する照合スキームによって決まります。たとえば、Oracleでは、すべての列

に対して初期設定の照合スキームとして照合スキーム「NLS_COMP : BINARY」および「NLS_SORT : BINARY」が使用され、タスク名文字列はASCII順序でソートされます。

イベントベースタスクを一時的な無効にする

既存のイベントベースタスクが実行されないようにするには、このタスクを右クリックして、[無効] をクリックします。たとえば、特定の管理作業の実行時に他のアクティビティが発生しないようにするには、イベントベースタスクを一時的に無効にします。

イベントベースタスクを再び有効にするには、このタスクを右クリックして、[有効] をクリックします。

AWSオートスケーリングとDeep Security

AWS オートスケーリングで作成された新しいインスタンスに対して、Deep Securityで自動保護を設定できます。

オートスケーリングで作成された各インスタンスには、Deep Security Agentをインストールする必要があります。Agentのインストールには、AMIの作成に使用されたEC2インスタンスにインストール済みのAgentを組み込む方法と、AMIの起動設定にインストールスクリプトを組み込んでAgentをインストールする方法があります。それぞれのオプションにはメリットとデメリットがあります。

- インストール済みAgentを組み込むと、Agentソフトウェアをダウンロードしてインストールする必要がなくなるため、インスタンスが稼働するまでの時間を短縮できます。
- インストールスクリプトを使用してAgentをインストールする場合、スクリプトはDeep Security Managerから常に最新バージョンのAgentソフトウェアを取得します。インストール済みAgentを使用する場合は、AMIに組み込まれているバージョンが使用されます。

Agentをプレインストールする

Deep Security Agentを設定済みのEC2インスタンスがある場合は、そのインスタンスを使用してオートスケーリング用のAMIを作成できます。AMIを作成する前に、EC2インスタンスのAgentを無効にし、インスタンスを停止する必要があります。

```
dsa_control -r
```


注意: 有効化されたAgentを含むAMIは作成しないでください。各Agentは個別に有効化する必要があります。

オートスケーリングで新規に作成された各EC2インスタンスでAgentを有効にし、ポリシーがまだない場合は適用する必要があります。これには次の2つの方法があります。

- Agentを有効にしてポリシーを適用 (オプション) するインストールスクリプトを作成します。このインストールスクリプトをAWS起動設定に追加して、新しいインスタンスが作成されたときに実行されるようにします。手順については、この後の「インストールスクリプトでAgentをインストールする」を参照してください。ただし、インストールスクリプトの、Agentを取得してインストールするセクションは除外します。必要なのは、スクリプトのdsa_control -aセクションだけです。

注意: インストールスクリプトが機能するためには、Deep Security ManagerでAgentからの通信を有効にする必要があります。この設定の詳細については、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on page 408を参照してください。

- インスタンスの起動時および「コンピュータの作成 (システムによる)」イベント発生時にAgentを有効にしてポリシーを適用する (オプション) イベントベースタスクを、Deep Security Managerで設定することができます。

インストールスクリプトでAgentをインストールする

Deep Securityカスタマイズしたインストールスクリプトを生成して、EC2インスタンスの作成時に実行することができます。EC2インスタンスにインストール済みAgentが含まれていない場合は、インストールスクリプトでAgentをインストールして有効にし、ポリシーを適用し、オプションでコンピュータをコンピュータグループとRelayグループに割り当てる必要があります。

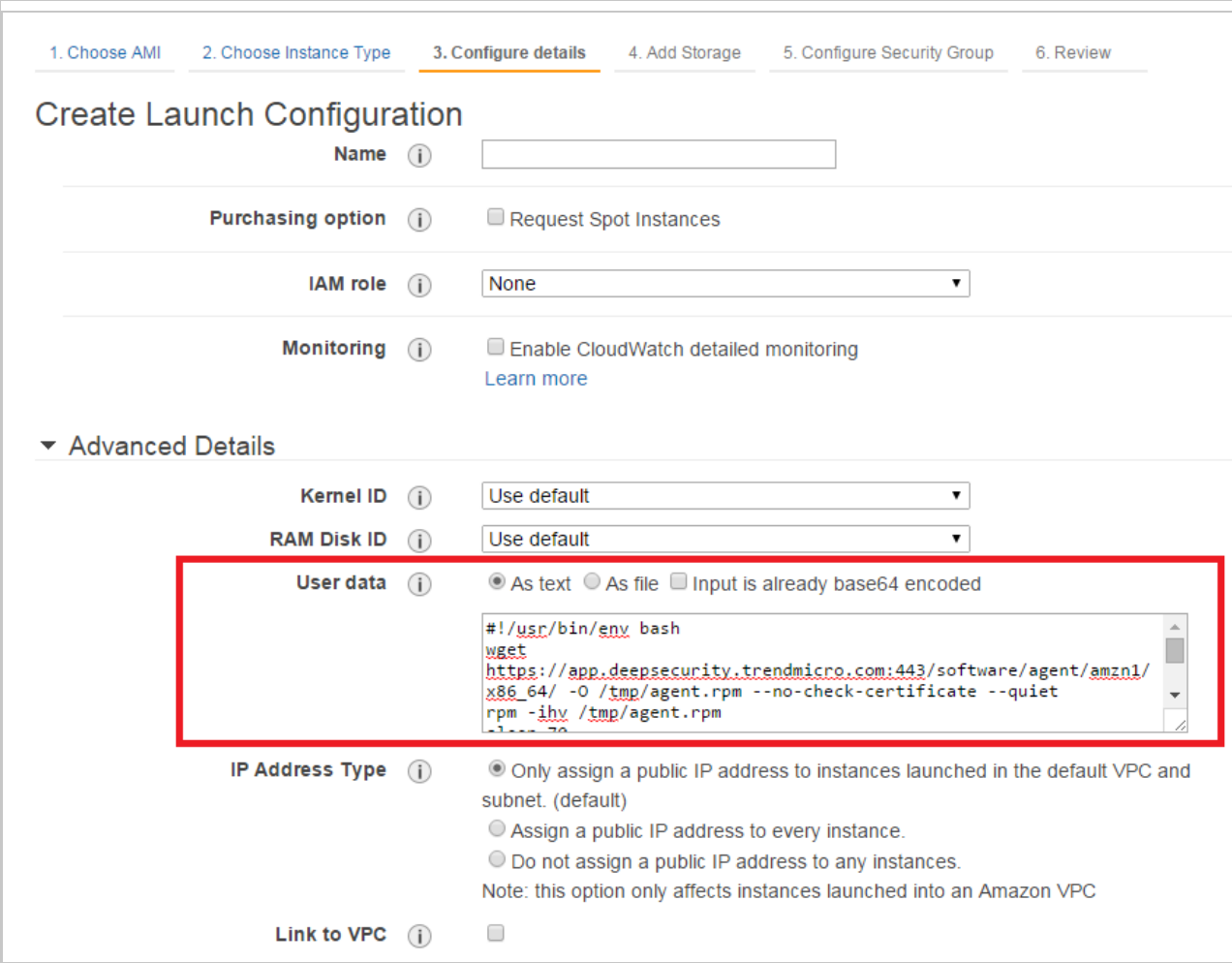
ヒント: Deep Security APIを使用して、Agentのインストールを自動化するためのインストールスクリプトを生成できます。詳細については、"[Generate an agent deployment script](#)"を参照してください。

インストールスクリプトが機能するためには、以下の要件を満たす必要があります。

- 停止したコンピュータからAMIを作成する必要があります。
- Deep Security ManagerでAgentからの通信を有効にする必要があります。この設定についての詳細は、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on page 408を参照してください。

インストールスクリプトを使用してインスタンスの自動保護を設定するには

1. Deep Security Managerにログオンします。
2. 右上の [サポート情報] メニューで、[インストールスクリプト] を選択します。
3. プラットフォームを選択します。
4. [インストール後にAgentを自動的に有効化] を選択します。
5. 適切な [セキュリティポリシー]、[コンピュータグループ]、および [Relayグループ] を選択します。
6. [クリップボードにコピー] をクリックします。
7. AWS起動設定に移動し、[Advanced Details] を展開して [User Data] にインストールスクリプトを貼り付けます。



1. Choose AMI 2. Choose Instance Type 3. Configure details 4. Add Storage 5. Configure Security Group 6. Review

Create Launch Configuration

Name

Purchasing option Request Spot Instances

IAM role

Monitoring Enable CloudWatch detailed monitoring [Learn more](#)

▼ Advanced Details

Kernel ID

RAM Disk ID

User data As text As file Input is already base64 encoded

```
#!/usr/bin/env bash
wget
https://app.deepsecurity.trendmicro.com:443/software/agent/amzn1/
x86_64/ -O /tmp/agent.rpm --no-check-certificate --quiet
rpm -ihv /tmp/agent.rpm
```

IP Address Type Only assign a public IP address to instances launched in the default VPC and subnet. (default)
 Assign a public IP address to every instance.
 Do not assign a public IP address to any instances.
Note: this option only affects instances launched into an Amazon VPC

Link to VPC

注意: Microsoft WindowsベースのAMIでPowerShellインストールスクリプトを実行する際に問題が発生した場合は、実行中のインスタンスからAMIを作成したことが原因である可能性があります。AWSでは実行中のインスタンスからAMIを作成できますが、そのAMIから作成されるインスタンスで起動時に実行されるEc2Configタスクがすべて無効になります。その結果、インスタンスはPowerShellスクリプトを実行できなくなります。

注意: WindowsにAMIを作成する場合は、ユーザデータ処理を手動で、またはイメージ作成プロセスの一環として、再有効化する必要があります。ユーザデータ処理は、明示的に指定されていないかぎり、WindowsベースのAMIの最初の起動時にのみ実行される (最初の起動プロセスの実行中に無効になる) ため、カスタムAMIから作成されたインスタンスでは、この機能を再び有効にしないとユーザデータが実行されません。この機能をリセットする方法または最初の起動で無効にならないようにする方法については、[「EC2Configサービスを使用したWindowsインスタンスの設定」](#)で詳しく説明されています。EC2Configバージョン2.1.10以降を使用している場合は、`<persist>>true</persist>` をユーザデータに組み込むのが最も簡単な方法です。

オートスケーリングの結果としてDeep Securityからインスタンスを削除する

Deep Security ManagerでAWSアカウントを追加すると、オートスケーリング後にAWSに存在しなくなったインスタンスはDeep Security Managerから自動的に削除されます。

AWSアカウントの追加に関する詳細については、["AWSクラウドアカウントの追加" on page 516](#)を参照してください。

Azure Virtual Machine Scale SetsとDeep Security

Azure Virtual Machine Scale Sets (VMSS) を使用すると、一連の同一の仮想マシンを配置して管理できます。仮想マシンの数は、設定可能なスケーリングルールに基づいて自動的に増加または減少します。詳細については、[「Azure Virtual Machine Scale Sets とは」](#)を参照してください。

Deep Security Agentが事前にインストールされ、有効化された基本的な仮想マシンイメージを含めるようにVMSSを設定できます。VMSSがスケールアップすると、スケールセットの新しい仮想マシンインスタンスにAgentが自動的に含まれます。

AgentをVMSSに追加するには:

- ["手順1: \(推奨\) AzureアカウントをDeep Security Managerに追加する" below](#)
- ["手順2: インストールスクリプトを準備する" below](#)
- ["手順3: カスタムスクリプト拡張機能を介してAgentをVMSSインスタンスに追加する" on the next page](#)

手順1: (推奨) AzureアカウントをDeep Security Managerに追加する

AzureアカウントをDeep Security Managerに追加すると、このアカウントで作成したすべてのAzureインスタンスがDeep Security Managerに読み込まれ、[コンピュータ]に表示されます。インスタンスは、Agentがインストールされているかどうかに関係なく表示されます。Agentを含まないインスタンスの[ステータス]は[Agent/Applianceなし]です。インスタンスにAgentをインストールして有効化したら、[ステータス]は[管理対象 (オンライン)]に変更されます。

Azureアカウントの追加後にスケールセットが手動または自動でスケールアップすると、Deep Securityは新しいAzureインスタンスを検出し、[コンピュータ]のリストに追加します。同様に、スケールセットがスケールダウンすると、インスタンスがビューから削除されます。そのため、Deep Security Managerは、スケールセット内で利用可能なAzureインスタンスの現在のリストを常に表示します。

ただし、AzureアカウントをDeep Security Managerに追加しないで、他の方法で使用して個々のAzureインスタンスを追加する場合は、Deep Securityは発生する可能性のあるスケールダウンを検出せず、存在しないAzureインスタンスをリストから削除しません。Deep Security ManagerでAzure仮想マシンのリストが拡大しないようにして、ある時点のスケールセットで利用可能なAzureインスタンスを常に正確に表示するには、AzureアカウントをDeep Security Managerに追加することを強くお勧めします。

Azureアカウントの追加手順については、["Deep SecurityへのMicrosoft Azureアカウントの追加" on page 539](#)を参照してください。

手順2: インストールスクリプトを準備する

Deep Security Managerで、インストールスクリプトをDeep Security Managerから準備します。手順については、["インストールスクリプトを使用したコンピュータの追加と保護" on page 498](#)を参照してください。このインストールスクリプトは、次に設定するカスタムスクリプト拡張機能で参照されます。

注意: 次のVMSSスクリプトを使用してカスタムスクリプトを実行するには、Azure Blobストレージに、または有効なURLを介してアクセス可能な場所にスクリプトを保存する必要があります。

ります。Azure Blobストレージへファイルをアップロードする手順については、[「Azure PowerShellでAzure Blobストレージ操作を実行する」](#)を参照してください。

手順3: カスタムスクリプト拡張機能を介してAgentをVMSSインスタンスに追加する

次に、PowerShellを使用してAgentを追加する方法に関する例を示します。

- [例1](#)では、Agentを含む新しいVMSSを作成する方法を示します。
- [例2](#)では、既存のVMSSにAgentを追加する方法を示します。

両方の例:

- [Add-AzureRmVmssExtension cmdlet](#)を使用して拡張機能をVMSSに追加します。
- Azure PowerShell 5.1.1を使用します。

注意: PowerShell cmdletを使用して新しいVMSSを作成する手順については、[このMicrosoft チュートリアル](#)を参照してください。Linuxプラットフォームについては、<https://github.com/Azure/custom-script-extension-linux>を参照してください。

例1: Agentを含む新しいVMSSを作成する

```
$resourceGroupName = <VMSSのリソースグループ>
$vmssname = <VMSSの名前>

# Create ResourceGroup
New-AzureRmResourceGroup -ResourceGroupName $resourceGroupName -Location EastUS

# Create a config object
$vmssConfig = New-AzureRmVmssConfig `
  -Location EastUS `
  -SkuCapacity 2 `
  -SkuName Standard_DS2 `
```

```
-UpgradePolicyMode Automatic
```

```
# Define the script for your Custom Script Extension to run on the Windows Platform
```

```
$customConfig = @{
```

```
    "fileUri" = (,"deploymentscript.ps1などのインストールスクリプトのコピーのURL");
```

```
    "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File  
deploymentscript.ps1"
```

```
}
```

```
# Define the script for your Custom Script Extension to run on the Linux Platform
```

```
#$customConfig = @{
```

```
# "fileUri" = (,"deploymentscript.shなどのインストールスクリプトのコピーのURL");
```

```
# "commandToExecute" = "bash deploymentscript.sh"
```

```
#}
```

```
# The section is required only if deploymentscript has been located within  
Azure StorageAccount
```

```
$storageAccountName = <deploymentscriptがAzure Storage内に配置されている場合の  
StorageAccountName>
```

```
$key = (Get-AzureRmStorageAccountKey -Name $storageAccountName -  
ResourceGroupName $resourceGroupName).Value[0]
```

```
$protectedConfig = @{
```

```
    "storageAccountName" = $storageAccountName;
```

```
    "storageAccountKey" = $key
```

```
}
```

```
# Use Custom Script Extension to install Deep Security Agent (Windows)
```

Trend Micro Deep Security(オンプレミス) 12.0

```
Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
  -Name "customScript" `
  -Publisher "Microsoft.Compute" `
  -Type "CustomScriptExtension" `
  -TypeHandlerVersion 1.8 `
  -Setting $customConfig `
  -ProtectedSetting $protectedConfig

# Use Custom Script Extension to install Deep Security Agent (Linux)
#Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
# -Name "customScript" `
# -Publisher "Microsoft.Azure.Extensions" `
# -Type "customScript" `
# -TypeHandlerVersion 2.0 `
# -Setting $customConfig `
# -ProtectedSetting $protectedConfig

# Create a public IP address
# Create a frontend and backend IP pool
# Create the load balancer
# Create a load balancer health probe on port 80
# Create a load balancer rule to distribute traffic on port 80
# Update the load balancer configuration
# Reference a virtual machine image from the gallery
# Set up information for authenticating with the virtual machine
# Create the virtual network resources
# Attach the virtual network to the config object
```

```
# Create the scale set with the config object (this step might take a few minutes)
```

```
New-AzureRmVmss `
  -ResourceGroupName $resourceGroupName `
  -Name $vmssname `
  -VirtualMachineScaleSet $vmssConfig
```

例2: 既存のVMSSにAgentを追加する

```
$resourceGroupName = <VMSSのリソースグループ>
```

```
$vmssname = <VMSSの名前>
```

```
# Get the VMSS model
```

```
$vmssobj = Get-AzureRmVmss -ResourceGroupName $resourceGroupName -
VMScaleSetName $vmssname
```

```
# Show model data if you prefer
```

```
# Write-Output $vmssobj
```

```
# Define the script for your Custom Script Extension to run on the Windows platform
```

```
$customConfig = @{
  "fileUri" = (,"deploymentscript.ps1などのインストールスクリプトのコピーのURL");
  "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File
deploymentscript.ps1"
}
```

```
# Define the script for your Custom Script Extension to run on the Linux platform
```

```
#$customConfig = @{
#  "fileUri" = (,"deploymentscript.shなどのインストールスクリプトのコピーのURL");
```


Trend Micro Deep Security(オンプレミス) 12.0

```
# "commandToExecute" = "bash deploymentscript.sh"
#}

# The section is required only if deploymentscript has been located within
Azure StorageAccount

$storageAccountName = <deploymentscriptがAzure Storage内に配置されている場合の
StorageAccountName>

$key = (Get-AzureRmStorageAccountKey -Name $storageAccountName -
ResourceGroupName $resourceGroupName).Value[0]

$protectedConfig = @{
    "storageAccountName" = $storageAccountName;
    "storageAccountKey" = $key
}

# Use Custom Script Extension to install Deep Security Agent (Windows)
$newvmssobj = Add-AzureRmVmssExtension `
    -VirtualMachineScaleSet $vmssobj `
    -Name "customScript" `
    -Publisher "Microsoft.Compute" `
    -Type "CustomScriptExtension" `
    -TypeHandlerVersion 1.8 `
    -Setting $customConfig `
    -ProtectedSetting $protectedConfig

# Use Custom Script Extension to install Deep Security Agent (Linux)
#$newvmssobj = Add-AzureRmVmssExtension `
#     -VirtualMachineScaleSet $vmssobj `
#     -Name "customScript" `
```

```
# -Publisher "Microsoft.Azure.Extensions" `
# -Type "customScript" `
# -TypeHandlerVersion 2.0 `
# -Setting $customConfig `
# -ProtectedSetting $protectedConfig

# Update the virtual machine scale set model
Update-AzureRmVmss -ResourceGroupName $resourceGroupName -name $vmssname -
VirtualMachineScaleSet $newvmssobj -Verbose

# Get Instance ID for all instances in this VMSS, and decide which
instance you'd like to update

# Get-AzureRmVmssVM -ResourceGroupName $resourceGroupName -VMScaleSetName
$vmssname

# Now start updating instances

# If upgradePolicy is Automatic in the VMSS, do NOT execute the next
command Update-AzureRmVmssInstance. Azure will auto-update the VMSS.

# There's no PowerShell command to update all instances at once. But you
could refer to the output of Update-AzureRmVmss, and loop all instances
into this command.

Update-AzureRmVmssInstance -ResourceGroupName $resourceGroupName -
VMScaleSetName $vmssname -InstanceId 0
```

インストールスクリプトを使用したコンピュータの追加と保護

Deep Securityで保護対象リソースのリストにコンピュータを追加し、保護を実装するには、複数の手順を実行する必要があります。ほとんどの手順は、コンピュータのコマンドラインから実行できるので、スクリプト化が可能です。Deep Security Managerには、インストールスクリプトの作成を支援する機能が用意されており、[サポート]メニューからアクセスできます。

Agentからのリモート有効化を有効にする

インストールスクリプトのインストール後にDeep Security Agentを自動的に有効にする場合は、Agentからのリモート有効化を許可するようにDeep Security Managerを設定する必要があります。"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 408の[「Agentからのリモート有効化を有効にする」](#)セクションを参照してください。

インストールスクリプトを生成する

1. Deep Security Managerコンソールの右上隅で、[サポート]→[インストールスクリプト]をクリックします。
2. ソフトウェアをインストールするプラットフォームを選択します。

リスト内のプラットフォームは、Deep Security ManagerにインポートされたAgentソフトウェアに対応します。Deep Securityソフトウェアのインポートの詳細については、"[Deep Security Agentソフトウェアの入手](#)" on page 372を参照してください。

3. [インストール後にAgentを自動的に有効化]を選択します。

Agentはコンピュータを保護するポリシーの適用前に有効にする必要があります。有効化により、最初の通信時にManagerにAgentが登録されます。

4. 必要に応じて、[セキュリティポリシー]、[コンピュータグループ]、[Relayグループ]、[Deep Security Managerへの接続に使用するプロキシ]、[Relayへの接続に使用するプロキシ]を選択します。
5. 必要に応じて(ただし、強く推奨します)、[Deep Security ManagerのTLS証明書を確認する]を選択します。

このオプションを選択すると、AgentソフトウェアをダウンロードするときにDeep Security Managerが信頼できる認証局 (CA) の有効なTLS証明書を使用するため、「中間者」攻撃を回避できます。Deep Security Managerコンソールのブラウザバーで、Deep Security Managerが有効なCA証明書を使用しているかどうかをチェックできます。初期設定では、Deep Security Managerは自己署名証明書を使用するため、[Deep Security Manager TLS証明書の検証] オプションと互換性がありません。Deep Security Managerがロードバランサの背後に配置されていない場合に、初期設定の自己署名証明書と信頼できる認証局の証明書を置き換えるときの手順については、"[Deep Security Manager TLS証明書の置き換え](#)" on page 1057を参照してください。Managerがロードバランサの背後に配置されている場合は、ロードバランサの証明書を置き換える必要があります。

6. オプションで を強くお勧めします。 を選択してください。 エージェントインストーラファイルのデジタル署名チェックを開始するには、エージェントインストーラの署名の妥当性検査を実行します。チェックに成功すると、エージェントのインストールが続行されます。チェックに失敗した場合、エージェントのインストールは中止されます。このオプションを有効にする前に、次の点を理解してください。
- このオプションはLinuxおよびWindowsインストーラ（RPM、DEB、またはMSIファイルの）のみでサポートされます。
 - （Linuxのみ）このオプションでは、公開スクリプトを実行するクライアントコンピュータごとにパブリック署名キーをインポートする必要があります。詳細は、["RPMファイルの署名の確認" on page 219](#) および ["DEBファイルの署名の確認" on page 221](#)の署名を確認します。
7. インストールスクリプトジェネレータにスクリプトが表示されます。[クリップボードにコピー] をクリックして、使用する配信ツールにインストールスクリプトを貼り付けるか、[ファイルに保存] をクリックします。

インストールスクリプト

Deep Security Agentは、RightScale、Chef、Puppet、SSHなどのツールを使用して配信できます。このインストールスクリプトジェネレータを使用して、必要なスクリプトを生成できます。

WindowsとLinux以外のプラットフォームについては、インストールガイドを参照してください。

プラットフォーム:

備考 インストールスクリプトは、Deep Security ManagerからAgentソフトウェアをダウンロードする手順が含まれています。インストールスクリプトを実行する前に、Deep Security ManagerにAgentソフトウェアをインポートしておく必要があります。スクリプトは管理者権限で実行する必要があります。[追加ソフトウェアのインポート...](#)

インストール後にAgentを自動的に有効化（セキュリティポリシーを割り当てる場合は必ず有効化してください）

Deep Security ManagerのTLS証明書を確認する。[詳細を表示](#)

```
#/bin/bash
# This script detects platform and architecture, then downloads and installs the matching Deep Security Agent package
if [[ $(/usr/bin/id -u) -ne 0 ]]; then echo You are not running as the root user. Please try again with root privileges;
  logger -t You are not running as the root user. Please try again with root privileges;
  exit 1;
fi
if type curl >/dev/null 2>&1; then
  SOURCEURL='https://ec2-54-149-40-176.us-west-2.compute.amazonaws.com:4119'
  curl $SOURCEURL/software/deploymentscript/platform/linux/ -o /tmp/DownloadInstallAgentPackage --insecure --silent --tlsv 1.2

  if [ -s /tmp/DownloadInstallAgentPackage ]; then
    ./tmp/DownloadInstallAgentPackage
```

注意: Deep Security ManagerによってWindows Agent環境用に生成されるインストールスクリプトには、Windows PowerShell 4.0以降が必要です。Powershellは管理者として実行

する必要があり、スクリプトを実行するために次のコマンドを実行しなければならない場合があります。Set-ExecutionPolicy RemoteSigned

注意: PowerShell 4.0またはcurl 7.34.0を最低限必要とする以前のバージョンのWindowsまたはLinuxにエージェントを配信する場合は、初期のTLSがマネージャおよびリレーで許可されていることを確認してください。詳細については、"[TLS 1.2が強制されているかどうかを確認する](#)" on page 1489および"[初期のTLS \(1.0\) を有効にする](#)" on page 1487を参照してください。また、次のように配置スクリプトを編集します。

- Linux: `--tls1.2` タグを削除します。
- Windows: `#requires -version 4.0` 行を削除します。また、初期のTLS (バージョン1.0) がManagerとの通信に使用されるように、
`[Net.ServicePointManager]::SecurityProtocol =`
`[Net.SecurityProtocolType]::Tls12;` 行も削除します。

Amazon Web Servicesを使用していて、新しいAmazon EC2、Amazon WorkSpacesまたはVPCのインスタンスを作成する場合は、生成したスクリプトをコピーして [User Data] フィールドに貼り付けます。このスクリプトによって既存のAmazon Machine Image (AMI) が起動され、Agentが自動的にインストールされて有効化されます。新しいインスタンスは、生成したインストールスクリプトで指定されているURLにアクセスする必要があります。つまり、Deep Security Managerがインターネットに接続されているか、Amazon Web ServicesにVPN接続または直接接続されているか、またはDeep Security ManagerがAmazon Web Servicesにもインストールされている必要があります。

Linux環境用の [User Data] フィールドにインストールスクリプトをコピーする場合、インストールスクリプトをそのまま [User Data] フィールドにコピーすると、CloudInitによってsudoでスクリプトが実行されます(エラーが発生した場合、`/var/log/cloud-init.log`に記録されます)。

注意: [User Data] フィールドは、CloudFormationなどの他のサービスでも使用します。詳細については次を参照してください。

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html>

トラブルシューティングおよびヒント

- インストールスクリプトを実行しようとして、終了コード2「AgentパッケージダウンロードでTLS証明書の検証に失敗しました。Deep Security Manager TLS証明書が信頼さ

れたルート証明機関によって署名されていることを確認してください。詳細については、Deep Securityヘルプセンターで「インストールスクリプト」を検索してください。」が表示された場合、インストールスクリプトは、[Deep Security Manager TLS証明書の検証] チェックボックスを使用して作成されています。このエラーは、Deep Security ManagerがDeep Security ManagerとそのAgentの間の接続に公的に信頼されていない証明書(初期設定の自己署名証明書など)を使用している場合、または証明書と信頼済みCAの間の信頼チェーンの証明書が見つからないなど、サードパーティの証明書に問題がある場合に表示されます。証明書の詳細については、"[Deep Security Manager TLS証明書の置き換え](#)" on page 1057を参照してください。信頼済み証明書を置き換える代わりに、インストールスクリプトの生成時に [Deep Security Manager TLS証明書の検証] チェックボックスをオフにできます。セキュリティ上の理由から、この方法はお勧めしません。

- PowerShell (x86) を使用してAgentをインストールする場合、次のエラーメッセージが表示されます。C:\Program Files (x86)\Trend Micro\Deep Security Agent\dsa_control' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

PowerShellスクリプトではProgramFilesの環境変数が「Program Files (x86)」ではなく、「Program Files」に設定されている必要があります。この問題を解決するには、PowerShell (x86) を終了して、スクリプトをPowerShellで管理者として実行します。

- Windowsコンピュータでは、ローカルOSと同じプロキシ設定を使用してインストールスクリプトが実行されます。ローカルOSがプロキシを使用するように設定されていて、直接接続でしかDeep Security Managerにアクセスできない場合、インストールスクリプトは失敗します。
- 展開スクリプトはrpm -Uにrpm -ihvを変更することで、エージェントの更新の代わりに、新規インストールを実行するように変更することができます。

AWSインスタスタグに基づくポリシーの自動割り当て

使用しているリソースの分類をAWSタグで許可するには、キーと値の形式で[AWS EC2インスタンスにメタデータを割り当てる](#)ことにより、リソースを分類できます。同様にキーと値のペアで[Amazon WorkSpacesのタグ付け](#)もできます。Deep Securityではこのメタデータを使用して、Deep SecurityAgentが有効化されたときにそのAgentに対するポリシーの自動割り当てがトリガされます。そのためには、Deep Securityでイベントベースタスクを作成し、イベント、ポリシー、およびメタデータを定義します。イベントベースタスクは、特定のイベントについて保護対象リソースを監視し、所定の条件に応じてタスクを実行するために使用します。この

ケースでは、Agentからのリモート有効化がイベントで、特定のAWSインスタスタグが条件です。

ここでは、次の例を使用して手順を説明します。

- ポリシー:AIA_Policy
- AWSタグキー: Group
- AWSタグ値: development

注意: 以下の例は、ポリシーAIA_Policyがすでに作成されていることを前提とします。

1. Deep SecurityManagerコンソールで [管理]→[イベントベースタスク] に進み、[新規] をクリックします。
2. [イベント] リストから [Agentからのリモート有効化] を選択し、[次へ] をクリックします。
3. [ポリシーの割り当て] チェックボックスを選択し、リストからAIA_Policyを選択し、[次へ] をクリックします。
4. リストから [クラウドインスタンスのメタデータ] を選択し、キーフィールドに「Group」、値フィールドに「development」と入力し、[次へ] をクリックします。

一致条件をすべて指定してください (すべての条件が満たされた場合にのみ操作が実行されます)。

クラウドインスタンスのメタデータ = Group development +

< 戻る 次へ > キャンセル

5. イベントベースタスクに名前を指定し、[完了] をクリックして保存します。

以上で、キー「Group」と値「development」でタグ付けされたインスタンスでAgentが有効化された時にそのインスタンスにAIA_Policyを適用するイベントベースタスクが作成されました。

保護

Trend Micro Deep Securityでは、緊密に統合された次の各モジュールを使用して、セキュリティ機能を簡単に拡張できます。

- ["侵入防御" below](#)
- ["不正プログラム対策" on the next page](#)
- ["ファイアウォール" on the next page](#)
- ["Webレピュテーション" on the next page](#)
- ["変更監視" on the next page](#)
- ["セキュリティログ監視" on page 506](#)
- ["アプリケーションコントロール" on page 506](#)

侵入防御

侵入防御モジュールは、受信/送信トラフィックを検査することで不審なアクティビティを検出してブロックし、既知またはゼロデイの脆弱性に対する攻撃を防ぎます。Deep Securityでは「仮想パッチ」をサポートしており、パッチが適用されるまでの間、侵入防御ルールを使用して既知の脆弱性に対する攻撃にさらされないようにすることができます。これは、さまざまな規制に準拠する際に重要な役割を果たします。新しいルールを自動で受信するようにDeep Securityを設定すれば、新たな脆弱性が検出された場合も、いち早く対応するルールを受け取ることができます。

侵入防御モジュールは、コード修正が完了するまでの間、SQLインジェクション攻撃、クロスサイトスクリプティング攻撃、およびその他のWebアプリケーションの脆弱性からWebアプリケーションとデータを保護します。

詳細については、["侵入防御の設定" on page 793](#)を参照してください。

不正プログラム対策

不正プログラム対策モジュールは、WindowsおよびLinuxのワークロードを不正プログラム、スパイウェア、トロイの木馬などの不正なソフトウェアから保護します。Trend Micro™ Smart Protection Network™により強化された不正プログラム対策モジュールを使用すると、不正プログラムを特定および削除し、コマンドおよび制御サーバとして知られているドメインをただちにブロックできます。

詳細については、"[不正プログラム対策の有効化と設定](#)" on page 730を参照してください。

ファイアウォール

ファイアウォールモジュールは受信/送信トラフィックを制御し、監査用にファイアウォールログを生成します。

詳細については、"[Deep Securityファイアウォールの設定](#)" on page 836を参照してください。

Webレピュテーション

最近の攻撃の多くは、不正プログラムを配信するURLにアクセスすることから始まります。Webレピュテーションモジュールは、犯罪者が使用する不正ドメインや既知のC&Cサーバへのアクセスをブロックするコンテンツフィルタを提供します。WebレピュテーションモジュールはTrend Micro Smart Protection Networkと連携しているため、新たな脅威を迅速かつ正確に特定することが可能です。

詳細については、"[Webレピュテーションによる不正なURLへのアクセスのブロック](#)" on page 933を参照してください。

変更監視

変更監視モジュールでは、インスタンスに対する許可された変更と許可されない変更の両方を追跡し、意図しない不正な変更があった場合にアラートを受け取ることができます。許可されない変更を検出する機能は、クラウドセキュリティ戦略における非常に重要な要素です。この機能によって、インスタンスの感染につながる可能性のある変更に対する可視性が提供されるためです。

詳細については、"[変更監視の設定](#)" on page 887を参照してください。

セキュリティログ監視

セキュリティログ監視モジュールは、システムログをキャプチャして分析し、PCI DSSの要件や組織独自の内部要件に対する監査証拠を提供します。多数のログエントリの中から重要なセキュリティイベントを識別するのに役立ちます。セキュリティログ監視で見つかった不審なイベントをSIEMシステムまたは中央ログサーバに転送するように設定して、関連付け、レポート、およびアーカイブに使用することができます。

詳細については、"[セキュリティログ監視の設定](#)" on page 903を参照してください。

アプリケーションコントロール

アプリケーションコントロールモジュールは、コンピュータの元のソフトウェアと比較し、未承認ソフトウェアや新規ソフトウェアなどの変更点を監視します。アプリケーションコントロールが有効になると、すべてのソフトウェアの変更が記録され、新しいソフトウェアまたは変更されたソフトウェアがファイルシステム上で検出されるとイベントが作成されます。Deep Security Agentで変更が検出されると、ソフトウェアを許可またはブロックしたり、必要に応じてコンピュータをロックダウンできます。

詳細については、"[アプリケーションコントロールの有効化の確認](#)" on page 703を参照してください。

保護対象コンピュータの管理

次のタスクを実行し、Deep Securityを使用してコンピュータを保護および監視します。

- "[Deep Security Managerにコンピュータおよびその他のリソースの追加](#)" below
- "[コンピュータおよびAgentのステータス](#)" on page 556
- "[プロキシの背後に配置されたAgentの接続](#)" on page 410

Deep Security Managerにコンピュータおよびその他のリソースの追加

Deep Security Managerの [コンピュータ] 画面を使用すると、Deep Securityによる保護対象のコンピュータの管理と監視ができます。

この画面は定期的に自動更新され、最新情報が表示されます(更新頻度はユーザごとに変更できます。[管理]→[ユーザ管理]→[ユーザ]の順に選択し、ユーザアカウントをダブルクリックして[プロパティ]画面を表示します。[設定] タブの [更新頻度] セクションで更新頻度を変更します)。

Managerにコンピュータを追加する

注意: Agentは、コンピュータにインストール後にDeep Security Managerで有効化する必要があります。有効化時に、Deep Security ManagerによってフィンガープリントがAgentに送信されると、Agentはその一意のフィンガープリントのManagerからのみ指示を受け付けます。

注意: 以前にDeep Security Virtual ApplianceによってAgentレスで保護されていた仮想マシンにAgentをインストールする場合は、Managerから仮想マシンを再有効化してコンピュータ上のAgentを登録する必要があります。

コンピュータは次のいずれかの方法で追加できます。

- ["ローカルネットワークコンピュータの追加" on page 509](#)
ローカルにアクセス可能なネットワーク上のコンピュータを保護する場合は、コンピュータのIPアドレスまたはホスト名を指定するか、Deep Security Managerから参照可能なすべてのコンピュータを検索する検出操作を実行して、コンピュータを個別に追加できます。
- ["Microsoft Active Directoryからのコンピュータグループの追加" on page 549](#)
Microsoft Active Directoryまたはその他のLDAPベースのディレクトリサービスからコンピュータグループをインポートできます。
- ["VMware vCenterの追加" on page 512](#)
Deep Security Managerは、VMware vCenterおよびESXiサーバとの緊密な統合をサポートします。vCenterノードとESXiノードから構成や運用に関する情報を同期し、企業のVMwareインフラストラクチャにセキュリティを詳細に適用できます。
- ["VMware vCloudでホストされる仮想マシンの追加" on page 545](#)
- ["AWSクラウドアカウントの追加" on page 516](#)
- ["Deep SecurityへのMicrosoft Azureアカウントの追加" on page 539](#)
- ["AgentのAMIまたはWorkSpaceバンドルへの統合" on page 393](#)
事前に有効化したDeep Security AgentをAmazon Machine Image (AMI) のベースであるインスタンスにインストールできます。

- ["インストールスクリプトを使用したコンピュータの追加と保護" on page 498](#)
多数のコンピュータを追加または保護する場合は、Agentのインストールおよび有効化のプロセスを自動化できます。Deep Security Managerのインストールスクリプトジェネレータを使用すると、Agentのインストールと、Agentの有効化やポリシーの割り当てなどの後続タスクをオプションで実行するスクリプトを生成できます。このスクリプトは、さまざまな追加コマンドを実行するカスタマイズスクリプトを作成する際のテンプレートとして使用することもできます。

コンピュータのグループ化

組織でコンピュータグループを作成すると、ポリシーの適用と管理のプロセスを迅速化できるため、便利です。グループは、[コンピュータ]画面の左側のツリー構造に表示されます。新しいグループを作成するには、新しいコンピュータグループを作成するコンピュータグループを選択して、[追加]→[グループの作成]の順にクリックします。

グループにコンピュータを移動するには、コンピュータを選択して、[処理]→[グループへの移動]の順にクリックします。ポリシーは、コンピュータグループレベルではなく、コンピュータレベルで適用されることに注意してください。コンピュータグループ間でコンピュータを移動しても、そのコンピュータに割り当てられているポリシーへの影響はありません。

グループを削除するには、グループを右クリックして、[グループの削除]をクリックします。コンピュータが含まれていないコンピュータグループおよびサブグループのないコンピュータグループのみ削除できます。

["スマートフォルダによるコンピュータの動的なグループ化" on page 1427](#)もできます。

コンピュータリストをエクスポートする

[コンピュータ]画面で[エクスポート]をクリックして、コンピュータリストをXMLまたはCSVファイルにエクスポートできます。コンピュータの情報をバックアップしたり、情報を他のレポートシステムと統合したり、コンピュータを別のDeep Security Managerに移行したりする場合にエクスポートを使用します(エクスポートすると、新しいManagerでコンピュータの再検出や検索が必要ありません)。

注意: エクスポートされるコンピュータファイルには、割り当てられたポリシー、ファイアウォールルール、ファイアウォールステートフル設定、または侵入防御ルールは含まれません。この設定情報をエクスポートするには、[ポリシー]画面にあるポリシーのエクスポートオプションを使用します。

コンピュータを削除する

コンピュータを削除すると (コンピュータを選択して [削除] をクリック)、そのコンピュータに関連するすべての情報も削除されます。コンピュータを再度検出する場合は、ポリシーおよび以前に割り当てられていたルールを割り当て直す必要があります。

ローカルネットワークコンピュータの追加

Agentからのリモート有効化

Deep Security Managerが保護対象のコンピュータとの通信を開始できない場合 (コンピュータが別のローカルネットワーク上にある場合やファイアウォールで保護されている場合など) は、コンピュータからManagerとの通信を開始する必要があります。これには、Agentを有効化するための通信も含まれます。Agentからのリモート有効化を使用するには、対象のコンピュータにDeep Security Agentをインストールし、Deep Security Managerと通信するようにAgentを設定する一連のコマンドラインの手順を実行する必要があります。通信時には、Deep Security ManagerがAgentを有効化します。また、セキュリティポリシーの割り当て、コンピュータグループへのコンピュータの追加など、その他の操作を実行するように設定することもできます。

多数のコンピュータを一度にDeep Security Managerに追加する場合は、CLIコマンドを使用して処理を自動化するスクリプトを作成できます。Agentからのリモート有効化、スクリプト、コマンドラインオプションの詳細については、"[コマンドラインの基本](#)" on page 447を参照してください。

コンピュータを手動で追加する

IPアドレスまたはホスト名を指定して、手動でコンピュータを個別に追加できます。

1. [コンピュータ] 画面に移動し、ツールバーの[追加]→[コンピュータの追加] をクリックして新規コンピュータウィザードを開きます。
2. 新しいコンピュータのIPアドレスまたはホスト名を入力します。
3. 割り当てるポリシーをリストから選択します。
4. 新しいコンピュータがセキュリティアップデートのダウンロード元として使用するRelayグループを選択します。
5. [次へ] をクリックしてコンピュータの検索を開始します。

コンピュータが検出され、そのコンピュータにAgentがインストールされていて稼働中の場合は、コンピュータリストにコンピュータが追加されて、Agentが有効になります。

注意: Agentの「有効化」とは、ManagerがAgentと通信して、一意の「フィンガープリント」をAgentに送信する処理です。これにより、Agentはこのフィンガープリントを使用してDeep Security Managerを一意に識別し、Agentに接続しようとする他のManagerからの指示を許可しなくなります。

コンピュータにポリシーが割り当てられている場合、そのポリシーはAgentに配信され、ポリシーを設定するすべてのルールと設定によってコンピュータが保護されます。

Relayグループによって配信されるセキュリティアップデートには、新しい不正プログラムパターンファイルが初期設定で含まれています。[9.0 (およびそれ以前) のAgentをサポート] オプション ([管理]→[システム設定]→[アップデート] 画面) を有効にしている場合は、エンジンのアップデートも含まれます。

コンピュータが検出され、Deep Security Agentが存在しない場合、コンピュータリストへのコンピュータの追加は可能ですが、コンピュータへのAgentのインストールを求められます。コンピュータにAgentをインストールしたら、コンピュータリストでコンピュータを検索して右クリックし、コンテキストメニューの [有効化/再有効化] を選択する必要があります。

コンピュータが検出されない場合 (Managerでは認識できない場合)、コンピュータの追加は可能ですが、コンピュータがManagerで認識されるようになった後、上記と同様にコンピュータを有効化する必要があります。

コンピュータを検出する

検出操作では、ネットワーク上の表示可能なコンピュータを検索します。検出操作を開始するには、[コンピュータ] 画面に移動し、[追加]→[検出] の順にクリックします。[コンピュータの検出] 画面が表示されます。

検索範囲を制限するためのいくつかのオプションがあります。検出された各コンピュータのポート検索を実行するように選択できます。

注意: ポート検索で多数のコンピュータを検出または検索する場合は、完了までに時間がかかり、パフォーマンスが低下することがあります。

コンピュータを検出するときは、コンピュータの追加先のコンピュータグループを指定できます。選択したコンピュータグループの構成方法によっては、複数のネットワークセグメントを検索する場合に、「新しく検出されたコンピュータ」または「ネットワークセグメントXで新しく検出されたコンピュータ」というコンピュータグループを作成すると便利ことがあります。その後、検出されたコンピュータを、プロパティに基づいて別のコンピュータグループに移動し、有効にすることができます。

検出を実行する際にManagerは、まだリストされていないネットワーク上の表示可能なコンピュータを検索します。コンピュータが見つかったら、ManagerはAgentが存在するかどうかの検出を試行します。検出が完了すると、Managerは検出したすべてのコンピュータを表示します。[ステータス]列にはコンピュータのステータスが表示されます。

注意: 検出操作で確認されるのは、新しく検出されたコンピュータのステータスのみです。すでに一覧表示されているコンピュータのステータスをアップデートするには、選択したコンピュータを右クリックし、[処理]→[ステータスの確認]の順にクリックします。

検出操作後のコンピュータの状態は、次のいずれかになります。

- 検出済み (Agentなし): コンピュータが検出されましたが、Agentが存在しません。また、インストール済みのAgentが以前に有効にされており、Agentからの通信用に設定されている場合にも、コンピュータがこの状態になる可能性があります。この場合、Agentを無効にしてから再度有効にする必要があります(また、Agentがインストールされているが稼働中でない場合にも、「Agentなし」とレポートされます)。
- 検出済み (有効化が必要): Agentがインストールされ待機中で、有効にされていますが、Managerによって管理されていません。この状態は、このManagerが一時Agentを管理していましたが、Agentの公開鍵がManagerのデータベースに存在しなくなったことを示します。コンピュータがManagerから削除された後に再び検出される場合は、これに該当する可能性があります。このコンピュータでAgentの管理を開始するには、コンピュータを右クリックし、[有効化/再有効化]を選択します。再度有効にしたコンピュータのステータスは「オンライン」に変更されます。
- 検出済み (無効化が必要): Agentはインストールされ待機中ですが、別のManagerによってすでに有効にされています。この場合、AgentをこのManagerで有効にする前に、いったん無効に(リセット)する必要があります。Agentの無効化は、そのAgentを有効にしたManagerを使用して行う必要があります。または、コマンドラインを使用してAgentをリセットできます。ManagerからAgentを無効にするには、コンピュータを右クリックし、[処理]→[無効化]を選択します。Agentをコマンドラインから無効にする場合は、"[Agentをリセットする](#)" on page 463を参照してください。
- 検出された (アクティベートされた): エージェントは、現在のマネージャによってインストールおよびアクティベートされています。この場合、次のハートビートでステータスは「オンライン」に変わります。エージェントの管理を開始するには、コンピュータを右クリックして、[Activate/Reactivate]を選択します。再度有効にしたコンピュータのステータスは「オンライン」に変更されます。

注意: 検出操作では、vCenterで仮想マシンとして実行されているコンピュータ、Microsoft Active Directoryのコンピュータ、またはその他のLDAPディレクトリのコンピュータは検出されません。

VMware vCenterの追加

ヒント: [Deep Security 12 - Scoping Environment Pt](#)を見ることができます。1 - YouTubeの[ワークロード](#)を特定して、環境のスコープを決定する際の検討事項を確認してください。

VMware vCenterをDeep Security Managerにインポートし、その仮想マシンをAgentレス、Agentベース、またはコンバインモードで保護できます(これらのオプションについては、"[Agentレスによる保護またはコンバインモードの保護の選択](#)" on page 315を参照してください。)

注意: vShield Managerを使用しているvCenterはインポートできません。vShield Managerからサポート対象のVMware製品への移行については、"[Deep Securityのインストールまたはアップグレード](#)" on page 223を参照してください。

vCenterの追加には、次のオプションがあります。

- "[vCenterの追加](#)" belowを追加
- "[vCenter - FIPSモードを追加する](#)" on page 515

vCenterの追加

1. Deep Security Managerで、[Computers]→[追加]→[VMware vCenterの追加]の順に移動します。
2. vCenter Serverの情報を入力します。
 - vCenter ServerのIPアドレス (または、DNSが設定されており、FQDNをIPアドレス)に解決できる場合はホスト名を入力します。
 - [vCenterに接続するポート番号](#)を入力します (初期設定では443)。
 - vCenterユーザアカウントのユーザ名とパスワードを入力します。このアカウントは、次の表に示す仕様に一致する必要があります。このユーザは、vCenterとDeep Security Managerの間でVMインベントリを同期するために必要となります。

保護方法	NSXタイプ	vCenterのユーザアカウントの仕様
エージェントレスモードまたは複合モード	VMware NSX Data Center for vSphere (NSX-V)	vCenterのユーザアカウントには、次の2つの役割が必要です。 <ul style="list-style-type: none"> NSX Managerで割り当てられたエンタープライズ管理者ロール。NSX-V Managerでのロールの割り当てについては、VMwareのこちらの記事を参照してください。 vCenterでデータセンターレベルで割り当てられた管理者ロール
	VMware NSX-T Data Center (NSX-T)	vCenterのユーザアカウントに次の役割（または同等以上の権限を持つ別の役割）が必要です。): <ul style="list-style-type: none"> Guest Introspection管理者。VMwareの各種ロールに割り当てられた権限の詳細については、VMwareのこちらの記事を参照してください。NSX-T Managerでのロールの割り当ての詳細については、VMwareのこちらの記事を参照してください。
エージェントのみ	NSX-VまたはNSX-Tの統合なし	vCenterの読み取り専用の役割（または権限以上の権限を持つ別の役割）が、データセンターレベルでvCenterのユーザアカウントに必要です。

注意: vCenterの[ホスト]、[クラスタ]、または[仮想マシン]のレベルで読み取り専用または管理者の役割を適用すると、同期の問題が発生します。

- [Next] をクリックします。
3. vCenterのTLS (SSL) 証明書を受け入れます。
 4. エージェントレスまたは複合モードの保護を使用する場合は、NSX情報を次のように入力します。それ以外の場合は、[Next] をクリックしてこの手順をスキップします。
 - NSX ManagerのIPアドレス（またはDNSが設定されており、FQDNをIPアドレスに解決できる場合はホスト名）を入力します。
 - [NSX Managerに接続するポート番号](#)を入力します（初期設定では443）。

- NSXまたはvCenterのユーザアカウントのユーザ名とパスワードを入力します。このアカウントは、次の表に示す仕様に一致する必要があります。このユーザは、NSXセキュリティポリシーおよびセキュリティグループをDeep Security Managerと同期するために必要となります。

NSXタイプ	ユーザアカウントの仕様
VMware NSX Data Center for vSphere (NSX-V)	<p>ユーザアカウントは次である必要があります。</p> <ul style="list-style-type: none"> • すべての権限を持つ、NSXの組み込みの管理者アカウント <p>または</p> <ul style="list-style-type: none"> • 次の2つのロールを持つvCenterユーザアカウント: <ul style="list-style-type: none"> • NSX Managerで割り当てられたエンタープライズ管理者ロール。NSX-V Managerでのロールの割り当てについては、VMwareのこちらの記事を参照してください。 • vCenterでデータセンターレベルで割り当てられた管理者ロール(クラスタレベルでこのロールが割り当てられている場合はエラーが発生します)。
VMware NSX-T Data Center (NSX-T)	<p>ユーザアカウントは次である必要があります。</p> <ul style="list-style-type: none"> • すべての権限を持つ、NSXの組み込みの管理者アカウント <p>または</p> <ul style="list-style-type: none"> • 次のロール、または同等以上の権限がある別のロールを持つvCenterユーザアカウント: <p>Guest Introspection管理者。VMwareの各種ロールに割り当てられた権限の詳細については、VMwareのこちらの記事を参照してください。NSX-T Managerでのロールの割り当ての詳細については、VMwareのこちらの記事を参照してください。</p>

- [次へ](#) をクリックします。

5. プロンプトが表示されたら、NSX ManagerのTLS (SSL) 証明書に同意します。
6. vCenterの情報を確認し、[完了] をクリックします。
7. 「VMware vCenterの追加に成功しました。」というメッセージが表示されます。[閉じる] をクリックします。[コンピュータ] 画面にvCenterが表示されます。

ヒント: vCenterを追加する場合に [このvCenterの保護対象NSXセキュリティグループに追加された仮想マシンを自動的に有効化する、イベントベースタスクを作成します。]をオンにすると、イベントベースタスクが2つ作成されます。1つは、保護が追加されたときに仮想マシンを有効化し、もう1つは、保護が削除されたときに仮想マシンを無効化します。詳細については、"[NSX環境での自動ポリシー管理](#)" on page 359を参照してください。

前述のようにNSX情報を入力した場合、Deep Security ManagerはNSX Manager内にDeep Securityサービスを登録します。この登録により、ESXiサーバへのDeep Securityサービスの配信が許可されます。

大規模環境では、このプロセスが完了するまで時間がかかることがあります。vCenterの [最近のタスク] セクションで、実行中のアクティビティがないか確認してください。

Deep Security ManagerとこのVMware vCenterがリアルタイムで同期され、Deep Security Managerに表示される情報 (仮想マシンの数、ステータスなど) が最新に保たれます。

vCenter - FIPSモードを追加する

Deep Security ManagerがFIPSモードの場合にvCenterを追加するには

1. vCenterおよびNSX ManagerのTLS (SSL) 証明書を Deep Security Managerにインポートしてから、vCenterをマネージャに追加します。"[信頼された証明書の管理](#)" on page 424を参照してください。
2. "[VMware vCenterの追加](#)" on page 512の手順に従って、vCenterを追加します。これらの手順はまったく同じですが、FIPSモードの場合は、vCenterページの[信頼する証明書] セクションが表示されます。[接続テスト]をクリックして、vCenterのSSL証明書がDeep Security Managerに正常にインポートされたかどうかを確認します。エラーがない場合は、[次へ]の順をクリックし、ウィザードを続行します。

保護されたNSXクラスタへのESXiの追加

注意: このトピックは [NSX-T配置](#) には適用されません。

すでにDeep Security Virtual Applianceがインストールされているクラスタ内のESXiサーバを保護している場合に、そのクラスタに別のESXiを追加する場合は、次の手順に従って新しいESXiサーバが保護されていることを確認してください。

1. 開始する前に、アプライアンスをクラスタに配置していることを確認してください。手順については、[アプライアンス \(NSX-V\)](#) の配信を参照してください。

2. ESXiをデータセンターに追加します。クラスタには直接追加しないでください。
3. ESXiを仮想分散スイッチ (vDS) に接続します。
4. ESXiをクラスタに移動します。

ESXiホストをクラスタに移動すると、NSXによってDeep Securityサービスが自動的に配信されます。

注意: NSX Managerへの接続は、FIPSモードでサポートされています。"[FIPS 140-2のサポート](#)" on page 1457を参照してください。

AWSクラウドアカウントの追加

ヒント: [Deep Security 12 - Scoping Environment Pt](#)を見ることができます。1 - ワークロードの特定に関連する環境の範囲を検討するため、[YouTubeのワークロード](#) を特定する

AWSアカウントをDeep Securityに追加すると、そのアカウントにおけるAmazon EC2とAmazon WorkSpaceのすべてのインスタンスがDeep Security Managerにインポートされ、次のいずれかの場所で確認できるようになります。

- EC2インスタンスは、[コンピュータ]→[<ご使用のAWSアカウント>]→[<ご使用のリージョン>]→[<ご使用のVPC>]→[<ご使用のサブネット>]の左側に表示されます。
- Amazon WorkSpacesは、[コンピュータ]→[<ご使用のAWSアカウント>]→[<ご使用のリージョン>]→[WorkSpaces]の左側に表示されます。

インポートの完了後は、他のコンピュータと同じようにEC2とWorkSpaceのインスタンスを管理できます。これらのインスタンスはツリー構造であり、コンピュータグループとして扱われます。

注意: Amazon EC2インスタンスまたはAmazon WorkSpacesが個別のコンピュータとして追加済みで、ご使用のAWSアカウントに含まれている場合は、アカウントのインポート後に、インスタンスは前述の[ツリー構造](#)に移動します。

このセクションのトピック:

- ["AWSアカウントを追加することのメリットは何ですか?" on the next page](#)
- ["サポートされるAWSリージョン" on the next page](#)
- ["AWSアカウントを追加する方法の概要" on page 518](#)
- ["方法: Managerインスタンスロールとクロスアカウントロール" on page 519](#)

- "方法: IAMユーザとクロスアカウントロール" on page 525
- "方法: Managerインスタンスロール (1つのAWSアカウント)" on page 531
- "方法: AWSアクセスキー" on page 533
- "クラウドアカウントを編集する" on page 535
- "Managerからクラウドアカウントを削除する" on page 535
- "AWSアカウントを同期する" on page 535

AWSアカウントを追加することのメリットは何ですか？

個別のEC2インスタンスとワークスペース（「Deep Security Manager」→「コンピュータ」→「コンピュータの追加」）, を使用）を追加するのではなく、AWSアカウント（Deep Security Manager→コンピュータ→AWSアカウントの追加）の利点は次のとおりです。

- EC2およびWorkspaceのインベントリの変更は、Deep Security Managerに自動的に反映されます。たとえば、AWSでいくつかのEC2またはWorkspaceインスタンスを削除すると、これらのインスタンスは自動的にマネージャから非表示になります。一方、の[コンピュータ]→[コンピュータの追加]を使用する場合、AWSから削除されたEC2およびWorkspaceのインスタンスは、手動で削除されるまでマネージャに表示されたままです。
- EC2およびWorkspaceのインスタンスは、マネージャの[AWS region]→[VPC]のサブネットに編成されており、どのインスタンスが保護されているか、どのインスタンスが保護されていないかを簡単に確認できます。AWSアカウントがないと、すべてのEC2インスタンスとWorkspaceインスタンスが同じルートレベルの Computersに表示されます。
- [イベントベースタスク \(EBT\)](#) でAWSメタデータを使用してポリシーの割り当てを簡素化できます。 [スマートフォルダ](#) でメタデータを使用して、AWSインスタンスを編成することもできます。
- Deep Security AMI from AWS Marketplace hourly pricing

サポートされるAWSリージョン

Deep Security Managerの[コンピュータ]→[追加]→[AWSアカウントの追加] オプションは、`iam.amazonaws.com`でグローバルAWS IDアクセス管理 (IAM) サービスを使用するAWS領域のみをサポートします。お住まいの地域でグローバルサービスが使用されているかどうかを確認するには、 [this table](#)を参照してください。

次の地域では、ではではグローバルIAMサービス (`iam.amazonaws.com`):) を使用していません。

- 中国 (北京)
- 中国 (寧夏回族自治区)
- AWS GovCloud (米国 - 東)
- AWS GovCloud (米国)

上記のリージョンおよびグローバルIAMサービスを使用しない可能性のあるリージョンについては、[Deep Security REST APIを使用して](#)、EC2およびWorkSpaceのインスタンスをマネージャにロードできます。トレンドマイクロでは、この[サンプルスクリプトを](#)に提供しています。

AWSアカウントを追加する方法の概要

AWSアカウントをDeep Security Managerに追加するにはいくつかの方法があります。

- ["方法: Managerインスタンスロールとクロスアカウントロール" on the next page](#)。複数のAWSアカウントを追加する場合、Deep Security ManagerがAWSの内部にある場合は、この方法を使用します。

この方法は次の製品で使用できます。

- Deep Securityオンプレミス (AWS内のEC2インスタンス上に存在)

- ["方法: IAMユーザとクロスアカウントロール" on page 525](#)。複数のAWSアカウントを追加する場合や、Deep Security ManagerがAWSの外部にある場合は、この方法を使用します。

この方法は次の製品で使用できます。

- Deep Security VM for Azure Marketplace
- Deep Securityオンプレミス (AWS外のサーバ上に存在)

- ["方法: Managerインスタンスロール \(1つのAWSアカウント\)" on page 531](#)。Deep Security Managerが属しているAWSアカウントに追加する場合は、この方法を使用します。

この方法は次の製品で使用できます。

- Deep Security AMI from AWS Marketplace
- Deep Securityオンプレミス (AWS内のEC2インスタンス上に存在)

- ["方法: AWSアクセスキー" on page 533](#)。この方法は、Deep Security ManagerがAWS外

のサーバ上にあり、追加するAWSアカウントが1つしかない場合、または別の方法を試しても機能しない場合にのみお勧めします。

上記に該当しない場合、他の方法のご使用をお勧めします。キーは定期的にアップデートする必要があり (セキュリティ上の理由のため)、管理オーバーヘッドが発生するため、Deep Security Managerでのアクセスキーの指定はお勧めしません。

この方法は次の製品で使用できます。

- Deep Security AMI from AWS Marketplace
- Deep Securityオンプレミス
- Deep Security Manager VM for Azure Marketplace

方法: Managerインスタンスロールとクロスアカウントロール

この方法の概要については、"[AWSアカウントを追加する方法の概要](#)" on the previous pageを参照してください。

以下の手順は、AWSアカウントが2つあり、その両方のアカウントに、保護する必要のあるAmazon EC2インスタンスとAmazon WorkSpacesが含まれていることを前提としています。この例で使用されているアカウントの名前は次のとおりです。

- AWS DSMアカウント (Deep Security Managerが常駐するアカウント)
- AWSアカウントA

手順の概要は次のとおりです。詳細については後で説明します。

1. "[AWS DSMアカウントを設定する](#)" on the next page : AWS DSMアカウントにログインし、IAMポリシーを作成し、IAMポリシーを参照するマネージャインスタンスの役割を作成し、 Deep Security Manager EC2インスタンスにアタッチします。
2. "[AWSアカウントAを設定する](#)" on page 522: AWSアカウントAへのログイン、IAMポリシーの設定、Managerインスタンスロールを参照するクロスアカウントロールの作成を行います。
3. "[AWSアカウントをDeep Security Managerに追加する](#)" on page 524: Deep Security ManagerでManagerインスタンスロールを使用していることを示し、AWS DSMアカウントとAWSアカウントAを追加します。

これらの手順を完了すると、Deep Security ManagerではManagerインスタンスロールを使用して、AWS DSMアカウントにアクセスし、そのAmazon EC2インスタンスとAmazon WorkSpacesを表示できます。また、Managerインスタンスロールを参照するクロスアカウントロールを使用して、AWSアカウントAのリソースに (間接的に) アクセスできます。

AWS DSMアカウントを設定する

最初に、AWS DSMアカウント (Deep Security Managerが存在するアカウント) にログインし、IAMポリシーを設定します。

1. AWSマネジメントコンソールにログインし、[IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeTags",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "sts:AssumeRole"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```



```
]
}
```

注意: "sts:AssumeRole"権限は、クロスアカウントロールを使用している場合にのみ必要です。

注意: "iam:GetRole"権限と"iam:GetRolePolicy"権限はオプションですが、これらの権限により、追加のAWS権限が必要なManagerの更新が発生したときに、正しいポリシーがあるかどうかをDeep Securityが判断できるため、推奨します。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。名前の例: Deep_Security_Policy。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、Deep Security Managerを実行しているEC2インスタンス用のEC2インスタンスロールを作成します。

1. [IAM] サービスに移動します。
2. [Roles] をクリックします。
3. [Create role] をクリックします。
4. [AWS service] ボックスが選択されていることを確認します。
5. サービスリストで [EC2] をクリックします。オプションがさらに表示されます。
6. [EC2 Allows EC2 instances to call AWS services on your behalf] をクリックします。
[Next: Permissions] をクリックします。
7. 作成したIAMポリシーの横にあるチェックボックスをオンにします。[Next: Review] をクリックします。
8. [Role name] と [Role description] を入力します。
ロール名の例: Deep_Security_Manager_Instance_Role
9. [Create role] をクリックします。
10. リスト内のロールを選択して、詳細を表示します。
11. 画面の上部にある [Role ARN] フィールドを探します。フィールド値は以下のように表示されます。
arn:aws:iam::1234567890:role/Deep_Security_Manager_Instance_Role
12. ARNのロールアカウントIDをメモします。IDは数値 (1234567890) です。後で必要になります。

次の手順でManagerインスタンスロールをEC2インスタンスに関連付けます。

1. [EC2] サービスに移動します。
2. 左側にある [Instances] をクリックし、Deep Security ManagerがインストールされているEC2インスタンスの横にあるチェックボックスをオンにします。

3. [Actions]→[Instance Settings]→[Attach/Replace IAM Role] の順にクリックします。
4. [IAM role] ドロップダウンリストから、Managerインスタンスロール (Deep_Security_Manager_Instance_Role) を選択します。
5. [Apply] をクリックします。

これで、正しいIAMポリシーでManagerインスタンスロールが作成され、Deep Security ManagerのEC2インスタンスに関連付けられました。

AWSアカウントAを設定する

最初にAWSからログアウトし、AWSアカウントAを使用して再度ログインします。これはAmazon EC2インスタンスおよびAmazon WorkSpacesの一部またはすべてが存在するアカウントです。

AWSアカウントAにログインしたら、AWSアカウントA用のIAMポリシーを設定します。このポリシーは、AWS DSMアカウントのものと同じですが、sts:AssumeRole権限は必要ありません。

1. AWSマネジメントコンソールにログインし、[IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
```

```

        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeTags",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:GetRolePolicy"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
}

```

注意: "iam:GetRole"権限と"iam:GetRolePolicy"権限はオプションですが、これらの権限により、追加のAWS権限が必要なManagerの更新が発生したときに、正しいポリシーがあるかどうかをDeep Securityが判断できるため、推奨します。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。名前の例: Deep_Security_Policy_2。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、Managerインスタンスロールを参照するクロスアカウントロールを作成します。

1. [IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Roles] をクリックします。
3. メイン画面で、[Create role] をクリックします。
4. [Another AWS account] ボックスをクリックします。
5. アカウントID フィールドに、マネージャーインスタンスの役割のアカウントIDを入力します。

AWC内で Deep Security AMI from AWS Marketplace または Deep Security Managerのオンプレミス版を使用している場合は、以前に作成したマネージャインスタンスのアカウントIDをメモしておいたはずですが、この例では、次の番号です。1234567890

6. [Options] の横にある [Require external ID] を有効にします。[External ID] フィールドに、長いランダムな秘密の文字列を入力します。
7. 外部IDをメモします。この情報は、後で必要になります。
8. [Next: Permissions] をクリックします。
9. 先ほど作成したIAMポリシー (上記の例ではDeep_Security_Policy_2) を選択し、[Next: Review] をクリックします。
10. [Review] ページで、役割名と説明を入力します。役割名の例: Deep_Security_Role_2。

11. メインロール画面で、作成したロール (Deep_Security_Role_2) を検索します。
12. 検索した役割をクリックします。
13. 上部にある [Role ARN] フィールドを探して、値をメモします。後で必要になります。次のような値です:
arn:aws:iam::1234567890:role/Deep_Security_Role

これで、正しいポリシーが設定された、Managerインスタンスロールを参照するクロスアカウントロールがAWSアカウントAに作成されました。

AWSアカウントをDeep Security Managerに追加する

最初に、Managerインスタンスロールを使用することを示します。

1. Deep Security Managerで、上部の [管理] をクリックします。
2. 左側にある [システム設定] をクリックします。
3. メイン画面の [詳細] タブをクリックします。
4. 下にスクロールして、[Manager AWS ID] セクションを探します。
5. [Managerインスタンスロールを使用] が選択されていることを確認します。

注意: [Managerインスタンスロールを使用] が表示されない場合は、Deep Security ManagerがインストールされているEC2インスタンスにそのロールを関連付けたことを確認し、"[Deep Security Managerの再起動](#)" on page 993します。再起動時に、Deep SecurityでManagerのEC2インスタンスのロールが検出され、[Managerインスタンスロールを使用] オプションが表示されます。

6. [保存] をクリックします。

次に、AWS DSMアカウントを追加します。

1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. メイン画面で、[追加]→[AWSアカウントの追加] の順にクリックします。
3. [詳細] を選択し、[次へ] をクリックします。
4. [Managerインスタンスロールを使用] を選択します。
5. AWS DSMアカウントにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める] を選択して、Amazon EC2インスタンスとAmazon WorkSpacesを追加します。チェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerの[ツリー構造](#)内の適切な場所に表示され、適切なレートで課金されるようになります。
6. [次へ] をクリックします。

Deep Security Managerでは、Amazon EC2インスタンスに割り当てられたManagerインスタンスロールを使用して、AWS DSMアカウントのEC2およびWorkSpaceインスタンスをDeep Security Managerに追加します。

最後に、クロスアカウントロールを使用してAWSアカウントAを追加します。

1. 上部の [コンピュータ] をクリックします。
2. [追加]→[AWSアカウントの追加] の順にクリックします。
3. [詳細] を選択し、[次へ] をクリックします。
4. [クロスアカウントロールを使用] を選択します。
5. AWSアカウントAの [クロスアカウントロールのARN] と [外部ID] を入力します。クロスアカウントロール作成時にメモしたものを使用します。
6. AWSアカウントAにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める] を選択して、Amazon EC2インスタンスとAmazon WorkSpacesを追加します。チェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerの [ツリー構造](#) 内の適切な場所に表示され、適切なレートで課金されるようになります。
7. [次へ] をクリックします。
AWSアカウントAのAmazon EC2インスタンスとAmazon WorkSpacesがロードされません。

これで、AWS DSMアカウントとAWSアカウントAがDeep Security Managerに追加されました。

方法: IAMユーザとクロスアカウントロール

この方法の概要については、"[AWSアカウントを追加する方法の概要](#)" on page 518を参照してください。

次の手順では、Deep Security ManagerがAWSの外部にあり、なおかつ、保護するAmazon EC2インスタンスとWorkSpaceインスタンスを含んだ2つの異なるAWSアカウントがあることを想定しています。この例で使用されているアカウントの名前は次のとおりです。この例で使用されているアカウントの名前は次のとおりです。

- AWSアカウントX (プライマリ)
- AWSアカウントY

手順の概要は次のとおりです。詳細については後で説明します。

1. "[AWSアカウントXを設定する](#)" on the next page: AWSアカウントX (プライマリアカウント) へのログイン、IAMポリシーの設定、アクセスキーを使用したIAMユーザの作成を行います。

2. ["AWSアカウントYを設定する" on page 528](#): AWSアカウントYへのログイン、IAMポリシーの設定、AWSアカウントXを参照するクロスアカウントロールの作成を行います。
3. ["Deep Security Managerにアクセスキーを追加する" on page 529](#): Deep Security Managerで、AWSアカウントXのアクセスキーIDと秘密アクセスキーを追加します。
4. ["AWSアカウントをDeep Security Managerに追加する" on page 530](#): Deep Security Managerで、AWSアカウントXとAWSアカウントYを追加します。

これらの手順を完了すると、Deep Security ManagerではAWSアカウントXのアクセスキーIDと秘密アクセスキーを使用して、AWSアカウントXにログインし、Amazon EC2およびAmazon WorkSpaceインスタンスを表示できます。また、AWSアカウントXを参照するクロスアカウントロールを使用して、AWSアカウントYのリソースに (間接的に) アクセスできます。

AWSアカウントXを設定する

最初に、AWSアカウントXにログインし、IAMポリシーを設定します。

1. AWSマネジメントコンソールにログインし、[IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
      ]
    }
  ]
}
```

```
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeTags",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "sts:AssumeRole"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
```

注意: "sts:AssumeRole"権限は、クロスアカウントロールを使用している場合にのみ必要です。

注意: "iam:GetRole"権限と"iam:GetRolePolicy"権限はオプションですが、これらの権限により、追加のAWS権限が必要なManagerの更新が発生したときに、正しいポリシーがあるかどうかをDeep Securityが判断できるため、推奨します。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。名前例: Deep_Security_Policy。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、アクセスキーIDと秘密アクセスキーを使用してIAMユーザを作成します。

1. [IAM] サービスに移動します。
2. [Users] をクリックします。
3. [Add user] をクリックします。
4. ユーザ名を入力します。例: Deep_Security_IAM_User。
5. [Access type] では [Programmatic access] を選択します。
6. [Next: Permissions] をクリックします。
7. [Attach existing policies directly] ボックスをクリックします。
8. 作成したIAMポリシーを探し、その横にあるチェックボックスをオンにします。
9. [Next: Review] をクリックします。
10. [Create user] をクリックします。アクセスキーIDと秘密アクセスキーがテーブルに表示されます。
11. アクセスキーIDと秘密アクセスキーを安全な場所にコピーします。後で必要になります。

次に、AWSアカウントXのアカウントIDを確認します。

1. AWSの右上で [Support]→[Support Center] の順にクリックします。
2. 右上に表示される [Account Number] (この例では1234567890) をメモします。後でクロスアカウントロールの作成に必要なになります。

AWSアカウントYを設定する

最初に、AWSアカウントYにログインし、IAMポリシーを設定します。このポリシーは、AWSアカウントXのものと同じですが、sts:AssumeRole権限は必要ありません。

1. AWSマネジメントコンソールにログインし、[IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeTags",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
    },
  ],
}
```



```
        "Effect": "Allow",
        "Resource": "*"
    }
]
}
```

注意: "iam:GetRole"権限と"iam:GetRolePolicy"権限はオプションですが、これらの権限により、追加のAWS権限が必要なManagerの更新が発生したときに、正しいポリシーがあるかどうかをDeep Securityが判断できるため、推奨します。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。名前の例: Deep_Security_Policy_2。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、AWSアカウントXを参照するクロスアカウントロールを作成します。

1. [IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Roles] をクリックします。
3. メイン画面で、[Create role] をクリックします。
4. [Another AWS account] ボックスをクリックします。
5. [Account ID] フィールドに、AWSアカウントXのアカウントIDを入力します (この例では 1234567890)。
6. [Options] の横にある [Require external ID] を有効にします。[External ID] フィールドに、長いランダムな秘密の文字列を入力します。
7. 外部IDをメモします。この情報は、後でDeep Security Managerにこのアカウントを追加するときに必要になります。
8. [Next: Permissions] をクリックします。
9. 以前に作成したIAMポリシーを選択し、[Next: Review] をクリックします。
10. [Review] ページで、役割名と説明を入力します。役割名の例:Deep_Security_Role。
11. メインの役割ページで、作成した役割 (Deep_Security_Role) を検索します。
12. 検索した役割をクリックします。
13. 上部にある [Role ARN] フィールドを探して、値をメモします。この値は、後でDeep Security Managerにこのアカウントを追加するときに必要になります。次のような値です:

```
arn:aws:iam::544739704774:role/Deep_Security_Role
```

Deep Security Managerにアクセスキーを追加する

1. Deep Security Managerにログインします。
2. 上部の [管理] をクリックします。
3. 左側にある [システム設定] をクリックします。

4. メイン画面の [詳細] タブをクリックします。
5. 下にスクロールして、[Manager AWS ID] の見出しを探します。
6. [アクセスキー - Managerの識別に使用されるAWSユーザのアクセスキー] の横に、作成済みのIAMユーザのアクセスキーを入力します。
7. [秘密鍵 - Managerの識別に使用されるAWSユーザの秘密アクセスキー] の横に、作成済みのIAMユーザの秘密鍵を入力します。
8. [保存] をクリックします。

AWSアカウントをDeep Security Managerに追加する

最初に、アクセスキーを使用してアカウントXを追加します。

1. 上部の [コンピュータ] をクリックします。
2. [追加]→[AWSアカウントの追加] の順にクリックします。
3. [AWSアクセスキーを使用] を選択します。
4. 作成済みのAWSアカウントXのIAMユーザの [アクセスキーID] と [秘密アクセスキー] を入力します。
5. AWSアカウントにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める] を選択して、Amazon EC2インスタンスとAmazon WorkSpacesを追加します。チェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerの [ツリー構造](#) 内の適切な場所に表示され、適切なレートで課金されるようになります。AWSアカウントXのAmazon EC2インスタンスとAmazon WorkSpacesがロードされません。

次に、クロスアカウントロールを使用してAWSアカウントYを追加します。

1. 上部の [コンピュータ] をクリックします。
2. [追加]→[AWSアカウントの追加] の順にクリックします。
3. [クロスアカウントロールを使用] を選択します。
4. AWSアカウントYの [クロスアカウントロールのARN] と [外部ID] を入力します。
5. AWSアカウントにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める] を選択して、Amazon EC2インスタンスとAmazon WorkSpacesを追加します。チェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerの [ツリー構造](#) 内の適切な場所に表示され、適切なレートで課金されるようになります。
6. [次へ] をクリックします。
AWSアカウントYのAmazon EC2インスタンスとAmazon WorkSpacesがロードされません。

これで、AWSアカウントXとAWSアカウントYがDeep Security Managerに追加されました。

方法: Managerインスタンスロール (1つのAWSアカウント)

この方法の概要については、"[AWSアカウントを追加する方法の概要](#)" on page 518を参照してください。

最初に、Deep Security Managerが含まれているアカウントを使用してAWSにログインし、IAMポリシーを設定します。

1. AWSマネジメントコンソールにログインし、[IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeTags",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Effect": "Allow",
```

```
        "Resource": "*"
    }
]
}
```

注意: "iam:GetRole"権限と"iam:GetRolePolicy"権限はオプションですが、これらの権限により、追加のAWS権限が必要なManagerの更新が発生したときに、正しいポリシーがあるかどうかをDeep Securityが判断できるため、推奨します。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。名前の例: Deep_Security_Policy_2。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、IAMポリシーを含むIAMロールを作成します。これは「Managerインスタンスロール」と呼ばれます。

次に、Managerインスタンスロールを、Deep Security ManagerがインストールされているEC2インスタンスに関連付けます。

1. Deep Security Managerが含まれているアカウントを使用して、AWSにログインします。
2. [EC2] サービスに移動します。
3. 左側にある [Instances] をクリックし、Deep Security ManagerがインストールされているEC2インスタンスの横にあるチェックボックスをオンにします。
4. [Actions]→[Instance Settings]→[Attach/Replace IAM Role] の順にクリックします。
5. [IAM role] ドロップダウンリストから、Managerインスタンスロールを選択します。
6. [Apply] をクリックします。

最後に、AWSアカウントをDeep Security Managerに追加します。

1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. [追加]→[AWSアカウントの追加] の順にクリックします。
3. [Managerインスタンスロールを使用] を選択します。

注意: [Managerインスタンスロールを使用] が表示されない場合は、Deep Security ManagerがインストールされているEC2インスタンスにManagerインスタンスロールを関連付けたことを確認し、"[Deep Security Managerの再起動](#)" on page 993をします。再起動時に、Deep SecurityでManagerのEC2インスタンスのロールが検出され、[Managerインスタンスロールを使用] オプションが表示されます。

4. AWSアカウントにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める] を選択して、Amazon EC2インスタンスとAmazon WorkSpacesを追加しま

す。チェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerのツリー構造内の適切な場所に表示され、適切なレートで課金されるようになります。

5. [次へ] をクリックします。

AWSアカウントのAmazon EC2インスタンスとAmazon WorkSpacesがロードされます。

方法: AWSアクセスキー

この方法の概要については、"[AWSアカウントを追加する方法の概要](#)" on page 518を参照してください。

最初に、保護対象のAmazon EC2インスタンスとAmazon WorkSpacesが含まれているアカウントを使用して、AWSにログインします。

次に、IAMポリシーを設定します。

1. AWSマネジメントコンソールにログインし、[IAM] サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspaceDirectories",
```

```
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeTags",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:GetRolePolicy"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
```

注意: "iam:GetRole"権限と"iam:GetRolePolicy"権限はオプションですが、これらの権限により、追加のAWS権限が必要なManagerの更新が発生したときに、正しいポリシーがあるかどうかをDeep Securityが判断できるため、推奨します。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。名前の例: Deep_Security_Policy_2。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、IAMユーザアカウントを作成します。

1. [IAM] サービスに移動します。
2. [Users] をクリックします。
3. [Add user] をクリックします。
4. ユーザ名を入力します。例: Deep_Security_IAM_User。
5. [Access type] では [Programmatic access] を選択します。
6. [Next: Permissions] をクリックします。
7. [Attach existing policies directly] ボックスをクリックします。
8. 作成したIAMポリシーを探し、その横にあるチェックボックスをオンにします。
9. [Next: Review] をクリックします。
10. [Create user] をクリックします。アクセスキーIDと秘密アクセスキーがテーブルに表示されます。
11. アクセスキーIDと秘密アクセスキーを安全な場所にコピーします。後で必要になります。

最後に、AWSアカウントをDeep Securityに追加します。

1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. メイン画面で、[追加]→[AWSアカウントの追加] の順にクリックします。
3. [AWSアクセスキーを使用] を選択します。
4. IAMユーザ作成時に生成した [アクセスキーID] と [秘密アクセスキー] を指定します。

5. AWSアカウントにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める]を選択して、Amazon EC2インスタンスとAmazon WorkSpacesを追加します。チェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerのツリー構造内の適切な場所に表示され、適切なレートで課金されるようになります。
6. [次へ]をクリックします。

AWSアカウントのAmazon EC2インスタンスとAmazon WorkSpacesがロードされます。

クラウドアカウントを編集する

Deep Security Managerで、クラウドアカウントの設定を編集できます。AWSアカウントにAmazon WorkSpacesを含めるよう設定する必要がある場合などに、この編集が必要になることがあります。クラウドアカウントを編集するには、次の手順に従います。

1. Deep Security Managerにログインします。
2. 上部の [コンピュータ] をクリックします。
3. 左側にあるクラウドアカウント名を右クリックし、[プロパティ] を選択します。
4. 設定を編集して、[OK] をクリックします。

Managerからクラウドアカウントを削除する

クラウドアカウントをDeep Security Managerから削除すると、そのアカウントはDeep Securityのデータベースとそのベースとなるコンピュータから削除されます。クラウドプロバイダのアカウントに影響はありません。また、インスタンスにインストールされていたDeep Security Agentはアンインストールされず、実行と保護が継続します (ただしセキュリティアップデートは受信しなくなります)。クラウドアカウントからコンピュータを再インポートすると、Deep Security Agentによって、次の予約時に最新のセキュリティアップデートがダウンロードされます。

1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. ナビゲーションパネルでクラウドアカウントを右クリックし、[クラウドアカウントの削除...] を選択します。
3. アカウントを削除することを確認します。
アカウントがDeep Security Managerから削除されます。

AWSアカウントを同期する

AWSアカウントを同期 (同期) すると、Deep Security ManagerはAWS APIに接続して、最新のAWS EC2インスタンスとWorkSpaceインスタンスを取得して表示します。

強制的に同期を強制するには

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 左側で、AWSアカウントを右クリックし、[同期する]を選択します。をクリックします。

10分ごとに発生するバックグラウンド同期もあり、この間隔は設定できません。同期を強制すると、バックグラウンドの同期は影響を受けず、元のスケジュールに従って引き続き実行されます。

Amazon WorkSpacesの追加

Amazon WorkSpacesは、Amazon Web Services (AWS) で実行される仮想クラウドデスクトップです。これらは、次のいずれかのセクションの手順に従うことにより、Deep Securityで保護できます。

- ["Amazon WorkSpacesを保護する \(AWSアカウントをすでに追加している場合\)" below](#)
- ["Amazon WorkSpacesを保護する \(AWSアカウントをまだ追加していない場合\)" on the next page](#)

注意: Deep Security Agentは、WindowsデスクトップでのみAmazon WorkSpacesをサポートします。Linuxデスクトップではサポートされません。

上記セクションのいずれかの手順の完了後:

- Amazon WorkSpacesは、Deep Security Managerの [コンピュータ]→[<ご使用のAWSアカウント>]→[<ご使用のリージョン>]→[WorkSpaces] の左側に表示されます。
- Amazon WorkSpacesはDeep Security Agentによって保護されます。

Amazon WorkSpacesを保護する (AWSアカウントをすでに追加している場合)

Amazon EC2インスタンスを保護するためにAWSアカウントをすでにDeep Security Managerに追加している場合、Deep SecurityとAmazon WorkSpacesの連携を設定するには、このセクションの手順を実行します。

1. Deep Security Managerをバージョン10.3以降にバージョンアップします。"[Deep Securityのインストールまたはアップグレード" on page 223](#)を参照してください。
2. Amazon WorkSpaceを起動し、Deep Security Agent 10.2以降をインストールして有効化します。詳細については、"[Amazon EC2およびWorkSpacesへのAgentのインストール" on page 387](#)を参照してください。オプションで、カスタムWorkSpaceバンドルを作成し、多数のユーザに配信できるようにします。インストール、有効化、およびバンドル作成の詳細については、"[AgentのAMIまたはWorkSpaceバンドルへの統合" on page 393](#)を参照してください。

3. Amazon WorkSpacesの権限を含むようにIAMポリシーを変更します。
 - a. Deep Security Managerに追加したアカウントを使ってAWSにログインします。
 - b. [IAM] サービスに移動します。
 - c. Deep SecurityIAMポリシーを探します。これは、左側の [ポリシー] の下か、ポリシーを参照するDeep Security IAMロールまたはIAMユーザを探してからその中のポリシーをクリックすると見つかります。
 - d. ["AWSクラウドアカウントの追加" on page 516](#)で示されているようにDeep Security IAMポリシーを変更します。このポリシーには、Amazon WorkSpacesの権限が含まれます。複数のAWSアカウントをDeep Securityに追加した場合は、すべてのAWSアカウントでIAMポリシーをアップデートする必要があります。
4. Deep Security Managerで、AWSアカウントを編集します。
 - a. 左側でAWSアカウントを右クリックし、[プロパティ] を選択します。
 - b. [Amazon WorkSpacesを含める] を有効にします。
 - c. [保存] をクリックします。

これで、Amazon WorkSpacesがDeep Securityに追加されました。

Amazon WorkSpacesを保護する (AWSアカウントをまだ追加していない場合)

AWSアカウントをDeep Security Managerにまだ追加していない場合は、次のセクションのいずれかの手順を実行します。

- 既存のAmazon WorkSpacesを保護する場合、["Amazon EC2およびWorkSpacesへのAgentのインストール" on page 387](#)を参照してください。
- Agentが「統合」されている新しいAmazon WorkSpacesを起動できるようにするには、["AgentのAMIまたはWorkSpaceバンドルへの統合" on page 393](#)を参照してください。

新しいクラウドコネクタ機能への移行方法

以前に [クラウドアカウントの追加] ウィザードを使用してAmazon Web ServicesリソースをDeep Security Managerにインポートした場合、[コンピュータ] タブではそれらのリソースがAWSリージョン別に表示されます。AWSリージョンが複数ある場合は、2回以上ウィザードを実行している可能性があります。

最新バージョンのDeep Securityでは、AWSインスタンスをAWSアカウント名の下にまとめ、AWSリージョン、VPC、およびサブネットを含む階層に整理して表示できるようになりました。

AWSリソースを移行する前に、Deep SecurityからAWSアカウントへのアクセスを許可するポリシーを編集する必要があります。

1. AWSマネジメントコンソールにログインし、[Identity and Access Management (IAM)]に移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。
3. ポリシーのリストで、Deep SecurityからAWSアカウントへのアクセスを許可するポリシーを選択します。
4. [Policy Document] タブに移動し、[Edit] をクリックします。
5. ポリシードキュメントを編集し、次のJSONコードを追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "iam:ListAccountAliases",
        "sts:AssumeRole"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

注意:「sts:AssumeRole」権限は、クロスアカウントロールアクセスを使用している場合にのみ必要です。IAMロールの詳細については、[「チュートリアル: AWS アカウント間の IAM ロールを使用したアクセスの委任」](#)を参照してください。

6. [Save as default version] を選択します。

Deep Security ManagerのAWSリソースを移行するには

1. Deep Security Managerで、[コンピュータ] 画面に進みます。
2. [コンピュータ] ツリーでAWSリージョンを右クリックし、[Amazonアカウントにアップグレード] を選択します。

3. [完了] をクリックし、[閉じる] をクリックします。これで、AWSインスタンスがAWSアカウント名の下にまとめられ、AWSリージョン、VPC、およびサブネットを含む階層に整理して表示されるようになります。

Deep SecurityへのMicrosoft Azureアカウントの追加

ヒント: [Deep Security 12 - Scoping Environment Pt](#)を見ることができます。 [1 - YouTubeのワークロード](#) を特定して、環境を特定する際の検討事項を確認します。具体的には、ワークロードの特定に関連しています。

Deep Security Managerでは、Microsoft AzureアカウントをDeep Security Managerに接続することで、Microsoft Azure仮想マシンの追加および保護ができます。仮想マシンは[コンピュータ]画面に表示され、その他のコンピュータと同じように管理できます。

このセクションのトピック:

- "Azureアカウントを追加することのメリットは何ですか?" below
- "Azureアカウントのプロキシを設定する" on the next page
- "Microsoft AzureアカウントからDeep Securityに仮想マシンを追加する" on the next page
- "Azure Resource Managerコネクタを使用してAzureクラシック仮想マシンを管理する" on page 541
- "Azureアカウントを削除する" on page 541
- "Azureアカウントを同期する" on page 542

Azureアカウントを追加することのメリットは何ですか？

個別のAzure仮想マシンを（Deep Security Manager> コンピュータ>コンピュータの）、を追加することで追加するのではなく、Azureアカウントを（Deep Security Manager> コンピュータ> Azureアカウントの追加を使用して）追加することの利点は次のとおりです。

- Azure仮想マシンインベントリの変更は、自動的にDeep Security Managerに反映されません。たとえば、Azureでいくつかのインスタンスを削除すると、それらのインスタンスは自動的にマネージャから消えます。対照的に、の[コンピュータ]→[コンピュータの追加]を使用している場合、Azureから削除されたAzureインスタンスは、手動で削除されるまでManagerに残ります。

- 仮想マシンはマネージャで独自のブランチに編成されており、どのAzureインスタンスが保護されており、保護されていないかを簡単に確認できます。Azureアカウントがないと、すべての仮想マシンが Computersの同じルートレベルに表示されます。

Azureアカウントのプロキシを設定する

Azureアカウントのリソースへのアクセスに[プロキシサーバを使用](#)するよう、Deep Security Managerを設定できます。

1. [管理]→[システム設定]→[プロキシ]の順に選択します。
2. [プロキシサーバの使用] セクションで [Deep Security Manager (クラウドアカウント - HTTPプロトコルのみ)] リストからプロキシを選択します。

Microsoft AzureアカウントからDeep Securityに仮想マシンを追加する

以下の手順に従って、Microsoft AzureアカウントをDeep Securityに追加します。

1. 開始する前に、[Deep Security用のAzureアプリケーションを作成](#)します。
2. Deep Security Managerで、[コンピュータ]→[追加]→[Azureアカウントの追加] に移動します。

注意: Deep Security Manager 12.0以降では、「クイック」モードを利用できなくなりました。詳細については、「[新機能](#)」 on page 85を参照してください。

3. [表示名] を入力したら、手順1で記録した次のAzureアクセス情報を入力します。
 - Active Directory ID
 - サブスクリプションID
 - アプリケーションID
 - アプリケーションパスワード

注意: AzureクラシックコネクタからAzure Resource Managerコネクタにアップグレードする場合は、既存のコネクタの表示名とサブスクリプションIDが使用されます。

注意: Azureサブスクリプションが複数ある場合は、[サブスクリプションID] フィールドで1つだけサブスクリプションを指定します。残りは後から追加できます。

4. [次へ] をクリックします。
5. 概要情報を確認し、[完了] をクリックします。
6. 毎回異なるサブスクリプションIDを指定して、Azureサブスクリプションごとにこの手順を繰り返します。

Azure仮想マシンが、Deep Security Managerの [コンピュータ] 画面に、それぞれ別個の項目として表示されます。

ヒント: Azureアカウント名を右クリックし、[同期する]をクリックして、Azure VMの最新セットを確認できます。

ヒント: このアカウントに含まれるすべての仮想マシンが表示されます。特定の仮想マシンのみを表示する場合は、スマートフォルダを使用して結果を絞り込みます。詳細については、"[スマートフォルダによるコンピュータの動的なグループ化](#)" on page 1427を参照してください。

注意: 以前このAzureアカウントで仮想マシンを追加したことがある場合は、[コンピュータ] ツリーのこのアカウントの下に仮想マシンが移動します。

Azure Resource Managerコネクタを使用してAzureクラシック仮想マシンを管理する

Azure Resource Managerコネクタでは、Azureクラシックコネクタを使用して追加した仮想マシンも管理できます。このため、1つのコネクタでAzureクラシック仮想マシンとAzure Resource Manager仮想マシンの両方を管理することが可能です。

詳細については、"[新しいAzure Resource Manager接続機能へのアップグレードについて](#)" on page 545を参照してください。

1. [コンピュータ] 画面で、[コンピュータ] ツリーの [Azureクラシックポータル] を右クリックし、[プロパティ] をクリックします。
2. [Resource Manager接続を有効化] をクリックします。
3. [次へ] をクリックします。該当する前述の手順に従います。

Azureアカウントを削除する

AzureアカウントをDeep Security Managerから削除すると、そのアカウントはDeep Securityのデータベースから削除されます。これによるAzureアカウントへの影響はありません。Deep Security Agentがインストールされた仮想マシンは引き続き保護されますが、セキュリティアップデートは受信しません。後で同じAzureアカウントからこれらの仮想マシンをインポートすると、Deep Security Agentによって、次回の予約アップデート時に最新のセキュリティアップデートがダウンロードされます。

1. [コンピュータ] 画面を開き、ナビゲーションパネルでMicrosoft Azureアカウントを右クリックし、[クラウドアカウントの削除...] を選択します。

2. アカウントを削除することを確認します。
3. アカウントがDeep Security Managerから削除されます。

Azureアカウントを同期する

Azureアカウントを同期（同期）すると、Deep Security ManagerはAzure APIに接続し、Azure VMの最新のセットを取得して表示します。

強制的に同期を強制するには

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 左側でAzureアカウントを右クリックし、[同期する]を選択します。[]をクリックします。

10分ごとに発生するバックグラウンド同期もあり、この間隔は設定できません。同期を強制すると、バックグラウンドの同期は影響を受けず、元のスケジュールに従って引き続き実行されます。

Deep Security用のAzureアプリケーションの作成

ご使用の動作環境で、Azure Active Directoryのグローバル管理者ロールとAzureサブスクリプションのサブスクリプション所有者ロールの両方が指定されたアカウントを使用して、Deep Security ManagerがAzureリソースにアクセスできるようにすることが適していない場合があります。その代わりにとして、Azureリソースへの読み取り専用アクセスが可能なDeep Security Manager用のAzureアプリケーションを作成できます。

ヒント: Azureサブスクリプションが複数あり、すべてのサブスクリプションが同じActive Directoryに関連付けられている場合は、すべてのサブスクリプションで利用できる単一のDeep Security Azureアプリケーションを作成できます。詳細については、以下の手順を参照してください。

Azureアプリケーションを作成するには、次の手順を実行する必要があります。

1. ["適切な役割を割り当てる"](#) on the next page。
2. ["Azureアプリケーションを作成する"](#) on the next page。
3. ["AzureアプリケーションID、Active Directory ID、およびパスワードを記録する"](#) on the next page。
4. ["サブスクリプションIDを記録する"](#) on page 544。
5. ["Azureアプリケーションに役割とコネクタを割り当てる"](#) on page 544。

適切な役割を割り当てる

Azureアプリケーションを作成するには、Azure Active Directoryのユーザ管理者ロールとAzureサブスクリプションのユーザアクセス管理者ロールがアカウントに割り当てられている必要があります。先に進む前に、これらの役割をAzureアカウントに割り当ててください。

Azureアプリケーションを作成する

1. [Azure Active Directory] ブレードで、[App registrations] をクリックします。
2. [New registration] をクリックします。
3. [Name] (Deep Security Azureコネクタなど) を入力します。
4. [Supported account types] で、[Accounts in this organizational directory only] を選択します。
5. [Register] をクリックします。

[App registrations] リストに、上記の手順3で選択した[Name]と共にAzureアプリケーションが表示されます。

AzureアプリケーションID、Active Directory ID、およびパスワードを記録する

1. [App registrations] リストで、Azureアプリケーションをクリックします。

注意: "Azureアプリケーションを作成する" [above](#)の手順3で選択した[Name]と共に、Azureアプリケーションが表示されます。

2. [Application (client) ID] を記録します。
3. [Active Directory ID] を記録します。
4. [Certificates & secrets] をクリックします。
5. [New client secret] をクリックします。
6. クライアントシークレットの[Description]を入力します。
7. 適切な [Duration] を選択します。この時間が経過すると、クライアントシークレットが期限切れになります。
8. [Add] をクリックします。

クライアントシークレットの[Value]が表示されます。

9. クライアントシークレットの[Value]を記録します。これは、AzureアプリケーションをDeep Securityに登録する際にアプリケーションパスワードとして使用されます。

警告: クライアントシークレットの値は一度しか表示されないため、この時点で必ず記録してください。ここで記録しておかないと、後でクライアントシークレットを再生成して新しい値を取得することが必要になります。

注意: クライアントシークレットの値が期限切れになった場合は、再生成して、古い値が関連付けられているAzureアカウントで値を更新する必要があります。

サブスクリプションIDを記録する

1. 左側の [All Services] に移動し、 [Subscriptions] をクリックします。
サブスクリプションのリストが表示されます。
2. Azureアプリケーションに関連付ける各サブスクリプションの [Subscription ID] を記録します。このIDは、後でAzureアカウントをDeep Securityに追加するときに必要になります。

Azureアプリケーションに役割とコネクタを割り当てる

1. [All Services]→[Subscriptions] で、Azureアプリケーションに関連付けるサブスクリプションをクリックします。

注意: 必要な場合は、後で別のサブスクリプションをAzureアプリケーションに関連付けることもできます。

2. [Access Control (IAM)] をクリックします。
3. メイン画面で、 [Add] をクリックし、ドロップダウンメニューから [Add Role Assignment] を選択します。
4. [Role] で「Reader」と入力し、表示される [Reader] ロールをクリックします。
5. [Assign access to] で、 [Azure AD user, user group, or service principal] を選択します。
6. [Select] で、Azureアプリケーションの[Name] (Deep Security Azure Connectorなど) を入力します。

"[Azureアプリケーションを作成する](#)" on the previous pageの手順3で選択した[Name]と共に、Azureアプリケーションが表示されます。

7. [Save] をクリックします。
8. Azureアプリケーションを別のサブスクリプションに関連付ける場合は、そのサブスクリプションに対してこの手順 ("[Azureアプリケーションに役割とコネクタを割り当てる](#)" above) を繰り返します。

この時点で、"[Deep SecurityへのMicrosoft Azureアカウントの追加](#)" on page 539の手順に従うことにより、Deep Securityを設定してAzure仮想マシンを追加できるようになります。

新しいAzure Resource Manager接続機能へのアップグレードについて

Deep Security ManagerにAzureクラウドアカウントを追加しようとする、新しいResource Manager接続機能へのアップグレードを推奨するメッセージが表示されます。この新しい機能を使用すると、簡単に言えば、Deep SecurityからAzure仮想マシンにResource Managerインタフェースを使用して接続できるようになります。Azureユーザには周知のことですが、Azureの初期設定のデプロイモデルは、クラシックモデルから新しいResource Managerに変更になっています。新しいリソースは初期設定でこのモデルを使用してデプロイされるため、Deep SecurityがResource Managerインタフェースと通信できない場合、[コンピュータ] ページには新しいモデルでデプロイされた仮想マシンリソースが表示されません。新しい機能にアップグレードすることで、Resource Managerデプロイモデルとクラシックデプロイモデルのどちらでデプロイされた仮想マシンリソースも、Deep Securityの [コンピュータ] ページに表示されるようになります。

- この機能は、新しい Deep Security Manager VM for Azure Marketplace コンソールです。すでに使用でき、アップグレードは必要ありません。
- このアップグレードを実行しなくても、Resource Managerを使用してデプロイされた仮想マシンは引き続きDeep Securityで保護されますが、コンピュータオブジェクトとして追加しないと [コンピュータ] ページには表示されません。詳細については、"[Deep SecurityでAzureサブスクリプションの一部の仮想マシンが表示されない](#)" on page 1540 を参照してください。

VMware vCloudでホストされる仮想マシンの追加

ヒント: [Deep Security 12 - Scoping Environment Pt](#)を見ることができます。 [1 - YouTubeのワークロード](#) を特定して、環境のスコープを決定する際の検討事項を確認してください。

クラウドプロバイダのアカウントからDeep Security Managerにリソースをインポート後、アカウント内のコンピュータをローカルネットワーク内の他のコンピュータと同じように管理できます。

クラウドリソースを Deep Security Managerにインポートするには、まず Deep Security ユーザがクラウドプロバイダサービスリソースにアクセスするためのアカウントを持っている必要があります。トレンドマイクロでは、Deep Security Managerにクラウドアカウントをインポートする各Deep Securityユーザに対して、Deep Security Managerがクラウドリソースにアクセスするための専用アカウントを作成することを推奨します。つまり、ユーザには、仮想マシンへのアクセスと制御に使用する単一のアカウントと、Deep Security Managerがそれらのリソースに接続するための個別のアカウントを作成します。

注意: Deep Security専用のアカウントがあると、いつでも権限を詳細に設定したり、このアカウントを無効にしたりできます。Deep Securityでは、常に読み取り専用のアクセスキーまたは秘密鍵を使用することが推奨されます。

注意: Deep Security Managerでは、クラウドのリソースをインポートし、セキュリティを管理する場合、読み取り専用アクセスだけが必要です。

注意: FIPSモードを有効にした場合は、VMware vCloudでホストされる仮想マシンを追加できません。"[FIPS 140-2のサポート](#)" on page 1457を参照してください。Azureアカウントを追加することのメリットは何ですか？

このセクションのトピック:

- "[vCloudアカウントを追加することのメリットは何ですか。](#)" below
- "[クラウドアカウント用のプロキシ設定](#)" on the next page
- "[Manager用のVMware vCloud Organizationアカウントを作成する](#)" on the next page
- "[VMware vCloud Organizationアカウントからコンピュータをインポートする](#)" on page 548
- "[VMware vCloud Airデータセンターからコンピュータをインポートする](#)" on page 548
- "[クラウドアカウントのソフトウェアアップデートを設定する](#)" on page 549
- "[クラウドアカウントを削除する](#)" on page 549

vCloudアカウントを追加することのメリットは何ですか。

個々のvCloudリソースを（Deep Security Manager> コンピュータ>コンピュータの）、を追加することで追加するのではなく、vCloudアカウントを（Deep Security Manager> コンピュータ> Azureアカウントの追加を使用して）追加すると、次の利点があります。

- クラウドリソースインベントリの変更は、自動的にDeep Security Managerに反映されません。たとえば、vSphereから多数のインスタンスを削除すると、それらのインスタンスは自動的にマネージャから非表示になります。対照的に、[コンピュータ]→[コンピュータの追加]を使用する場合、vCenterから削除されたクラウドインスタンスは手動で削除されるまでマネージャに表示されたままです。
- クラウドリソースは、マネージャで独自のブランチに編成されているため、保護対象リソースと保護対象リソースを簡単に確認できます。vCloudアカウントがないと、クラウドリソースはすべて Computersの同じルートレベルに表示されます。

クラウドアカウント用のプロキシ設定

クラウドアカウントで保護されているインスタンスへの接続にプロキシサーバを使用するよう、Deep Security Managerを設定できます。プロキシ設定は、[管理]→[システム設定]→[プロキシ]→[プロキシサーバの使用]→[Deep Security Manager (クラウドアカウント - HTTPプロトコルのみ)]で行います。

Manager用のVMware vCloud Organizationアカウントを作成する

1. VMware vCloud Directorにログインします。
2. [System] タブで、[Manage And Monitor] に移動します。
3. 左側のナビゲーションペインで [Organizations] をクリックします。
4. Deep Securityのユーザにアクセス権を付与する組織をダブルクリックします。
5. [Organizations] タブで [Administration] をクリックします。
6. 左側のナビゲーションペインで [Members]→[Users] の順にクリックします。
7. 「プラス」記号 (+) をクリックして新しいユーザを作成します。
8. 新しいユーザの資格情報などの情報を入力し、ユーザの [Role] で [Organization Administrator] を選択します。

注意: [Organization Administrator] は、新しいユーザアカウントに割り当て可能な定義済みのシンプルなロールです。ただし、アカウントに必要な権限は [All Rights]→[General]→[Administrator View] のみなので、この権限のみを付与した新しいvCloudロールの作成を検討してください。Deep SecurityでvCloudのリソースを使用する方法の詳細については、"[vCloud環境でのAgentレスによる保護の実施](#)" on page 354を参照してください。

9. [OK] をクリックしてユーザのプロパティ画面を閉じます。

これで、Deep Security ManagerからvCloudアカウントにアクセスする準備は完了です。

注意:

VMware vCloudリソースを Deep Security Managerにインポートするには、vCloudのアドレス、ユーザ名、およびパスワードの入力を求めるメッセージが表示されます。

ユーザ名に "@を含める必要があります。orgName"。たとえば、vCloudアカウントのユーザ名が kevin で、アカウントへのアクセス権を付与したvCloud Organizationの名前が CloudOrgOneの場合、vCloudリソースをインポートする際に、 kevin @ CloudOrgOne をユーザ名として入力する必要があります。

(vCloud管理者の場合、@systemを使用します)。

VMware vCloud Organizationアカウントからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ]に進みます。
2. ナビゲーションパネルで[コンピュータ]を右クリックし、[vCloudアカウントの追加]を選択してvCloudアカウント追加ウィザードを開きます。
3. [名前]と[説明]に、追加するリソースを入力します。(Deep Security Managerでの表示に使用されます)。
4. [アドレス]に、vCloud Directorのホスト名とアドレスを入力します。
5. [ユーザ名]と[パスワード]に、vCloudの認証資格情報を入力します。ユーザ名は、username@vcloudorganizationの形式で指定する必要があります。
6. [次へ]をクリックします。
7. Deep Security Managerによってクラウドリソースへの接続が確認され、インポート処理の概要が表示されます。[完了]をクリックします。

VMware vCloudのリソースが、Deep Security Managerの[コンピュータ]に、それぞれ別個の項目として表示されます。

VMware vCloud Airデータセンターからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ]セクションに移動し、ナビゲーションパネルで[コンピュータ]を右クリックし、[vCloudアカウントの追加]を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するvCloud Airデータセンターの名前と説明を入力します(Dep Security Managerでの表示に使用されます)。
3. vCloud Airデータセンターのアドレスを入力します。

vCloud Airデータセンターのアドレスを確認するには、次の手順を実行します。

- a. vCloud Airポータルにログインします。
 - b. [ダッシュボード][]タブで、Deep Securityにインポートするデータセンターをクリックします。仮想データセンターの詳細情報ページが表示されます。
 - c. 仮想データセンターの詳細ページの[関連リンク]セクションで、[vCloud Director API URL]をクリックします。vCloud Director APIの完全なURLが表示されます。
 - d. ホスト名のみ(フルURLではなく)をDeep SecurityにインポートするvCloud Airデータセンターのアドレスとして使用します。
4. [ユーザ名]と[パスワード]に、仮想データセンターの資格情報を入力します。ユーザ名は、「username@virtualdatacenterid」の形式で指定する必要があります。
 5. [次へ]をクリックします。
 6. Deep SecurityvCloud Airデータセンターへの接続が確認され、インポート処理の概要が表示されます。[完了]をクリックします。

VMware vCloud Airデータセンターが、Deep Security Managerの [コンピュータ] に、それぞれ別個の項目として表示されます。

クラウドアカウントのソフトウェアアップデートを設定する

RelayはDeep Security Agentのモジュールで、セキュリティアップデートやソフトウェアアップデートのダウンロードおよび配布を行います。通常、新しいアップデートが入手可能になるとDeep Security ManagerからRelayに通知され、Relayがアップデートを取得して、AgentがRelayからアップデートを取得します。

ただし、Deep Security Managerがエンタープライズ環境にあり、クラウド環境でコンピュータを管理している場合は、クラウドのRelayがDeep Security Managerと通信できないことがあります。Deep Security Managerに接続できない場合は、解決策としてソフトウェアアップデートをトレンドマイクロのダウンロードセンターから直接取得できるようにRelayを設定できます。このオプションを有効にするには、[管理]→[システム設定]→[アップデート]の順に選択し、[ソフトウェアアップデート]で[Deep Security Managerにアクセスできない場合、トレンドマイクロのダウンロードセンターからのソフトウェアアップデートのダウンロードをRelayに許可]を選択します。

クラウドアカウントを削除する

クラウドプロバイダアカウントをDeep Security Managerから削除すると、そのアカウントはDeep Securityのデータベースから削除されます。クラウドプロバイダのアカウントに影響はありません。また、インスタンスにインストールされていたDeep Security Agentはアンインストールされず、実行と保護が継続します(ただしセキュリティアップデートは受信しなくなります)。クラウドプロバイダアカウントからコンピュータを再インポートすると、Deep Security Agentによって、次回の予約時に最新のセキュリティアップデートがダウンロードされます。

1. [Computers]画面に移動し、ナビゲーションパネルでCloud Providerアカウントを右クリックして、[Cloud Accountを削除]を選択します。
2. アカウントを削除することを確認します。
3. アカウントがDeep Security Managerから削除されます。

Microsoft Active Directoryからのコンピュータグループの追加

Deep Securityでは、Microsoft Active DirectoryなどのLDAPサーバを使用してコンピュータを検出し、ユーザアカウントやその連絡先を作成できます。Deep Security Managerがサーバから検出したコンピュータグループがディレクトリの構造に従って表示されます。

注意: FIPSモードでDeep Securityを使用している場合は、Active DirectoryのSSL証明書をDeep Security ManagerにインポートしてからManagerとディレクトリを接続する必要があります。["信頼された証明書の管理" on page 424](#)を参照してください。

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. メイン画面で、[追加]→[Active Directoryの追加] の順にクリックします。
3. Active Directoryサーバのホスト名またはIPアドレス、名前、説明、およびポート番号を入力します。アクセス方法と資格情報も入力します。次のガイドラインに従います。
 - アクセス方法がLDAPSである場合、[サーバのアドレス] は、Active DirectoryのSSL証明書で使用されている共通名 (CN) と一致している必要があります。
 - [名前] はActive Directoryのディレクトリ名と一致していなくてもかまいません。
 - [サーバのポート] は、[Active DirectoryのLDAPポートまたはLDAPSポート](#)です。初期設定は389 (LDAPおよびStartTLS) および636 (LDAPS) です。
 - [ユーザ名] にはドメイン名が含まれている必要があります。
例:EXAMPLE/Administrator
 - FIPSモードでDeep Securityを使用している場合は、[信頼された証明書] セクションの [接続テスト] をクリックして、Active DirectoryのSSL証明書がDeep Security Managerに正常にインポートされたかどうかを確認します。

[次へ] をクリックして続行します。

4. ディレクトリのスキーマを指定します。スキーマをカスタマイズしていない場合は、Microsoft Active Directoryサーバの初期設定値のままかまいません。

注意: Deep Security Managerでは、各コンピュータの [詳細] 画面に [説明] フィールドがあります。Active Directoryの「コンピュータ」オブジェクトクラスの属性を使用して [説明] フィールドに入力するには、[コンピュータの詳細の属性] テキストボックスに属性名を入力します。

Deep Security Managerのディレクトリ構造とActive Directoryサーバとの同期を自動的に維持する場合は、[このディレクトリとの同期をとる予約タスクの作成] を選択します。ディレクトリの追加が完了すると、予約タスクウィザードが表示されます。(この設定は、予約タスクウィザード ([管理]→[予約タスク]) を使用して後から行うことができます)。

5. [次へ] をクリックして続行します。
6. Managerによるディレクトリのインポートが完了すると、追加されたコンピュータの

ストが表示されます。[完了]をクリックします。

[コンピュータ]画面にディレクトリ構造が表示されます。

Active Directoryのその他のオプション

Active Directory構造を右クリックすると、次のオプションが表示されます。これらのオプションは、ディレクトリ以外のコンピュータグループには使用できません。

- ディレクトリの削除
- 今すぐ同期

ディレクトリの削除

Deep Security Managerからディレクトリを削除するときは、次のオプションを使用できません。

- ディレクトリおよびすべての下位コンピュータ/グループをDeep Security Managerから削除します: ディレクトリのデータをすべて削除します。
- ディレクトリを削除しますが、コンピュータのデータおよびグループの階層は維持します: インポートされたディレクトリ構造を、同じ構成の通常のコンピュータグループに変換します。Active Directoryサーバとのリンクは解除されます。
- ディレクトリを削除し、コンピュータのデータを維持しますが、グループの階層は削除します: Active Directoryサーバへのリンクを削除し、ディレクトリ構造を破棄し、すべてのコンピュータを同じコンピュータグループに配置します。

今すぐ同期

Deep Security ManagerとActive Directoryサーバとの同期を手動で開始して、コンピュータグループの情報を更新することができます。

ヒント: この処理は、予約タスクを作成して自動化できます。

サーバ証明書を使用する

Active DirectoryサーバでSSLを有効にしていない場合は有効にします。

コンピュータの検出にはSSL/TLSまたは暗号化されていないクリアテキストを使用できますが、ユーザアカウント (パスワードや連絡先を含む) のインポートには認証とSSL/TLSが必要です。

SSL/TLS接続には、Active Directoryサーバのサーバ証明書が必要です。SSL/TLSのハンドシェイクで、この証明書がサーバを証明する識別情報としてサーバからクライアントに渡されます。この証明書には、自己署名証明書または認証局 (CA) が署名した証明書を使用できます。サーバに証明書があるかどうかを確認するには、Active DirectoryサーバでInternet Information Services (IIS) Managerを開いて、[サーバー証明書] を選択します。サーバに署名入りのサーバ証明書がない場合はインストールする必要があります。

ユーザおよび連絡先をインポートする

Deep Securityでは、Active Directoryからユーザアカウント情報をインポートして、対応するDeep Securityのユーザまたは連絡先を作成できます。この機能には次の利点があります。

- ユーザはActive Directoryで定義されたネットワークパスワードを使用できる。
- 管理者は、Active Directory内からアカウントを集中的に削除できます。
- Active Directory内の既存情報を利用できるため、連絡先情報 (メール、電話番号など) の保守が簡単になる。

ユーザと連絡先の両方をActive Directoryからインポートできます。ユーザにはDeep Security Managerの設定権限が付与されます。連絡先はDeep Security Managerの通知のみ受信することができます。同期ウィザードを使用すると、ユーザとしてインポートするActive Directoryオブジェクトと、連絡先としてインポートするActive Directoryオブジェクトを選択できます。

注意: Active DirectoryのユーザアカウントをDeep Securityのユーザまたは連絡先としてDeep Securityにインポートするには、Active Directoryのユーザアカウントに属性値userPrincipalNameが設定されている必要があります(userPrincipalName属性は、Active Directoryのアカウント所有者の「ユーザログオン名」に相当します)。

1. [管理]→[ユーザ管理] の順にクリックし、[ユーザ] または [連絡先] をクリックします。
2. [ディレクトリとの同期] をクリックします。
ユーザまたは連絡先情報をはじめてインポートする場合は、サーバ情報の画面が表示されます。それ以外の場合は、ディレクトリとの同期ウィザードが表示されます。
3. 適切なアクセスオプションを選択し、ログオン資格情報を入力して、[次へ] をクリックします。
4. 同期するグループを左の列から選択し、[>>] をクリックして右の列に追加し、[次へ] をクリックします。

ヒント: 複数のグループを選択するには、<Shift> または <Ctrl> キーを押しながらグループをクリックします。

5. ディレクトリグループのすべてのメンバーにDeep Securityの同じ役割を割り当てるかディレクトリグループのメンバーシップに基づいてDeep Securityの役割を割り当てるかを選択し、初期設定の役割をリストから選択して、[次へ]をクリックします。
6. ディレクトリグループのメンバーシップに基づいてDeep Securityの役割を割り当てた場合は、各グループの同期オプションを指定し、[次へ]をクリックします。

同期後、インポートしたオブジェクト数を示すレポートが生成されます。

ヒント: 同期が完了する前に、ユーザおよび連絡先を定期的に同期する予約タスクを作成することもできます。

7. [完了]をクリックします。

インポートしたアカウントは一般情報を変更できないため、本来の(インポートしていない)Deep Securityアカウントと簡単に区別することができます。

Active Directoryオブジェクトの同期を維持する

一度インポートしたActive Directoryオブジェクトは、Active Directoryサーバと継続的に同期して、最新のアップデートを反映させる必要があります。その結果、たとえばActive Directoryでコンピュータを削除した場合、Deep Security Managerでも該当するコンピュータが削除されます。Deep Security ManagerにインポートされたActive Directoryオブジェクトが引き続きActive Directoryと同期されるようにするには、Active Directoryのデータを同期する予約タスクを設定することが必要です。コンピュータのインポートウィザードには、これらの予約タスクを作成するためのオプションが用意されています。

このタスクは予約タスクウィザードを使用して作成することもできます。必要に応じて同期を実行するには、コンピュータの場合は[今すぐ同期] オプションを使用し、ユーザおよび連絡先の場合は[ディレクトリとの同期] ボタンを使用します。

注意: 必ずしもユーザおよび連絡先の同期を維持するための予約タスクを作成する必要はありません。Deep Security Managerへのログイン時に、ユーザがActive Directoryに存在するかどうかを確認されます。ユーザ名とパスワードが有効で、ユーザが所属するグループで同期が有効になっていれば、そのユーザはDeep Security Managerに追加されてログインが許可されます。

注意: Active Directory内のアカウントを無効にしても、削除しないと、そのユーザはDeep Security Managerに表示され、アクティブになります。

Active Directoryとの同期を無効にする

コンピュータグループとユーザアカウントの両方について、Deep Security ManagerとActive Directoryとの同期を中止できます。

Active Directoryとの同期からコンピュータグループを削除する

1. [コンピュータ] に移動します。
2. ディレクトリを右クリックし、[ディレクトリの削除] を選択します。
3. Deep Security Managerとの同期が中断された場合に、このディレクトリのコンピュータのリストをどのように処理するかを次の中から選択します。
 - ディレクトリおよびすべての下位コンピュータ/グループをDeep Security Managerから削除します: このディレクトリ構造を削除します。
 - ディレクトリを削除しますが、コンピュータのデータおよびグループの階層は維持します: フォルダやコンピュータに対するユーザおよび役割ごとのアクセス権限を含む、既存の構造を維持します。
 - ディレクトリを削除し、コンピュータのデータを維持しますが、グループの階層は削除します: ディレクトリにちなんだ名前を持つグループ内のフラットなコンピュータのリストにディレクトリ構造を変換します。新しいコンピュータグループでは、以前の構造と同じユーザおよび役割ごとのアクセス権限が維持されます。
4. 確認して処理を開始します。

Active Directoryのユーザおよび連絡先を削除する

コンピュータグループのディレクトリを削除する場合とは異なり、ユーザおよび連絡先を削除すると、該当するすべてのアカウントがDeep Security Managerから削除されます。そのため、ディレクトリサーバからインポートしたユーザアカウントでDeep Security Managerにログインしているときは削除することはできません。この処理を実行すると、エラーが表示されます。

1. [ユーザ] または [連絡先] で [ディレクトリとの同期] をクリックします。
2. [同期を中止する] を選択して、[OK] をクリックします。
3. [完了] をクリックします。

Dockerコンテナの保護

Docker環境の導入にはメリットがあるのはもちろんですが、同時にDockerホストのOS自体が攻撃の対象になることに注意が必要です。他のソフトウェアの導入同様に、OSの強化や環境に

応じたベストプラクティス ([Center for Internet Security \(CIS\) のDocker Benchmark](#)など) を利用することで、最初に強固な基盤を構築することが重要になります。安全な基盤を構築したら、環境にDeep Securityを追加して、物理、仮想、およびクラウドのワークロードを保護するトレンドマイクロの豊富な経験や、[Trend Micro Smart Protection Network](#)のリアルタイムの脅威情報を活用できます。Deep Securityは、環境の保護だけでなく、継続的なコンプライアンス要件への対応と維持にも役立ちます。サポート対象のDockerのエディションとリリースについては、"[Deep Security Agentのプラットフォーム](#)" on page 182を参照してください。

Deep Securityは、Linuxディストリビューションで実行されるDockerホストおよびコンテナに対して保護を提供します。Deep Securityでは次のことが可能です。

- [アイコン](#)と[スマートフォルダ](#)により、環境内のDockerホストを特定、検索、および保護する
- 新たに見つかった脆弱性に対して仮想パッチを適用することで、Dockerホストおよびコンテナを[脆弱性に対する既知またはゼロデイの攻撃コードから保護](#)する
- Dockerホスト上およびコンテナ内で使用されているファイルシステムに対する[リアルタイムの不正プログラム検出](#)を提供する
- 次の手法を使用して、継続的なコンプライアンスの維持と環境の保護のためにDockerホストの変更をアサートする
 - Dockerデーモンに加えて[実行を許可するアプリケーションを制御](#)することで、Dockerホストでのアプリケーションの不正な実行を防御する
 - Dockerホストの[システムファイルに対して予想外の変更](#)が発生しないように監視する
 - [OSログの不審なイベントを通知](#)する

注意: Deep SecurityによるDockerの保護は、OSレベルで動作します。そのため、Deep Security Agentはコンテナ内ではなく、DockerホストのOSにインストールする必要があります。

注意: ポッド内のコンテナ間の通信はサポートされていません。

Deep Security 10.1以降、Deep Securityはオーバーレイネットワークを使用しながらswarmモードでDockerをサポートします。

Deep SecurityによるDockerホストの保護

Dockerホストの保護には、次のDeep Securityモジュールを使用できます。

- 侵入防御 (IPS)
- 不正プログラム対策
- 変更監視
- セキュリティログ監視
- アプリケーションコントロール
- ファイアウォール
- Webレピュテーション

Deep SecurityによるDockerコンテナの保護

Dockerコンテナの保護には、次のDeep Securityモジュールを使用できます。

- 侵入防御
- 不正プログラム対策

侵入防御の推奨検索に関する制限事項

Deep Securityの侵入防御はホストレベルで動作しますが、公開されたコンテナポート番号のコンテナトラフィックも保護されます。Dockerでは複数のアプリケーションを同じDockerホスト上で実行できるため、単一の侵入防御ポリシーがすべてのDockerアプリケーションに適用されます。そのため、推奨設定の検索はDocker環境に対しては推奨されません。

コンピュータおよびAgentのステータス

Deep Security Managerの [コンピュータ] 画面:

- [ステータス] 列にはコンピュータのネットワーク接続の状態が表示され、保護を提供するAgentまたはApplianceが存在する場合は、その状態がカッコ内に表示されます。[ステータス] 列には、システムイベントやAgentイベントも表示されることがあります。"[\[ステータス\] 列 - コンピュータの状態](#)" on the next pageと"[\[ステータス\] 列 - AgentまたはApplianceの状態](#)" on the next pageを参照してください。
- [タスク] 列にはタスクの状態が表示されます。"[\[タスク\] 列](#)" on page 558を参照してください。

イベントのリストについては、"[Agentイベント](#)" on page 1265と"[システムイベント](#)" on page 1271を参照してください。

その他の情報:

- "コンピュータのエラー" on page 562
- "保護モジュールのステータス" on page 563
- "コンピュータでその他の処理を実行する" on page 564
- "コンピュータのアイコン" on page 570
- "各種コンピュータのステータス情報" on page 571

[ステータス] 列 - コンピュータの状態

ステータス	説明
有効化済み	AgentまたはApplianceは有効化されています。"コンピュータでその他の処理を実行する" on page 564を参照してください。
検出済み	検出処理によって、コンピュータがコンピュータリストに追加されました。("コンピュータを検出する" on page 510を参照してください)。
オフラインのFilter Driver	ESXiのFilter Driverがオフラインです。
管理対象	Agentが存在して有効化されており、保留中の処理やエラーはありません。
複数のエラー	このコンピュータで複数のエラーが発生しています。詳細については、コンピュータのシステムイベントを参照してください。
複数の警告	このコンピュータに複数の警告があります。詳細については、コンピュータのシステムイベントを参照してください。
準備完了	ESXiにVirtual Applianceをインストールする準備ができました (Filter Driverはインストール済みです)。
再有効化が必要	AgentまたはApplianceはインストール済みで、Deep Security Managerによる再有効化を待機しています。
非管理対象	このコンピュータのAgentは有効化されていないため、このDeep Security Managerで管理されていません。Agentを有効化するまで、Deep Security ManagerはAgentと通信できません。
準備が未完了	ESXiにVirtual Applianceをインストールする準備ができていません (Filter Driverがインストールされていません)。
アップグレード推奨	AgentまたはApplianceの新しいバージョンが使用可能です。ソフトウェアのアップグレードをお勧めします。
Agentのアップグレード中	このコンピュータのAgentソフトウェアを新しいバージョンにアップグレード処理中です。

[ステータス] 列 - AgentまたはApplianceの状態

ステータス	説明
有効化済み	AgentまたはApplianceが正常に有効化されました。Deep Security Managerで管理できます。
有効化が必	有効化されていないAgentまたはApplianceが対象のコンピュータで検出されまし

ステータス	説明
要	た。Deep Security Managerで管理するには、有効化する必要があります。
無効化が必要	他のDeep Security Managerによってすでに有効化されたAgentまたはApplianceを、Managerで有効化しようとした。新しいManagerで有効化する前に、元のDeep Security ManagerでAgentまたはApplianceを無効にする必要があります。
Agent /Appliance なし	コンピュータでAgentまたはApplianceが検出されませんでした。
オフライン	<p>コンピュータエディタまたはポリシーエディタ¹→[設定]→[一般]で指定されたハートビート回数でAgentまたはApplianceがManagerに接続されませんでした。</p> <p>この状態は、ネットワークファイアウォールまたはプロキシ、AWSセキュリティグループ、Agentソフトウェアアップデートによって接続が中断されたり、修復のためにコンピュータの電源がオフになるときに発生します。</p> <p>ファイアウォール設定で必要なポート番号を許可していることと、コンピュータの電源がオンになっていることを確認してください。</p>
オンライン	AgentまたはApplianceがオンラインで、予期したとおりに動作しています。
不明	AgentまたはApplianceが存在するかどうか判定されていません。
仮想マシン一時停止	仮想マシンが「一時停止」状態です。
仮想マシン停止	仮想マシンが「停止」状態です。

[タスク] 列

ステータス	説明
有効化中	ManagerがAgentまたはApplianceを有効化しています。
有効化中 (遅延)	関連するイベントベースタスクで指定した時間だけ、AgentまたはApplianceの有効化が遅延します。
有効化の保留中	AgentまたはApplianceを有効化するコマンドが処理待ちになっています。
Agentソフトウェアの配信の保留中	Agentソフトウェアをインストールする命令がコンピュータへの送信処理待ちになっています。
Agentソフトウェアの削除の保留中	Agentソフトウェアを削除する命令がコンピュータへの送信処理待ちになっています。
アプリケーションコントロールのインベントリ検索 - 実行	アプリケーションコントロールのインベントリ検索が実行中です。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ステータス	説明
中	
アプリケーションコントロールのインベントリ検索 - 保留中 (ハートビート)	アプリケーションコントロールのインベントリ検索を開始する命令は、次回のハートビートでManagerから送信されます。
アプリケーションコントロールのインベントリ検索 - 保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがアプリケーションコントロールのインベントリ検索を開始します。
アプリケーションコントロールルールセットのアップデート - 実行中	アプリケーションコントロールルールセットがアップデート中です。
アプリケーションコントロールルールセットのアップデート - 保留中 (ハートビート)	アプリケーションコントロールルールセットのアップデートを実行する命令は、次回のハートビートでManagerから送信されます。
アプリケーションコントロールルールセットのアップデート - 保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがアプリケーションコントロールルールセットのアップデートを開始します。
ベースライン再構築の実行中	変更監視エンジンが現在システムベースラインを再構築しています。
ベースライン再構築の一時停止	ベースライン再構築が一時停止になっています。
ベースライン再構築の保留中	変更監視のためにシステムベースラインを再構築する命令が送信処理待ちになっています。
ベースライン再構築の保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。Managerとこのコンピュータ間の通信が再度確立されると、変更監視エンジンがシステムベースラインを再構築します。
ベースライン再構築の処理待ち	ベースライン再構築を実行する命令が処理待ちになっています。
ステータスの確認	Agent/Applianceの状態を確認しています。
無効化の保留中 (ハートビート)	次回のハートビート時にManagerから無効化命令が送信されます。
無効化の実行中	ManagerがAgentまたはApplianceを無効化しています。つまり、他のDeep Security Managerが、AgentまたはApplianceを有効化および管理できます。
Agentソフトウェアの配信中	Agentソフトウェアをコンピュータにインストールしています。
ファイルバックアップのキャンセルの実行中	ファイルバックアップがキャンセルされています。
ファイルバックアップのキャンセルの保留中	ファイルバックアップをキャンセルする命令が送信処理待ちになっています。
ファイルバックアップのキャンセルの保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがファイルバックアップのキャンセルを開始します。
ファイルバックアップの実行中	ファイルバックアップが実行中です。
ファイルバックアップの保留中	ファイルバックアップを開始する命令が送信処理待ちになっています。

ステータス	説明
ファイルバックアップの保留中(オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがファイルバックアップを開始します。
ファイルバックアップの処理待ち	ファイルバックアップを実行する命令が処理待ちになっています。
イベントの取得	ManagerがAgentまたはApplianceからイベントを取得しています。
変更の検索の実行中	変更の検索が現在処理中です。
変更の検索の一時停止	変更の検索が一時停止になっています。
変更の検索の保留中	変更の検索を開始するコマンドが送信処理待ちになっています。
変更の検索の保留中(オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerが変更の検索を開始します。
変更の検索の処理待ち	変更の検索を開始する命令が送信処理待ちになっています。
不正プログラムの手動検索キャンセルの実行中	手動で開始した不正プログラムの検索をキャンセルする命令が送信されました。
不正プログラムの手動検索キャンセルの保留中	手動で開始した不正プログラムの検索をキャンセルするコマンドが送信処理待ちになっています。
不正プログラムの手動検索キャンセルの保留中(オフライン)	Applianceがオフラインです。通信が再度確立されると、手動で開始した不正プログラムの検索をキャンセルする命令が送信されます。
不正プログラムの手動検索の実行中	手動で開始した不正プログラムの検索が処理中です。
不正プログラムの手動検索の一時停止	手動で開始した不正プログラムの検索が一時停止になっています。
不正プログラムの手動検索の保留中	手動で開始した不正プログラムの検索の実行命令がまだ送信されていません。
不正プログラムの手動検索の保留中(オフライン)	AgentまたはApplianceがオフラインです。通信が再度確立されると、手動で開始した不正プログラムの検索を開始する命令が送信されます。
不正プログラムの手動検索の処理待ち	手動で開始した不正プログラムの検索の実行命令が処理待ちになっています。
不正プログラムの予約検索キャンセルの実行中	不正プログラムの予約検索をキャンセルする命令が送信されました。
不正プログラムの予約検索キャンセルの保留中	不正プログラムの予約検索をキャンセルする命令が送信処理待ちになっています。
不正プログラムの予約検索キャンセルの保留中(オフライン)	AgentまたはApplianceがオフラインです。通信が再度確立されると、不正プログラムの予約検索をキャンセルする命令が送信されます。
不正プログラムの予約検索の実行中	不正プログラムの予約検索が処理中です。
不正プログラムの予約検索の一時停止	不正プログラムの予約検索が一時停止になっています。
不正プログラムの予約検索の保留中	不正プログラムの予約検索をキャンセルするコマンドがまだ送信されていません。
不正プログラムの予約検索の	AgentまたはApplianceがオフラインです。通信が再度確立され

ステータス	説明
保留中 (オフライン)	ると、不正プログラムの予約検索を開始する命令が送信されま す。
不正プログラムの予約検索の 処理待ち	不正プログラムの予約検索をキャンセルする命令が処理待ちに なっています。
不正プログラムのクイック検 索キャンセルの実行中	不正プログラムのクイック検索がキャンセルされています。
不正プログラムのクイック検 索キャンセルの保留中	不正プログラムのクイック検索をキャンセルする命令が送信処 理待ちになっています。
不正プログラムのクイック検 索キャンセルの保留中 (オフ ライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立 されると、Managerが不正プログラムのクイック検索キャンセ ルを開始します。
不正プログラムのクイック検 索の実行中	不正プログラムのクイック検索が実行中です。
不正プログラムのクイック検 索の一時停止	不正プログラムのクイック検索が一時停止になっています。
不正プログラムのクイック検 索の保留中	不正プログラムのクイック検索を開始する命令が送信処理待ち になっています。
不正プログラムのクイック検 索の保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立 されると、Managerが不正プログラムのクイック検索を開始し ます。
不正プログラムのクイック検 索の処理待ち	不正プログラムのクイック検索の実行命令が処理待ちになって います。
Agentソフトウェアの削除中	Agentソフトウェアをコンピュータから削除しています。
セキュリティアップデートの ロールバックの実行中	セキュリティアップデートがロールバックされています。
セキュリティアップデートの ロールバックの保留中	セキュリティアップデートをロールバックする命令が送信処理 待ちになっています。
セキュリティアップデートの ロールバックの保留中 (ハート ビート)	セキュリティアップデートをロールバックする命令は、次回の ハートビートでManagerから送信されます。
セキュリティアップデートの ロールバックの保留中 (オフ ライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立 されると、Managerがセキュリティアップデートのロールバッ クを開始します。
推奨設定の検索の保留中 (ハートビート)	次回のハートビート時にManagerが推奨設定の検索を開始しま す。
推奨設定の検索の保留中 (オ フライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立 されると、Managerが推奨設定の検索を開始します。
推奨設定の検索の保留中 (仮 想マシンがオフライン)	Applianceが現在オフラインです。通信が再度確立されると、 Managerが推奨設定の検索を開始します。
オープンポートの検索中	Managerがコンピュータのオープンポートを検索しています。
推奨設定の検索中	推奨設定の検索が進行中です。
セキュリティアップデートの 実行中	セキュリティアップデートが実行中です。
セキュリティアップデートの 保留中	セキュリティアップデートを実行する命令が送信処理待ちに なっています。


ステータス	説明
セキュリティアップデートの保留中(ハートビート)	セキュリティアップデートを実行する命令は、次回のハートビートでManagerから送信されます。
セキュリティアップデートの保留中(オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがセキュリティアップデートを開始します。
ポリシー送信中	ポリシーをコンピュータに送信中です。
設定のアップデートの保留中(ハートビート)	ポリシー変更に対応するために設定をアップデートする命令は、次回のハートビートでManagerから送信されます。
設定のアップデートの保留中(オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがポリシー変更に対応するための設定のアップデートを開始します。
ソフトウェアをアップグレードしています(実行中)	ソフトウェアアップグレードが実行中です。
ソフトウェアをアップグレードしています(インストールプログラムの送信)	ソフトウェアアップグレードが実行中です。インストールプログラムはコンピュータに送信されています。
ソフトウェアをアップグレードしています(保留中)	ソフトウェアアップグレードを実行する命令が送信処理待ちになっています。
ソフトウェアをアップグレードしています(アップグレードを完了するには再起動する必要があります)	ソフトウェアのアップグレードが要求されましたが、Agentコンピュータが再起動されるまで完了しません。コンピュータは、この状態の場合でも、古いバージョンのDeep Security Agentによって保護されています。
ソフトウェアをアップグレードしています(結果の受信)	ソフトウェアアップグレードが実行中です。結果を受信しています。
ソフトウェアをアップグレードしています(スケジュール)	コンピュータのアクセススケジュールが許可されると、ソフトウェアアップグレードが実行されます。

コンピュータのエラー

ステータス	説明
通信エラー	一般的なネットワークエラーです。
コンピュータへのルートなし	通常は、Managerとコンピュータの間のファイアウォールによってブロックされているか、Managerとコンピュータの間のルータが停止しているため、コンピュータに到達できません。
ホスト名解決不能	未解決のソケットアドレスです。
有効化が必要	有効化されていない場合、AgentまたはApplianceに命令が送信されます。
Agent/Applianceとの通信失敗	AgentまたはApplianceとの通信に失敗しました。
プロトコルエラー	IP、TCP、またはHTTP層での通信エラーです。

ステータス	説明
	たとえば、ファイアウォール、ルータ、またはAWSセキュリティグループによって接続がブロックされているためにDeep Security ManagerのIPアドレスにアクセスできない場合、接続は失敗します。このエラーを解決するには、有効化の ポート番号 が許可されていること、およびルートが存在することを確認します。
無効化が必要	AgentまたはApplianceは、現在別のDeep Security Managerによって有効化されています。
Agent /Appliance なし	ターゲットでAgentまたはApplianceが検出されませんでした。
有効なソフトウェアバージョンなし	要求したプラットフォームおよびバージョンのインストーラが見つからないことを示します。
ソフトウェアの送信失敗	コンピュータへのバイナリパッケージの送信でエラーが発生しました。
内部エラー	内部エラーです。サポート担当者にお問い合わせください。
重複するコンピュータ	Deep Security Managerのコンピュータリストにある2台のコンピュータのIPアドレスが同じです
VMware Toolsがインストールされていない	VMware Tools (vShield Endpoint Thin Agent) が、ゲスト仮想マシンにインストールされていません。Deep Security不正プログラム対策および変更監視保護を使用するには、vShield Endpoint Thin Agentが必要です。このエラーステータスは、Deep SecurityがVMware NSX環境に配置されている場合にのみ表示されます。
未解決のソフトウェア変更数の上限に達しました	ファイルシステムで検出されたソフトウェア変更数が上限を超えました。アプリケーションコントロールは引き続き既存のルールを適用しますが、これ以上の変更は記録されず、このコンピュータでのソフトウェアの変更は表示されなくなります。 "大量のソフトウェア変更後にアプリケーションコントロールをリセットする" on page 713 を参照してください。

保護モジュールのステータス

[コンピュータ] 画面でコンピュータ名の上にマウスを置くと、[プレビュー] アイコン () が表示されます。このアイコンをクリックすると、コンピュータの保護モジュールの状態が表示されます。

オンおよびオフの状態:

ステータス	説明
オン	モジュールはDeep Security Managerで設定済みであり、Deep Security Agentにインストールされ、動作しています。
オフ	モジュールはDeep Security Managerで設定されていないか、Deep Security Agentにインストールされておらず動作していないか、またはその両方の状態です。
不明	保護モジュールでエラーが発生しています。

インストール状態:

ステータス	説明
インストールされていません	モジュールを含むソフトウェアパッケージはDeep Security Managerにダウンロード済みですが、モジュールがDeep Security Managerで有効になっていないか、Agentにインストールされていません。
インストール保留中	モジュールはDeep Security Managerで設定済みですが、Agentにインストールされていません。
インストール実行中	モジュールをAgentにインストール中です。
インストールされています	モジュールはAgentにインストールされています。このステータスは、モジュールの状態が「オフ」の場合にのみ表示されます (状態が「オン」の場合、モジュールはAgentにインストール済みです)。
一致するモジュールプラグインが見つかりません	Deep Security Managerにインポートされた、モジュールを含むソフトウェアパッケージのバージョンが、Agentから報告されたバージョンと一致しません。
サポートされていません/アップデートはサポートされていません	一致するソフトウェアパッケージがAgentに見つかりましたが、プラットフォームでサポートされているモジュールが含まれていません。このモジュールの任意のバージョンがAgentにインストールされているかどうかに応じて、[サポートされていません] または [アップデートはサポートされていません] が表示されます。

コンピュータでその他の処理を実行する

[コンピュータ] 画面の [処理] ボタンには、選択したコンピュータで実行できる処理が多数用意されています。

処理	説明
ステータスの確認	検索や有効化を実行せず、コンピュータの ステータス を確認します。

処理	説明
有効化/再有効化	コンピュータ上のAgentまたはApplianceを有効化/再有効化します。 "Agentの有効化" on page 430 を参照してください。
無効化	別々にインストールされたDeep Security Manager間で、管理するコンピュータを移動する場合があります。その場合は、AgentまたはApplianceを無効にしてから、新しいManagerで再度有効にする必要があります。
ポリシーの割り当て	<p>画面が開き、リストからコンピュータにポリシーを割り当てることができます。コンピュータに割り当てたポリシーの名前は、[コンピュータ] 画面の [ポリシー] 列に表示されます。</p> <p>注意: ファイアウォールルールの追加やファイアウォールステートフル設定の変更など、他の設定をコンピュータに適用する場合は、ポリシーの名前の横に初期設定が変更されたことがわかるよう太字で表示されます。</p>
ポリシーの送信	Deep Security Managerを使用してコンピュータ上のAgentまたはApplianceの設定を変更した場合 (新規侵入防御ルールの適用やログ設定の変更など) は、Deep Security Managerから新しい情報をAgentまたはApplianceに送信する必要があります。これが「ポリシーの送信」命令です。ポリシーのアップデートは通常ただちに実行されますが、[ポリシーの送信] をクリックして強制的にアップデートすることもできます。
セキュリティアップデートのダウンロード	設定済みのRelayからAgentまたはApplianceに最新のセキュリティアップデートをダウンロードします。 "セキュリティアップデートの取得と配布" on page 1039 を参照してください。
セキュリティ	AgentまたはApplianceの最新のセキュリティアップデートをロールバックします。

処理	説明
ティアアップデートのロールバック	
イベントの取得	通常のイベント取得スケジュール (通常はハートビートごと) をオーバーライドし、コンピュータから今すぐイベントログを取得します。
警告/エラーのクリア	<p>コンピュータのすべての警告とエラーをクリアします。このコマンドは、次の場合に便利です。</p> <ul style="list-style-type: none"> • コンピュータのAgentがローカルでリセットされたとき • コンピュータのリストでコンピュータを無効にするかリストから削除する前に、ネットワークからコンピュータが切断されたとき
Agentソフトウェアのアップグレード	AgentまたはApplianceをアップグレードするには、まず新しいバージョンのAgentまたはApplianceソフトウェアパッケージをDeep Security Managerにインポートする必要があります (" アップグレードについて " on page 994を参照してください)。
推奨設定の検索	Deep Security Managerでは、コンピュータ上のセキュリティルールを検索し、推奨設定を作成できます。推奨設定の検索の結果は、コンピュータの [ルール] 画面の [詳細] 画面に表示されます。" 推奨設定の検索の管理と実行 " on page 592を参照してください。
推奨設定をクリア	このコンピュータの推奨設定の検索の結果として作成されたルールの推奨をクリアします。また、推奨設定の検索によって生成されたアラートに一覧表示された中から該当するコンピュータを削除します。

処理	説明
	<p>注意: この処理では、過去の推奨設定によって割り当てられたルールの割り当ては解除されません。</p>
不正プログラムのフル検索	<p>選択したコンピュータで不正プログラムのフル検索を実行します。フル検索で実行される処理は、このコンピュータで有効になっている不正プログラムの手動検索の設定に応じて変わります。"不正プログラム検索の設定" on page 733を参照してください。</p>
不正プログラムのクイック検索	<p>重要なシステム領域で、現在アクティブな脅威の検索だけが実行されます。クイック検索では、現在アクティブな不正プログラムが検索されますが、活動のない、または保存されている感染ファイルを検索するためにファイルが詳細に検索されることはありません。大容量のドライブでは、フル検索よりも短時間で終了します。</p> <p>注意: クイック検索は、手動でのみ実行できます。予約タスクの一部としてクイック検索を予約することはできません。</p>
オープンポートの検索	<p>選択したすべてのコンピュータでポート検索を実行し、コンピュータにインストールされているAgentを確認して、その状態が「無効化が必要」、「有効化が必要」、「再有効化が必要」、または「オンライン」のいずれであるかを判別します。初期設定では、ポート1~1024が検索されます。この範囲は、コンピュータエディタまたはポリシーエディタ¹→[設定]→[一般]で変更できます。</p> <p>注意: Agentのハートビートの待機ポート番号は、ポート範囲の設定に関係なく常に検索されます。ManagerはAgentと通信する際、このポート番号を使用して接続します。ただし、コンピュータで通信方向を [Agent/Applianceから開始] (コンピュータエディタまたはポリシーエディタ²→[設定]→[一般]→[通信方向])に設定すると、このポート番号は開かれませんが、使用されるポートのリストにつ</p>

















¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。







処理	説明
	<p data-bbox="293 296 1357 348">いては、"Deep Securityのポート番号" on page 191を参照してください。</p> <p data-bbox="293 432 342 569">注意： ：</p> <p data-bbox="293 684 342 1766">ネットワーク上の新しいコンピュータは検出され</p>

処理	説明
	<p>ません。新しいコンピュータを検索するには、検出ツールを使用します。</p>
<p>実行中のポート検索をキャンセル</p>	<p>多数のコンピュータまたは広範囲のポートに対して一連のポート検索を開始し、検索に時間がかかりすぎる場合、[実行中のポート検索をキャンセル] オプションを使用して、検索をキャンセルできます。</p>
<p>変更の検索</p>	<p>変更監視では、コンピュータのシステムおよびファイルに対する変更を追跡します。そのためにはベースラインを作成し、定期的に検索してコンピュータの現在の状態とベースラインとを比較します。詳細については、"変更監視の設定" on page 887を参照してください。</p>
<p>整合性ベースラインの再構築</p>	<p>このコンピュータの変更監視のベースラインを再構築します。</p>
<p>資産評価の割り当て</p>	<p>資産評価を使用すると、コンピュータおよびイベントを重要度別にソートできます。セキュリティルールにはそれぞれ固有の重要度があります。コンピュータでルールがトリガされると、ルールの重要度とコンピュータの資産評価が乗算されます。この値は、重要度の順にイベントにランクを付けるために使用されます。"イベントのランク付けによる重要度の数値化" on page 1139を参照してください。</p>
<p>Relayグループの割り当て</p>	<p>アップデートのダウンロード元となるこのコンピュータのRelayグループを選択するには、コンピュータを右クリックして、[処理]→[Relayグループの割り当て]の順に選択します。</p>

コンピュータのアイコン

-  通常のコンピュータ
-  Deep Security Relay (Relay有効化済みAgentがインストールされたコンピュータ)
-  Deep Security Scanner (Scanner有効化済みAgentがインストールされたコンピュータ)
-  Dockerホスト (物理コンピュータ)
-  DockerがインストールされたAzure仮想マシン
-  DockerがインストールされたAmazon EC2
-  DockerがインストールされたVMware仮想マシン
-  ScannerがインストールされたAzure仮想マシン
-  ScannerがインストールされたAzure仮想マシン (起動済み)
-  ScannerがインストールされたAzure仮想マシン (停止)
-  ScannerがインストールされたAzure仮想マシン (一時停止)
-  ScannerがインストールされたAmazon EC2
-  ScannerがインストールされたAmazon EC2 (起動済み)
-  ScannerがインストールされたAmazon EC2 (停止)
-  ScannerがインストールされたAmazon EC2 (一時停止)
-  Amazon WorkSpace (起動済み)

vSphere環境のその他のコンピュータアイコン:

















-  ESXiサーバ
-  仮想マシン (VMware vCenterによって管理される仮想マシン)
-  仮想マシン (起動済み)
-  仮想マシン (停止)
-  仮想マシン (一時停止)
-  仮想マシン (Relay有効化済み)

-  仮想マシン (起動済み、Relay有効化済み)
-  仮想マシン (停止、Relay有効化済み)
-  仮想マシン (一時停止、Relay有効化済み)
-  仮想マシン (Scanner有効化済み)
-  仮想マシン (起動済み、Scanner有効化済み)
-  仮想マシン (停止、Scanner有効化済み)
-  仮想マシン (一時停止、Scanner有効化済み)
-  Virtual Appliance
-  Virtual Appliance (起動済み)
-  Virtual Appliance (停止)
-  Virtual Appliance (一時停止)

各種コンピュータのステータス情報

通常のコンピュータ

通常のコンピュータのプレビュー画面には、Agentとその[ステータス](#)、および[保護モジュールのステータス](#)が表示されます。

 Agent	
	 管理対象 (オンライン)
 不正プログラム対策	 オン、リアルタイム
 Web レビューテーション	 オン
 ファイアウォール	 オン、41 個のルール
 侵入防御	 オン、防御、193 個のルール
 変更監視	 オン、ルールなし
 セキュリティログ監視	 オン、5 個のルール
 アプリケーションコントロール	 オフ、サポートなし

Relay

Deep Security Relay有効化済みAgentのプレビュー画面には、[ステータス](#)、配信可能なセキュリティアップデートコンポーネントの数、および組み込みのDeep Security Agentが提供する保護モジュールのステータスが表示されます。

 Agent		 Relay 192 個のコンポーネントを利用可能
	● 管理対象 (オンライン)	
 不正プログラム対策	● オン、リアルタイム	
 Web レピュテーション	● オン	
 ファイアウォール	● オン、41 個のルール	
 侵入防御	● オン、防御、316 個のルール	
 変更監視	● オン、30 個のルール	
 セキュリティログ監視	● オン、6 個のルール	
 アプリケーションコントロール	● オフ、サポートなし	

Deep Security Scanner

Deep Security Scannerのプレビュー画面には、AgentまたはAppliance (コンバインモードの場合はその両方) とその[ステータス](#)、保護モジュールのステータス、およびScannerのステータス (SAP) が表示されます。

 Agent		 Scanner (SAP): オン
	● 管理対象 (オンライン)	
 不正プログラム対策	● オン、リアルタイム	
 Web レピュテーション	● オン	
 ファイアウォール	● オン、41 個のルール	
 侵入防御	● オン、防御、316 個のルール	
 変更監視	● オン、30 個のルール	
 セキュリティログ監視	● オン、6 個のルール	
 アプリケーションコントロール	● オフ、サポートなし	

Dockerホスト

Dockerホストのプレビュー画面には、Agentとそのステータス、保護モジュールのステータス、およびDockerの[ステータス](#)が表示されます。

Agent		Docker ホストの検出	
	● 管理対象 (オンライン)		
不正プログラム対策	● オン、リアルタイム		
Web レピュテーション	● オン		
ファイアウォール	● オン、16 個のルール		
侵入防御	● オン、防御、145 個のルール		
変更監視	● オン、21 個のルール		
セキュリティログ監視	● オン、4 個のルール		
アプリケーションコントロール	● オフ、サポートなし		

ESXiサーバ





ESXiサーバのプレビュー画面には、ESXiサーバの[ステータス](#)とESXiソフトウェアのバージョン番号が表示されます。[ゲスト] エリアには、設定されているDeep Security Virtual Applianceと、このホストで実行されている仮想マシンが表示されます。

ESXi		ゲスト	
	● 管理対象		localhost.localdom (Trend Micro Deep Security)
ESXiのバージョン	5.5.0		localhost.localdom (Guest Introspection (1))
			Ubuntu1404 (Ubuntu_14.04_x64 (d67951a3-dc7
			WIN-FTV5H918C7R (Jack_Win7_x86_SP1)

Virtual Appliance

Virtual Applianceのプレビュー画面には、Applianceの[ステータス](#)とバージョン番号が表示されます。[ゲストが保護される対象] エリアには、保護されている仮想マシンが表示されます。

 **Appliance**
 管理対象 (オンライン)
 Applianceのバージョン 10.0.0.2043

ゲストが保護される対象  10.201.95.227
 GL-D5A-W6132 (Clover-Upgrade-W6_1-x
 GL-D5A-W664 (Clover-Upgrade-W6-x64)
 Ubuntu1404 (Ubuntu_14.04_x64 (d67951a3)

仮想マシンをAgentレスで保護する

仮想マシンのプレビュー画面には、仮想マシンがVirtual Applianceまたはゲスト内Agentのいずれかまたは両方で保護されているかが表示されます。また、仮想マシンで実行されているコンポーネントの詳細も表示されます。

 Appliance		
	 管理対象 (オンライン)	 ESXi 10.201.95.227
 不正プログラム対策	 オン, リアルタイム	 Appliance localhost.localdom (Trend Micro Deep Security (1))
 Webレピュテーション	 オフ	
 ファイアウォール	 オン, 14 ルール	
 侵入防御	 オン, 防御, 14 ルール	
 変更監視	 オン, ルールなし	
 セキュリティログ監視	 オン, 6 ルール	

Deep Securityでのiptablesの使用

Deep Security Agent 10.1以前をLinuxにインストールした場合は、ファイアウォールの競合を避けるために、初期設定でiptablesサービスが無効になっていました(ただし、この変更を防止する設定ファイルが追加されていた場合は例外です)。iptablesサービスはファイアウォール以外にも使用されているため(たとえば、Dockerは通常動作の一貫としてiptablesルールを管理します)、iptablesを無効にすると、悪影響を及ぼすことができました。

Deep Security 10.2以降 (Deep Security 11を含む) では、iptablesに関連する動作が変更されています。Deep Security Agentによりiptablesが無効化されなくなりました(iptablesが有効な場合は、Agentのインストール後も有効のままです。iptablesが無効な場合は、無効のままです)。ただし、iptablesサービスが有効な場合、Deep Security AgentとDeep Security Managerを正常に実行するには、以下に示すiptablesルールが必要になります。

Deep Security Managerの実行に必要なルール

Deep Security Managerがインストールされているコンピュータでiptablesが有効な場合に必要なiptablesルールが2つあります。初期設定では、Deep Security Managerの起動時にこれらのルールが追加され、Managerを停止またはアンインストールするとこれらのルールが削除されます。あるいは、"[Deep Securityによるiptablesルールの自動追加を防ぐ](#)" on the next page、手動で次のルールを追加することもできます。

- ポート4119で受信トラフィックを許可します。このルールは、Deep Security ManagerのWeb UIおよびAPIへのアクセスに必要です。
- ポート4120で受信トラフィックを許可します。このルールは、Agentのハートビートの待機に必要です(詳細については、"[AgentとManagerの通信](#)" on page 400を参照してください)。

注意: これらのポート番号は初期設定の番号のため、環境によっては異なるポートが使用されている場合もあります。Deep Securityで使用するすべてのポートのリストについては、"[ポート番号、URL、およびIPアドレス](#)" on page 190を参照してください。

Deep Security Agentの実行に必要なルール

Deep Security Agentがインストールされているコンピュータでiptablesが有効な場合は、iptablesルールの追加が必要になる場合があります。初期設定では、Deep Security Agentの起動時にこれらのルールが追加され、Agentを停止またはアンインストールするとこれらのルールが削除されます。あるいは、"[Deep Securityによるiptablesルールの自動追加を防ぐ](#)" on the next page、手動で次のルールを追加することもできます。

- ポート4118で受信トラフィックを許可します。このルールは、AgentがManagerからの通信または双方向通信を使用している場合に必要です(詳細については、"[AgentとManagerの通信](#)" on page 400を参照してください)。
- ポート4122で受信トラフィックを許可します。このルールは、AgentがRelayとして機能する場合に、ソフトウェアのアップデートを配信できるようにするために必要です(詳細については、"[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照してください)。

注意: これらのポート番号は初期設定の番号のため、環境によっては異なるポートが使用されている場合もあります。Deep Securityで使用するすべてのポートのリストについては、"[ポート番号、URL、およびIPアドレス](#)" on page 190を参照してください。

Deep Securityによるiptablesルールの自動追加を防ぐ

必要なルールを自動ではなく手動で追加する場合は、Deep Security ManagerとDeep Security Agentによるiptablesの変更を防ぐことができます。iptablesの自動変更を防ぐには、Deep Security ManagerとDeep Security Agentをインストールする予定があるコンピュータ上で次のファイルを作成します。

```
/etc/do_not_open_ports_on_iptables
```

Agentセルフプロテクションの有効化または無効化

注意: Agentセルフプロテクション機能はWindows版Agentでのみ使用できます。Linuxでは使用できません。

Agentセルフプロテクションにより、ローカルユーザはAgentを改ざんできなくなります。有効の場合は、ユーザがAgentを改ざんしようとする、「このアプリケーションの削除や変更はセキュリティ設定により禁止されています」という内容のメッセージが表示されます。

更新したり Deep Security Agentまたは リレーアンインストール、またはコマンドラインからの支援のための診断パッケージを作成しようとしているローカルユーザーなら (あなたは一時的に無効エージェント自己保護しなければならない ["診断パッケージとログの作成" on page 1573](#)), を参照してください。

注意: ユーザがAgentを停止したり、Agent関連のファイルやWindowsレジストリエントリを変更したりしないように、不正プログラム対策保護を「オン」にする必要があります。ただし、Agentのアンインストール防止には必要ありません。

Deep Security ManagerまたはAgentのコンピュータのコマンドラインを使用して、Agentセルフプロテクションを設定できます。

Deep Security Managerを介してセルフプロテクションを設定する

1. Agentセルフプロテクションを有効にする **コンピュータまたはポリシーエディタ**¹を開きます。
2. [設定]→[一般] をクリックします。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

3. [Agentセルフプロテクション] セクションで、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] で [はい] を選択します。
4. [ローカルでの変更許可にパスワードを要求] で [はい] を選択して認証パスワードを入力します。認証パスワードは、[dsa_controlコマンドラインユーティリティ](#)の不正使用の防止に役立つため、設定することを強くお勧めします。ここでパスワードを指定した場合は、そのパスワードを、Agentでのコマンド実行時に毎回-pまたは--passwd=オプションを使用してdsa_controlコマンドラインユーティリティに入力する必要があります。
5. [保存] をクリックします。
6. 設定を無効にするには、[いいえ] を選択します。[保存] をクリックします。

コマンドラインを使用してセルフプロテクションを設定する

セルフプロテクションの有効化および無効化、コマンドラインからも行えます。ただし、コマンドラインには、[認証パスワード](#)を指定できないという制限があります。認証パスワードを指定するには、Deep Security Managerを使用する必要があります。詳細については、"[Deep Security Managerを介してセルフプロテクションを設定する](#)" on the previous pageを参照してください。

1. Windows Agentにローカルでログインします。
2. 管理者権限でコマンドプロンプト (`cmd.exe`) を開きます。
3. 現在のディレクトリをDeep Security Agentのインストールフォルダに変更します (初期設定のインストールフォルダは次のとおりです)。

```
cd C:\Program Files\Trend Micro\Deep Security Agent
```

4. 次のいずれかのコマンドを入力します。

Agentセルフプロテクションを有効にするには、次のコマンドを入力します。

```
dsa_control --selfprotect=1
```

Agentセルフプロテクションを無効にするには、次のコマンドを入力します。

```
dsa_control --selfprotect=0 -p <password>
```

-p <password>の部分には、Deep Security Managerで事前に指定した認証パスワードを入力します。このパスワードの詳細については、「[Deep Security Managerを介してセルフプロテクションを設定する](#)" on the previous page」を参照してください。


Deep Securityによる「オフライン」Agentの保護

Deep Security Managerで「オフライン」として表示されるAgentは、最後に確認された設定に従って保護されています。ただし、Deep Security Managerとの通信が復元されるまで、ソフトウェア、セキュリティ、またはポリシーのアップデートを受信しません。

Agentを「オフライン」状態から移行する方法については、"[「オフライン」のAgent](#)" on [page 1541](#)を参照してください。

Deep Security Notifier

Deep Security Notifierは、Deep Security AgentおよびDeep Security Relayのステータスを通知する、Windowsのシステムトレイアプリケーションです。Notifierを実行すると、Deep Security Agentが検索を開始したとき、不正プログラムをブロックしたとき、または不正なWebページにアクセスしたときに、ユーザにポップアップ通知が表示されます。

Notifierがクライアントマシン上で占有するスペースは小さく、必要なディスク容量は約1MB、メモリの使用容量は約3MBとなります。Notifierの実行中は、システムトレイにNotifierアイコン () が表示されます。初期設定では、NotifierはDeep Security Agentと一緒にWindowsコンピュータに自動的にインストールされます。アップグレード用の最新バージョンをインポートするには、[管理]→[アップデート]→[ソフトウェア]→[ローカル] 画面を使用します。

注意: Relay有効化済みAgentを実行しているコンピュータでは、ローカルコンピュータで有効なコンポーネントではなく、AgentまたはApplianceに配布されているコンポーネントがNotifierに表示されます。

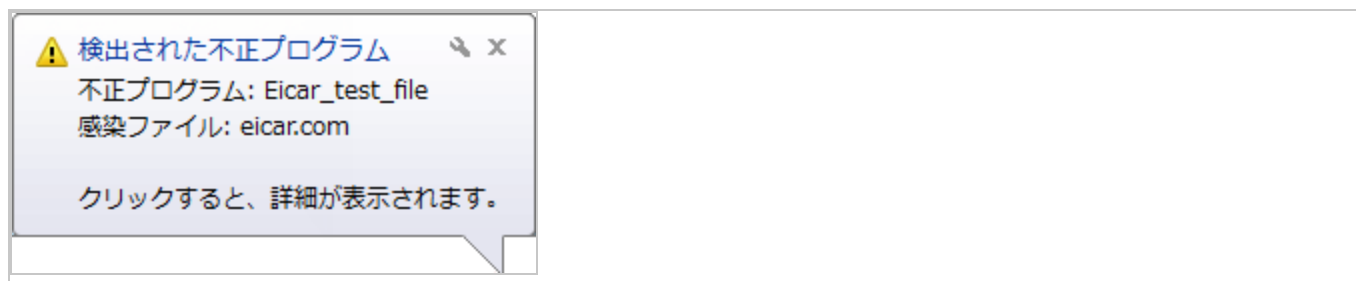
スタンドアロンバージョンのNotifierをダウンロードし、Deep Security Virtual Applianceで保護されている仮想マシンにインストールできます。"[Deep Security Notifierのインストール](#)" on [page 437](#)を参照してください。

注意: Deep Security Notifierに情報が表示されるためには、Virtual Applianceで保護されている仮想マシンに不正プログラム対策モジュールのライセンスがあり、モジュールが有効になっている必要があります。

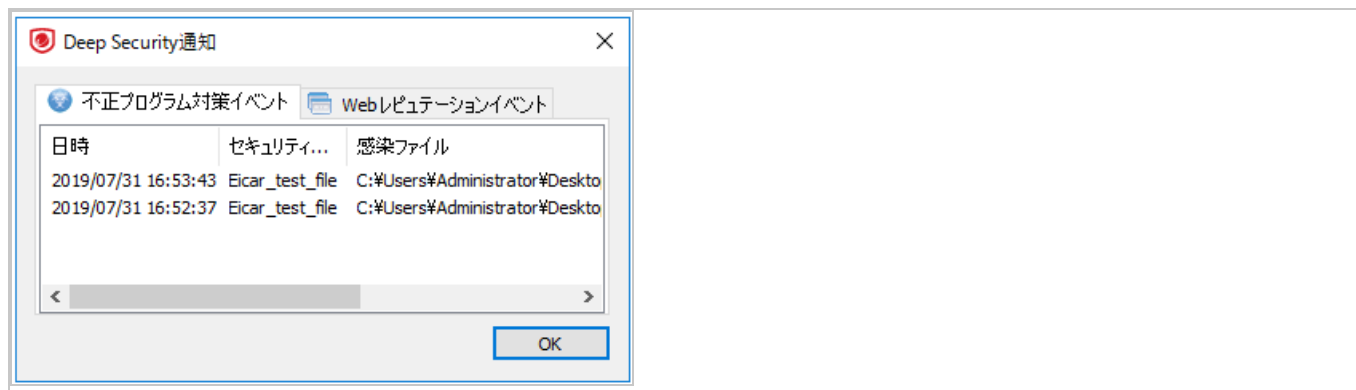
Notifierの仕組み

不正プログラムが検出されるか、不正サイトがブロックされると、Deep Security AgentはNotifierにメッセージを送信し、システムトレイにポップアップメッセージが表示されます。

不正プログラムを検出した場合、Notifierは次のようなポップアップメッセージをシステムトレイに表示します。



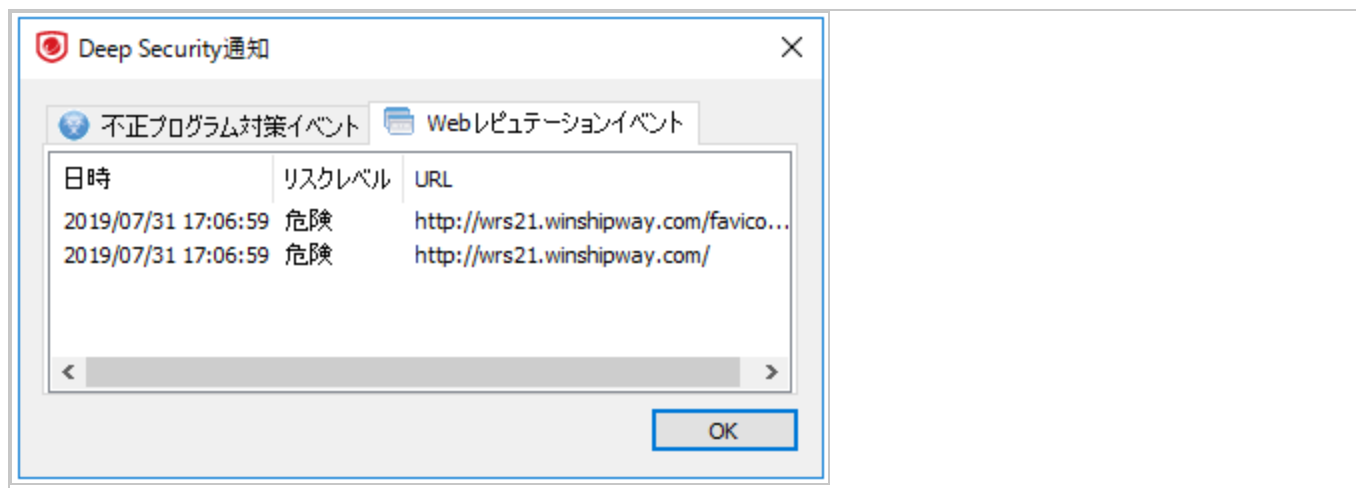
ユーザがメッセージをクリックすると、不正プログラム対策イベントの詳細を示す画面が表示されます。



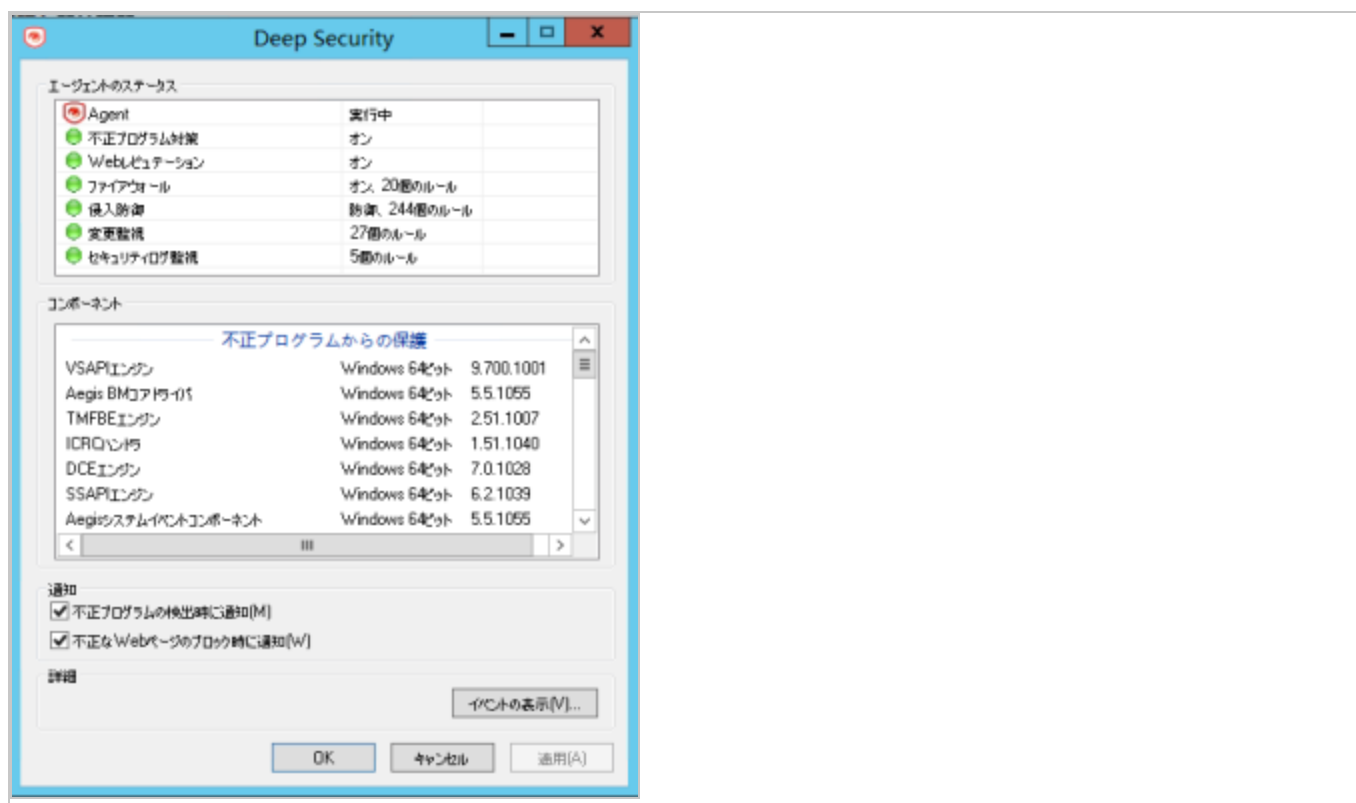
不正Webページをブロックした場合、Notifierは次のようなポップアップメッセージをシステムトレイに表示します。



ユーザがメッセージをクリックすると、Webレピュテーションイベントの詳細を示す画面が表示されます。



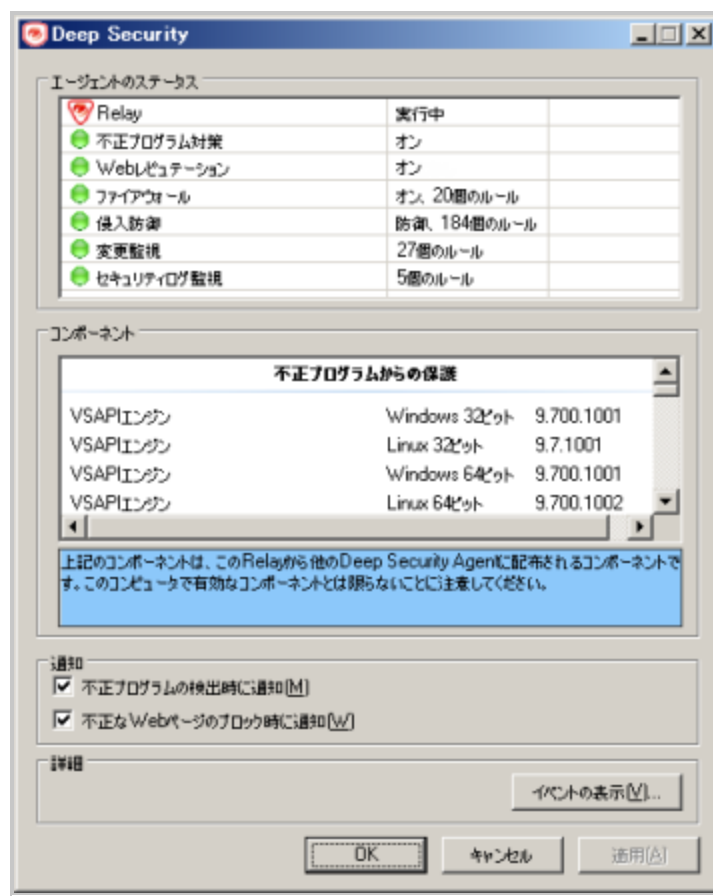
Notifierには、パターンのバージョンなど、現在の保護ステータスやコンポーネント情報を表示するためのコンソールユーティリティもあります。このコンソールユーティリティを使用して、ポップアップ通知のオンとオフを切り替えたり、詳細なイベント情報にアクセスしたりできます。



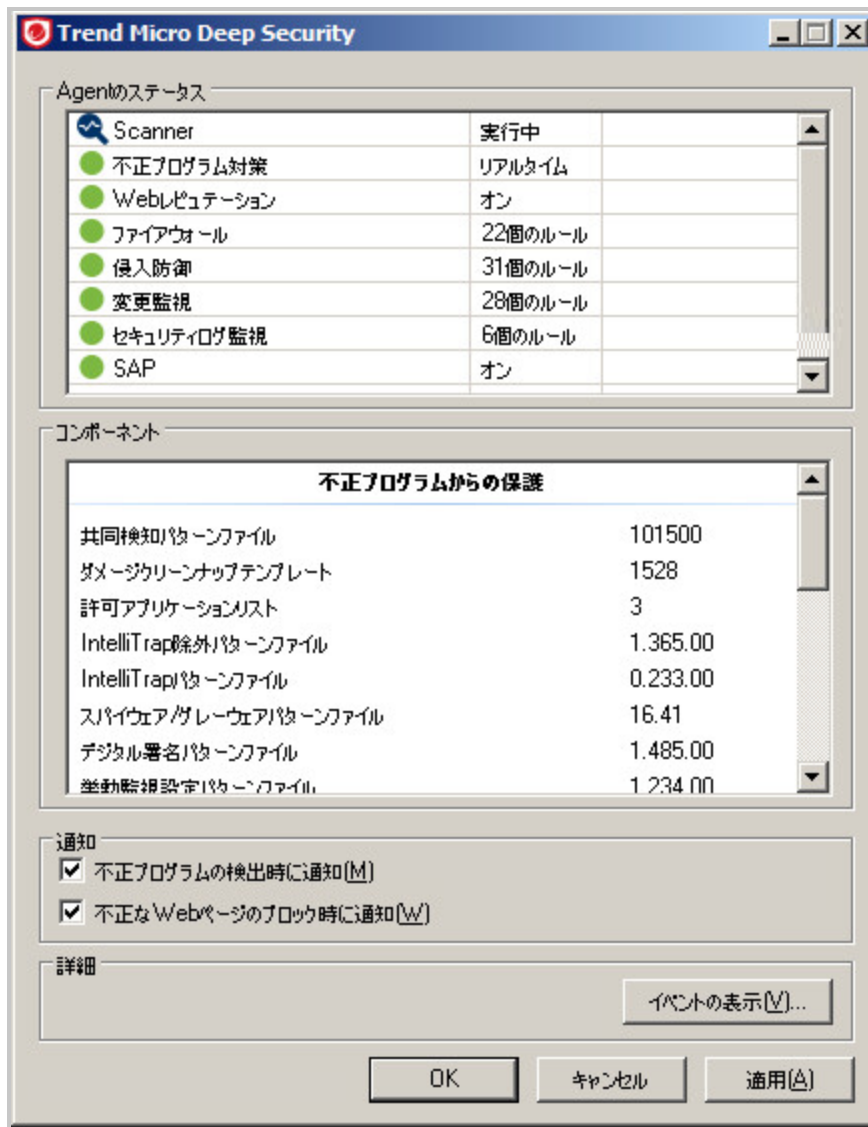
ヒント: また、Deep Security Managerのコンピュータ/ポリシーエディタで [設定]→[一般] の順に選択し、[ホストのすべてのポップアップ通知を抑制] を [はい] に設定すると、特定のコンピュータや特定のポリシーが割り当てられているコンピュータでポップアップ通知をオフ

にすることもできます。オフにしても、メッセージはDeep Security Managerのアラートやイベントとして表示されます。

NotifierがRelay有効化済みAgentをホストするコンピュータで実行されている場合、Notifierには、コンピュータ上で有効になっているコンポーネントではなく、Relayによって配布されているコンポーネントが表示されます。



NotifierがDeep SecurityScannerをホストするコンピュータで実行されている場合、Notifierには、Scanner機能が有効になっていること、およびそのコンピュータをRelayにはできないことが表示されます。



コンピュータとその他のリソースを保護するためのポリシーの作成

ポリシーでは、ルールや設定をまとめて保存し、複数のコンピュータに簡単に割り当てることができます。**ポリシーエディタ**¹でポリシーを作成および編集し、1台以上のコンピュータに割り当てることができます。また、ポリシーエディタに似た**コンピュータエディタ**²を使用して、特定のコンピュータに設定を適用することもできますが、コンピュータエディタで設定を編集するよりも特殊なポリシーを作成することを推奨します。

ヒント: ポリシーの作成と設定は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド [「Create and Configure Policies」](#) を参照してください。

このトピックの内容:

- "新規ポリシーを作成する" [below](#)
- "ポリシーを作成するその他の方法" [on the next page](#)
- "ポリシーまたは個々のコンピュータの設定を編集する" [on page 585](#)
- "ポリシーをコンピュータに割り当てる" [on page 585](#)
- "ポリシーの自動アップデートを無効にする" [on page 586](#)
- "ポリシーの変更を手動で送信する" [on page 586](#)
- "ポリシーをエクスポートする" [on page 587](#)

新規ポリシーを作成する

1. [ポリシー]→[新規]→[新規ポリシー] の順にクリックします。
2. ポリシーの名前を入力します。既存のポリシーの設定を新規ポリシーに継承する場合は、[継承元] リストからポリシーを選択します。[次へ] をクリックします。

¹ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

²コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ヒント: 継承の詳細については、"[ポリシー、継承、およびオーバーライド](#)" on [page 587](#)を参照してください。

3. 既存のコンピュータの設定をこのポリシーのベースにするかどうかを選択し、[次へ]をクリックします。
4. 手順3で [はい] を選択した場合は、以下を実行します。
 - a. 新規ポリシーのベースとして使用するコンピュータを選択し、[次へ]をクリックします。
 - b. 新規ポリシーに対して有効にする保護モジュールを指定します。既存のポリシーから設定を継承する場合は、それらの設定が表示されます。[次へ]をクリックします。
 - c. 次の画面で、新規ポリシーに組み込むプロパティを選択し、[次へ]をクリックします。設定を確認し、[完了]をクリックします。
5. 手順3で [いいえ] を選択した場合は、新規ポリシーに対して有効にする保護モジュールを指定します。既存のポリシーから設定を継承する場合は、それらの設定が表示されます。[完了]をクリックします。
6. [閉じる] をクリックします。次にポリシーの設定を編集できます。手順については"[ポリシーまたは個々のコンピュータの設定を編集する](#)" on [the next page](#)を参照してください。

ポリシーを作成するその他の方法

[ポリシー] 画面ではいくつかの方法でポリシーを作成できます。

- 前述した手順で新規ポリシーを作成します。
- [新規]→[ファイルからインポート] の順に選択してXMLファイルからポリシーをインポートします。
- **注意:** ポリシーをインポートする場合、ポリシーを作成したシステムと受け取るシステム両方に最新のセキュリティアップデートが適用されていることを確認してください。ポリシーを受け取るシステムが古いセキュリティアップデートを実行していると、最新のシステムのポリシーで参照されている一部のルールがそのシステムにない可能性があります。
- 既存のポリシーを複製し、変更して名前を変更します。複製するポリシーを右クリックして [複製] をクリックします。
- コンピュータの推奨設定の検索に基づいて新規ポリシーを作成します。[コンピュータ] 画面に移動し、コンピュータを右クリックして [処理]→[推奨設定の検索] の順に選択します。検索が終了したら、[ポリシー] 画面に戻り、[新規] をクリックして新規ポリシーウィ

ガードを起動します。プロンプトが表示されたら、新規ポリシーのベースを「既存のコンピュータの現在の設定」にします。次に、コンピュータのプロパティから [推奨されるアプリケーションの種類と侵入防御ルール]、[推奨される変更監視ルール]、および [推奨されるセキュリティログ監視ルール] を選択します。

- **注意:** ポリシーは、現在コンピュータにどのようなルールが割り当てられていたとしても、そのコンピュータの推奨エレメントのみで構成されます。

ポリシーまたは個々のコンピュータの設定を編集する

[ポリシー] 画面には、階層型のツリー構造で既存のポリシーが表示されます。ポリシーの設定を編集するには、ポリシーを選択し、[詳細] をクリックしてポリシーエディタを開きます。

コンピュータエディタとポリシーエディタ¹には以下のセクションがあります。

- 概要 ("ポリシーエディタの [概要] セクション" on page 611と"コンピュータエディタの [概要] セクション" on page 605は異なります)
- "不正プログラム検索の設定" on page 733
- [Webレピュテーションによる不正なURLへのアクセスのブロック](#)
- "ファイアウォールの設定" on page 866
- [侵入防御](#)
- [変更監視](#)
- [セキュリティログ監視の設定](#)
- "コンピュータで使用可能なインタフェースの検出と設定" on page 603
- "ネットワークエンジン設定" on page 612
- "オーバーライド" on page 589

ポリシーをコンピュータに割り当てる

1. [コンピュータ] に移動します。
2. コンピュータリストからコンピュータを選択し、右クリックして [処理]→[ポリシーの割

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

り当て]の順に選択します。

3. 階層ツリーからポリシーを選択し、[OK]をクリックします。

次のいずれかが実行されます。

- [通信方向](#)を [Managerから開始] または [双方向] に設定している場合、ポリシーはAgentコンピュータにただちに送信されます。
- 通信方向を [Agent/Applianceから開始] に設定している場合、ポリシーは次のAgentハートビートが発生したときに送信されます。

階層ツリーの子ポリシーで親ポリシーの設定やルールを継承またはオーバーライドする方法については、"[ポリシー、継承、およびオーバーライド](#)" on the next pageを参照してください。

ポリシーをコンピュータに割り当てた後も、定期的に推奨設定の検索を実行して、コンピュータ上にあるすべての脆弱性を保護してください。詳細については、"[推奨設定の検索の管理と実行](#)" on page 592を参照してください。

ポリシーの自動アップデートを無効にする

初期設定では、セキュリティポリシーが変更された場合、変更内容はそのポリシーを使用するコンピュータに自動的に送信されます。これを変更して、自動送信を無効にできます。この場合、手動でポリシーを送信する必要があります。

1. 設定するポリシーの[ポリシーエディタ](#)¹を開きます。
2. [設定]→[一般]→[ポリシーの変更をすぐに送信]の順に選択します。
3. ポリシー変更の自動送信を許可するには、[ポリシーの変更をコンピュータに自動的に送信]の隣にある[はい]を選択します。自動送信を無効にして手動送信のみを許可するには、[いいえ]を選択します。
4. [保存]をクリックして変更を適用します。

ポリシーの変更を手動で送信する

ポリシーを変更し、ポリシーの変更を特定のコンピュータに手動で送信する場合は、次の手順に従います。

1. [コンピュータ]に移動します。
2. コンピュータリストから自分のコンピュータをダブルクリックします。

¹ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。

3. ナビゲーション画面で [概要] が選択されていることを確認します。
4. メイン画面で [処理] タブをクリックします。
5. [ポリシー] で、[ポリシーの送信] をクリックします。

次のいずれかが実行されます。

- [通信方向](#)を [Managerから開始] または [双方向] に設定している場合、ポリシーはAgent コンピュータにただちに送信されます。
- 通信方向を Agent/Applianceから開始 に設定している場合、ポリシーは次のAgentハートビートが発生したときに送信されます。

ポリシーをエクスポートする

ポリシーをXMLファイルにエクスポートするには、ポリシーツリーからポリシーを選択し、[エクスポート]→[選択したアイテムをXML形式でエクスポート (インポート用)] の順にクリックします。

エクスポートされたポリシーは、同じ [マルチノードクラスター](#)内の別のDeep Security Manager によってのみインポートできます。

注意: Deep Security Managerでは、カスタムルールを使用したポリシーのエクスポートおよびインポートはサポートされません。

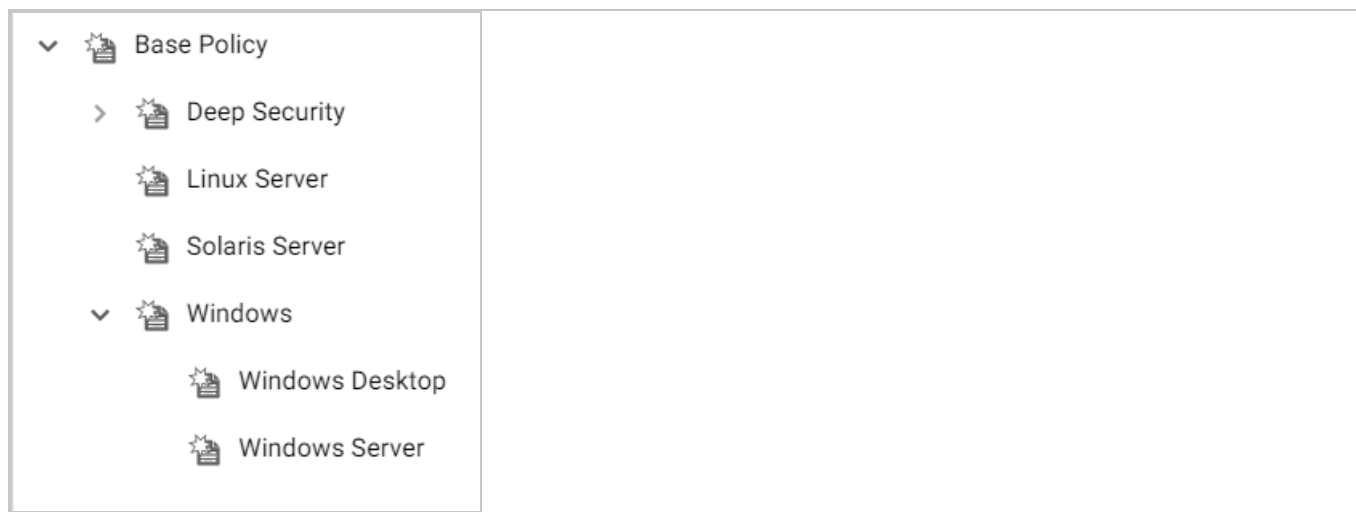
注意: 選択したポリシーをXMLにエクスポートすると、子ポリシー (存在する場合) もエクスポートパッケージに追加されます。エクスポートパッケージには、ポリシーに関連するすべての実際のオブジェクトが含まれます。ただし、侵入防御ルール、セキュリティログ監視ルール、変更監視ルール、およびアプリケーションの種類は含まれません。

ポリシー、継承、およびオーバーライド

Deep Securityでは、階層構造でポリシーを作成できます。管理者は、最初に1つ以上のベースポリシーを作成し、そこから複数レベルの子ポリシーを作成し、細分化していきます。つまり、最上位のポリシーで広範囲に適用するルールや設定を割り当ててから、子ポリシーのレベルで対象を絞って具体化し、最終的に個々のコンピュータレベルでルールや設定を割り当てることができます。

ポリシーツリーの下位になるほど設定が詳細になるだけでなく、ポリシーツリーの上位の設定から下位の設定をオーバーライドできます。

Deep Securityは、環境に合わせて独自のポリシーを設計するための開始テンプレートとして使用できる一連のポリシーを提供します。



このトピックの内容:

- ["継承" below](#)
- ["オーバーライド" on the next page](#)
- ["コンピュータまたはポリシーのオーバーライド項目をまとめて確認する" on page 591](#)

継承

子ポリシーは、親ポリシーから設定を継承します。これにより、すべてのコンピュータに適用する設定とルールが定義された親ベースポリシーから始まるポリシーツリーを作成できます。さらに、この親ポリシーには、より対象を具体化した設定を含む子および子孫のポリシーのセットを追加できます。ポリシーツリーは、環境に適した分類システムに基づいて構築できます。たとえば、Deep Securityに含まれるポリシーツリーのブランチには、2つの子ポリシーがあります。1つはDeep Security Managerをホストするサーバ向けに設計されたポリシーで、もう1つはDeep Security Virtual Appliance向けに設計されたポリシーです。これは役割に基づいたツリー構造です。また、Deep Securityには、特定のOS (Linux、Solaris、およびWindows) 向けに設計された3つのブランチがあります。Windowsブランチには、さまざまなサブタイプのWindows OS用の子ポリシーが用意されています。

[概要] 画面のWindowsポリシーエディタでは、Windowsポリシーがベースポリシーの子として作成されたことを確認できます。ポリシーの不正プログラム対策設定は [継承 (オフ)] です。

ポリシー: Base Policy > Windows

概要

- 不正プログラム対策
- Webレピュテーション
- ファイアウォール
- 侵入防御
- 変更監視
- セキュリティログ監視
- アプリケーション制御
- インタフェースの種類
- 設定
- オーバーライド

一般 このポリシーを使用しているコンピュータ イベント

名前: Windows

説明: An example policy from which all the example Windows policies inherit. Any settings that are common to all Windows policies can be set here.

継承

親ポリシー: なし, Base Policy, Deep Security, Linux Server

モジュール

モジュール	設定	状態
不正プログラム対策	継承 (オフ)	オフ
Webレピュテーション	継承 (オフ)	オフ
ファイアウォール	継承 (オフ)	オフ, 1つのルール
侵入防御	継承 (オフ)	オフ, ルールなし
変更監視	継承 (オフ)	オフ, ルールなし
セキュリティログ監視	継承 (オフ)	オフ, ルールなし
アプリケーション制御	継承 (オフ)	オフ

保存 閉じる

つまり、この設定は親ベースポリシーから継承されます。また、ベースポリシーの不正プログラム対策設定を [オフ] から [オン] に変更する場合は、Windowsポリシーの設定も変更されます (これにより、Windowsポリシーの設定は [継承 (オン)] になります。カッコ内の値は、継承された現在の設定を示しています)。

オーバーライド

[オーバーライド] 画面には、対象のポリシーまたは特定のコンピュータレベルでオーバーライドされた設定の数が表示されます。このレベルのオーバーライドを取り消すには、[削除] ボタンをクリックします。

次の例では、Windows ServerポリシーがWindowsポリシーの子ポリシーとなっています。ここでは、不正プログラム対策設定は継承されていません。オーバーライドされ、[オン] になっています。

コンピュータ: ec2-54-244-167-159.us-west-2.compute.amazonaws.com (Windows Server) ヘルプ

概要

- 不正プログラム対策
- Webレピュテーション
- ファイアウォール
- 侵入防御
- 変更監視
- セキュリティログ監視
- アプリケーションコントロール
- インタフェース
- 設定
- アップデート
- オーバーライド

一般 処理 システムイベント

ホスト名: ec2-54-244-167-159.us-west-2.compute.amazonaws.com (前回使用されたIP: 172.31.44.211)

表示名: Windows Server

説明: ec2-54-244-167-159.us-west-2.compute.amazonaws.com

プラットフォーム: Microsoft Windows Server 2012 R2 (64 bit) Build 9600

グループ: コンピュータ

ポリシー: Lockdown_9432104d-4ace-4dff-aff5-e96a25c80e69_DSAF 編集

資産の重要度: なし 編集

セキュリティアップデートのダウンロード元: 初期設定のRelayグループ ?

	Agent
<input checked="" type="checkbox"/> 不正プログラム対策	<input checked="" type="checkbox"/> 管理対象 (オンライン)
<input checked="" type="checkbox"/> Webレピュテーション	<input checked="" type="checkbox"/> オン, リアルタイム
<input checked="" type="checkbox"/> ファイアウォール	<input type="checkbox"/> オフ, インストールされていません
<input checked="" type="checkbox"/> 侵入防御	<input type="checkbox"/> オフ, インストールされていません, ルールなし
<input checked="" type="checkbox"/> 変更監視	<input type="checkbox"/> オフ, インストールされていません, ルールなし
<input checked="" type="checkbox"/> セキュリティログ監視	<input type="checkbox"/> オフ, インストールされていません, ルールなし
<input checked="" type="checkbox"/> アプリケーションコントロール	<input type="checkbox"/> オフ, インストールされていません, ルールなし
オンライン	<input checked="" type="checkbox"/> オン, 承認されていないソフトウェアをブロック
前回の通信	はい 2018-05-15 12:04

保存 閉じる

ヒント: オーバーライドの確認、作成、削除は、Deep Security APIを使用して自動化できません。例については、Deep Security Automation Centerにあるガイド [「Configure Computers to Override Policies」](#) を参照してください。

オブジェクトのプロパティをオーバーライドする

このポリシーに含まれる侵入防御ルールは、Deep Security Managerによって保存されている侵入防御ルールのコピーであり、他のポリシーで使用できます。特定のルールのプロパティを変更する場合は、ルールのプロパティをグローバルに変更して、そのルールを使用しているすべてのインスタンスに変更を適用するか、またはプロパティをローカルで変更して、その変更をローカルにのみ適用します。コンピュータまたはポリシーのエディタの初期設定の編集モードはローカルです。[現在割り当てられている侵入防御ルール] エリアにあるツールバーの [プロパティ] をクリックすると、[プロパティ] 画面で行うすべての変更が表示され、その変更がローカルにのみ適用されます(ルール名などの一部のプロパティはローカルでは編集できません。これらはグローバルでのみ編集できます)。

ルールを右クリックすると、コンテキストメニューが表示されます。このメニューから2つのプロパティ編集モードオプションを選択できます。[プロパティ]を選択すると、ローカルエディタ画面が表示されます。[プロパティ (グローバル)]を選択すると、グローバルエディタ画面が表示されます。

Deep Securityで共有される大部分の共通オブジェクトのプロパティを、ポリシー階層内のすべてのレベルおよびその下位の個々のコンピュータレベルでオーバーライドできます。

ルールの割り当てをオーバーライドする

ポリシーレベルまたはコンピュータレベルで、追加のルールをいつでも割り当てることができます。ただし、特定のポリシーレベルまたはコンピュータレベルで有効なルールの割り当てをローカルで解除することはできません。これは、そのルールの割り当てが親ポリシーから継承されているためです。このようなルールの割り当ては、ルールが最初に割り当てられたポリシーレベルで解除する必要があります。

ヒント: オーバーライドする設定が多数ある場合は、親ポリシーのブランチを作成することを検討してください。

コンピュータまたはポリシーのオーバーライド項目をまとめて確認する

ポリシーまたはコンピュータでオーバーライドした設定の数を確認するには、コンピュータまたはポリシーのエディタで [オーバーライド] 画面に移動します。

コンピュータ: ec2-54-244-167-159.us-west-2.compute.amazonaws.com (Windows Server) ヘルプ

概要

不正プログラム対策

Webレピュテーション

ファイアウォール

侵入防御

変更監視

セキュリティログ監視

アプリケーションコントロール

インタフェース

設定

アップデート

オーバーライド

オーバーライド

不正プログラム対策		
不正プログラム対策設定	2個のオーバーライド	削除
割り当てられた不正プログラム検索設定	1個のオーバーライド	削除
Webレピュテーション		
Webレピュテーションの設定	1個のオーバーライド	削除
ファイアウォール		
ファイアウォールの設定	2個のオーバーライド	削除
割り当てられたファイアウォールルール	継承	削除
オーバーライドされたファイアウォールルール	継承	削除
割り当てられたファイアウォールステータス設定	継承	削除
侵入防御		
侵入防御の設定	2個のオーバーライド	削除
割り当てられた侵入防御ルール	継承	削除
オーバーライドされた侵入防御ルール	継承	削除
割り当てられたアプリケーションの種類	継承	削除
オーバーライドされたアプリケーションの種類	継承	削除
変更監視		
変更監視の設定	2個のオーバーライド	削除
現在割り当てられている変更監視ルール	継承	削除
オーバーライドされた変更監視ルール	継承	削除
セキュリティログ監視		
セキュリティログ監視の設定	2個のオーバーライド	削除
現在割り当てられているセキュリティログ監視ルール	継承	削除
オーバーライドされたセキュリティログ監視ルール	継承	削除
アプリケーションコントロール		
アプリケーションコントロール設定	継承	削除
システム		
オーバーライドされたコンピュータ設定	2個のオーバーライド	削除

[すべて削除](#) [閉じる](#)

保護モジュール別のオーバーライド項目が表示されます。[削除] ボタンをクリックすれば、システムまたはモジュールのオーバーライド項目を元に戻すことができます。

推奨設定の検索の管理と実行

Deep Securityでは、コンピュータで推奨設定の検索を実行して、適用または削除すべき侵入防御ルール、変更監視ルール、およびセキュリティログ監視ルールを検出できます。

ヒント: 推奨設定の検索は、実装すべきルールリストを確立するための適切な開始ポイントとなりますが、推奨設定の検索では検出されない重要な追加ルールがいくつかあります。これらのルールは手動で実装する必要があります。"[一般的な脆弱性の追加ルールを実装する](#)" on [page 600](#)を参照してください。

推奨設定の検索を設定し、個々のコンピュータまたはポリシーレベルで推奨されたルールを実装できます。大規模な環境の場合、トレンドマイクロでは、ポリシーを使用して推奨設定を管理することを推奨します。これにより、1つのソース (ポリシー) からすべてのルールを割り当てることができます。各コンピュータで個々のルールを管理する必要はありません。そのため、一部のルールが、それを必要としていないコンピュータに割り当てられる可能性があります。しかし、パフォーマンスにわずかな影響が及ぶことよりも、ポリシーを通じて行われる処理によって管理が簡素化されるメリットの方が重要です。ポリシーで推奨設定の検索を有効にする場合は、WindowsルールがLinuxコンピュータに割り当てられないように、またはその逆が行われられないように、WindowsコンピュータとLinuxコンピュータの検出用に別のポリシーを使用してください。

- ["検索内容" below](#)
- ["検索の制限" on the next page](#)
- ["推奨設定の検索を実行する" on page 595](#)
- ["推奨設定を自動的に適用する" on page 598](#)
- ["検索結果を確認して手動でルールを割り当てる" on page 599](#)
- ["推奨ルールを設定する" on page 600](#)
- ["一般的な脆弱性の追加ルールを実装する" on page 600](#)
- ["トラブルシューティング: 推奨設定の検索失敗" on page 602](#)

検索内容

推奨設定の検索では、Deep Security AgentはOSについて次の項目を検索します。

- インストール済みアプリケーション
- Windowsレジストリ
- オープンポート
- ディレクトリリスト
- ファイルシステム
- 実行中のプロセスとサービス

- 環境変数
- ユーザ

Deep Security Virtual Applianceでは、Agentレスによる推奨設定の検索を仮想マシンで実行できますが、対象はWindowsプラットフォームのみであり、OSについて検索できる項目は次のものに限定されます。

- インストール済みアプリケーション
- Windowsレジストリ
- ファイルシステム

検索の制限

技術的または論理的な一部の制限により、ソフトウェアの種類によっては、ルールが正確には推奨されない、またはまったく推奨されないものになります。

- UnixシステムまたはLinuxシステムでは、推奨設定の検索エンジンが、Apache Struts、Wordpress、JoomlaなどのOSの初期設定のパッケージマネージャを使用してインストールされていないソフトウェアを検出できない可能性があります。標準のパッケージマネージャを使用してインストールされたアプリケーションについては、問題はありません。
- UnixシステムまたはLinuxシステムでは、ブラウザやメディアプレーヤなどのデスクトップアプリケーションの脆弱性またはローカルの脆弱性に関するルールは推奨設定の検索に含まれません。
- 一般的なWebアプリケーション保護ルールは推奨設定の検索に含まれません。
- スマートルールは通常、主要な脅威または特定の脆弱性に対応していない限り、推奨設定の検索に含まれません。スマートルールは、1つ以上の既知または未知の(ゼロデイ)脆弱性に対応します。Deep Security Managerのルールリストでは、スマートルールは[種類]列に「スマート」と表示されています。
- コンテンツ管理システム(CMS)に関連するルールを扱っているときには、推奨設定の検索でCMSインストールとインストールされているバージョンを検出できません。CMSとともにインストールされているプラグインとそのバージョンも検出できません。そのため、推奨設定の検索で、Webサーバがインストールされ、PHPがシステムでインストールまたは実行されていることが検出されると、すべてのCMS関連の侵入防御ルールが推奨されます。これにより、ルールが過度に推奨されることになりませんが、セキュリティのニーズと精度のバランスが取れます。
- 次のWeb技術に関する推奨設定では、必要以上のルールが提案されることがあるため、調整が必要な場合があります。

- Red Hat JBoss
 - Eclipse Jetty
 - Apache Struts
 - Oracle WebLogic
 - WebSphere
 - Oracle Application Testing Suite
 - Oracle Golden Gate
 - Nginx
- OpenSSLルールは、OpenSSLが明示的にインストールされている場合にのみ、Windowsで推奨されます。アプリケーションが内部で使用しているOpenSSLが別のパッケージとしてインストールされていない場合は、推奨設定の検索では検出されません。
 - Linuxシステムでは、Webブラウザのみが該当ベクタである場合は、Java関連の脆弱性のルールは推奨されません。
 - 推奨設定の検索では、初期設定のChromeインストールに含まれているAdobe Flash Playerプラグインは検出できません。推奨設定は、Chromeバージョンに基づいて決められます。つまり、不必要なルールが推奨されることがあります。

推奨設定の検索を実行する

環境の変更は推奨されるルールに影響を与えることがあるため、推奨設定の検索は定期的に行うことをお勧めします (推奨設定の検索は週1回の頻度で行うことをお勧めします)。トレンドマイクロは、毎週火曜日に新しい侵入防御ルールをリリースするので、推奨設定の検索をこれらのリリースの直後に予約することをお勧めします。推奨設定の検索中はCPUサイクル、メモリ、ネットワーク帯域幅などのシステムリソースの使用量が増えるため、検索はピーク時以外に予約することをお勧めします。

推奨設定の検索実行にはいくつかの方法があります。

- 予約タスク: 設定したスケジュールに従って推奨設定の検索を実行する予約タスクを作成します。予約タスクはすべてのコンピュータ、1台のコンピュータ、定義したコンピュータグループ、または特定のポリシーで保護されているすべてのコンピュータに割り当てることができます。"[予約タスクを作成して定期的に推奨設定の検索を実行する](#)" on the [next page](#)を参照してください。
- 継続検索: 該当ポリシーで保護されるすべてのコンピュータで定期的に推奨設定の検索が実行されるようにポリシーを設定します。継続検索は、個々のコンピュータにも設定できます。このような検索では、実行済みの最後の検索のタイムスタンプが確認され、設定さ

れた間隔後に以降の検索が実行されます。こうすることで、環境内で異なる時間に推奨設定の検索が実行されます。この設定は、Agentが2~3日以上オンラインにならない可能性がある環境で役立ちます(たとえば、頻繁にインスタンスを構築および廃止するクラウド環境など)。"継続検索を設定する" on the next pageを参照してください。

- 手動検索: 1台以上のコンピュータで推奨設定の検索を1回実行します。手動検索は、プラットフォームやアプリケーションを最近大きく変更し、予約タスクを待つのではなく、強制的に新しい推奨設定を確認したい場合に便利です。"推奨設定の検索を手動で実行する" on the next pageを参照してください。
- コマンドライン: Deep Securityのコマンドラインインターフェースを使用して推奨設定の検索を開始します。"コマンドラインの基本" on page 447を参照してください。
- API: Deep Security APIを使用して推奨設定の検索を開始します。"Deep Security APIを使用したタスクの自動化" on page 478を参照してください。

注意: 予約タスクと進行中の検索では、それぞれ独自の設定で個別に推奨検索を実行できます。予約タスクまたは継続検索のどちらかを使用してください(ただし両方は使用しないでください)。

推奨設定の検索が実行されると、推奨設定の作成の対象となるすべてのコンピュータでアラートが発令されます。

予約タスクを作成して定期的に推奨設定の検索を実行する

1. Deep Security Managerで、[管理]→[予約タスク]画面に進みます。
2. ツールバーの [新規] をクリックし、[新規予約タスク] を選択して新規予約タスクウィザードを表示します。
3. [種類] リストで [コンピュータの推奨設定を検索] を選択して、検索を実行する頻度を選択します。[次へ] をクリックします。
4. 手順3で選択した内容に応じて、次の画面で検索の頻度をより詳細に指定できます。該当する項目を選択し、[次へ] をクリックします。
5. 検索対象のコンピュータを選択し、[次へ] をクリックします。

注意: すべてのコンピュータ、個々のコンピュータ、コンピュータのグループ、または特定のポリシーが割り当てられているコンピュータを選択できます。大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

6. 新しい予約タスクの名前を指定し、終了時にタスクを実行するかどうか ([[完了] でタスクを実行]) を選択して、[完了] をクリックします。

継続検索を設定する

1. 個々のコンピュータの検索を設定するか、ポリシーを使用するすべてのコンピュータの検索を設定するかに応じて、Deep Security Managerで、**コンピュータエディタまたはポリシーエディタ**¹を開きます。

注意: 大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

2. [設定] をクリックします。[Recommendations]の[General]タブで、の進行中の推奨設定の検索 設定で、進行中の推奨検索を有効または無効にします。[継続検索の間隔] 設定で、検索を実行する間隔を指定します。どちらの設定も、コンピュータまたはポリシーの親から継承できます (継承の仕組みの詳細については"[ポリシー、継承、およびオーバーライド](#)" on page 587を参照してください)。

推奨設定の検索を手動で実行する

1. Deep Security Managerで、[コンピュータ] 画面に進みます。
2. 検索対象のコンピュータ (複数台も可) を選択します。
3. [処理]→[推奨設定の検索] の順にクリックします。

推奨設定の検索をキャンセルする

推奨設定の検索は開始前にキャンセルできます。

1. Deep Security Managerで、[コンピュータ] 画面に進みます。
2. 検索をキャンセルするコンピュータ (複数台も可) を選択します。
3. [処理]→[推奨設定の検索のキャンセル] をクリックします。

推奨設定の検索からルールまたはアプリケーションの種類を除外する

推奨設定の検索結果に特定のルールまたはアプリケーションの種類を含めたくない場合は、それらを検索から除外できます。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

1. Deep Security Managerで**コンピュータエディタまたはポリシーエディタ**¹を開きます。

注意: 大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

2. 除外するルールの種類に応じて、[侵入防御] 画面、[変更監視] 画面、または [セキュリティログ監視] 画面に移動します。
3. [一般] タブで、[割り当て/割り当て解除] (ルールの場合) または [アプリケーションの種類] (アプリケーションの種類の場合) をクリックします。
4. 除外するルールまたはアプリケーションの種類をダブルクリックします。
5. [オプション] タブに進みます。ルールの場合は、[推奨設定から除外] を [はい] または [継承 (はい)] に設定します。アプリケーションの種類の場合は、[推奨設定から除外] チェックボックスをオンにします。

推奨設定を自動的に適用する

推奨設定の検索の結果を自動的に実装するのが適切な場合は、そのようにDeep Securityを設定できます。

1. Deep Security Managerで**コンピュータエディタまたはポリシーエディタ**²を開きます。

注意: 大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

2. 自動的に実装するルールの種類に応じて、[侵入防御] 画面、[変更監視] 画面、および/または [セキュリティログ監視] 画面に移動します(設定は保護モジュールごとに独立して変更できます)。
3. [一般] タブの [推奨設定] の設定を [はい] または [継承 (はい)] に変更します。

しかし、すべての推奨設定を自動的に実装できるわけではありません。次のような例外があります。

- 適用する前に設定が必要なルール。
- 推奨設定の検索から除外されたルール。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

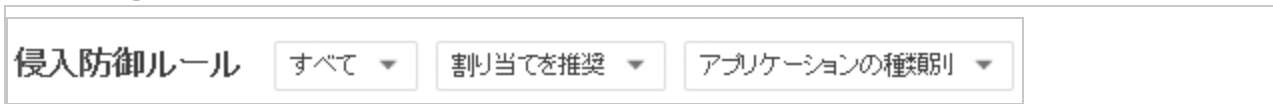
- 自動的に割り当てられた、または割り当て解除されたが、ユーザがオーバーライドしたルール。たとえば、Deep Securityによって自動的に割り当てられたルールをユーザが割り当て解除した場合、次回の推奨設定の検索の後にそのルールが再割り当てされることはありません。
- ポリシー階層の上位のレベルで割り当てられたルールは、下位のレベルでは割り当てを解除できません。ポリシーレベルでコンピュータに割り当てられたルールは、ポリシーレベルで割り当てを解除する必要があります。
- トレンドマイクロから発行されたものであるが、誤判定のリスクの可能性があるルール(ルールの説明を参照してください)。

検索結果を確認して手動でルールを割り当てる



最新の推奨設定の検索結果は、**コンピュータエディタまたはポリシーエディタ**¹の保護モジュールの [一般] タブ ([侵入防御]、[変更監視]、および [セキュリティログ監視]) に表示されます。

次の例は、ポリシーを使用して侵入防御の推奨設定の検索結果を扱う方法を示しています。

1. 推奨設定の検索が完了したら、検索したコンピュータに割り当てられているポリシーを開きます。
2. [侵入防御]→[一般] の順に選択します。存在する場合は未解決の推奨設定の数が [推奨設定] セクションに表示されます。
3. [現在割り当てられている侵入防御ルール] エリアの [割り当て/割り当て解除] をクリックしてルールの割り当て画面を開きます。
4. ルールを [アプリケーションの種類別] でソートし、フィルタの表示メニューから [割り当てを推奨] を選択します。



すると、割り当てが推奨されているが割り当てられていないルールのリストが表示されます。

5. ルールをポリシーに割り当てるには、ルール名の横にあるチェックボックスをオンにします。 アイコンが表示されているルールには、設定できる設定オプションがあります。 アイコンが表示されているルールには、ルールを有効にする前に設定する必要がある設定があります。


¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

また、複数のルールを一度に割り当てるには、<Shift> キーまたは <Control> キーを使用してルールを選択し、選択項目を右クリックして [ルールの割り当て] をクリックします。

ヒント: 推奨設定の検索の結果には、ルールの割り当てを解除する推奨設定を含めることもできます。この処理は、アプリケーションをアンインストールする場合、ベンダからのセキュリティパッチを適用する場合、または不要なルールが手動で適用されている場合に行うことができます。割り当ての解除が推奨されているルールを表示するには、フィルタの表示メニューから [割り当て解除を推奨] を選択します。

注意: 推奨ルールには完全フラグ (■) が示されます。部分フラグ (◀) は、アプリケーションの種類に属する一部のルールのみが推奨されているアプリケーションの種類を示します。

推奨ルールを設定する

適用前に設定が必要なルールもあります。たとえば、一部のセキュリティログ監視ルールでは、変更について監視するログファイルの場所を指定する必要があります。この場合、推奨設定が作成されるコンピュータでアラートが発令されます。アラートのテキストには、ルールの設定に必要な情報が含まれます。ポリシーエディタまたはコンピュータエディタで  アイコンが表示されているルールには、設定できる設定オプションがあります。アイコンが表示されているルールには、ルールを有効にする前に設定する必要がある設定があります。

一般的な脆弱性の追加ルールを実装する

推奨設定の検索は、実装する必要があるルールリストを作成するための適切な開始ポイントとなりますが、一般的な脆弱性には推奨設定の検索では特定されない追加のルールがいくつかあります。これらのルールは「防御」(ブロック) モードで実装される前に慎重に設定しテストする必要があるためです。トレンドマイクロでは、これらのルールを設定およびテストしてから、ポリシー (または個々のコンピュータ) で手動で有効にすることをお勧めします。

ヒント: 次のリストに、設定すべき最も一般的な追加ルールを示します。Deep Security Managerのその他のルールを確認するには、種類が「スマート」または「ポリシー」のルールを検索します。

ルール名	アプリケーションの種類
1007598 - Identified Possible Ransomware File Rename Activity Over Network Share	DCERPCサービス
1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network Share	DCERPCサービス
1006906 - Identified Usage Of PsExec Command Line Tool	DCERPCサービス
1007064 - Executable File Uploaded On System32 Folder Through SMB Share	DCERPCサービス
1003222 - Block Administrative Share	DCERPCサービス
1001126 - DNS Domain Blocker	DNSクライアント
1000608 - Generic SQL Injection Prevention 詳細については" SQLインジェクション防御ルールの設定 " on page 810 を参照	Webアプリケーション共通
1005613 - Generic SQL Injection Prevention - 2	Webアプリケーション共通
1000552 - Generic Cross Site Scripting (XSS) Prevention	Webアプリケーション共通
1006022 - Identified Suspicious Image With Embedded PHP Code	Webアプリケーション共通
1005402 - Identified Suspicious User Agent In HTTP Request	Webアプリケーション共通
1005934 - Identified Suspicious Command Injection Attack	Webアプリケーション共通
1006823 - Identified Suspicious Command Injection Attack - 1	Webアプリケーション共通
1005933 - Identified Directory Traversal Sequence In Uri Query Parameter	Webアプリケーション共通
1006067 - Identified Too Many HTTP Requests With Specific HTTP	Webサーバ共通

ルール名	アプリケーションの種類
Method	
1005434 - Disallow Upload Of A PHP File	Webサーバ共通
1003025 - Web Server Restrict Executable File Uploads	Webサーバ共通
1007212 - Disallow Upload Of An Archive File	Webサーバ共通
1007213 - Disallow Upload Of A Class File	Webサーバ共通

トラブルシューティング: 推奨設定の検索失敗

サーバでの推奨設定の検索失敗の場合は、次の手順に従って問題を解決します。トラブルシューティング後も問題が解決しない場合は、[Agentから診断パッケージを作成](#)して、サポートに問い合わせてください。

通信

通常、通信障害が発生すると、エラーメッセージ本文に「プロトコルエラー」が示されます。

Deep Security ManagerからAgentへの受信ファイアウォールを開いていなかった場合は、[ポート](#)を開くか、Agentからの通信に切り替えます。詳細については、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on page 408を参照してください。

サーバリソース

サーバのCPUリソースとメモリリソースを監視します。検索中にメモリまたはCPUが使い尽くされそうになる場合は、リソースを増やします。

タイムアウト値

推奨設定の検索のタイムアウト値を大きくします。

1. コマンドプロンプトを開いて、Deep Security Managerのインストールフォルダに移動します。
2. 以下のコマンドを入力します (マルチテナント環境の場合は、テナント名を追加します)。

```
dsm_c -action changesetting -name  
settings.configuration.agentSocketTimeoutOverride -value 1200
```

```
dsm_c -action changesetting -name  
settings.configuration.defaultSocketChannelTimeout -value 1200000
```

```
dsm_c -action changesetting -name  
settings.configuration.recoScanKeepAliveTimeInterval -value 180000
```

3. Deep Security Virtual Applianceを使用している場合は、次のコマンドも入力します。

```
dsm_c -action changesetting -name  
settings.configuration.timeoutEpssecScanRequest -value 1770
```

```
dsm_c -action changesetting -name  
settings.configuration.timeoutDsamCommandChannel -value 1800
```

コンピュータで使用可能なインタフェースの検出と設定

コンピュータエディタとポリシーエディタの [インタフェース] セクション (コンピュータエディタ) と [インタフェースの種類] セクション (ポリシーエディタ) には、コンピュータで検出されたインタフェースが表示されます。インタフェースが複数割り当てられたポリシーがコンピュータに割り当てられている場合、ポリシーで定義されたパターンと一致するインタフェースが検出されます。

ポリシーエディタの [インタフェースの種類] セクションにはこの他にも以下の機能があります。

複数のインタフェースに対してポリシーを設定する

コンピュータに複数のインタフェースがある場合は、ファイアウォールルールなどのポリシーの各種エレメントを各インタフェースに割り当てることができます。

1. ポリシーエディタで [インタフェースの種類] をクリックします。
2. [ネットワークインタフェースの種類] セクションで、[ルールを特定のインタフェースに適用] を選択します。
3. 表示された [インタフェースの種類] セクションで、名前とパターン照合文字列を入力します。

インタフェースの種類の名前は、参照用でのみ使用されます。一般的な名前には、「LAN」、「WAN」、「DMZ」、「Wi-Fi」などがありますが、どのような名前をネットワークのトポロジで使用してもかまいません。

すべてのコンテナネットワークインタフェースとホスト仮想インタフェースに使用されるインタフェース名は「integrated_veth」であり、MACアドレスは02:00:00:00:00:00です。

パターン照合ではワイルドカードによるインタフェース名の照合ができ、インタフェースを適切な種類へ自動マッピングします。たとえば、「ローカルエリア接続*」、「eth*」、「Wireless*」などのように照合します。自動でインタフェースをマッピングできないときは、アラートがトリガされます。その際は、特定のコンピュータのコンピュータエディタの [インタフェース] 画面から手動でマッピングできます。

注意: コンピュータ上で検出されたインタフェースが指定されたどの値とも一致しない場合、Managerはアラートをトリガします。

インタフェース制限を強制する

インタフェース制限が有効な場合、ファイアウォールでは、ローカルコンピュータのインタフェース名が、正規表現パターンと照合されます。インタフェース制限を強制するには、ポリシーエディタまたはコンピュータエディタの [ファイアウォール]→[インタフェース制限] タブにある [インタフェース制限の有効化] オプションをクリックして、コンピュータのインタフェース名と一致する文字列パターンを優先度順に入力します。

警告: インタフェース制限を有効にする前に、インタフェースパターンを適切な順序で設定し、必要な文字列パターンをすべて追加し、不要なパターンは削除してください。優先度が最も高いパターンのインタフェースのみが、トラフィックの転送を許可されます。それ以外のインタフェース (リスト内にある残りのパターンのいずれかと一致するインタフェース) は、「制限」されます。制限されたインタフェースは、ファイアウォールの [許可] ルールを使用して特定のトラフィックを許可しないかぎり、すべてのトラフィックをブロックします。

[1つのアクティブインタフェースに制限] を選択すると、優先度が最も高いパターンのインタフェースが複数見つかった場合でも、1つのインタフェースからのトラフィックのみが許可されます。

注意: Deep Securityは、POSIX基本正規表現を使用してインタフェース名を照合します。基本的なPOSIX正規表現の詳細については、https://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03を参照してください。

コンピュータエディタの [概要] セクション

コンピュータエディタの [概要] 画面には、次のタブがあります。

- "[一般] タブ" below
- "[処理] タブ" on page 608
- "[TPM] タブ" on page 610
- "[システムイベント] タブ" on page 611

[一般] タブ

- **ホスト名:** [コンピュータ] 画面の [名前] 列に表示されます。名前は、コンピュータのIPアドレスまたはコンピュータのホスト名のいずれかを指定する必要があります。IPアドレスの代わりにホスト名を使用する場合は、完全修飾ホスト名または相対ホスト名のいずれも使用できます。解決可能なホスト名、またはDeep Security Managerがアクセスできる有効なIPアドレスを指定する必要があります。これは、Deep Security ManagerとAgentコンピュータ間の通信がホスト名に基づいて行われるためです。Relay有効化済みAgentでは、Relayグループ内のすべてのコンピュータが、指定したIPアドレスまたはホスト名にアクセスする必要があります。Deep Security Managerが対象コンピュータにアクセスできない場合は、通信方向を [Agent/Applianceから開始] に設定する必要があります ([設定]→[コンピュータ])。
- **前回使用されたIP: <IP_address>:** コンピュータで前回使用されたIP。前回使用されたIPに表示されるのは、Deep Security AgentのホストのIPアドレスとは限りません。Deep Security Managerとの通信にAgentが使用するプロキシ、ロードバランサ、Elastic Load Balancer (ELB) などのIPアドレスである場合もあります。
- **表示名:** [表示名] 列、およびホスト名の値の横にある丸カッコ内に表示されます。
- **説明:** コンピュータの説明です。
- **プラットフォーム:** コンピュータのOSの詳細は、ここに表示されます。
- **グループ:** コンピュータの所属するコンピュータグループがリストに表示されます。コンピュータの割り当てを既存の別のコンピュータグループに変更できます。
- **ポリシー:** このコンピュータに割り当てたポリシーです (存在する場合)。

注意: ルールがポリシーとは独立して割り当てられている場合は、コンピュータでポリシーの割り当てを解除しても、そのルールが引き続きコンピュータ上で有効となることがあるので注意してください。

- 資産の重要度: Deep Security Managerでは、ランク付けシステムを使用してセキュリティイベントの重要度が数値化されます。ルールには重要度 (高、中、低など) が割り当てられ、資産 (コンピュータ) には「資産の重要度」レベルが割り当てられます。これらのレベルは、数値で表記されます。コンピュータでルールがトリガされると、資産の重要度の値とルールの重要度の値が乗算されます。この結果がスコアとなり、イベントを重要度別にソートする際に使用されます(イベントのランク付けは [イベント] 画面で参照できます)。この [資産の重要度] リストを使用して、コンピュータに資産の重要度を割り当てます (ルールおよび資産の重要度レベルを表す数値は、[管理]→[システム設定]→[ランク付け] で編集できます)。
- セキュリティアップデートのダウンロード元: このコンピュータ上のAgent/Applianceがセキュリティアップデートのダウンロード元として使用するRelayグループをリストから選択します (AgentがRelayとして機能している場合には表示されません)。

コンピュータのステータス

[ステータス] エリアには、コンピュータの最新情報と、そのコンピュータで有効になっている保護モジュールの最新情報が表示されます。1行目には、コンピュータがAgentまたはAppliance (コンバインモードの場合はその両方) によって保護されているかどうかが表示されます。

- ステータス:
 - コンピュータが管理対象外の場合、ステータスには、AgentまたはApplianceの有効性に関する状態が表示されます。ステータスには「検出済み」または「新規」が表示され、その後のカッコ内にAgentまたはApplianceの状態が示されます (「Agent/Applianceなし」、「不明」、「再有効化が必要」、「有効化が必要」、または「無効化が必要」)。
 - コンピュータが管理対象で、コンピュータのエラーがない場合は、ステータスに「管理対象」と表示され、その後のカッコ内にAgentまたはApplianceの状態が示されます (「オンライン」または「オフライン」)。
 - コンピュータが管理対象で、AgentまたはApplianceが変更の検索やAgentのアップグレード (インストールプログラムの送信) などの処理を実行している場合は、そのタスクのステータスが表示されます。
 - コンピュータに、「オフライン」、「アップデートの失敗」などのエラーがある場合、ステータスにはそのエラーが表示されます。複数のエラーが存在する場合、ステータスには「複数のエラー」と表示され、その下に各エラーが一覧表示されます。

保護モジュールのステータス

Deep Security 9.5以降の保護モジュールを実装するソフトウェアは、必要に応じてAgentに配信されます。Agentが最初にインストールされた時点では、コアモジュールだけが含まれています。

[ステータス] エリアには、Deep Securityモジュールの状態に関する情報が表示されます。ステータスには、Agent上のモジュールの状態およびDeep Security Managerでのモジュールの設定が反映されます。あるモジュールのステータスが「オン」の場合、そのモジュールはDeep Security Managerで設定済みであり、Deep Security Agentにインストールされて実行中です。

モジュールが「オン」で動作している場合、ステータスライトは緑色になります。個別にルールを割り当て可能なモジュールの場合、ステータスライトが緑色になるためには、少なくとも1つのルールが割り当てられている必要があります。

- 不正プログラム対策: 不正プログラム対策保護がオンとオフのどちらであるか、およびリアルタイム検索または手動検索のどちらについて設定されているかを示します。
- Webレピュテーション: Webレピュテーションがオンとオフのどちらであることを示します。
- ファイアウォール: ファイアウォールのオン/オフの状態と有効なルールの数を示します。
- 侵入防御: 侵入防御のオン/オフの状態と有効なルールの数を示します。
- 変更監視: 変更監視のオン/オフの状態と有効なルールの数を示します。
- セキュリティログ監視: セキュリティログ監視のオン/オフの状態と有効なルールの数を示します。
- アプリケーションコントロール: アプリケーションコントロールがオンとオフのどちらであることを示します。
- Scanner (SAP): Deep Security ScannerSAP機能のステータス。
- オンライン: Managerが現在AgentまたはApplianceと通信可能かどうかを示します。
- 前回の通信: ManagerがこのコンピュータのAgentまたはApplianceと正常に通信した前回の日時です。
- ステータスの確認: Managerによってただちにハートビート操作が強制実行されて、AgentまたはApplianceのステータスが確認されます。ステータスの確認では、AgentまたはApplianceのセキュリティアップデートは実行されません。ManagerとAgentまたはAppliance間の通信が [Agent/Applianceから開始] に設定されている場合は、[ステータスの確認] ボタンが無効になります。ステータスを確認しても、コンピュータのログはアッ

プデートされません。コンピュータのログをアップデートするには、[処理] タブに進みます。

- 警告/エラーのクリア: このコンピュータに対するアラートまたはエラーを消去します。
- ESXiサーバ: コンピュータがVirtual Applianceによって保護されている仮想マシンの場合は、コンピュータをホストするESXiサーバが表示されます。
- Appliance: コンピュータがVirtual Applianceによって保護されている仮想マシンの場合は、コンピュータを保護するApplianceが表示されます。
- ESXiバージョン: コンピュータがESXiサーバの場合は、ESXiのバージョン番号が表示されます。
- Filter Driverのバージョン: コンピュータがESXiサーバの場合は、Filter Driverのバージョン番号が表示されます。Deep Security Virtual Appliance 10.0以降とESXi 6.0以降を使用している場合は、Filter Driverを使用していないため「なし」と表示されます。
- ゲスト: コンピュータがESXiサーバの場合は、Virtual Applianceとゲストが表示されます。
- Applianceのバージョン: コンピュータがVirtual Applianceの場合は、Applianceのバージョン番号が表示されます。
- ゲストが保護される対象: コンピュータがVirtual Applianceの場合は、ESXiサーバのIPと保護されているゲストが表示されます。

VMware仮想マシンの概要

このセクションには、AgentまたはApplianceが実行される仮想マシンに関するハードウェアとソフトウェアの設定情報の概要が表示されます (VMware仮想マシンのみ)。

[処理] タブ

有効化

新たにインストールされたDeep Security AgentまたはApplianceは、ポリシー、ルール、イベントログへのリクエストなどを受信する前にDeep Security Managerにより「有効化」する必要があります。有効化処理では、Manager (またはそのいずれかのノード) とAgent/Aplianceが互いを一意に識別するためのSSLキーが交換されます。Deep Security Managerによって有効化されたAgent/Aplianceは、有効化を実施したDeep Security Manager (またはそのいずれかのノード) からの指示または通信のみを許可するようになります。

有効化されていないAgentまたはApplianceは、どのDeep Security Managerでも有効化できません。

AgentおよびApplianceの無効化は、コンピュータ上でローカルに実施するか、または有効化を行ったDeep Security Managerで実施する必要があります。AgentまたはApplianceがすでに有効化されている場合は、このエリアのボタンが [有効化] ではなく [再有効化] と表示されます。再有効化の作用は、有効化と同じです。再有効化すると、AgentまたはApplianceは最初にインストールされたときの状態にリセットされ、新しいSSLキーセットの交換が行われます。

ポリシー

Deep Security Managerを使用してコンピュータ上のAgentまたはApplianceの設定を変更した場合 (新しい侵入防御ルールの適用やログ設定の変更など) は、Deep Security Managerから新しい情報をAgentまたはApplianceに送信する必要があります。これが「ポリシーの送信」命令です。ポリシーのアップデートは通常ただちに実行されますが、[ポリシーの送信] ボタンをクリックして強制的にアップデートすることもできます。

Agentソフトウェア

ここには、コンピュータ上で現在実行されているAgentまたはApplianceのバージョンが表示されます。コンピュータのプラットフォームに対応する新しいバージョンのAgentまたはApplianceが入手可能な場合は、[Agentのアップグレード] または [Applianceのアップグレード] ボタンをクリックして、Deep Security ManagerからリモートでAgentまたはApplianceをアップグレードできます。いずれかのコンピュータで新しいバージョンのAgentまたはApplianceソフトウェアが実行されている場合にDeep Security Managerでアラートをトリガするように設定するには、[管理]→[システム設定]→[アップデート] の順に選択します。

注意: WindowsでDeep Security AgentやRelayをアップデートまたはアンインストールする際は、Agentセルフプロテクションを無効にしておく必要があります。この操作を行うには、Deep Security Managerで、**コンピュータエディタ**¹の [設定]→[一般] に移動します。[Agentセルフプロテクション] で、[ローカルのエンドユーザーによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。

Agentでこの機能を有効にするには、[Relayの有効化] をクリックします。Relay機能が有効なAgentは、最新のセキュリティアップデートとソフトウェアアップデートを取得し、既存のアップデート設定に従って配布します。Relayの詳細については、"[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照してください。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

サポート情報

[診断パッケージの作成] ボタンでは、コンピュータのAgentまたはApplianceの状態に関するスナップショットを作成できます。スナップショットは、サポート担当者がトラブルシューティングの目的で要求することがあります。

コンピュータとの通信が失われた場合は、診断パッケージをローカルに作成できます。詳細については、"[診断パッケージとログの作成](#)" on page 1573を参照してください。

[TPM] タブ

注意: [TPM] タブは、ESXiサーバの [処理] タブの代わりに表示されます。

Trusted Platform Module (TPM) は、ハードウェア認証に使用されるチップの一種です。VMwareは、ESXiハイパーバイザでTPMを使用します。起動シーケンスの間、ESXiは各ハイパーバイザコンポーネントのSHA-1ハッシュを、読み込み時に一連のレジスタに書き込みます。ある起動シーケンスから次の起動シーケンスまでの間、これらの値に想定外の変更が発生した場合は、セキュリティの問題があることを示している可能性があるため、調査することをお勧めします。Deep Securityでは、起動のたびにESXiのTPMを監視し、変更が検出された場合はアラートを発令できます。TPMをサポートしないESXiでTPM監視を有効にするオプションを選択すると、そのオプションは自動的に無効になります。

TPM監視の有効化: 選択すると、TPM監視が有効化されます。

TPMの監視で有効なレジスタ値を取得できなかった場合にアラートを発令します: 選択すると、ESXi起動シーケンスの間にTPMモジュールがハイパーバイザコンポーネントの有効なレジスタ値を取得できなかった場合に、Deep Securityによってアラートが発令されます。

TPMのレジスタデータのインポート: TPMデータがインポートされているかどうかを示します。

前回のTPMチェック: 前回いつTPMがチェックされたかを示します。[今すぐ確認] をクリックすると、TPMチェックを開始できます。

注意: TPM監視の最小要件は次のとおりです。

- ESXiにTPM/TXTがインストールされ、有効になっている (詳細についてはVMwareドキュメントを参照)
- Deep Securityの変更監視およびアプリケーションコントロールモジュールの適切なライセンスがある

[システムイベント] タブ

イベントについては、"[システムイベント](#)" on page 1271を参照してください。

ポリシーエディタの [概要] セクション

ポリシーエディタの [概要] セクションには、次のタブがあります。

- "[一般] タブ" below
- "[このポリシーを使用しているコンピュータ] タブ" on the next page
- "[イベント] タブ" on the next page

[一般] タブ

一般

- 名前:[表示名] 列、およびホスト名の値の横にある丸カッコ内に表示されます。
- 説明: コンピュータの説明です。

継承

現在のポリシーの設定の継承元である親ポリシー (ある場合) を特定します。

モジュール

- 不正プログラム対策:不正プログラム対策保護がオンとオフのどちらであるか、およびリアルタイム検索または手動検索のどちらについて設定されているかを示します。
- Webレピュテーション:Webレピュテーションがオンとオフのどちらであるかを示します。
- ファイアウォール:ファイアウォールのオン/オフの状態と有効なルールの数を示します。
- 侵入防御:侵入防御のオン/オフの状態と有効なルールの数を示します。
- 変更監視:変更監視のオン/オフの状態と有効なルールの数を示します。
- セキュリティログ監視:セキュリティログ監視のオン/オフの状態と有効なルールの数を示します。
- アプリケーションコントロール:アプリケーションコントロールがオンとオフのどちらであるかを示します。

[このポリシーを使用しているコンピュータ] タブ

このポリシーが割り当てられているコンピュータを一覧表示します。

[イベント] タブ

イベントについては、"[システムイベント](#)" on page 1271を参照してください。

ネットワークエンジン設定

ポリシーまたはコンピュータのネットワークエンジンの設定を編集するには、設定するポリシーまたはコンピュータの[ポリシーエディタ](#)¹または[コンピュータエディタ](#)²を開き、[設定]→[詳細] をクリックします。

注意: [詳細] タブには、[イベント] 設定もあります。これらの設定については、"[ログファイルのサイズを制限する](#)" on page 1125を参照してください。このタブには、[Agentの設定パッケージが最大サイズを超えた場合にアラートを生成する] 設定もあります。この設定を使用して、[Agentの設定パッケージが大きすぎる] 設定の表示を制御します。

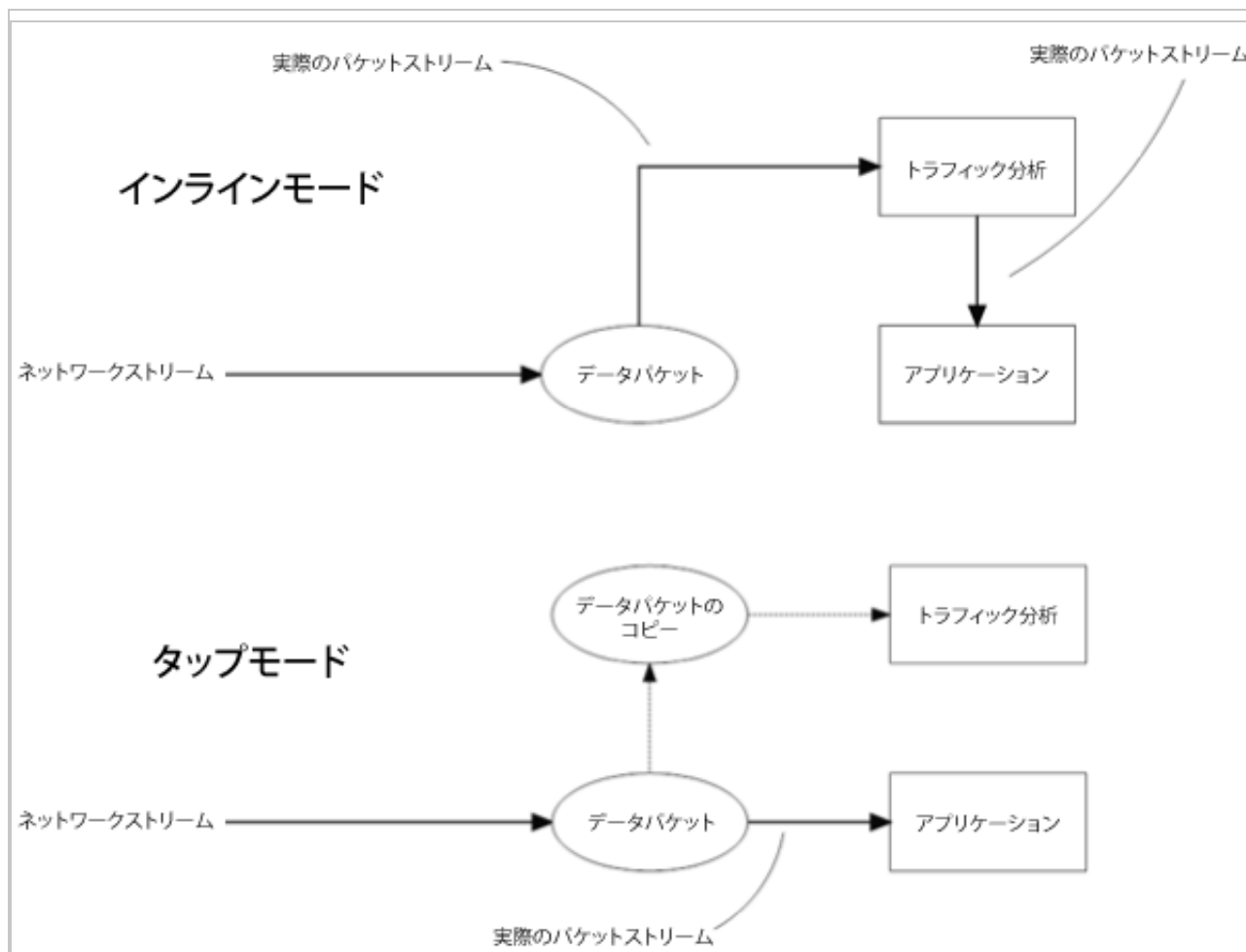
以下の設定を使用できます。

- ネットワークエンジンモード: ネットワークエンジンは、パケットをブロックするか許可するかを決定するコンポーネントであり、侵入防御、ファイアウォール、Webレピュテーションの各モジュール内にあります。ファイアウォール および 侵入防御 モジュールの場合、ネットワークエンジンはパケットの健全性チェックを実行し、各パケットがファイアウォール ルールと 侵入防御 ルール (「」に一致するルール」 とも呼ばれます) を通過することも確認します。ネットワークエンジンは、インラインモードまたはタップモードで動作できます。インラインで動作している場合、パケットストリームはネットワークエンジンを通り、設定したルールに基づいて破棄または転送されます。ステートフルテーブルが維持され、ファイアウォール ルールが適用され、侵入防御 ルールとファイアウォール ルールを適用できるようにトラフィックの正規化が実行されます。タップモードで動作している場合、パケットは常に渡されます。ただし、ドライバのフッ

¹ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

²コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

クの問題またはインターフェースの隔離は例外です。タップモードでは、パケット遅延も導入されるため、スループットが低下する可能性があります。



- エラー発生時の処理: この設定では、不良パケット検出時のネットワークエンジンの動作を決定します。初期設定 (Fail-Closed) では、不良パケットはブロックされますが、後述する理由により、一部の不良パケットを通過させることもできます (Fail-Open)。
 - ネットワークエンジンのシステムエラー: この設定では、メモリ不足エラー、割り当てメモリエラー、ネットワークエンジン (DPI) デコードエラーなど、ネットワークエンジンホストのシステムエラーによって生じる不良パケットを、ネットワークエンジンでブロックするか許可するかを決定します。オプションは次のとおりです。
 - Fail-Closed (初期設定): ネットワークエンジンで不良パケットをブロックします。ルールマッチングは実行しません。このオプションを使用すると、最も高いレベルのセキュリティが提供されます。

- Fail-Open: ネットワークエンジンで不良パケットの通過を許可します。ルールマッチングは実行せず、イベントをログに記録します。高負荷やリソース不足によりAgentまたはVirtual Applianceでネットワーク例外が頻繁に発生する場合は、[Fail-Open]の使用を検討してください。
- ネットワークパケットのサニティチェックエラー: この設定では、パケットのサニティチェックでエラーとなるパケットを、ネットワークエンジンでブロックするか許可するかを決定します。健全性チェック失敗の例: ファイアウォール 正常性検査の失敗、ネットワーク層2,3、または4属性の確認の失敗、TCPの状態の確認の失敗。オプションは次のとおりです。
 - Fail-Closed (初期設定): ネットワークエンジンでエラーパケットをブロックします。ルールマッチングは実行しません。このオプションを使用すると、最も高いレベルのセキュリティが提供されます。
 - Fail-Open: ネットワークエンジンでエラーパケットの通過を許可します。エラーパケットに対するルールマッチングは実行せず、イベントをログに記録します。ルールマッチング機能を維持しつつ、パケットのサニティチェックを無効にしたい場合は、[Fail-Open]の使用を検討してください。
- 回避技術対策モード: 回避技術対策の設定では、分析を回避しようとする異常なパケットに対するネットワークエンジンによる処理を管理します。詳細については、"[回避技術対策の設定](#)" on page 827を参照してください。
- ネットワークエンジンの詳細オプション: [継承] チェックボックスをオフにすると、以下の設定をカスタマイズできます。
 - CLOSEDタイムアウト: ゲートウェイで使用します。ゲートウェイが「ハードクローズ」(RST)を伝えると、RSTを受信したゲートウェイ側は、接続を終了するまで、設定された時間の間、接続をアライブにします。
 - SYN_SENTタイムアウト: 接続を終了するまでSYN_SENT状態になっている時間。
 - SYN_RCVDタイムアウト: 接続を終了するまでSYN_RCVD状態になっている時間。
 - FIN_WAIT1タイムアウト: 接続を終了するまでFIN_WAIT1状態になっている時間。
 - ESTABLISHEDタイムアウト: 接続を終了するまでESTABLISHED状態になっている時間。
 - ERRORタイムアウト: エラー状態で接続を保持する時間(UDP接続の場合、エラーはさまざまなUDPの問題が原因で発生する可能性があります。TCP接続の場合、おそらく、ファイアウォール。)によってパケットが破棄されたためです。
 - DISCONNECTタイムアウト: 切断するまで接続がアイドル状態になっている時間。

- CLOSE_WAITタイムアウト: 接続を終了するまでCLOSE_WAIT状態になっている時間。
- CLOSINGタイムアウト: 接続を終了するまでCLOSING状態になっている時間。
- LAST_ACKタイムアウト: 接続を終了するまでLAST_ACK状態になっている時間。
- ACKストームタイムアウト: ACKストーム内で再送されるACK間の最長期間。つまり、ACKが再送される頻度が低く、このタイムアウトが発生した場合、ACKはACKストームの一部とはみなされません。
- ブートスタートタイムアウト: ゲートウェイで使われます。ゲートウェイが再起動される時、ゲートウェイを通過している既存の接続が確立している場合があります。このタイムアウトでは、ゲートウェイが再起動される前に、確立された接続の一部である非SYNパケットを許可する時間が定義されます。
- コールドスタートタイムアウト: ステートフル機能が開始される前に、確立された接続に属している非SYNパケットを許可する時間。
- UDPタイムアウト: UDP接続の最大時間。
- ICMPタイムアウト: ICMP接続の最大時間。
- Null IPを許可: 送信元または送信先IPアドレスがないパケットを許可またはブロックします。
- バージョン8以前のAgentとApplianceでIPv6をブロック: バージョン8.0以前のAgentおよびApplianceでIPv6パケットをブロックまたは許可します。

注意: Deep Security AgentおよびApplianceバージョン8.0以前では、ファイアウォール またはDPIルールをIPv6ネットワークトラフィックに適用できないため、これらの古いバージョンの初期設定ではIPv6トラフィックをブロックします。

- バージョン9以降のAgentとApplianceでIPv6をブロック: バージョン9.0以降のAgentおよびApplianceでIPv6パケットをブロックまたは許可します。
- 接続クリーンアップタイムアウト: 切断された接続のクリーンアップ時間 (次を参照)。
- 最大接続数 (クリーンアップ単位): 定期的な接続クリーンアップごとに実施するクリーンアップで切断される接続の最大数 (前を参照)。
- 送信元と送信先が同じIPアドレスをブロック: 送信元および送信先IPアドレスが同じパケットをブロックまたは許可します(ループバックインタフェースには適用されません)。
- 最大TCP接続数: 最大TCP同時接続数。

- 最大UDP接続数: 最大UDP同時接続数。
- 最大ICMP接続数: 最大ICMP同時接続数。
- 最大イベント数 (秒単位): 毎秒書き込み可能なイベントの最大数。
- TCP MSSの制限: 「TCP MSS」は、TCPセグメントの最大セグメントサイズをバイト単位で定義するTCPヘッダ内のパラメータです。[TCP MSS制限]設定は、TCP MSSパラメータに許可される最小値を定義します。このパラメータの下限值を設定することは重要です。なぜなら、リモートの攻撃者が最大セグメントサイズ (TCP / IP) が非常に小さいセグメント (MSS) を設定した場合に発生するカーネルパニック攻撃やDoS (サービス拒否) 攻撃を防ぐためです。これらの攻撃の詳細については、CVE-2019-11477、CVE-2019-11478、およびCVE-2019-11479を参照してください。「TCP MSS Limit」の初期設定は128バイトで、ほとんどの攻撃サイズに対して保護されます。「No Limit」の値は、下限がなく、TCP MSS値が許可されていることを意味します。

注意: [TCP MSS制限]オプションは、次のDeep Security Agentのバージョンでのみ機能します。

Deep Security Agent 20

Deep Security Agent 12.0アップデート1以降

Deep Security Agent 11.0アップデート13以降

Deep Security Agent 10.0アップデート20以降

- イベントノードの数: いつでもログ/イベントを折りたためるよう、ドライバがそれらを格納するのに使用するカーネルメモリの最大容量。

注意: イベントの折りたたみは、同じ種類のイベントが連続して多く発生したときに実行されます。このとき、Agent/Applianceはすべてのイベントを1つに折りたたみます。

- ステータスコードの無視: このオプションは、特定の種類のイベントを無視します。たとえば、たくさんの「不正なフラグ」が表示される場合は、そのイベントの全インスタンスを無視してかまいません。
- 詳細なログ記録ポリシー:
 - バイパス: イベントをフィルタしません。上記の [ステータスコードの無視] 設定およびその他の詳細設定をオーバーライドします。ただし、Deep Security Managerで定義された他のログ設定はオーバーライドしません。たとえば、Deep Security Managerの[ファイアウォール ステートフル設定のプロパティ]画

面でファイアウォールステートフル設定ログオプションが設定されても、影響を受けることはありません。

- 標準: 再送の破棄を除くすべてのイベントがログに記録されます。
- 初期設定: エンジンがタップモードの場合は下の [タップモード] に切り替わり、インラインモードの場合は、[標準] に切り替わります。
- 下位互換性モード: サポートでのみ使用します。
- 詳細モード: 「標準モード」で記録されるログに加え、再送の破棄イベントも記録します。
- ステートフルおよび正規化の抑制: 「再送の破棄」、「セッション情報なし」、「不正なフラグ」、「不正なシーケンス」、「不正なACK」、「許可されていないUDP応答」、「許可されていないICMP応答」、および「ポリシーで未許可」を無視します。
- ステートフル、正規化、およびフラグメントの抑制: フラグメンテーション関連のイベントに加え、[ステートフルおよび正規化の抑制] が無視するものすべても無視します。
- ステートフル、フラグメント、および検証機能の抑制: [ステートフル、正規化、およびフラグメントの抑制] が無視するものすべてに加えて、確認に関するイベントも無視します。
- タップモード: 「再送の破棄」、「セッション情報なし」、「不正なフラグ」、「不正なシーケンス」、「不正なACK」、「ACK再送の上限」、「切断された接続上のパケット」を無視します。

注意: [ステートフルおよび正規化の抑制]、[ステートフル、正規化、およびフラグメントの抑制]、[ステートフル、フラグメント、および検証機能の抑制]、[タップモード]の各モードで無視されるイベントの包括的なリストについては、"[ログに記録するイベントの数を減らす](#)" on page 1136を参照してください。

- サイレントTCP接続拒否: サイレントTCP接続の破棄がオンの場合、RSTパケットはローカルスタックへのみ送信され、送信元にRSTパケットは送信されません。これにより、潜在的な攻撃者に返す情報量は削減されます。

注意: [サイレントTCP接続拒否]を有効化する場合、DISCONNECTタイムアウトも調整する必要があります。DISCONNECTタイムアウトの値の範囲は、0秒から10分までの間で設定します。この値は、Deep Security Agent/Applianceが接続を切断する前にアプリケーション側で切断できるように、十分に高く設定する必要があります。

す。DISCONNECTタイムアウト値に影響を与える要因としては、OS、接続を確立するアプリケーション、およびネットワークトポロジーが挙げられます。

- デバッグモードを有効にする: デバッグモードの場合、Agent/Applianceは特定のパケット数を取り込みます (下記の [デバッグモードで保持するパケットの数] 内の設定を参照)。ルールがトリガされてデバッグモードがオンになると、Agent/Applianceはルールがトリガされる前に通過した最後のパケット数Xを記録として保持します。これらのパケットは、デバッグイベントとしてManagerに返されます。

注意: デバッグモードでは簡単に大量のログが生成されるので、サポート担当者が指示した場合にのみ使用してください。

- デバッグモードで保持するパケットの数: デバッグモードがオンのとき、維持してログするパケット数。
- すべてのパケットデータをログに記録: 特定の ファイアウォール または 侵入防御ルールに関連付けられていないイベントのパケットデータを記録します。つまり、「再送の破棄」や「不正なACK」などのイベントのパケットデータを記録します。

注意: イベントの集約によってまとめられたイベントのパケットデータは保存できません

- 期間内で1つのパケットデータのみをログに記録する: このオプションを有効にして [すべてのパケットデータをログに記録する] を有効にしない場合、ほとんどのログにはヘッダデータのみが含まれます。パケット全体は、[1つのパケットデータのみをログに記録する期間] の指定に従って定期的に記録されます。
- 1つのパケットデータのみをログに記録する期間: [1つのパケットデータのみをログに記録する期間] を有効にした場合、この設定にログにパケット全体のデータを含める頻度を指定できます。
- パケットデータがキャプチャされたときに格納する最大データサイズ: ログに追加されるヘッダデータまたはパケットデータの最大サイズ。
- TCP用接続イベントの生成: TCP接続が確立されるたびに、ファイアウォール イベントを生成します。
- ICMP接続イベントの生成: ICMP接続が確立されるたびに、ファイアウォール イベントが生成されます。
- UDPの接続イベントを生成する: UDP接続が確立されるたびに、ファイアウォール イベントを生成します。

- Cisco WAAS接続のバイパス: このモードでは、専用のCISCO WAAS TCPオプションを選択して開始された接続に対して、TCPシーケンス番号のステートフル分析をバイパスします。このプロトコルは、ステートフル ファイアウォール チェックに干渉する無効なTCPシーケンス番号およびACK番号の余分な情報を保持します。CISCO WAASを使用していて、ファイアウォール ログに無効なSEQまたは無効なACKが表示されている場合にのみ、このオプションを有効にしてください。このオプションを選択すると、WAASが有効化されていない接続に対してもTCPステートフルシーケンス番号の確認が実行されます。
- 回避再送の破棄: 処理済みのデータを含む受信パケットは、回避再送の攻撃を避けるため、破棄されます。
- TCPチェックサムの確認: セグメントのチェックサムフィールドのデータは、セグメントの整合性を評価するために使用されます。
- 最小フラグメントオフセット: 許容可能な最小のIPフラグメントオフセットを定義します。オフセットがこの値未満のパケットは、「最小オフセット値以下のIPフラグメント」という理由で破棄されます。0を設定すると制限がなくなります。初期設定は60です。
- 最小フラグメントサイズ: 許容可能な最小のIPフラグメントサイズを定義します。この値より小さいフラグメント化されたパケットは、「最初のフラグメントが最小サイズ未満」という不正の可能性により破棄されます。初期設定は120です。
- SSLセッションのサイズ: SSLセッションキーに保持されるSSLセッションエントリの最大数を設定します。
- SSLセッションの時間: SSLセッション更新キーの有効期間を設定します。
- Ipv4トンネルのフィルタ: このバージョンのDeep Securityでは使用されません。
- IPv6トンネルのフィルタ: このバージョンのDeep Securityでは使用されません。
- 厳密なTeredoのポート確認: このバージョンのDeep Securityでは使用されません。
- Teredoの異常のドロップ: このバージョンのDeep Securityでは使用されません。
- 最大トンネル深度: このバージョンのDeep Securityでは使用されません。
- 最大トンネル深度超過時の処理: このバージョンのDeep Securityでは使用されません。
- Ipv6拡張タイプ0のドロップ: このバージョンのDeep Securityでは使用されません。
- 最小MTU未満のIPv6フラグメントのドロップ: IETF RFC 2460によって規定された最小MTUサイズに満たないIPv6フラグメントがドロップされます。

- IPv6予約済みアドレスのドロップ: 次の予約済みアドレスをドロップします。
 - IETFによって予約済み 0000::/8
 - IETFによって予約済み 0100::/8
 - IETFによって予約済み 0200::/7
 - IETFによって予約済み 0400::/6
 - IETFによって予約済み 0800::/5
 - IETFによって予約済み 1000::/4
 - IETFによって予約済み 4000::/2
 - IETFによって予約済み 8000::/2
 - IETFによって予約済み C000::/3
 - IETFによって予約済み E000::/4
 - IETFによって予約済み F000::/5
 - IETFによって予約済み F800::/6
- Ipv6サイトローカルアドレスのドロップ: サイトローカルアドレスFEC0::/1をドロップします。
- IPv6 Bogonアドレスのドロップ: 次のアドレスをドロップします。
 - ループバック ::1
 - IPv4互換アドレス ::/96
 - IPv4にマッピングされたアドレス ::FFFF:0.0.0.0/96
 - IPv4にマッピングされたアドレス ::/8
 - OSI NSAP用プレフィックス (RFC4048非推奨) 0200::/7
 - 6bone (非推奨) 3ffe::/16
 - 文書記述用アドレスプレフィックス 2001:db8::/32
- 6to4 Bogonアドレスのドロップ: 次のアドレスをドロップします。
 - 6to4 IPv4マルチキャスト 2002:e000:: /20
 - 6to4 IPv4ループバック 2002:7f00:: /24
 - 6to4 IPv4初期設定 2002:0000:: /24
 - 6to4 IPv4無効 2002:ff00:: /24
 - 6to4 IPv4 10.0.0.0/8 2002:0a00:: /24

- 6to4 IPv4 172.16.0.0/12 2002:ac10:: /28
- 6to4 IPv4 192.168.0.0/16 2002:c0a8:: /32
- ゼロペイロードのIPパケットのドロップ: ゼロ長ペイロードのIPパケットをドロップします。
- 不明なSSLプロトコルを破棄: クライアントが間違っただプロトコルでDeep Security Managerに接続しようとした場合に接続を破棄します。初期設定では、プロトコルが「http/1.1」以外であるとエラーになります。
- Allow DHCP DNS : 次の ファイアウォール ルールが有効かどうかを制御します。

ルールの種類	優先度	方向	プロトコル	送信元ポート	送信先ポート
強制的に許可	4	送信	DNS	任意	53
強制的に許可	4	送信	DHCP	68	67
強制的に許可	4	受信	DHCP	67	68

ルールを有効にすると、Agentコンピュータは表示されているプロトコルとポートを使用してManagerに接続できます。このプロパティには、以下の値を使用できます。

- 継承: ポリシーから設定を継承します。
 - ルールをオフにする: ルールを無効にします。この設定によって、Agentコンピュータがオフラインで表示されることがあります。
 - DNSクエリを許可: DNS関連のルールのみを有効にします。
 - DNSクエリとDHCPクライアントを許可: 3つすべてのルールを有効にします。
- 強制ICMPタイプ3コード4 : 次の非表示の ファイアウォール ルールが有効かどうかを制御します。

ルールの種類	優先度	方向	プロトコル	種類	コード
強制的に許可	4	受信	ICMP	3	4

有効にすると、これらのルールによって、RelayコンピュータをManagerに接続してRelayのハードビートが送信されるようになります。以下の値を使用できます。

- 継承: ポリシーから設定を継承します。
 - ルールをオフにする: ルールを無効にします。この値によって、接続がタイムアウトするか、「送信先に到達できません」という応答が発生する可能性があります。
 - ICMP type3 code4の「強制的に許可」ルールの追加: このルールを有効にします。
-
- フラグメントタイムアウト: このように設定されている場合、侵入防御ルールは、パケット（またはパケットフラグメント）の内容が不審と判断された場合、その内容を検査します。この設定では、検査後、パケットを破棄するまで残りのパケットフラグメントを待機する時間が定義されます。
 - 保持するフラグメント化されたIPパケットの最大数: Deep Securityで保持されるフラグメント化されたIPパケットの最大数を指定します。
 - フラグメント化されたパケットのタイムアウトを超過したことを示すためにICMPを送信する: この設定を有効にした場合、フラグメントのタイムアウトを過ぎるとICMPパケットがリモートコンピュータに送信されます。
 - ホストに属さないMACアドレスのバイパス: 送信先MACアドレスがホストに属していない受信パケットをバイパスします。このオプションを有効にすると、バージョン10.2以降のAgentおよびAppliance上で、NICチームングまたはプロミスキャスモードのNICのために作成されるパケットの取得によって発生するネットワークイベントの数が減少します。

ポリシーのルール、リスト、およびその他の共通オブジェクトの定義

[共通オブジェクト] 画面 (Deep Security Managerで [ポリシー]→[共通オブジェクト] の順に選択) で作成したオブジェクトは、さまざまなポリシーやルールで再利用できます。作成した共通オブジェクトをポリシーエディタまたはコンピュータエディタで使用する際には、オブジェクトの設定をそのポリシーまたはコンピュータ向けにオーバーライドできます。ポリシーまたはコンピュータレベルで共通オブジェクトのプロパティを継承またはオーバーライドする方法については、"[ポリシー、継承、およびオーバーライド](#)" on page 587を参照してください。

ヒント: 共通オブジェクトの作成と設定は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド [「Create and Configure Common Objects for Policies and Computers」](#) を参照してください。

ルール

一部の保護モジュールはルールを利用します。

- ["ファイアウォールルールの作成" on page 850](#)
- [ポリシーで使用する侵入防御ルールの設定](#)
- ["変更監視ルールの作成" on page 895](#)
- ["ポリシーで使用するセキュリティログ監視ルールを定義する" on page 907](#)

リスト

- ["ポリシーで使用するディレクトリリストの作成" on page 669](#)
- ["ポリシーで使用するファイル拡張子リストの作成" on page 672](#)
- ["ポリシーで使用するファイルリストの作成" on page 674](#)
- ["ポリシーで使用するIPアドレスリストの作成" on page 677](#)
- ["ポリシーで使用するMACアドレスリストの作成" on page 679](#)
- ["ポリシーで使用するポートリストの作成" on page 678](#)

その他

- ["ポリシーで使用するコンテキストの定義" on page 680](#)
- ["ステートフルファイアウォールの設定の定義" on page 878](#)
- ["不正プログラム検索の設定" on page 733](#)
- ["ルールに適用するスケジュールの定義" on page 687](#)

ファイアウォールルールの作成

ファイアウォールルールは、個々のパケットの制御情報を確認し、定義された条件に従ってブロックまたは許可します。ファイアウォールルールは、ポリシー、または直接コンピュータに割り当てることができます。

注意: ここでは、ファイアウォールルールの作成方法を具体的に説明します。ファイアウォールモジュールの設定方法については、["Deep Securityファイアウォールの設定" on page 836](#)を参照してください。

新しいファイアウォールルールを作成するには、次の手順を実行する必要があります。

1. "新しいルールを追加する" below。
2. "ルールの動作とプロトコルを選択する" below。
3. "パケットの送信元と送信先を選択する" on page 627。

ファイアウォールルールを作成したら、次の方法も学習できます。

- "ルールイベントとアラートを設定する" on page 628
- "ルールのスケジュールを設定する" on page 628
- "ルールが割り当てられているポリシーとコンピュータを確認する" on page 629
- "ルールにコンテキストを割り当てる" on page 629

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[ファイアウォールルール] ページで新しいファイアウォールルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新規ファイアウォールルール] の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存のルールをコピーして変更します。[ファイアウォールルール] リストで、該当のルールを右クリックし、[複製] をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ] をクリックします。

ルールの動作とプロトコルを選択する

1. ルールの [名前] と [説明] を入力します。

ヒント: ファイアウォールルールへの変更をそのルールの [説明] フィールドに記録することを推奨します。ファイアウォールのメンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールがパケットに対して実行する [処理] を選択します。次の5つの処理のいずれかを選択できます。

注意: 1つのパケットに適用されるのは、1つのルール処理だけです。同じ優先度のルールが複数ある場合は、下記の優先順序で適用されます。

- トラフィックにファイアウォールのバイパスを許可できます。バイパスルールにより、トラフィックはファイアウォールと侵入防御エンジンを可能な限り早く通過できます。バイパスルールは、フィルタリングを望まないマルチメディア系プロトコルを使用するトラフィックや、信頼済みソースからのトラフィックに対して使用します。

ヒント: ポリシーで信頼済みソース用のバイパスルールを作成して使用方法の例については、"[信頼済みトラフィックに対するファイアウォールのバイパス許可](#)" on page 857を参照してください。

注意: バイパスルールは単一方向です。トラフィックの各方向に対して明確なルールが必要です。

ヒント: 次の設定を使用して、バイパスルールで最大のスループットパフォーマンスを達成できます。

- 優先度: 最高
 - フレームの種類: IP
 - プロトコル: TCP、UDP、またはその他のIPプロトコル (「任意」オプションは使用しないでください)
 - 送信元および送信先のIPおよびMAC: すべて「任意」
 - プロトコルがTCPまたはUDPでトラフィックの方向が「受信」の場合は、送信先ポートを「任意」ではなく1つ以上指定する必要があり、送信元ポートを「任意」にする必要があります。
 - プロトコルがTCPまたはUDPでトラフィックの方向が「送信」の場合は、送信元ポートを「任意」ではなく1つ以上指定する必要があり、送信先ポートを「任意」にする必要があります。
 - スケジュール: なし
- ログ記録のみが可能です。この処理では、ログにエントリは作成されますが、トラフィックは処理されません。
 - 定義済みのトラフィックを強制的に許可できます (他のトラフィックを除外することなく、このルールによって定義されたトラフィックを許可できます)。
 - トラフィックの拒否が可能です (このルールによって定義されたトラフィックを拒否します)。
 - トラフィックの許可が可能です (このフィルタによって定義されたトラフィックを例外的に許可します)。

注意: コンピュータに有効な許可ルールがない場合、拒否ルールでブロックされていないかぎり、すべてのトラフィックが許可されます。許可ルールを1つ作成したら、許可ルールの条件を満たしていないかぎり、その他すべてのトラフィックがブロックされます。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていない限り、常に許可されます。

3. ルールの [優先度] を選択します。優先度により、ルールが適用される順序を決定します。ルール処理に「強制的に許可」、「拒否」、または「バイパス」を選択した場合は、0 (最低) から4 (最高) の優先度を設定できます。優先度を設定すると、ルール処理を組み合わせ、階層型のルール効果を実現できます。

注意: ログのみルールでの優先度は4のみ設定でき、許可ルールでは0のみが設定できません。

注意: 優先度の低いルールよりも優先度の高いルールが優先的に適用されます。たとえば、ポート80の受信を強制的に許可する優先度2のルールが適用されるより前に、ポート80の受信を拒否する優先度3のルールが適用され、パケットを破棄します。

処理と優先度の関係の詳細については、"[ファイアウォールルールの処理と優先度](#)" on [page 858](#)を参照してください。

4. [パケットの方向] を選択します。このルールを受信 (ネットワークからコンピュータ) または送信 (コンピュータからネットワーク) トラフィックのどちらに適用するかを選択します。

注意: 個々のファイアウォールルールは、単一のトラフィック方向にのみ適用されます。特定の種類のトラフィックに対しては、受信および送信ファイアウォールルールをペアで作成する必要があります。

5. イーサネットの [フレームの種類] を選択します。「フレーム」とはイーサネットフレームを指し、フレームで送信されるデータは、使用可能なプロトコルによって指定されます。フレームの種類として「その他」を選択する場合は、[フレーム番号](#)を指定する必要があります。
6. **注意:** [IP] は、IPv4とIPv6両方をサポートしています。[IPv4] または [IPv6] を個別に選択することもできます。

注意: LinuxのAgentは、フレームの種類がIPまたはARPの packetsのみ確認します。その他のフレームの種類のパケットは許可されます。Virtual Applianceにはこのような制限事項はありません。保護する仮想マシンのOSに関係なく、すべてのフレームの種類を確認できます。

フレームの種類としてインターネットプロトコル (IP) を選択した場合は、トランスポートの [プロトコル] を選択する必要があります。プロトコルとして「その他」を選択する場合は、[プロトコル番号](#)も指定する必要があります。

パケットの送信元と送信先を選択する

[IP] アドレスと [MAC] アドレスの組み合わせを選択し、フレームの種類で利用できる場合は、パケット送信元およびパケット送信先の [ポート] および [指定フラグ] を選択します。

ヒント: 以前に作成した[IP](#)、[MAC](#)、または[ポート](#)リストを使用できます。

サポートされているIPベースのフレームの種類は次のとおりです。

	IP	MAC	ポート	フラグ
任意	✓	✓		
ICMP	✓	✓		✓
ICMPV6	✓	✓		✓
IGMP	✓	✓		
GGP	✓	✓		
TCP	✓	✓	✓	✓
PUP	✓	✓		
UDP	✓	✓	✓	
IDP	✓	✓		
ND	✓	✓		
RAW	✓	✓		

	IP	MAC	ポート	フラグ
TCP+UDP	✓	✓	✓	✓

注意: ARPおよびREVARPのフレームの種類では、パケットの送信元と送信先としてMACアドレスの使用のみがサポートされています。

[任意のフラグ] を選択することも、以下のフラグを個別に選択することもできます。

- URG
- ACK
- PSH
- RST
- SYN
- FIN

ルールイベントとアラートを設定する

ファイアウォールルールがトリガされると、Deep Security Managerでイベントがログに記録され、パケットデータが記録されます。

注意: 「許可」、「強制的に許可」、および「バイパス」処理を使用するルールは、イベントのログを記録しません。

アラート

イベントのログを記録した場合に、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション] をクリックしてから、[このルールによってイベントが記録された場合にアラート] を選択します。

注意: アラートをトリガするように設定できるのは、処理が [拒否] または [ログ記録のみ] に設定されているファイアウォールルールのみです

ルールのスケジュールを設定する

予約された時間のみファイアウォールルールを有効化するかどうかを選択します。

その方法の詳細については、"[ルールに適用するスケジュールの定義](#)" on page 687を参照してください。

ルールにコンテキストを割り当てる

ルールコンテキストを使用すると、さまざまなネットワーク環境に独自のファイアウォールルールを設定できます。コンテキストは一般的に、オンサイトとオフサイトのノートパソコンで異なるルールを有効にするために使用されます。

コンテキストの作成方法については、"[ポリシーで使用するコンテキストの定義](#)" on page 680を参照してください。

ヒント: コンテキストを使用してファイアウォールルールを実装するポリシーの例については、「Windows Mobile ラップトップ」ポリシーのプロパティを参照してください。

ルールが割り当てられているポリシーとコンピュータを確認する

ファイアウォールルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべてのファイアウォールルールを、.csvまたは.xmlファイルにエクスポートするには、[エクスポート] をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[ファイアウォールルール] リストで該当のルールを右クリックしてから、[削除]→[OK] の順にクリックします。

注意: 1台以上のコンピュータに割り当てられたファイアウォールルール、またはポリシーの一部であるファイアウォールルールは削除できません。

侵入防御ルールの設定

次のタスクを実行して、侵入防御ルールを設定および使用します。

- "[侵入防御ルールのリストを表示する](#)" on the next page
- "[侵入防御ルールに関する情報を表示する](#)" on the next page

- "関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ)" on page 632
- "ルールを割り当てる/ルールの割り当てを解除する" on page 633
- "アップデートされた必須ルールを自動割り当てする" on page 633
- "ルールにイベントログを設定する" on page 634
- "アラートを生成する" on page 635
- "設定オプションを設定する (トレンドマイクロのルールのみ)" on page 635
- "有効な時間を予約する" on page 636
- "推奨設定から除外する" on page 636
- "ルールのコンテキストを設定する" on page 636
- "ルールの動作モードをオーバーライドする" on page 637
- "ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 637
- "ルールをエクスポート/インポートする" on page 638
- "SQLインジェクション防御ルールの設定" on page 810

侵入防御モジュールの概要については、"[侵入防御を使用した攻撃のブロックをブロックする](#)" on page 789を参照してください。

侵入防御ルールの一覧を表示する

[ポリシー] 画面には侵入防御ルールの一覧が表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。この一覧では、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの一覧の [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールの一覧でもTippingPointルールIDを表示できます。

一覧を確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

侵入防御ルールに関する情報を表示する

侵入防御ルールのプロパティには、ルールおよび防御対象の攻撃コードに関する情報が含まれます。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。

一般情報

- 名前:侵入防御ルールの名前。
- 説明: 侵入防御ルールの説明。
- 最小Agent/Applianceバージョン:この侵入防御ルールのサポートに必要なDeep Security **Agent/Appliance**¹の最小バージョン。

詳細

[新規] () または [プロパティ] () をクリックして、[侵入防御ルールプロパティ] 画面を表示します。

注意: [設定] タブを確認します。トレンドマイクロが提供する侵入防御ルールは、Deep Security Managerを使用して直接編集することはできません。その代わりに、侵入防御ルールに設定が必要な場合や設定が可能な場合は、[設定] タブの設定オプションを使用します。ユーザ自身で作成したカスタム侵入防御ルールは、[ルール] タブが表示され、直接編集可能です。

侵入防御ルールのリストを表示する

[ポリシー] 画面には侵入防御ルールのリストが表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。このリストでは、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールのリストでもTippingPointルールIDを表示できます。

リストを確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

¹Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

一般情報

- アプリケーションの種類:この侵入防御ルールが分類されているアプリケーションの種類。

ヒント:このパネルでアプリケーションの種類を編集できます。ここでアプリケーションの種類を編集すると、そのアプリケーションの種類を使用するすべてのセキュリティコンポーネントに対して変更内容が適用されます。

- 優先度: ルールの優先度。優先度の低いルールよりも優先度の高いルールが優先的に適用されます。
- 重要度:ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、侵入防御ルールを表示するときにソート条件として使用できます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します ([管理]→[システム設定]→[ランク付け] を参照してください)。
- CVSSスコア:[脆弱性情報データベース](#)に基づいた、脆弱性の重要度の基準。

ID (トレンドマイクロのルールのみ)

- 種類: [スマート] (1つ以上の既知または不明なゼロデイの脆弱性)、[攻撃コード] (通常、署名ベースの攻撃コード) または [脆弱性] (1つ以上の攻撃コードが存在する可能性のある特定の脆弱性) のいずれかになります。
- 発行日: ルールがリリースされた日付。ダウンロードされた日付ではありません。
- 前回のアップデート: ローカルで、またはセキュリティアップデートのダウンロード中に、ルールが変更された前回の日時。
- 識別子: ルールに一意のIDタグ。

関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ)

トレンドマイクロのルールには、ルールで防御する脆弱性に関する情報が含まれます。適用可能な場合は、共通脆弱性評価システム (CVSS) が表示されます(この評価システムの詳細は、[脆弱性情報データベース](#)のCVSSページを参照してください)。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [脆弱性] タブをクリックします。

ルールを割り当てる/ルールの割り当てを解除する

Agent検索時に侵入防御ルールを適用するには、該当するポリシーとコンピュータに割り当てます。脆弱性にパッチが適用されたため、ルールが必要でなくなった場合は、ルールを割り当て解除できます。

コンピュータエディタ¹で侵入防御ルールの割り当てを解除できない場合、そのルールがポリシーに割り当てられている可能性があります。ポリシーレベルで割り当てられたルールを削除するには**ポリシーエディタ**²を使用する必要があり、コンピュータレベルでは削除できません。

ポリシーに対する変更は、そのポリシーを使用するすべてのコンピュータに反映されます。たとえば、ポリシーからルールを割り当て解除すると、そのポリシーで保護しているすべてのコンピュータからルールが削除されます。継続してこのルールを他のコンピュータに適用するには、そのグループのコンピュータ用に新しいポリシーを作成します。 ("**ポリシー、継承、およびオーバーライド**" on page 587を参照してください)。

ヒント: ルールが割り当てられたポリシーとコンピュータを確認するには、ルールプロパティの [割り当て対象] タブをご覧ください。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御]→[一般] の順にクリックします。
ポリシーに割り当てられているルールのリストは、[現在割り当てられている侵入防御ルール] リストに表示されます。
3. [現在割り当てられている侵入防御ルール] で、[割り当て/割り当て解除] をクリックします。
4. ルールを割り当てるには、ルールの横にあるチェックボックスをオンにします。
5. ルールの割り当てを解除するには、ルールの横にあるチェックボックスをオフにします。
6. [OK] をクリックします。

アップデートされた必須ルールを自動割り当てする

セキュリティアップデートには、セカンダリ侵入防御ルールの割り当てが必要な新規またはアップデートされたアプリケーションの種類および侵入防御ルールが含まれている場合があります

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

ます。Deep Securityでは必要に応じて、これらのルールを自動割り当てできます。ポリシーまたはコンピュータプロパティで、次のように自動割り当てを有効化できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御]→[詳細] を順にクリックします。
3. 自動割り当てを有効にするには、[ルールアップデート] 領域で [はい] を選択します。
4. [OK] をクリックします。

ルールにイベントログを設定する

ルールのイベントをログに記録するかどうか、ログにパケットデータを含めるかどうかを設定します。

注意: Deep Securityの侵入防御イベントで、パケットデータにX-Forwarded-Forヘッダが含まれている場合は、このヘッダを表示できます。このヘッダの情報は、Deep Security Agentをロードバランサまたはプロキシの背後に配置している場合に役立ちます。X-Forwarded-Forヘッダデータは、イベントの [プロパティ] 画面に表示されます。ヘッダデータを含めるには、ログにパケットデータを追加します。また、ルール1006540 [X-Forwarded-For HTTPヘッダのログを有効にする] も割り当てる必要があります。

ルールがイベントをトリガするたびにすべてのパケットデータを記録するのは現実的ではないので、Deep Securityでは、一定時間内でイベントが最初に発生したときのデータのみを記録します。初期設定時間は5分ですが、ポリシーの [ネットワークエンジンの詳細設定] の [1つのパケットデータのみをログに記録する期間] プロパティを使用して期間を変更できます。(「[ネットワークエンジンの詳細オプション](#)」を参照してください)。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、「[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)」 on page 637を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [一般] タブで、[イベント] 領域に移動し、次のように必要なオプションを選択します。
 - ルールのログを無効化するには、[イベントログの無効化] を選択します。
 - パケットが破棄またはブロックされた場合にイベントのログを記録するには、[パケット破棄時にイベントを生成] を選択します。
 - ログエントリにパケットデータを含めるには、[常にパケットデータを含める] を選択します。

- ルールで検出されたパケットの前後のパケットをログに記録するには、[デバッグモードを有効にする]を選択します。サポート担当者から指示があった場合のみデバッグモードを使用します。

また、ログにパケットデータを含めるには、ルールを割り当てるポリシーで次のように、ルールによるパケットデータの取得を許可する必要があります。

1. [ポリシー]画面で、ルールを割り当てたポリシーを開きます。
2. [侵入防御]→[詳細]を順にクリックします。
3. [イベントデータ]領域で[はい]を選択します。

アラートを生成する


侵入防御ルールがイベントをトリガした場合にアラートを生成します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" on page 637を参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [オプション]タブをクリックして[アラート]領域で[オン]を選択します。
4. [OK]をクリックします。

設定オプションを設定する (トレンドマイクロのルールのみ)

トレンドマイクロの侵入防御ルールの一部には、ヘッダ長、HTTPに許可される拡張子、Cookie長など、1つ以上の設定オプションがあります。オプションには設定が必要なものもあります。必要なオプションを設定せずにルールを割り当てると、アラートが生成され、必要なオプションについての情報が表示されます。(これは、セキュリティアップデートによってダウンロードされ自動的に適用されたルールにも適用されます)。


設定オプションのある侵入防御ルールは、[侵入防御ルール]リストでルールのアイコンに小さなギアマークが付きます 。

注意: 独自のカスタム侵入防御ルールには、[ルール]タブがあり、ルールを編集できます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" on page 637を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [設定] タブをクリックします。
4. プロパティを設定して [OK] をクリックします。

有効な時間を予約する

侵入防御ルールが有効な時間を予約します。予約された時間のみ有効になる侵入防御ルールは、[侵入防御ルール] 画面でルールのアイコンに小さな時計マークが付きます .

注意: Agentベースの保護では、スケジュールで保護対象のエンドポイントと同じタイムゾーンが使用されます。Agentレスによる保護では、Deep Security Virtual Applianceと同じタイムゾーンが使用されます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" [on the next page](#)を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [スケジュール] 領域で [新規] を選択するか、頻度を選択します。
5. 必要に応じてスケジュールを編集します。
6. [OK] をクリックします。

推奨設定から除外する

推奨設定検索のルール推奨設定から侵入防御ルールを除外します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" [on the next page](#)を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [推奨設定オプション] 領域で [推奨設定から除外] を選択します。
5. [OK] をクリックします。

ルールのコンテキストを設定する

ルールが適用されるコンテキストを設定します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" [below](#)を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [コンテキスト] 領域で [新規] を選択するか、コンテキストを選択します。
5. 必要に応じてコンテキストを編集します。
6. [OK] をクリックします。

ルールの動作モードをオーバーライドする

新しいルールをテストする場合は、侵入防御ルールの動作モードを [検出] に設定します。[検出] モードでは、ルールは「検出のみ:」という言葉で始まるログエントリを作成しますが、トラフィックに干渉しません。侵入防御ルールには [検出] モードでのみ動作するものがあります。これらのルールについては、動作モードを変更できません。

注意: ルールのログを無効にすると、動作モードに関係なく、ルールのアクティビティはログに記録されません。

動作モードの詳細については、"[動作モードを使用してルールをテストする](#)" [on page 791](#)を参照してください。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" [below](#)を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [検出のみ] を選択します。

ルールおよびアプリケーションの種類の設定をオーバーライドする

コンピュータエディタとポリシーエディタ¹で、侵入防御ルールを編集して、ポリシーまたはコンピュータのコンテキストのみで変更を適用できます。グローバルに変更が適用されるようにルールを編集して、ルールが割り当てられた他のポリシーおよびコンピュータで変更を有効に

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

することもできます。同様に、1つのポリシー/コンピュータ、またはグローバルにアプリケーションの種類を設定できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御] をクリックします。
3. ルールを編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
 - プロパティ: そのポリシーのみのルールを編集します。
 - プロパティ (グローバル): グローバルに (すべてのポリシーとコンピュータに対して) ルールを編集します。
4. ルールのアプリケーションの種類を編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
 - アプリケーションの種類プロパティ: そのポリシーのみのアプリケーションの種類を編集します。
 - アプリケーションの種類プロパティ (グローバル): グローバルに (すべてのポリシーとコンピュータに対して) アプリケーションの種類を編集します。
5. [OK] をクリックします。

ヒント: ルールを選択して [プロパティ] をクリックした場合は、編集集中のポリシーのみでルールを編集します。

注意: 1つのポートを割り当てできるアプリケーションの種類は8個までです。9個以上割り当てると、そのルールは該当するポートで機能しません。

ルールをエクスポート/インポートする

1つ以上の侵入防御ルールをXMLまたはCSVファイルにエクスポートしたり、XMLファイルからルールをインポートできます。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. 1つ以上のルールをエクスポートするには、[エクスポート]→[選択したアイテムをCSV形式でエクスポート] または [エクスポート]→[選択したアイテムをXML形式でエクスポート] を順にクリックします。
3. すべてのルールをエクスポートするには、[エクスポート]→[CSV形式でエクスポート] または [エクスポート]→[XML形式でエクスポート] を順にクリックします。
4. ルールをインポートするには、[新規]→[ファイルからインポート] を順にクリックして、ウィザードの指示に従います。

変更監視ルールの作成

変更監視ルールを使用すると、Deep Security Agentで検索して、コンピュータのファイル、ディレクトリ、レジストリキーと値に対する変更、およびインストール済みのソフトウェア、プロセス、待機中のポート、実行中のサービスにおける変更を検出できます。変更監視ルールは、コンピュータに直接割り当てられることも、ポリシーの一部にすることもできます。

注意: ここでは、変更監視ルールの作成方法を具体的に説明します。変更監視モジュールの設定方法については、"[変更監視の設定](#)" on page 887を参照してください。

変更監視ルールには、ユーザ自身が作成したルールとトレンドマイクロが発行するルールの2種類があります。トレンドマイクロが発行するルールの設定方法については、"[トレンドマイクロが発行する変更監視ルールを設定する](#)" on page 641セクションを参照してください。

新しい変更監視ルールを作成するには、次の手順を実行する必要があります。

1. "[新しいルールを追加する](#)" below。
2. "[変更監視ルール情報を入力する](#)" on the next page。
3. "[ルールテンプレートを選択し、ルールの属性を定義する](#)" on the next page。

変更監視ルールを作成したら、次の方法も学習できます。

- "[ルールイベントとアラートを設定する](#)" on page 642
- "[ルールが割り当てられているポリシーとコンピュータを確認する](#)" on page 643
- "[ルールをエクスポートする](#)" on page 643
- "[ルールを削除する](#)" on page 643

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[変更監視ルール] ページで、新しい変更監視ルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新しい変更監視ルール] の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存のルールをコピーして変更します。[変更監視ルール] リストで、該当のルールを右クリックし、[複製] をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ] をクリックします。

変更監視ルール情報を入力する

1. ルールの [名前] と [説明] を入力します。

ヒント: すべての変更監視ルールへの変更をルールの [説明] フィールドに記録することを推奨します。メンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールの [重要度] を設定します。

注意: ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、変更監視ルールのリストを表示するとき条件をソートする際に役立ちます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します([管理]→[システム設定]→[ランク付け] を参照してください)。

ルールテンプレートを選択し、ルールの属性を定義する

[コンテンツ] タブに移動し、次の3つのテンプレートのいずれかを選択します。

レジストリ値テンプレート

特にレジストリ値への変更を監視する変更監視ルールを作成します。

注意: レジストリ値テンプレートは、Windowsベースコンピュータでのみ使用できます。

1. 監視する [基本キー]、およびサブキーのコンテンツを監視するかどうかを選択します。
2. 含まれる、または除外される [値の名前] が一覧表示されます。ワイルドカード文字として「?」および「*」を使用できます。
3. 監視する [属性] を入力します。「STANDARD」と入力すると、レジストリサイズ、コンテンツ、種類への変更が監視されます。レジストリ値テンプレートの属性の詳細については、「[RegistryValueSet](#)」ドキュメントを参照してください。

ファイルテンプレート

特にファイルへの変更を監視する変更監視ルールを作成します。

1. ルールの [基本ディレクトリ] を入力します (例: C:\Program Files\MySQL)。基本ディレクトリに関連するすべてのサブディレクトリのコンテンツも含めるには、[サブディレクトリも含む] を選択します。ベースディレクトリではワイルドカードはサポートされて

いません。

2. 特定のファイルを含める、または除外するには、[ファイル名] フィールドを使用します。ワイルドカード (「 ? 」を任意の1文字として、「 * 」を0個以上の文字として) 使用できます。

注意: [ファイル名] フィールドを空白のままにすると、基本ディレクトリ内のすべてのファイルが監視されます。この場合、基本ディレクトリに多数のファイルが含まれていると、大量のシステムリソースが消費されます。

3. 監視する [属性] を入力します。「STANDARD」と入力すると、ファイル作成日、最終更新日、権限、所有者、サイズ、コンテンツ、フラグ (Windows)、SymLinkPath (Linux) が監視されます。ファイルテンプレートの属性の詳細については、「FileSet」ドキュメントを参照してください。

カスタム (XML) テンプレート

Deep SecurityXMLベースの**変更監視ルール言語**を使用して、[ディレクトリ](#)、[レジストリ値](#)、[レジストリキー](#)、[サービス](#)、[プロセス](#)、[インストールされているソフトウェア](#)、[ポート](#)、[グループ](#)、[ユーザ](#)、[ファイル](#)、[WQL](#)を監視するカスタム変更監視ルールテンプレートを作成します。

ヒント: 希望するテキストエディタを使用してルールを作成し、完成したルールを [コンテンツ] フィールドに貼り付けることができます。

トレンドマイクロが発行する変更監視ルールを設定する

トレンドマイクロが発行する変更監視ルールは、作成したカスタムルールと同じ方法では編集できません。トレンドマイクロのルールには、まったく変更できないものと、限定的な設定オプションが提供されているものがあります。いずれのルールも「種類」列に「定義済み」として表示されますが、設定可能なルールは変更監視アイコンに歯車 (🔧) が表示されます。

現在割り当てられている変更監視ルール

名前 ^	重要度	種類	前回のアップ...
1002766 - Unix - Directory attrib...	● 高	定義済み	2009-07-29
1009628 - Applnit DLLs (ATT&C...	● 高	定義済み	2019-04-17
1009629 - AppCert DLLs (ATT&...	● 中	定義済み	2019-06-12
New Integrity Monitoring Rule	● 中	カスタム	なし

ルールの設定オプションにアクセスするには、ルールのプロパティを開き、[設定] タブをクリックします。

トレンドマイクロが発行するルールには、[一般] タブの下に補足情報も表示されます。

- ルールがはじめて発行された日付と、最後に更新された日付、およびルールの一意のID。
- ルールを機能させるために最低限必要なAgentとDeep Security Managerのバージョン。

トレンドマイクロが発行するルールは編集できませんが、複製した後にそのコピーを編集することはできます。

ルールイベントとアラートを設定する

変更監視ルールによって検出されたすべての変更は、イベントとしてDeep Security Managerのログに記録されます。

リアルタイムのイベント監視

初期設定では、イベントは発生時にログに記録されます。変更の検索を手動で実行している場合にのみイベントをログに記録するには、[リアルタイム監視を許可] の選択を解除します。

アラート

イベントのログを記録したときに、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション] をクリックしてから、[このルールによってイベントが記録された場合にアラート] を選択します。

ルールが割り当てられているポリシーとコンピュータを確認する

変更監視ルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべての変更監視ルールを、.csvまたは.xmlファイルにエクスポートするには、[エクスポート] をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[変更監視ルール] リストで該当のルールを右クリックしてから、[削除]→[OK] の順にクリックします。

注意: 1台以上のコンピュータに現在割り当てられている変更監視ルール、またはポリシーの一部である変更監視ルールは削除できません。

ポリシーで使用する セキュリティログ監視 ルールを定義する

OSSEC セキュリティログ監視 エンジン は Deep Security Agent に統合されており、Deep Security は、コンピュータ上で実行されているオペレーティングシステムおよびアプリケーションによって生成されたログおよびイベントを検査できます。Deep Security Manager には、コンピュータまたはポリシーに割り当てることができる、標準の OSSEC のセキュリティログ監視ルールセットが付属しています。要件に合う既存ルールが存在しない場合は、カスタムルールを作成することもできます。

トレンドマイクロが発行するセキュリティログ監視ルールは編集できませんが、コピーしたものを編集することはできます。

注意: 1台以上のコンピュータに割り当てられたセキュリティログ監視ルール、またはポリシーの一部であるセキュリティログ監視ルールは削除できません。

セキュリティログ監視ルールを作成するには、次の基本手順を実行します。

- 新しいセキュリティログ監視ルールを作成する
- ["デコーダ" on page 646](#)
- ["サブルール" on page 647](#)
- ["実際の使用例" on page 655](#)
- セキュリティログ監視ルールの重要度レベルと推奨される使用法
- ["strftime\(\) 変換指定子" on page 665](#)
- セキュリティログ監視ルールの確認

セキュリティログ監視 モジュールの概要については、["セキュリティログ監視によるログの分析" on page 903](#)を参照してください。

新しいセキュリティログ監視ルールを作成する

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[ルール]→[セキュリティログ監視ルール]に進みます。
2. [新規]→[新しいセキュリティログ監視ルール]をクリックします。
3. [一般] タブで、ルールの名前と説明を入力します (説明は省略できます)。
4. [コンテンツ] タブで、ルールを定義します。ルールを定義する一番簡単な方法は、[基本ルール]を選択し、表示されるオプションを使用してルールを定義する方法です。さらにカスタマイズが必要な場合は、[カスタム (XML)]を選択し、定義しているルールをXMLビューに切り替えることができます。

注意: [基本ルール] ビューに戻すと、[カスタム (XML)] ビューで加えた変更はすべて失われます。

XMLベースの言語を使用して独自のセキュリティログ監視ルールを作成する場合は、[OSSEC](#)のドキュメントを参照するか、サポートプロバイダにお問い合わせください。

基本ルールテンプレートでは以下のオプションを使用できます。

- ルールID: ルールIDは、ルールの一意の識別子です。OSSECでは、ユーザ指定のルール用に100000~109999を定義しますこのフィールドには、新しい一意のルールIDがDeep Security Managerによって事前に入力されています。
- レベル: ルールにレベルを割り当てます。ゼロ (0) は、ルールによってイベントが記録されないことを示しますが、このルールを監視する他のルールが発生する可能性があります

- グループ: 1つ以上のカンマ区切りのグループにルールを割り当てます。これが便利なのは、ある1つのルールの発生時に発生する複数のルール、または特定のグループに属するルールを作成した後に依存関係が使用されることです。
- ルールの説明: ルールの説明。
- パターン照合: これは、ルールがログ内を検索するパターンです。一致するものが検出されるとルールがトリガされます。パターン照合では、正規表現またはより簡単な文字列パターンをサポートします。「文字列パターン」というパターンの種類は正規表現よりも処理が高速ですが、サポートされるのは次に示す3つの特殊な処理のみです。
 - ^ (caret): テキストの先頭を指定します。
 - \$ (ドル記号): テキストの末尾を指定します。
 - | (パイプ): 複数のパターン間に「OR」を作成します。

セキュリティログ監視モジュールで使用される正規表現の構文については、<https://www.ossec.net/docs/syntax/regex.html>を参照してください。

- 依存関係: 別のルールへの依存関係を設定すると、現在のルールでは、このエリアに指定したルールがトリガされた場合にもイベントが記録されます。
- [頻度] は、ルールがトリガされるまでの特定の期間内にルールを照合する必要がある回数です。
- [期間] は、イベントを記録するためにルールを特定の回数 (上記の頻度) トリガするまでの期間 (秒数) です。

注意: [コンテンツ] タブは、自分で作成したセキュリティログ監視ルールに対してのみ表示されます。トレンドマイクロが発行するセキュリティログ監視ルールの場合は、代わりに [設定] タブが表示されます。このタブには、セキュリティログ監視ルールの設定オプションが表示されます。

1. [ファイル] タブで、ルールによって監視するファイルのフルパスを入力し、そのファイルの種類を指定します。
2. [オプション] タブの [アラート] セクションで、このルールでアラートをトリガするかどうかを選択します。

最小のアラート重要度は、基本ルールまたはカスタム (XML) テンプレートを使用してルールに対してアラートをトリガする最小の重大度レベルを設定します。

注意: 基本ルールテンプレートは、一度に1つのルールを作成します。1つのテンプレートに複数のルールを書き込むには、カスタム (XML) テンプレートを使用できます。カスタム (XML) テンプレート内でレベルが異なる複数のルールを作成する場合は、[最小のアラート重要度]設定を使用して、そのテンプレート内のすべてのルールに対するアラートをトリガする最小の重要度を選択できます。

3. [割り当て対象に割り当てられました]タブには、このセキュリティログ監視ルールを使用しているポリシーとコンピュータが表示されます。新しいルールは作成中であるため、まだ割り当てられていません。
4. [OK] をクリックします。このルールをポリシーとコンピュータに割り当てる準備ができました。

デコーダ

セキュリティログ監視ルールは、変更を監視するファイルのリストと、ルールがトリガするために満たす条件のセットで構成されます。セキュリティログ監視エンジンが監視対象のログファイルで変更を検出すると、その変更はデコーダによって解析されます。デコーダは、raw ログエントリを解析して次のフィールドを生成します。

- log: イベントのメッセージセクション
- full_log: イベント全体
- location: ログの生成元
- hostname: イベント発生元のホスト名
- program_name: イベントのSyslogヘッダで使用されるプログラム名
- srcip: イベント内の送信元のIPアドレス
- dstip: イベント内の送信先のIPアドレス
- srcport: イベント内の送信元のポート番号
- dstport: イベント内の送信先のポート番号
- protocol: イベント内のプロトコル
- action: イベント内で実行された処理
- srcuser: イベント内の送信元のユーザ
- dstuser: イベント内の送信先のユーザ
- id: イベントからのIDとしてデコードされたID
- status: イベント内のデコードされたステータス
- command: イベント内で呼び出されるコマンド

- url: イベント内のURL
- data: イベントから抽出される追加データ
- systemname: イベント内のシステム名

ルールは、このデコードされたデータを確認して、ルールで定義された条件に一致する情報を検索します。

一致する項目の重要度レベルが十分に高い場合は、次のいずれかの処理を実行できます。

- アラートの発令(セキュリティログ監視ルールの [プロパティ] 画面の [オプション] タブで設定できます)
- イベントのSyslogへの書き込み([管理]→[システム設定]→[イベントの転送] タブの [SIEM] エリアで設定できます)
- イベントのDeep Security Managerへの送信(ポリシーエディタまたはコンピュータエディタの [設定]→[イベントの転送] タブの [セキュリティログ監視のSyslog設定] で設定できます)。

サブルール

1つのセキュリティログ監視ルールに複数のサブルールを含めることができます。これらのサブルールには、アトミックとコンポジットという2つの種類があります。アトミックルールは1つのイベントを評価し、コンポジットルールは複数のイベントを確認して、頻度、繰り返し、およびイベント間の相関関係を評価できます。

グループ

各ルールまたはルールのグループは、<group></group> エlement内に定義する必要があります。属性名には、このグループに追加するルールを含めてください。次の例では、Syslogとsshdのルールをグループに含めています。

```
<group name="syslog,sshd,">
</group>
```

注意: グループ名の末尾にカンマが付いていることに注意してください。末尾のカンマは、<if_group></if_group> タグを使用して、このルールに別のサブルールを条件付きで追加する場合に必要です。

注意: セキュリティログ監視ルールのセットがエージェントに送信されると、エージェントのセキュリティログ監視エンジンは、割り当てられた各ルールからXMLデータを取得し、基本的に単一の長いセキュリティログ監視ルールになるように組み込みます。グループ定義の

中には、トレンドマイクロが作成したすべてのセキュリティログ監視ルールに共通のものがあります。そのため、トレンドマイクロには「Default Rules Configuration」と呼ばれるルールがあります。このルールはこれらのグループを定義し、常に他のトレンドマイクロのルールとともに割り当てられます(割り当てるルールに「Default Rules Configuration」ルールを選択しない場合は、「Default Rules Configuration」ルールが自動的に割り当てられることを知らせる通知が表示されます)。独自のセキュリティログ監視ルールを作成し、トレンドマイクロ作成ルールを割り当てずにコンピュータに割り当てる場合は、[初期設定ルール設定]ルールの内容を新しいルールにコピーするか、「初期設定ルールの設定」の「コンピュータへの割り当て」のルールを参照してください。

ルール、ID、およびレベル

グループには必要な数のルールを含めることができます。ルールは、<rule></rule> エレメントを使用して定義されます。ルールには少なくとも2つの属性(idおよびlevel)が必要です。idは、署名の一意の識別子です。levelは、アラートの重要度です。次の例では、ルールIDとレベルの異なる、2つのルールが作成されます。

```
<group name="syslog,sshd,">
  <rule id="100120" level="5">
  </rule>
  <rule id="100121" level="6">
  </rule>
</group>
```

注意: カスタムルールには、100,000以上のID値を指定する必要があります。

<group></group> タグを使用すると、親グループ内に追加のサブグループを定義できます。このサブグループは、次の表に示す任意のグループを参照できます。

グループの種類	グループ名	説明
攻撃の予兆	connection_attempt web_scan recon	接続の試行 Web検索 一般的な検索
認証制御	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser	成功 失敗 無効 ログイン拒否 複数の失敗 ユーザアカウントの追加 ユーザアカウントの変更または削除

グループの種類	グループ名	説明
	account_changed	
攻撃/悪用	automatic_attack exploit_attempt invalid_access spam multiple_spam sql_injection attack virus	ワーム (対象を指定しない攻撃) 攻撃コードのパターン 無効なアクセス スパム 複数のスパムメッセージ SQLインジェクション 一般的な攻撃 ウイルスの検出
アクセス管理	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	アクセス拒否 アクセス許可 存在しないリソースへのアクセス ファイアウォールによるドロップ 複数のファイアウォールによるドロップ クライアントの誤った設定 クライアントエラー
ネットワーク制御	new_host ip_spoof	新しいコンピュータの検出 ARPスプーフィングの疑い
システム監視	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed low_diskspace time_changed	サービスの開始 システムエラー シャットダウン ログのクリア 無効な要求 インタフェースのプロミスキャスモードへの切り替え ポリシーの変更 設定の変更 ディスク容量が少ない 時刻の変更

注意: イベントの自動タグ付けが有効な場合は、イベントにグループ名のラベルが付けられません。セキュリティログ監視 ルールでは、グループをユーザフレンドリなバージョンに変更する変換テーブルを使用します。そのため、たとえば、「login_denied」は「ログイン拒否」と表示されます。カスタムルールのリストには、ルール内に表示されるグループ名が表示されます。

説明

<description></description> タグを含めます。ルールがトリガされると、説明のテキストがイベントに表示されます。

```
<group name="syslog,sshd,">
  <rule id="100120" level="5">
    <group>authentication_success</group>
```

```

        <description>SSHD testing authentication success</description>
    </rule>
    <rule id="100121" level="6">
        <description>SSHD rule testing 2</description>
    </rule>
</group>

```

デコード形式

<decoded_as></decoded_as> タグでは、指定されたデコーダがログをデコードした場合にのみルールを適用するようにセキュリティログ監視エンジンを設定します。

```

<rule id="100123" level="5">
    <decoded_as>sshd</decoded_as>
    <description>Logging every decoded sshd message</description>
</rule>

```

注意: 使用可能なデコーダを表示するには、[セキュリティログ監視ルール] 画面で [デコーダ] をクリックします。[1002791-Default Log Decoders] を右クリックして、[プロパティ] を選択します。[設定] タブに進み、[デコーダの表示] をクリックします。

一致項目

特定の文字列をログで検索するには、<match></match> を使用します。Linuxのsshdのパスワードエラーログを次に示します。

```

Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid
user jsmith from 192.168.1.123 port 1799 ssh2

```

「Failed password」という文字列を検索するには、<match></match> タグを使用します。

```

<rule id="100124" level="5">
    <decoded_as>sshd</decoded_as>
    <match>^Failed password</match>
    <description>Failed SSHD password attempt</description>
</rule>

```

注意: 文字列の先頭を示す正規表現のカレット (^) に注意してください。「Failed password」がログの先頭でない場合でも、セキュリティログ監視デコーダはログを複数のセクションに分割します詳細については、"[デコーダ](#)" on page 646を参照してください。これらのセクションの1つは、ログ全体を示す「full_log」ではなく、ログのメッセージ部分を示す「log」です。

次の表は、サポートされている正規表現の構文一覧です。

正規表現の構文	説明
\w	A～Z、a～z、0～9の英数字1文字
\d	0～9の数字1文字
\s	単一のスペース (空白文字)
\t	単一のタブ
\p	()*+,-.;;<=>?[]
\W	\w以外
\D	\d以外
\S	\s以外
\.	任意の文字
+	上記のいずれかの1つ以上に一致 (たとえば、\w+、\d+)
*	上記のいずれかの0個以上に一致 (たとえば、\w*、\d*)
^	文字列の先頭 (^<任意の文字列>)
\$	文字列の末尾 (<任意の文字列>\$)
	複数の文字列間の「OR」

条件文

ルールの評価では、trueと評価される他のルールを条件とすることができます。<if_sid></if_sid> タグでは、タグで識別されたルールがtrueと評価された場合にのみこのサブルールを評価するようにセキュリティログ監視エンジンを設定します。次の例では、100123、100124、および100125の3つのルールを示します。<if_sid></if_sid> タグを使用して、ルール100124と100125がルール100123の子になるように変更されています。

```
<group name="syslog,sshd,">
  <rule id="100123" level="2">
    <decoded_as>sshd</decoded_as>
    <description>Logging every decoded sshd message</description>
  </rule>
  <rule id="100124" level="7">
    <if_sid>100123</if_sid>
    <match>^Failed password</match>
    <group>authentication_failure</group>
    <description>Failed SSHD password attempt</description>
  </rule>
  <rule id="100125" level="3">
    <if_sid>100123</if_sid>
    <match>^Accepted password</match>
    <group>authentication_success</group>
    <description>Successful SSHD password attempt</description>
  </rule>
</group>
```

```
</rule>
</group>
```

評価の階層

<if_sid></if_sid> タグでは、基本的に階層型のルールセットを作成します。つまり、<if_sid></if_sid> タグをルールに含めることにより、そのルールは <if_sid></if_sid> タグで参照されるルールの子になります。ルールをログに適用する前に、セキュリティログ監視エンジンは、<if_sid></if_sid> タグを評価し、上位および下位のルールの階層を作成します。

注意: 階層型の親子構造を使用すると、ルールの効率を向上させることができます。親ルールがtrueと評価されない場合、セキュリティログ監視エンジンはその親の子を無視します。

注意: <if_sid></if_sid> タグを使用して、まったく異なるセキュリティログ監視ルール内のサブルールを参照できますが、後でルールを確認することが非常に困難になるため、この処理は避けてください。

次の表は、使用可能なアトミックルールの条件指定のオプションを一覧表示しています。

タグ	説明	備考
match	パターン	イベント (ログ) に対して照合される任意の文字列。
regex	正規表現	イベント (ログ) に対して照合される任意の正規表現。
decoded_as	文字列	事前一致する任意の文字列。
srcip	送信元のIPアドレス	送信元のIPアドレスとしてデコードされる任意のIPアドレス。IPアドレスの前に「!」を使用すると、指定した以外のIPアドレスを意味します。
dstip	送信先のIPアドレス	送信先のIPアドレスとしてデコードされる任意のIPアドレス。IPアドレスの前に「!」を使用すると、指定した以外のIPアドレスを意味します。
srcport	送信元のポート番号	任意の送信元のポート (形式の一致)。
dstport	送信先のポート番号	任意の送信先のポート (形式の一致)。
user	ユーザ名	ユーザ名としてデコードされる任意のユーザ名。
program_name	プログラム名	Syslogプロセス名からデコードされる任意のプログラム名。
hostname	システムのホスト名	Syslogのホスト名としてデコードされる任意のホスト名。
time	次の形式の時刻の範囲 hh:mm - hh:mmまたは	トリガするルールに対してイベントが発生する必要のある時刻の範囲。

タグ	説明	備考
	hh:mm am - hh:mm pm	
weekday	曜日 (日曜、 月曜、火曜な ど)	トリガするルールに対してイベントが発生する必要のある曜日。
id	ID	イベントからデコードされる任意のID。
url	URL	イベントからデコードされる任意のURL。

このルールを100125ルールに依存させるには、<if_sid>100125</if_sid> タグを使用します。このルールでは、成功したログインルールにすでに一致するsshdメッセージの確認のみが行われます。

```
<rule id="100127" level="10">
  <if_sid>100125</if_sid>
  <time>6 pm - 8:30 am</time>
  <description>Login outside business hours.</description>
  <group>policy_violation</group>
</rule>
```

ログエントリのサイズに関する制限

次の例では、maxsize属性を前の例に追加しています。この属性では、maxsizeよりも文字数が少ないルールの評価のみを行うようにセキュリティログ監視エンジンを設定します。

```
<rule id="100127" level="10" maxsize="2000">
  <if_sid>100125</if_sid>
  <time>6 pm - 8:30 am</time>
  <description>Login outside business hours.</description>
  <group>policy_violation</group>
</rule>
```

次の表は、使用可能なアトミックルールのツリーベースのオプションを一覧表示しています。

タグ	説明	備考
if_sid	ルールID	指定された署名IDに一致するルールの子ルールとしてこのルールを追加します。
if_group	グループID	指定されたグループに一致するルールの子ルールとしてこのルールを追加します。
if_level	ルールレベル	指定された重要度レベルに一致するルールの子ルールとしてこのルールを追加します。
description	文字列	ルールの説明。
info	文字列	ルールの追加情報。

タグ	説明	備考
cve	CVE番号	ルールに関連付ける任意のCommon Vulnerabilities and Exposures (CVE) 番号。
options	alert_by_email no_email_alert no_log	アラートの処理としてメール生成 (alert_by_email)、メール生成なし (no_email_alert)、またはログへの記録なし (no_log) のいずれかを指定する追加のルールオプション。

コンポジットルール

アトミックルールは、1つのログエントリを確認します。複数のエントリに関連付けるには、コンポジットルールを使用する必要があります。コンポジットルールは、現在のログを受信済みのログと照合します。複合ルールにはさらに2つのオプションが必要です。頻度 オプションは、イベントまたはパターンがアラートを生成するまでに何回発生する必要があるかを指定します。また、 の時間枠の オプションは、セキュリティログ監視 エンジンにどれくらいの時間 (秒) 遅れて通知します。以前のログを検索する必要があります。すべてのコンポジットルールの構造は次のようになります。

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

たとえば、10分以内にパスワードを5回間違えたら重要度の高いアラートを作成するコンポジットルールを作成できます。<if_matched_sid></if_matched_sid> タグを使用すると、アラートを作成する新しいルールに対して、目的の頻度および期間内にトリガする必要のあるルールを指定できます。次の例では、イベントの5つのインスタンスが発生したらトリガするようにfrequency属性が設定されています。また、timeframe属性で、期間が600秒に指定されています。

コンポジットルールが監視するその他のルールを定義する場合は、<if_matched_sid></if_matched_sid> タグが使用されます。

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_sid>100124</if_matched_sid>
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

より詳細なコンポジットルールを作成するのに使用できるタグが他にもいくつかあります。このようなルールを使用すると、次の表に示すように、イベントの特定の部分が同じになるよう

に指定できます。これにより、コンポジットルールを調整して誤判定を減らすことができます。

タグ	説明
same_source_ip	送信元のIPアドレスが同じになるように指定します。
same_dest_ip	送信先のIPアドレスが同じになるように指定します。
same_dst_port	送信先のポートが同じになるように指定します。
same_location	場所 (ホスト名またはAgent名) が同じになるように指定します。
same_user	デコードされるユーザ名が同じになるように指定します。
same_id	デコードされるIDが同じになるように指定します。

認証が失敗するたびにアラートを生成するようにコンポジットルールで指定するには、特定のルールIDを使用する代わりに、<if_matched_sid></if_matched_sid> タグを <if_matched_group></if_matched_group> タグに置き換えます。これにより、authentication_failureなどのカテゴリを指定して、インフラストラクチャ全体での認証の失敗を検索できます。

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_group>authentication_failure</if_matched_group>
  <same_source_ip />
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

<if_matched_sid></if_matched_sid> タグと <if_matched_group></if_matched_group> タグの他にも、<if_matched_regex></if_matched_regex> タグを使用して、受信したログを検索する正規表現を指定することができます。

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_regex>^Failed password</if_matched_regex>
  <same_source_ip />
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

実際の使用例

Deep Securityには、数十種類の一般的なアプリケーションに対応した、多数の初期設定のセキュリティログ監視ルールが含まれています。新しいルールは、セキュリティアップデートを使用して定期的に追加できます。セキュリティログ監視ルールでサポートされるアプリケーションが増えても、サポート対象外のアプリケーションやカスタムアプリケーション用のカスタムルールを作成することが必要な場合があります。

ここでは、Microsoft SQL Serverデータベースをデータリポジトリとして使用するMicrosoft Windows Server IISおよび.Netプラットフォームでホストされる、カスタムCMS (コンテンツ管理システム) の作成について説明します。

最初に、次に示すアプリケーションログの属性を特定します。

1. アプリケーションログを記録する場所
2. ログファイルのデコードに使用できるセキュリティログ監視デコーダ
3. ログファイルメッセージの一般的な形式

ここで示すカスタムCMSの例では、次のようになります。

1. Windowsイベントビューア
2. Windowsイベントログ (eventlog)
3. Windowsイベントログ形式 (次のコア属性を使用)
 - ソース: CMS
 - カテゴリ: なし
 - イベント: アプリケーションイベントID>

次に、アプリケーションの機能別にログイベントのカテゴリを特定し、そのカテゴリを監視用のカスケードグループの階層に分類します。監視対象のすべてのグループでイベントを発生させる必要はなく、一致する項目を条件文として使用できます。各グループについて、ルールで照合条件として使用できるログ形式の属性を特定します。これは、すべてのアプリケーションログの、ログイベントのパターンおよび論理分類を調べて実行することもできます。

たとえば、CMSアプリケーションでは、次の機能をサポートしています。セキュリティログ監視のルールは次のとおりです。

- CMSアプリケーションログ (ソース: CMS)
 - 認証 (イベント: 100~119)
 - ユーザログインの成功 (イベント: 100)
 - ユーザログインの失敗 (イベント: 101)
 - 管理者ログインの成功 (イベント: 105)
 - 管理者ログインの失敗 (イベント: 106)
 - 一般エラー (種類: エラー)
 - データベースエラー (イベント: 200~205)
 - ランタイムエラー (イベント: 206~249)

- アプリケーション監査 (種類: 情報)
 - コンテンツ
 - 新しいコンテンツの追加 (イベント: 450~459)
 - 既存のコンテンツの変更 (イベント: 460~469)
 - 既存のコンテンツの削除 (イベント: 470~479)
 - 管理
 - User
 - 新しいユーザの作成 (イベント: 445~446)
 - 既存のユーザの削除 (イベント: 447~449)

これは、ルール作成に役立つ基本的な構造です。次に、Deep Security Managerで新しいセキュリティログ監視ルールを作成します。

新しいCMSセキュリティログ監視ルールを作成するには

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[ルール]→[セキュリティログ監視ルール]に進み、[新規]をクリックし、[新しいセキュリティログ監視ルールのプロパティ]画面を表示します。
2. 新しいルールの名前と説明を指定し、[コンテンツ]タブをクリックします。
3. 新しいカスタムルールを作成する最も簡単な方法は、基本ルールテンプレートを使用することです。[基本ルール]オプションを選択します。
4. [ルールID]フィールドには、未使用のID番号(100,000以上)が自動的に入力されます。これは、カスタムルール用に予約されたIDです。
5. [レベル]を[低(0)]に設定します。
6. ルールに適切なグループ名を指定します。ここでは「cms」とします。

7. ルールの簡単な説明を入力します。

一般	コンテンツ	ファイル	オプション	割り当て対象
テンプレート				
<input checked="" type="radio"/> 基本ルール <input type="radio"/> カスタム (XML)				
一般情報				
ルールID:	<input type="text" value="100000"/>			
レベル:	<input type="text" value="低 (0)"/>			
グループ (カンマ区切り):	<input type="text" value="cms"/>			
ルールの説明:	<input type="text" value="windows events for 'cms' group"/>			
パターン照合				
照合するパターン:	<input type="text"/>			
パターンの種類:	<input type="text" value="文字列パターン"/>			
依存関係				
<input checked="" type="radio"/> なし <input type="radio"/> 別のルールのトリガ時にイベントをトリガ: <input type="radio"/> 特定のグループに属するルールのトリガ時にイベントをトリガ:				
コンポジット (オプション)				
このルールが、指定された期間 (秒単位) 内に指定の頻度で依存ルールと一致した場合のみ、トリガされます。				
頻度 (1~128):	<input type="text"/>			
期間 (1~86400):	<input type="text"/>			
				<input type="button" value="OK"/> <input type="button" value="キャンセル"/>

8. 次に、[カスタム (XML)] オプションを選択します。「基本」ルール用に選択したオプションがXMLに変換されます。

一般 コンテンツ **ファイル** オプション 割り当て対象

テンプレート

基本ルール
 カスタム (XML)

コンテンツ:

```
<group name="cms">
  <rule id="100000" level="0">
    <description>windows events for 'cms' group</description>
  </rule>
</group>
```

OK キャンセル

9. [ファイル] タブをクリックし、[ファイルの追加] ボタンをクリックして、ルールを適用するアプリケーションログファイルおよびログの種類を追加します。ここでは、「Application」、およびファイルの種類として「eventlog」を選択します。

一般 コンテンツ **ファイル** オプション 割り当て対象

ファイル:

Application eventlog ▼ 削除

ファイルの追加

OK キャンセル

注意: eventlogは、Deep Security固有のファイルの種類です。この場合、ログファイルの場所と名前を指定する必要はありません。その代わりに、Windowsイベントビューアに表示されるログの名前を入力してください。ファイルの種類がeventlogの場合の他

のログの名前は、「Security」、「System」、「Internet Explorer」、またはWindowsイベントビューアに表示されるその他のセクションになる可能性があります。その他のファイルの種類の場合は、ログファイルの場所と名前が必要です(ファイル名の照合にはC/C++ strftime() 変換指定子を使用できます。その他の役立つ変換指定子については、以降の表を参照してください)。

10. [OK] をクリックして基本ルールを保存します。
11. 作成された基本ルールのカスタム (XML) を使用すると、以前に特定されたログのグループに基づいて、グループへの新しいルールの追加を開始することができます。基本ルールの条件は初期ルールに設定します。次の例では、ソース属性が「CMS」のWindowsイベントログが、CMS基本ルールによって特定されています。

```
<group name="cms">
  <rule id="100000" level="0">
    <category>windows</category>
    <extra_data>^CMS</extra_data>
    <description>Windows events from source 'CMS' group
messages.</description>
  </rule>
```

12. 次に、特定されたロググループから後続のルールを作成します。次の例では、認証とログインの成功および失敗を特定し、イベントIDごとにログを記録します。

```
<rule id="100001" level="0">
  <if_sid>100000</if_sid>
  <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
  <group>authentication</group>
  <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
  <if_group>authentication</if_group>
  <id>100</id>
  <description>CMS User Login success event.</description>
</rule>

<rule id="100003" level="4">
  <if_group>authentication</if_group>
  <id>101</id>
  <group>authentication_failure</group>
  <description>CMS User Login failure event.</description>
```

```

</rule>
<rule id="100004" level="0">
  <if_group>authentication</if_group>
  <id>105</id>
  <description>CMS Administrator Login success event.</description>
</rule>
<rule id="100005" level="4">
  <if_group>authentication</if_group>
  <id>106</id>
  <group>authentication_failure</group>
  <description>CMS Administrator Login failure event.</description>
</rule>

```

13. 次に、設定済みのルールを使用して、任意のコンポジットルールまたは関連ルールを追加します。次の例は、重要度の高いコンポジットルールを示しています。このルールは、ログインの失敗が10秒間に5回繰り返されたインスタンスに適用されます。

```

<rule id="100006" level="10" frequency="5" timeframe="10">
  <if_matched_group>authentication_failure</if_matched_group>
  <description>CMS Repeated Authentication Login failure
event.</description>
</rule>

```

14. すべてのルールの重要度レベルが適切かどうかを確認します。たとえば、エラーログの重要度はレベル5以上でなければなりません。情報ルールの重要度は低くなります。
15. 最後に、新しく作成されたルールを開き、[設定] タブをクリックして、カスタムルールのXMLをルールフィールドにコピーします。[適用] または [OK] をクリックして変更内容を保存します。

ルールがポリシーまたはコンピュータに割り当てられると、セキュリティログ監視 エンジン は、指定されたログファイルの検査をただちに開始します。

完成したカスタムCMSセキュリティログ監視ルール:

```

<group name="cms">
  <rule id="100000" level="0">
    <category>windows</category>
    <extra_data>^CMS</extra_data>
    <description>Windows events from source 'CMS' group
messages.</description>
  </rule>
  <rule id="100001" level="0">
    <if_sid>100000</if_sid>

```

```
<id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
<group>authentication</group>
<description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
  <if_group>authentication</if_group>
  <id>100</id>
  <description>CMS User Login success event.</description>
</rule>

<rule id="100003" level="4">
  <if_group>authentication</if_group>
  <id>101</id>
  <group>authentication_failure</group>
  <description>CMS User Login failure event.</description>
</rule>

<rule id="100004" level="0">
  <if_group>authentication</if_group>
  <id>105</id>
  <description>CMS Administrator Login success event.</description>
</rule>

<rule id="100005" level="4">
  <if_group>authentication</if_group>
  <id>106</id>
  <group>authentication_failure</group>
  <description>CMS Administrator Login failure event.</description>
</rule>

<rule id="100006" level="10" frequency="5" timeframe="10">
  <if_matched_group>authentication_failure</if_matched_group>
  <description>CMS Repeated Authentication Login failure
event.</description>
</rule>

<rule id="100007" level="5">
  <if_sid>100000</if_sid>
  <status>^ERROR</status>
```

```

        <description>CMS General error event.</description>
        <group>cms_error</group>
</rule>

<rule id="100008" level="10">
    <if_group>cms_error</if_group>
    <id>^200|^201|^202|^203|^204|^205</id>
    <description>CMS Database error event.</description>
</rule>

<rule id="100009" level="10">
    <if_group>cms_error</if_group>
    <id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238
        ^239|^240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
    <description>CMS Runtime error event.</description>
</rule>

<rule id="100010" level="0">
    <if_sid>100000</if_sid>
    <status>^INFORMATION</status>
    <description>CMS General informational event.</description>
    <group>cms_information</group>
</rule>

<rule id="100011" level="5">
    <if_group>cms_information</if_group>
    <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
    <description>CMS New Content added event.</description>
</rule>

<rule id="100012" level="5">
    <if_group>cms_information</if_group>
    <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
    <description>CMS Existing Content modified event.</description>
</rule>

<rule id="100013" level="5">
    <if_group>cms_information</if_group>
    <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
    <description>CMS Existing Content deleted event.</description>

```

```

</rule>

<rule id="100014" level="5">
  <if_group>cms_information</if_group>
  <id>^445|^446</id>
  <description>CMS User created event.</description>
</rule>

<rule id="100015" level="5">
  <if_group>cms_information</if_group>
  <id>^447|^449</id>
  <description>CMS User deleted event.</description>
</rule>

</group>

```

セキュリティログ監視ルールの重要度レベルと推奨される使用法

レベル	説明	備考
レベル0	無視され、処理は行われない	主に誤判定を回避するために使用されます。これらのルールは、他のすべてのルールより先に検索され、セキュリティとは無関係のイベントが含まれません。
レベル1	事前定義された使用法はなし	
レベル2	システムの優先度の低い通知	セキュリティとは無関係のシステム通知またはステータスメッセージ。
レベル3	成功した/承認されたイベント	成功したログイン試行、ファイアウォールで許可されたイベントなど。
レベル4	システムの優先度の低いエラー	不正な設定または未使用のデバイス/アプリケーションに関連するエラー。セキュリティとは無関係であり、通常は初期設定のインストールまたはソフトウェアのテストが原因で発生します。
レベル5	ユーザによって生成されたエラー	パスワードの誤り、処理の拒否など。通常、これらのメッセージはセキュリティとは関係ありません。
レベル6	関連性の低い攻撃	システムに脅威を及ぼさないワームまたはウイルスを示します (Linuxサーバを攻撃するWindowsワームなど)。また、頻繁にトリガされるIDSイベントおよび一般的なエラーイベントも含まれます。
レベル7	事前定義された使用法	

レベル	説明	備考
レベル7	はなし	
レベル8	事前定義された使用法はなし	
レベル9	無効なソースからのエラー	不明なユーザとしてのログインの試行または無効なソースからのログインの試行が含まれます。特にこのメッセージが繰り返される場合は、セキュリティとの関連性がある可能性があります。また、adminまたはrootアカウントに関するエラーも含まれます。
レベル10	ユーザによって生成された複数のエラー	複数回の不正なパスワードの指定、複数回のログインの失敗などが含まれます。攻撃を示す場合や、単にユーザが資格情報を忘れた可能性もあります。
レベル11	事前定義された使用法はなし	
レベル12	重要度の高いイベント	システムやカーネルなどからのエラーまたは警告のメッセージが含まれます。特定のアプリケーションに対する攻撃を示す場合もあります。
レベル13	通常と異なるエラー (重要度: 高)	バッファオーバーフローの試行などの一般的な攻撃パターン、通常のSyslogメッセージ長の超過、または通常のURL文字列長の超過。
レベル14	重要度の高いセキュリティイベント	通常、複数の攻撃ルールと攻撃の兆候が組み合わさったもの。
レベル15	攻撃の成功	誤判定の可能性はほとんどありません。すぐに対処が必要です。

strftime() 変換指定子

指定子	説明
%a	曜日の省略名 (例: Thu)
%A	曜日の正式名 (例: Thursday)
%b	月の省略名 (例: Aug)
%B	月の正式名 (例: August)
%c	日時形式 (例: Thu Sep 22 12:23:45 2007)
%d	月初から数えた日 (01~31) (例: 20)
%H	24時間形式の時刻 (00~23) (例: 13)
%l	12時間形式の時刻 (01~12) (例: 02)

指定子	説明
%j	年初から数えた日 (001~366) (例: 235)
%m	10進表記の月 (01~12) (例: 02)
%M	分 (00~59) (例: 12)
%p	AMまたはPMの指定 (例: AM)
%S	秒 (00~61) (例: 55)
%U	1週目の最初の日を最初の日曜とした場合の週番号 (00~53) (例: 52)
%w	日曜を0とした場合の10進表記の曜日 (0~6) (例: 2)
%W	1週目の最初の日を最初の月曜とした場合の週番号 (00~53) (例: 21)
%x	日付形式 (例: 02/24/79)
%X	時刻形式 (例: 04:12:51)
%y	年の末尾2桁 (00~99) (例: 76)
%Y	年 (例: 2008)
%Z	タイムゾーン名または省略形 (例: EST)
%%	%記号 (例: %)

詳細については、次のWebサイトを参照してください。

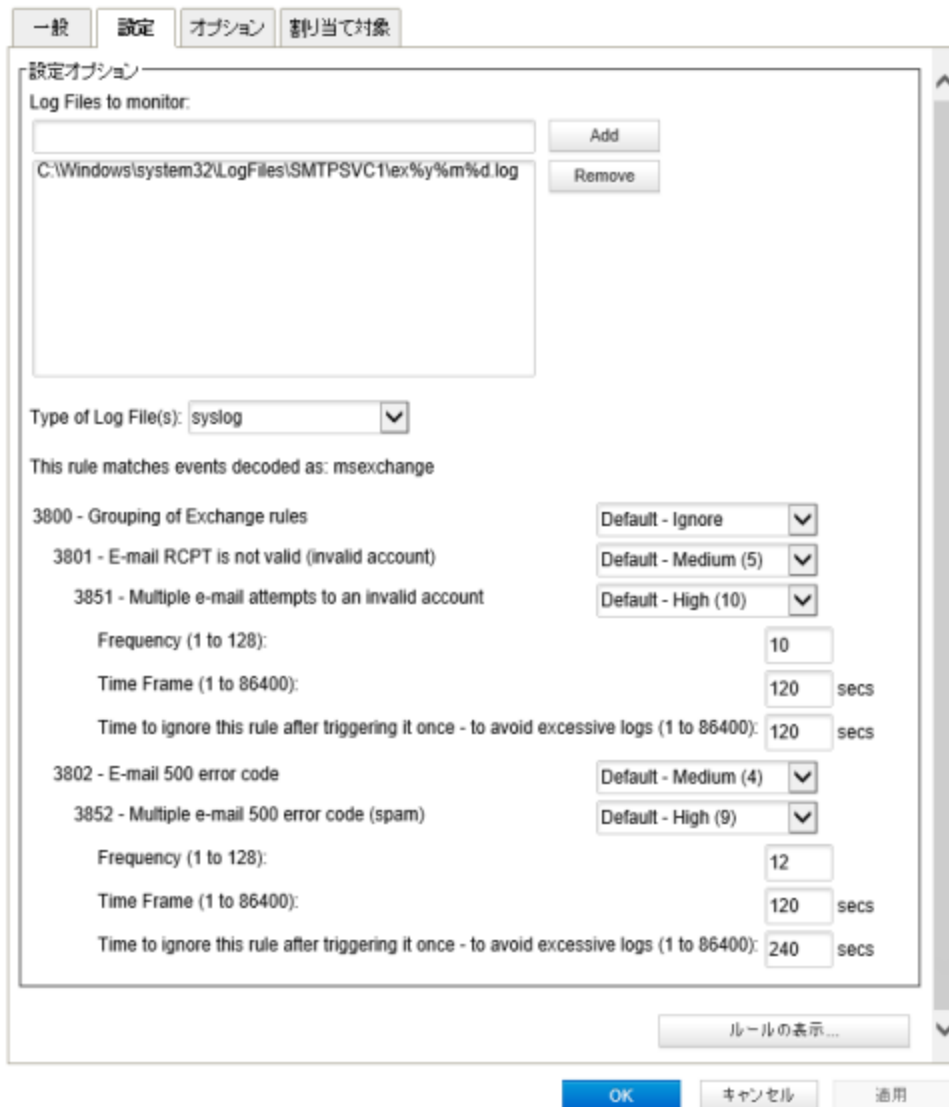
<https://www.php.net/manual/en/function.strftime.php>
www.cplusplus.com/reference/clibrary/ctime/strftime.html

セキュリティログ監視ルールの確認

セキュリティログ監視 ルールは、Deep Security Managerの Policies> Common Objects> Rules> セキュリティログ監視ルールにあります。

セキュリティログ監視 のルール構造とイベント照合プロセス

この画面ショットは、「Microsoft Exchange」セキュリティログ監視 ルールの[プロパティ]画面の[設定][設定]タブの内容を表示します。



次に、ルールの構造を示します。

- 3800 - Grouping of Exchange Rules - Default - ignore
 - 3801 - Email rcpt is not valid (invalid account) - Default - Medium (5)
 - 3851 - Multiple email attempts to an invalid account - Default - High (10)
 - Frequency (1 to 128) - 10
 - Time Frame (1 to 86400) - 120
 - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 120
- 3802 - E-mail 500 error code
 - 3852 - Multiple e-mail 500 error code (spam) - Default - High (9)
 - Frequency (1 to 128): 12
 - Time Frame (1 to 86400): 120 secs
 - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 240 secs

- 3802 - Email 500 error code - Default - Medium (4)
 - 3852 - Email 500 error code (spam) - Default - High (9)
 - Frequency (1 to 128) - 12
 - Time Frame (1 to 86400) - 120
 - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 240

セキュリティログ監視 エンジンは、ログイベントをこの構造に適用し、一致が発生したかどうかを確認します。たとえば、Exchange イベントが発生し、そのイベントが無効なアカウントに対するメールの受信である場合、このイベントは3800の行と一致します (3800の行がExchange イベントであるため)。また、同じイベントが、3800の行のサブルールである3801の行と3802の行にも適用されます。

これ以上の一致がない場合、この一致の「連鎖」は3800の行で停止します。3800の重大度は「Ignore」、」なので、セキュリティログ監視 イベントは記録されません。

ただし、無効なアカウントに対するメールの受信は、3800の行のサブルールの1つ、サブルール3801に一致しています。サブルール3801の重要度は「Medium (4)」です。ここで一致が停止した場合、重大度レベルが[中 (4)] のセキュリティログ監視 イベントが記録されます。

しかし、このイベントに該当するルールは他にもあります。サブルール3851です。同じイベントが過去120秒以内に10回発生した場合、サブルール3851とその3つの属性が一致するでしょう。その場合は、重大度が「高 (9)」 のセキュリティログ監視 イベントが記録されます。(「無視」属性は、サブルール3851に、サブルール3801と一致する個々のイベントを今後120秒間無視するように指示しています。これは、「ノイズ」の低減に役立ちます)。

サブルール3851のパラメータが一致したと仮定すると、重大度が「高 (9)」 のセキュリティログ監視 イベントが記録されます。

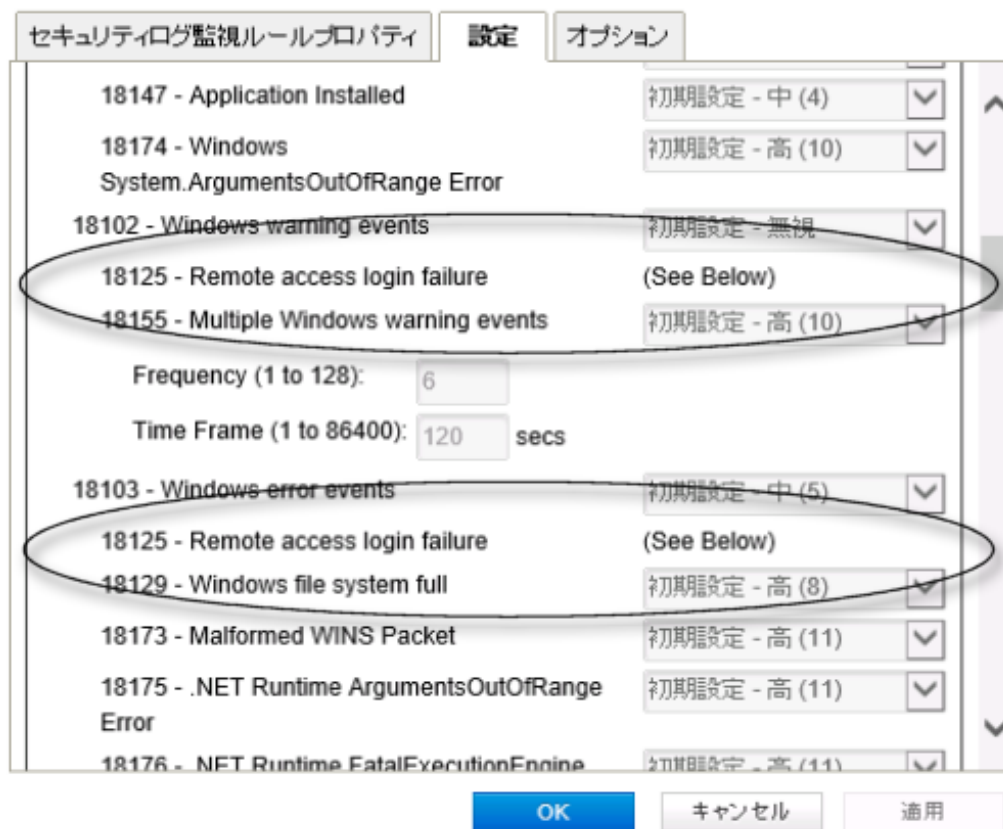
Mail Server - Microsoft Exchange ルールの [オプション] タブを調べてみると、重要度が「中 (4)」 のサブルールが一致していれば、Deep Security Managerによってアラートが発令されることがわかります。この例はこれに該当するため、アラートが発令されます ([このルールによってイベントが記録された場合にアラート] が選択されている場合)。

重複しているサブルール

一部のセキュリティログ監視 ルールに重複するサブルールがあります。例を見るには、[Microsoft Windows Events] ルールを開き、[設定] タブをクリックします。サブルール18125 (Remote access login failure) が、サブルール18102と18103の下に表示されています。また、

どちらの場合も、サブルール18125には重要度の値が示されておらず、単に [See Below] と表示されています。

重複して表示されるのではなく、ルール18125は、[設定] 画面の下部に1回だけ表示されています。



ポリシーで使用するディレクトリリストの作成

複数のポリシーで使用できるように、ディレクトリパスのリストを作成します。異なるポリシーごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。これらのリストの最も一般的な使用例は、不正プログラム対策検索の包含または除外の場合です。詳細については、"[検索対象ファイルを指定する](#)" on page 738するを参照してください。

ヒント: 既存のリストに類似するディレクトリリストを作成するには、既存のリストを複製して編集します。

次の表に、ディレクトリリストのアイテムを定義するための構文を示します。スラッシュ (/) とバックスラッシュ (\) の使用は、WindowsとLinux両方の命名規則でサポートされています。

ディレクトリ	形式	説明	例
ディレクトリ	DIRECTORY	指定したディレクトリとそのすべてのサブディレクトリにあるファイルをすべて含めます。	C:\Program Files\ 「Program Files」ディレクトリとそのすべてのサブディレクトリにあるファイルをすべて含めます。
ネットワークリソース	\\NETWORK RESOURCE	対象コンピュータのネットワークリソースに含まれている、コンピュータ上のファイルを含めます。	\\12.34.56.78 \ \\some-comp-name \ IPアドレスまたはホスト名を使用して識別されたネットワークリソース（およびそのサブフォルダ）のすべてのファイルが含まれます。 \\12.34.56.78 \ somefolder \ \\some-comp-name \ somefolder \ IPアドレスまたはホスト名を使用して識別されたネットワークリソース上の「somefolder」フォルダ内のすべてのファイルとそのサブフォルダを含めます。
ワイルドカード(*)を使用したディレクトリ	DIRECTORY*\	任意のサブディレクトリ名を持つすべてのサブディレクトリを含めます。ただし、指定したディレクトリにあるファイルは含めません。	C: abc * 「abc」のすべてのサブディレクトリにあるファイルをすべて含めます。ただし、「abc」ディレクトリにあるファイルは含めません。 C: abc wx*z 対象: C: abc wx\ C: abc wx123z\ 対象外: C: abc wxz C: abc wx123z C: abc *wx 対象: C: abc wx\ C: abc 123wx\ 対象外: C: abc wx

ディレクトリ	形式	説明	例
			C:\abc\123wx
ワイルドカード(*)を使用したディレクトリ	DIRECTORY*	名前が一致する任意のサブディレクトリを含めます。ただし、そのディレクトリにあるファイルおよび任意のサブディレクトリは含めません。	<p>C:\abc*</p> <p>対象: C:\abc\ C:\abc\1 C:\abc\123</p> <p>対象外: C:\abc C:\abc\123\ C:\abc\123\456 C:\abx\ C:\xyz\ C:\abc*wx 対象:: C:\abc\wx C:\abc\123wx 対象外:: C:\abc\wx\ C:\abc\123wx\ C:\abc\wx*z 対象: C:\abc\wxz C:\abc\wx123z 対象外:: C:\abc\wxz\ C:\abc\wx123z\ C:\abc\wx* 対象:: C:\abc\wx C:\abc\wx\ C:\abc\wx12 C:\abc\wx12\345\ C:\abc\wxz\ 対象外:: C:\abc\wx123z\ </p>
環境変数	\${ENV VAR}	`\${ENV VAR}`の形式を使用した環境変数で定義されるすべてのファイルおよびサブディレクトリを含めます。Virtual Applianceの場合は、環境変数の値のペアをポリシーエディタまたはコンピュータエディタの [設定]→[一般]→[環境変数のオーバーライド] で定義する必要があります。	`\${windir}` 変数が「c:\windows」に変換された場合、「c:\windows」とそのすべてのサブディレクトリにあるファイルをすべて含めます。
コメント	DIRECTORY # コメント	対象の定義にコメントを追加できます。	c:\abc #abcディレクトリを含めます

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ディレクトリリスト]の順にクリックします。
2. [新規]→[新しいディレクトリリスト]の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ディレクトリ]リストで、ディレクトリパスを1行に1つずつ追加します。
5. [OK]をクリックします。

ディレクトリリストをインポート/エクスポートする

1つ以上のディレクトリリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからディレクトリリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ディレクトリリスト]の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ディレクトリリストを使用するポリシーを確認する

ディレクトリリストを使用するポリシーを確認すると、変更によって影響を受けるポリシーを把握できるので便利です。たとえば、ポリシーによって使用されていないことを確認してから、ディレクトリリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ディレクトリリスト]の順にクリックします。
2. ディレクトリリストを選択し、[プロパティ]をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するファイル拡張子リストの作成

複数の不正プログラム検索設定で使用できるように、ファイル拡張子のリストを作成します。異なるルールごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。たとえば、検索に含めるファイルとして、あるファイル拡張子リストを複数の不正プログラム検索設定で使用できます。また、検索から除外するファイルとして、別のファイル拡張子リストを複数の不正プログラム検索設定で使用できます。

ヒント: 既存のリストに類似するファイル拡張子リストを作成するには、既存のリストを複製して編集します。

テキストの先頭にナンバー記号 (「#」) を付けたコメントをリストに挿入できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイル拡張子リスト] の順にクリックします。
2. [新規]→[新規ファイル拡張子リスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ファイル拡張子] リストで、拡張子を1行に1つずつ追加します。
5. [OK] をクリックします。

ファイル拡張子リストをインポート/エクスポートする

1つ以上のファイル拡張子リストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイル拡張子リスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ファイル拡張子リストを使用する不正プログラム検索設定を確認する

ファイル拡張子リストを使用する不正プログラム検索設定を確認すると、変更によって影響を受けるルールを把握できるので便利です。たとえば、検索設定によって使用されていないことを確認してから、ファイル拡張子リストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイル拡張子リスト] の順にクリックします。
2. リストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するファイルリストの作成

複数のポリシーで使用できるように、ファイルパスのリストを作成します。異なるポリシーごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。これらのリストの最も一般的な使用例は、不正プログラム対策検索の包含または除外の場合です。詳細については、"[検索対象ファイルを指定する](#)" on page 738するを参照してください。

ヒント: 既存のリストに類似するファイルリストを作成するには、既存のリストを複製して編集します。

次の表に、ファイルリストのアイテムを定義するための構文を示します。スラッシュ (/) とバックスラッシュ (\) の使用は、WindowsとLinux両方の命名規則でサポートされています。

対象	形式	説明	例
ファイル	FILE	場所やディレクトリに関係なく、指定したファイル名を持つすべてのファイルを含めます。	<code>abc.doc</code> すべてのディレクトリで「abc.doc」という名前のファイルをすべて含めます。「abc.exe」は含めません。
ファイルパス	FILEPATH	ファイルパスで指定された単一のファイルを含めます。	<code>C:\Documents\abc.doc</code> 「Documents」ディレクトリの「abc.doc」という名前のファイルのみ含めます。
ワイルドカード (*) を使用したファイルパス	FILEPATH	ファイルパスで指定されたすべてのファイルを除外します。	<code>C:\Documents\abc.co*</code> (Windows Agentプラットフォームのみ) 「Documents」ディレクトリで、ファイル名が「abc」で拡張子が「.co」で始まるファイルを除外します。
ファイル名はワイルドカード (*) です	FILEPATH*	パス内のすべてのファイルを除外しますが、指定されていないサブディレクトリ内のファイルは除外しません	<code>C:\Documents*</code> ディレクトリC:\Documents\にあるすべてのファイルを除外します。 <code>C:\Documents\SubDirName**</code> フォルダ名が「SubDirName」で始まるサブディレクトリ内のすべてのファイルを除外します。C:\Documents\またはその他のサブディレクトリにあるすべてのファイルを除外しません。 <code>C:\Documents**</code> C:\Documents下のすべての直

対象	形式	説明	例
			接サブディレクトリ内のすべてのファイルを除外します。以降のサブディレクトリにあるファイルは除外しません。
ワイルドカード(*)を使用したファイル	FILE*	パターンに一致するファイル名を持つすべてのファイルを含めます。	<p><i>abc*.exe</i> 接頭語が「abc」で拡張子が「.exe」のファイルを含めます。</p> <p><i>*.db</i> 対象: 123.db abc.db 対象外: 123db 123.abd cbc.dba</p> <p><i>*db</i> 対象: 123.db 123db ac.db acdb db 対象外: db123</p> <p><i>wxy*.db</i> 対象: wxy.db wxy123.db 対象外: wxydb</p>
ワイルドカード(*)を使用したファイル	FILE.EXT*	パターンに一致するファイルの拡張子を持つすべてのファイルを含めます。	<p><i>abc.v*</i> ファイル名が「abc」で拡張子が「.v」で始まるファイルを含めます。</p> <p><i>abc.*pp</i> 対象: abc.pp abc.app 対象外: wxy.app</p> <p><i>abc.a*p</i> 対象:</p>

対象	形式	説明	例
			abc.ap abc.a123p 対象外: abc.pp abc.* 対象: abc.123 abc.xyz 対象外: wxy.123
ワイルドカード(*)を使用したファイル	FILE*.EXT*	パターンに一致するファイル名と拡張子を持つすべてのファイルを含めます。	a*c.a*p 対象: ac.ap a123c.ap ac.a456p a123c.a456p 対象外: ad.aa
環境変数	\${ENV VAR}	\${ENV VAR} の形式を使用した環境変数で指定されるファイルを含めます。環境変数は、ポリシーエディタまたはコンピュータエディタの [設定]→[一般]→[環境変数のオーバーライド] で定義またはオーバーライドできます。	`\${myDBFile}` 「myDBFile」ファイルを含めます。
コメント	FILEPATH # コメント	対象の定義にコメントを追加できます。	C:\Documents\abc.doc #これはコメントです

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイルリスト] の順にクリックします。
2. [新規]→[新規ファイルリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ファイル] リストで、ファイルパスを1行に1つずつ追加します。
5. [OK] をクリックします。

ファイルリストをインポート/エクスポートする

1つ以上のファイルリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイルリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。

3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ファイルリストを使用するポリシーを確認する

ファイルリストを使用するポリシーを確認すると、変更によって影響を受けるポリシーを把握できるので便利です。たとえば、ポリシーによって使用されていないことを確認してから、ファイルリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイルリスト] の順にクリックします。
2. ファイルリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するIPアドレスリストの作成

複数のファイアウォールルールで使用できるように、IPアドレスのリストを作成します。異なるルールごとに定義された複数の同じリストよりも、単一のリストの方が容易に管理できます。

ヒント: 既存のリストに類似するIPリストを作成するには、既存のリストを複製して編集します。

個々のIPアドレスだけでなく、IP範囲とマスクされているIPも入力できます。テキストの先頭にナンバースケッチ記号 (「#」) を付けたコメントもIPリストに挿入できます。

マスクされているIPの例は、192.168.0/24、192.168.2.0/255.255.255.0、IPV6の場合は2001:0DB8::CD30:0:0:0/60です。IP範囲の例は、192.168.0.2 - 192.168.0.125、IPV6の場合はFF01::101 - FF01::102です。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] の順にクリックします。
2. [新規]→[新規IPリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [IP] リストで、IPアドレス、マスクされたIPアドレス、またはIP範囲 (1行ごとに1つ) を追加します。
5. [OK] をクリックします。

IPリストをインポート/エクスポートする

1つ以上のIPリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

IPリストを使用するルールを確認する

IPリストを使用するファイアウォールルールを確認すると、変更によって影響を受けるルールを把握できるので便利です。たとえば、ファイアウォールルールによって使用されていないことを確認してから、IPリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] の順にクリックします。
2. IPリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するポートリストの作成

複数のルールで使用できるように、ポート番号のリストを作成します。異なるルールごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。

ヒント: 既存のリストに類似するポートリストを作成するには、既存のリストを複製して編集します。

個々のポートおよびポート範囲をリストに含めることができます (例: 80、20-21)。テキストの先頭にナンバー記号 (「#」) を付けたコメントをポートリストに挿入できます。

注意: 一般的に受け入れられているポート番号割り当てのリストについては、[Internet Assigned Numbers Authority \(IANA\)](#) を参照してください。Deep Security Manager、Relay、またはAgentで使用されるポート番号のリストについては、"[ポート番号、URL、およびIPアドレス](#)" on page 190を参照してください。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順にクリックします。
2. [新規]→[新規ポートリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ポート] リストで、ポート番号を1行に1つずつ追加します。
5. [OK] をクリックします。

ポートリストをインポート/エクスポートする

1つ以上のポートリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ポートリストを使用するルールを確認する

ポートリストを使用するルールを確認すると、変更によって影響を受けるルールを把握できるので便利です。たとえば、ルールによって使用されていないことを確認してから、ポートリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順にクリックします。
2. ポートリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するMACアドレスリストの作成

複数のポリシーで使用できるように、MACアドレスのリストを作成します。異なるポリシーごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。

ヒント: 既存のリストに類似するMACリストを作成するには、既存のリストを複製して編集します。

MACリストは、ハイフン区切りおよびコロン区切り両方の形式のMACアドレスをサポートしています (例: 0A-0F-FF-F0-A0-AF、0A:0F:FF:F0:A0:AF)。テキストの先頭にナンバー記号 (「#」) を付けたコメントをMACリストに挿入できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[MACリスト] の順にクリックします。
2. [新規]→[新規MACリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [MAC] リストで、MACアドレスを1行に1つずつ追加します。
5. [OK] をクリックします。

MACリストをインポート/エクスポートする

1つ以上のMACリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[MACリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

MACリストを使用するポリシーを確認する

MACリストを使用するポリシーを確認すると、変更によって影響を受けるポリシーを把握できるので便利です。たとえば、ポリシーによって使用されていないことを確認してから、MACリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[MACリスト] の順にクリックします。
2. MACリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するコンテキストの定義

コンテキストは、コンピュータのネットワーク環境に応じてさまざまなセキュリティポリシーを実装する有効な方法です。

コンテキストは、ファイアウォールルールおよび侵入防御ルールと関連付けられるよう設計されています。ルールに関連付けられたコンテキストの定義条件に一致した場合、ルールは適用されます。

コンピュータがインターネットに接続されているかどうかを判別するオプションを設定する

1. Deep Security Managerで、[管理]→[システム設定]→[コンテキスト]の順に選択します。
2. [インターネットの接続テスト用URL] ボックスに、インターネットの接続をテストするために送信されるHTTP要求の宛先URLを入力します(「http://」を含める)。
3. [接続確認用の応答コンテンツの正規表現] ボックスに、HTTP通信が成功したことを確認する応答コンテンツに適用する正規表現を入力します(応答コンテンツがわかっている場合は、単純な文字列を使用できます)。
4. [テスト間隔] リストで、接続テストの間隔を選択します。

たとえば、インターネット接続をテストするには、「http://www.example.com」というURLと、そのURLのサーバから返される「This domain is established to be used for illustrative examples in documents」という文字列を使用できます。

コンテキストを定義する

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[その他]→[コンテキスト]の順に選択し、[新規]→[新規コンテキスト]の順にクリックします。
2. [一般情報] エリアで、コンテキストルールの名前と説明を入力します。このエリアには、このコンテキストルールをサポートするのに必要なDeep Security Agentのバージョンも表示されます。
3. [オプション] エリアで、コンテキストが適用されるタイミングを指定します。
 - 接続が次の場合にコンテキストを適用: このオプションは、コンピュータがドメインコントローラに接続する場合、またはインターネット接続に接続する場合、ファイアウォールルールを有効にするかどうかを決定します。インターネット接続テストの条件は [管理]→[システム設定]→[コンテキスト] で設定できます。

ドメインコントローラへICMP経由で直接接続できる場合は、「ローカル」接続になります。VPN経由でのみ接続できる場合は、「リモート」接続になります。

ドメインコントローラ接続のテスト間隔はインターネット接続のテスト間隔と同じで、[管理]→[システム設定]→[コンテキスト]で設定できます。インターネット接続テストは、コンピュータがドメインコントローラに接続できない場合にのみ実行されません。

- コンテキストをインタフェース制限に適用: このコンテキストは、インタフェース制限のためにトラフィックが制限されているネットワークインタフェースに適用されません。これは主に「許可」または「強制的に許可」ファイアウォールルールで使用され

まず、"[コンピュータで使用可能なインタフェースの検出と設定](#)" on page 603を参照してください。

コンテキストをルールに割り当てると、コンテキストの [割り当て対象] タブにそのルールが表示されます (コンテキストにセキュリティルールを関連付けるには、セキュリティルールの [プロパティ] 画面の [オプション] タブに移動し、[コンテキスト] リストからコンテキストを選択します)。

ステートフルファイアウォールの設定の定義

Deep Securityのステートフルファイアウォール設定メカニズムでは、トラフィック履歴との関連における各パケット、TCPおよびIPヘッダ値の正当性、およびTCP接続状態の推移が分析されます。UDPやICMPなどのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実装されます。パケットは、ステートフルメカニズムによって次のように処理されます。

1. 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
2. パケットを調べて、既存の接続に属しているかどうか判断されます。
3. TCPヘッダの正当性 (シーケンス番号、フラグの組み合わせなど) が調査されます。

新しいステートフル設定を作成するには、次の手順に従います。

1. "[ステートフル設定を追加する](#)" below
2. "[ステートフル設定情報を入力する](#)" on the next page.
3. "[パケットインスペクションオプションを選択する](#)" on the next page.

ステートフル設定の後には、次の操作について説明します。

- "[ステートフル設定が割り当てられたポリシーとコンピュータを表示する](#)" on page 687
- "[ステートフル設定をエクスポートする](#)" on page 687
- "[ステートフル設定を削除する](#)" on page 687

ステートフル設定を追加する

[ポリシー]→[共通オブジェクト]→[その他]→[ファイアウォールステートフル設定] でステートフル設定を定義する方法には次の3つがあります。

- 新しい設定を作成します。[新規]→[新規ファイアウォールステートフル設定] の順にクリックします。

- XMLファイルから設定をインポートします。[新規]→[ファイルからインポート]をクリックします。
- 既存の設定をコピーして変更します。[ファイアウォールステータフル設定] リストの設定を右クリックして、[複製]をクリックします。新しい設定を編集するには、その設定を選択し、[プロパティ]をクリックします。

ステータフル設定情報を入力する

設定の [名前] と [説明] を入力します。

パケットインスペクションオプションを選択する

IP、TCP、UDPおよびICMPパケットインスペクションのオプションを定義し、アクティブまたはパッシブFTPを有効化できます。

IPパケットインスペクション

[一般] タブで [フラグメント化されたすべての受信パケットを拒否する] を選択し、フラグメント化されたパケットをすべて破棄します。破棄されたパケットはフラグメント化分析をバイパスして、「IP fragmented packet」というログエントリが生成されます。全長がIPヘッダの長さよりも短いパケットはログに記録されずに破棄されます。

警告: 攻撃者は、ファイアウォールルールをバイパスするために、フラグメント化されたパケットを作成して送信する場合があります。

注意: 初期設定では、ファイアウォールエンジンは、フラグメント化されたパケットに対して一連のチェックを実行します。これは初期設定の動作で、変更することはできません。次のような特徴を持つパケットは、破棄されます。

- フラグメントのフラグ/オフセットが無効: IPヘッダ内のDFフラグまたはMFフラグのいずれかが1に設定されている、またはヘッダ内に含まれるDFフラグが1に設定されており、オフセット値が0以外に設定されているとき、パケットは破棄されます。
- 最初のフラグメントが最小サイズ未満: MFフラグが1に設定されていて、オフセット値が0、合計の長さが (最大組み合わせヘッダ長である) 120バイトよりも短い場合、パケットは破棄されます。
- IPフラグメントが範囲を超えている: 合計パケット長と組み合わせられたオフセットフラグの値が最大データグラム長である65,535バイトを超えた場合、パケットは破棄されません。

- IPフラグメントのオフセットが小さすぎる: 60バイトよりも小さい値を持つ0以外のオフセットフラグがある場合、パケットは破棄されます。

TCPパケットインスペクション

[TCP] タブで有効化するオプションを次の中から選択します。

- CWR、ECEフラグを含むTCPパケットを拒否する: これらのフラグは、ネットワーク輻輳時に設定されます。

注意: RFC 3168では、ECN (Explicit Congestion Notification) に使用する予約済みフィールドの6ビットのうち2ビットを、次のように定義しています。

- ビット8から15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
- TCPヘッダフラグのビット名参照:
 - ビット8: CWR (Congestion Window Reduced) [RFC3168]
 - ビット9: ECE (ECN-Echo) [RFC3168]

警告: パケットの自動転送 (特にDoS攻撃によって生成されたものなど) によって、これらのフラグが設定されたパケットが作成されることがよくあります。

- TCPステートフルインスペクションを有効にする: TCPレベルでのステートフルインスペクションを有効にします。ステートフルTCPインスペクションを有効にすると、次のオプションが利用可能です。
 - TCPステートフルログを有効にする: TCPステートフルインスペクションイベントがログに記録されます。
 - 単一コンピュータからの受信接続数の上限: 単一コンピュータからの接続数を制限すると、DoS攻撃の影響を低減できます。
 - 単一コンピュータへの送信接続数の上限: 単一コンピュータへの送信接続数を制限すると、Nimdaなどのワームの影響を大幅に低減できます。
 - 単一コンピュータからのハーフオープン接続数の上限: この制限を設定すると、SYNフラッドなどのDoS攻撃から保護できます。ほとんどのサーバでは、ハーフオープン接続を終了するためにタイムアウトが設定されています。この値を設定することにより、ハーフオープン接続が重大な問題にならないようにします。SYN-SENT (リモート) エントリが指定された制限に達した場合、その特定のコンピュータからの後続のTCPパケットは破棄されます。

注意: 単一コンピュータからのオープン接続を許可する数を決定する際に、使用している種類のプロトコルで妥当と考えられる単一コンピュータからのハーフオープン接続数と、輻輳を引き起こすことなくシステムが維持できる単一コンピュータからのハーフオープン接続数との間の数を選択します。

- すでに確認されたパケット数が次を超過したときにACKストーム防御を有効にする: このオプションを設定して、ACKストーム攻撃が発生した場合のイベントを記録します。
 - ACKストームが検出されたときに接続を中断する: このオプションを設定して、攻撃が検出された場合に接続を切断するようにします。

注意: ACKストーム保護オプションはDeep Security Agent 8.0以前でのみ使用可能です。

FTPオプション

[FTPオプション] タブで次のオプションを有効化できます。

注意: 以下のFTPオプションはDeep Security Agent 8.0以前で使用可能です。

- アクティブFTP
 - 受信を許可する: このコンピュータがサーバとして動作しているときにアクティブFTPを許可します。
 - 送信を許可する: このコンピュータがクライアントとして動作しているときにアクティブFTPを許可します。
- パッシブFTP
 - 受信を許可する: このコンピュータがサーバとして動作しているときにパッシブFTPを許可します。
 - 送信を許可する: このコンピュータがクライアントとして動作しているときにパッシブFTPを許可します。

UDPパケットインスペクション

[UDP] タブで次のオプションを有効化できます。

- UDPステートフルインスペクションを有効にする: UDPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

注意: UDPステートフル機能は、未承諾の受信UDPパケットを破棄します。送信UDPパケットごとに、ルールがそのUDP「ステートフル」テーブルをアップデートし、要求に対して60秒以内にUDP応答が発生した場合のみ、UDP応答を許可します。特定の受信UDPトラフィックを許可する場合は、強制的に許可ルールを作成する必要があります。たとえば、DNSサーバを実行している場合、送信先のポート53に受信UDPパケットを許可するには、強制的に許可ルールを作成する必要があります。

警告: UDPトラフィックのステートフルインスペクションがない場合、攻撃者はDNSサーバになりすまして、未承諾のUDP「応答」を送信元のポート53からファイアウォールの内側にあるコンピュータに送信する可能性があります。

- UDPステートフルログを有効にする: このオプションを選択すると、UDPステートフルインスペクションイベントのログを記録できるようになります。

ICMPパケットインスペクション

[ICMP] タブで次のオプションを有効にできます。

注意: ICMPステートフルインスペクションは、Deep Security Agent 8.0以前で使用できません。

- ICMPステートフルインスペクションを有効にする: ICMPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

注意: ICMP (擬似) ステートフル機能は、未承諾の受信ICMPパケットを破棄します。送信ICMPパケットごとに、ルールがそのICMP「ステートフル」テーブルを作成またはアップデートし、要求に対して60秒以内にICMP応答が発生した場合のみ、ICMP応答を許可します(サポートするICMPペアの種類は、タイプ0と8、13と14、15と16、17と18です)。

警告: たとえば、ステートフルICMPインスペクションを有効にすると、エコー要求が送信された場合にICMPエコー応答を許可できます。要求されていないエコー応答は、Smurf増幅攻撃、マスターとデーモン間のライブフラッドネットワーク通信、Loki2バックドアなど、さまざまな種類の攻撃の予兆である可能性があります。

- ICMPステートフルログを有効にする: このオプションを選択すると、ICMPステートフルインスペクションイベントのログを記録できるようになります。

ステートフル設定をエクスポートする

[エクスポート] をクリックし、リストから該当するエクスポート処理を選択すると、すべてのステートフル設定を.csvまたは.xmlファイルにエクスポートできます。ステートフル設定を選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のステートフル設定をエクスポートすることもできます。

ステートフル設定を削除する

ステートフル設定を削除するには、[ファイアウォールステートフル設定] リスト内の設定を右クリックして、[削除] をクリックした後、[OK] をクリックします。

注意: 1台以上のコンピュータに割り当てられたステートフル設定、またはポリシーの一部であるステートフル設定は削除できません。

ステートフル設定が割り当てられたポリシーとコンピュータを表示する

ステートフルインスペクション設定に割り当てられたポリシーとコンピュータは、[割り当て対象] タブに表示できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールに適用するスケジュールの定義

スケジュールは、ルール、Agentのアップグレードなどに割り当てることのできる再利用可能なタイムテーブルです。

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[その他]→[スケジュール]の順に選択します。
2. [新規]→[新規スケジュール]の順にクリックします。
3. [一般情報] エリアで、スケジュールを識別するための名前と説明を入力します。
4. グリッドからある時間枠をクリックするとその時間枠が選択されます。選択を解除するには、Shiftキーを押しながらその時間枠をクリックします。スケジュール期間は、1時間の時間枠で定義します。

スケジュールをルールに割り当てると、スケジュールの [割り当て対象] タブにそのルールが表示されます。スケジュールにセキュリティルールを関連付けるには、セキュリティルールの [プ

ロパティ] 画面の [オプション] タブに移動し、[スケジュール] リストからスケジュールを選択します。

注意: Agentベースの保護では、スケジュールで保護対象のコンピュータのOSと同じタイムゾーンが使用されます。Agentレスによる保護では、Deep Security Virtual Applianceと同じタイムゾーンが使用されます。

アプリケーションコントロールによるソフトウェアのロックダウン

注意: Deep Security Agent 10.0以上を実行しているコンピュータのアプリケーションコントロールを有効にできます。アプリケーションコントロールがサポートされるOSのリストについては、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。

アプリケーションコントロールは、保護対象サーバのソフトウェア変更を継続的に監視します。ポリシー設定に基づいて、アプリケーション制御は、許可されていないソフトウェアが明示的に許可されるまで実行されないようにしたり、許可されていないソフトウェアが明示的にブロックされるまで許可したりしないようにします。選択するオプションは、使用環境に必要なコントロールレベルに応じて異なります。

警告: アプリケーションコントロールは、継続的にサーバを監視し、ソフトウェアの変更が生じるたびにイベントをログに記録します。これは、一部のWebサーバやメールサーバなど、自動的に変更されるソフトウェアを使用する環境や通常実行可能ファイルを作成する環境には向いていません。アプリケーションコントロールがお使いの環境に適しているかどうかを確認するには、"[アプリケーションコントロールで検出されるソフトウェア変更](#)" on page 694を参照してください。

ヒント: アプリケーションコントロールの作成と設定は、Deep Security APIを使用して自動化できます。詳細については、Deep Security Automation Centerにあるガイド [「Configure Application Control」](#) を参照してください。

主な概念

対象となる保護の状態: アプリケーションコントロールの設定時に必要な主な決定事項の1つに、対象となる保護の状態の決定があります。新規または変更されたすべてのソフトウェアについて、許可するように手動で指定するまで実行されないようにしますか。または、明示的にブロックするまで初期設定で実行しますか。はじめてアプリケーションコントロールを有効にしたときに、承認されていないソフトウェアが大量にある場合、承認されていないソフトウェアを最初に許可する方法があります。アプリケーションコントロールルールを追加して、承認されていないソフトウェアの量を減らすと、ブロックモードに切り替えることができます。

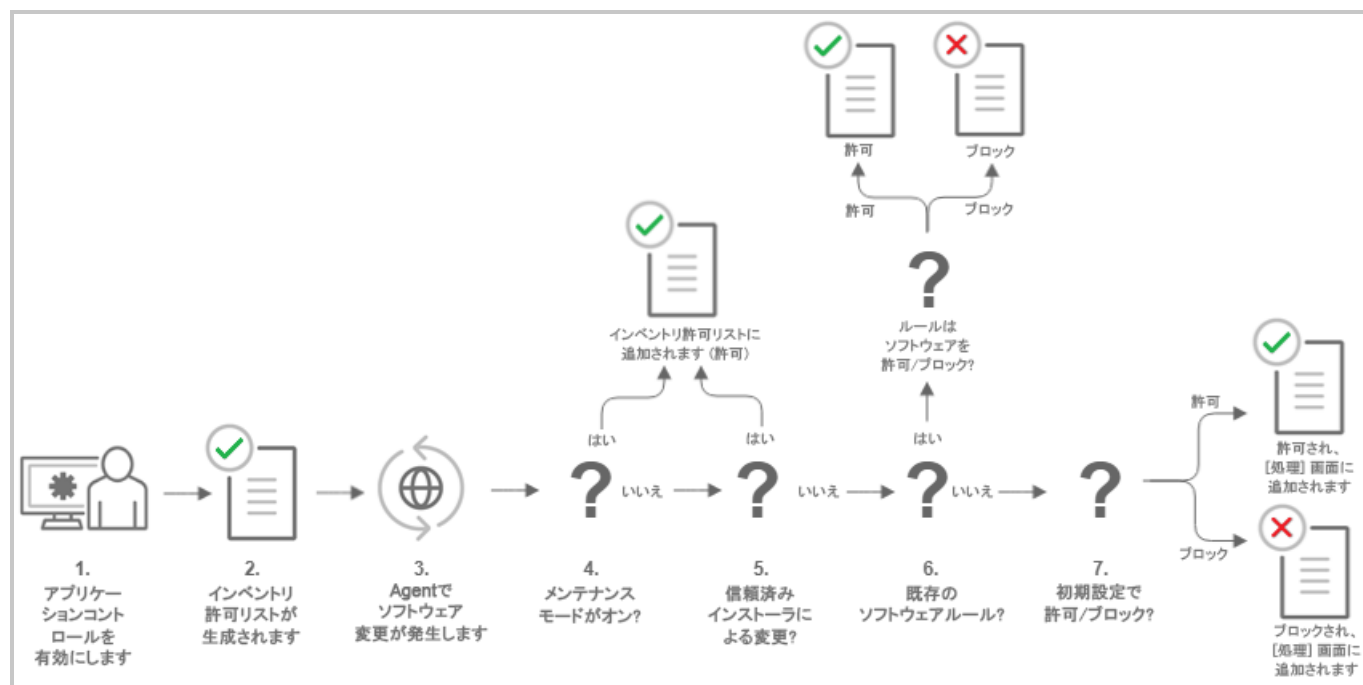
アプリケーションコントロールルール: ルールは、特定のコンピュータでのソフトウェアの許可またはブロックを指定します。

インベントリ: コンピュータにインストールされているソフトウェアの初期リストです。許可するソフトウェアのみをコンピュータにインストールするようにしてください。アプリケーション制御を有効にすると、現在インストールされているすべてのソフトウェアがコンピュータのインベントリに追加され、実行が許可されます。コンピュータがメンテナンスモードの場合、コンピュータに対するソフトウェアの変更がコンピュータのインベントリに追加され、実行されるようになります。コンピュータのソフトウェアインベントリはDeep Security Agentに格納されており、Deep Security Managerには表示されません。

承認されていないソフトウェア: コンピュータのインベントリに登録されていないソフトウェアで、アプリ制御ルールで保護されていないソフトウェアです。"[アプリケーションコントロールで検出されるソフトウェア変更](#)" on page 694を参照してください。

メンテナンスモード: ソフトウェアのインストールまたはアップデートを予定している場合は、メンテナンスモードをオンにすることをお勧めします。メンテナンスモードでは、アプリケーション制御は引き続きアプリケーションコントロールルールによってブロックされたソフトウェアをブロックしますが、新しいソフトウェアまたはアップデートされたソフトウェアを実行してコンピュータのインベントリに追加することができます。"[変更の計画時にメンテナンスモードをオンにする](#)" on page 701を参照してください。

アプリケーションコントロールの仕組み



1. ポリシーでアプリケーションコントロールを有効にして、Deep Security Agentで保護されているコンピュータにこのポリシーを割り当てます ("アプリケーションコントロールを有効にする" on page 696を参照)。
2. Agentがこのポリシーを受信すると、コンピュータにインストールされているすべてのソフトウェアのインベントリを作成します。インベントリに記載されているすべてのソフトウェアは安全であるとみなされ、そのコンピュータで実行できるようになります。このインベントリリストはDeep Security Managerからは表示されません。つまり、アプリケーション制御を有効にするコンピュータに適切なソフトウェアのみがインストールされていることを確認する必要があります。
3. インベントリの作成後、アプリケーションコントロールでコンピュータのあらゆるソフトウェア変更が認識されます。ソフトウェア変更により、新しいソフトウェアがコンピュータに表示されたり、既存のソフトウェアに変更が加えられたりします。
4. コンピュータがメンテナンスモードの場合、Deep Security Agentはそのソフトウェアをインベントリリストに追加し、実行を許可します。この変更はDeep Security Managerでは表示できません。"変更の計画時にメンテナンスモードをオンにする" on page 701を参照してください。
5. 信頼されたインストーラによって変更が行われた場合、Deep Security Agentはそのソフトウェアをインベントリリストに追加して実行します。たとえば、Microsoft Windowsがコンポーネントアップデートを自己始動する場合、数百の新しい実行可能ファイルがインストールされます。アプリケーションコントロールは、既知のWindowsプロセスによっ

て作成された多くのファイル変更を自動認証しますが、Deep Security Managerにはこの変更は表示されません。想定されるソフトウェア変更に関連する「ノイズ」を削除すると、注意が必要な変更を明確に確認できます。

注意: 信頼済みのインストーラ機能はDeep Security Agent 10.2以上で利用可能です。

6. コンピュータのルールセットに適切なソフトウェアのルールが含まれる場合、ソフトウェアは実行されるルールに従って許可またはブロックされます。["アプリケーションコントロールで検出されるソフトウェア変更" on page 694](#)を参照してください。
7. ソフトウェアがコンピュータのインベントリにない場合に、既存のルールで保護されていないソフトウェアは、認識されないソフトウェアとみなされます。コンピュータに割り当てられたポリシーでは、承認されていないソフトウェアの処理方法を指定します。ポリシー設定に応じて、実行が許可またはブロックされます。ソフトウェアがブロックされ、OSにエラーメッセージを表示できる場合、そのソフトウェアの実行が許可されない、またはアクセスが拒否されたことを示すエラーメッセージが保護対象のコンピュータに表示されます。

承認されていないソフトウェアは、Deep Security Managerの [アプリケーションコントロール - ソフトウェア変更] 画面に表示されます。この画面で、管理者は [許可] または [ブロック] をクリックし、特定のコンピュータに対して該当のソフトウェアの許可ルールまたはブロックルールを作成できます。許可ルールまたはブロックルールは、ポリシーで指定された初期設定アクションよりも優先されます。["新規および変更済みソフトウェアを監視する" on page 698](#)を参照してください。

アプリケーションコントロールインタフェースの紹介

Deep Security Managerには、アプリケーションコントロールに関連する変更を確認できる場所があります。

- ["アプリケーションコントロール: ソフトウェア変更 \(\[処理\]\)" on the next page](#)
- ["アプリケーションコントロールルールセット" on page 693](#)
- ["セキュリティイベント" on page 694](#)

アプリケーションコントロール: ソフトウェア変更 ([処理])

The screenshot shows the 'Application Control: Software Change' screen in the Deep Security Manager. The main area displays a list of software changes with columns for file hashes, file names, and actions. A sidebar on the right shows details for a selected file, including its name, size, version, and hashes.

File Hash	File Name	Count	Actions
3d3b0da9-3df1-456c-80a1-00996db53d39	F70DCD...	3件数	[許可] [ブロック]
3 / 3			
30388cf9-a8e7-4db5-b1e4-3b512dcc0529	9888B3...	2件数	[許可] [ブロック]
1beaac1e-45e0-4565-bd9b-9def29230db4	E3885F...	1件数	[許可] [ブロック]

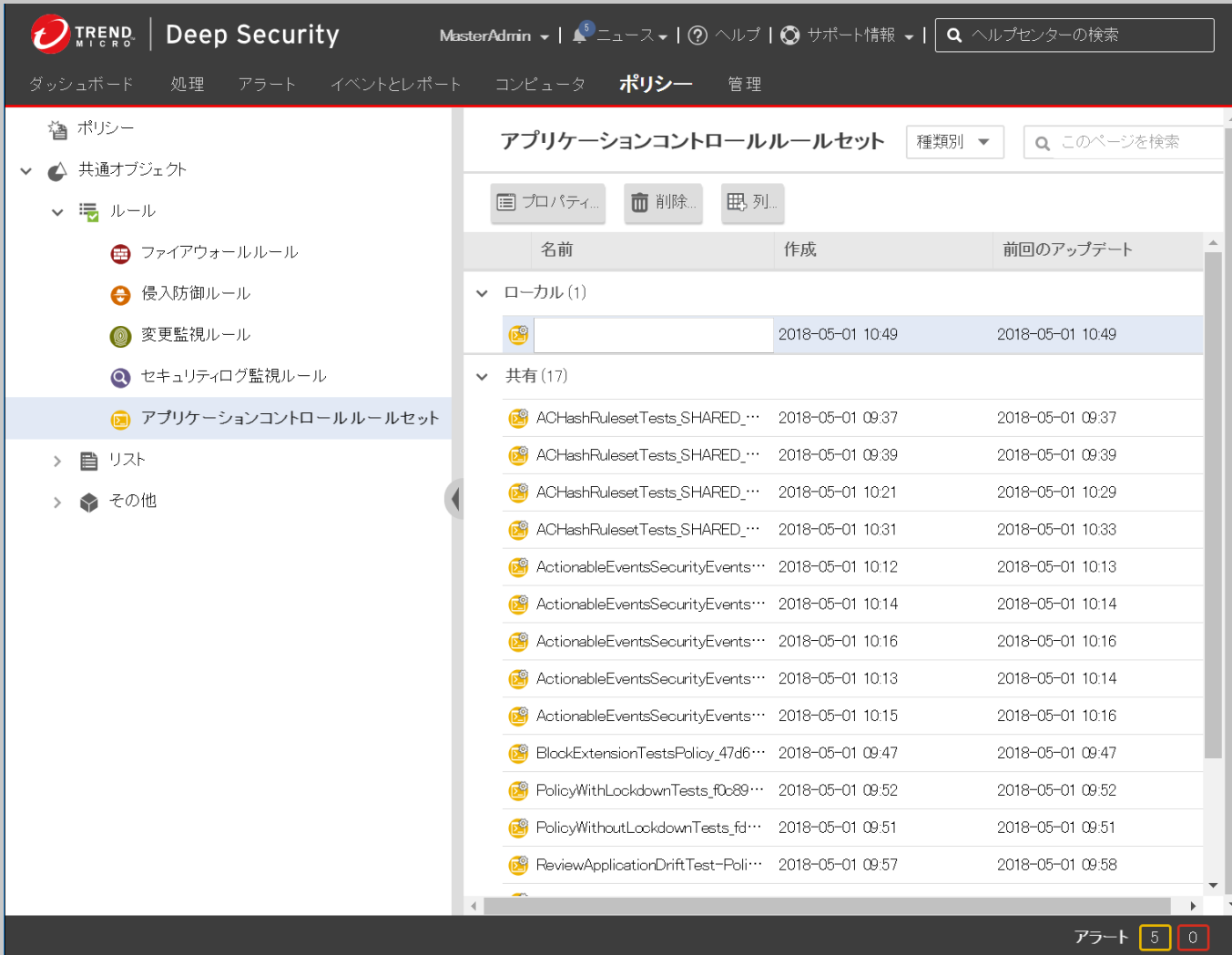
Right sidebar details for file 3d3b0da9-3df1-456c-80a1-00996db53d39:

- 製品名: 検出なし
- ファイル名: 3d3b0da9-3df1-456c-80a1-00996db53d39
- インストールパス: 検出なし
- ベンダ: 検出なし
- ファイルサイズ: 41 バイト
- ファイルバージョン: 検出なし
- 説明: 検出なし
- SHA256: F70DCD4B3F44FA3B240035FC24F97FCEA6625D2197F3A7292E01A39D32F9ECEB
- SHA1: 3926196CCDE3AB24434C316558843B9072D30065
- MDS: 8941DEF95ABCDD557DA1F7FCFCFE44

[アプリケーションコントロール: ソフトウェア変更]画面は、Deep Security Managerの [処理] をクリックすると表示されます。すべての認識されないソフトウェア（コンピュータのインベントリにないソフトウェアで、対応するアプリケーション制御ルール)がないソフトウェアが表示されます。ソフトウェア変更はコンピュータレベルで許可またはブロックされるため、特定のソフトウェアを50台のコンピュータにインストールすると、この画面に50回表示されます。ただし、特定のソフトウェアをすべての場所で許可またはブロックする必要がある場合は、[処理] 画面をフィルタしてファイルハッシュ別に変更をソートし、[すべて許可] をクリックしてソフトウェアがインストールされているすべてのコンピュータで許可します。

コンピュータに適用されるポリシーでは、承認されていないソフトウェアの実行を初期設定で許可またはブロックするかを指定しますが、[処理] 画面で [許可] または [ブロック] をクリックするまで、明示的なアプリケーションコントロールルールは作成されません。[許可] または [ブロック] をクリックすると、対応するルールがコンピュータのルールセットに表示されます。ルールセットは [アプリケーションコントロールルールセット] 画面に表示されます。

アプリケーションコントロールルールセット



Deep Security MasterAdmin | ニュース | ヘルプ | サポート情報 | ヘルプセンターの検索

ダッシュボード 処理 アラート イベントとレポート コンピュータ **ポリシー** 管理

ポリシー

- 共通オブジェクト
 - ルール
 - ファイアウォールルール
 - 侵入防御ルール
 - 変更監視ルール
 - セキュリティログ監視ルール
 - アプリケーションコントロールルールセット**
 - リスト
 - その他

アプリケーションコントロールルールセット 種類別 このページを検索

プロパティ... 削除... 列...

名前	作成	前回のアップデート
ローカル (1)		
	2018-05-01 10:49	2018-05-01 10:49
共有 (17)		
ACHashRulesetTests_SHARED_...	2018-05-01 09:37	2018-05-01 09:37
ACHashRulesetTests_SHARED_...	2018-05-01 09:39	2018-05-01 09:39
ACHashRulesetTests_SHARED_...	2018-05-01 10:21	2018-05-01 10:29
ACHashRulesetTests_SHARED_...	2018-05-01 10:31	2018-05-01 10:33
ActionableEventsSecurityEvents...	2018-05-01 10:12	2018-05-01 10:13
ActionableEventsSecurityEvents...	2018-05-01 10:14	2018-05-01 10:14
ActionableEventsSecurityEvents...	2018-05-01 10:16	2018-05-01 10:16
ActionableEventsSecurityEvents...	2018-05-01 10:13	2018-05-01 10:14
ActionableEventsSecurityEvents...	2018-05-01 10:15	2018-05-01 10:16
BlockExtensionTestsPolicy_47d6...	2018-05-01 09:47	2018-05-01 09:47
PolicyWithLockdownTests_fd0c89...	2018-05-01 09:52	2018-05-01 09:52
PolicyWithoutLockdownTests_fd...	2018-05-01 09:51	2018-05-01 09:51
ReviewApplicationDriftTest-Poli...	2018-05-01 09:57	2018-05-01 09:58

アラート 5 0

コンピュータのルールセットを確認するには、[ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット]に移動します。ルールセットに含まれるルールを確認するには、ルールセットをダブルクリックして[ルール]タブに移動します。[ルール]タブには、ルールが関連付けられたソフトウェアが表示され、許可ルールをブロックルールに変更したり、ブロックルールを許可ルールに変更したりすることもできます。

セキュリティイベント

時刻	コンピュータ	イベント	ルール	ルールセット	処理	理由	繰り返しカウ...	ファイル	ユーザ名
2018-05-14 12:18:17		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	libnumbers.so	root
2018-05-14 12:18:17		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	man	root
2018-05-14 12:12:07		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	libnumbers.so	root
2018-05-14 12:12:07		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	man	root
2018-05-14 12:09:22		承認されていないソフトウェアの...	ルールの変更...	なし	ブロック	承認されて...	1	ste1_d22e4778...	root
2018-05-14 12:08:23		承認されていないソフトウェアの...	ルールの変更...	なし	ブロック	承認されて...	1	ste1_750de939...	root
2018-05-14 12:06:03		承認されていないソフトウェアの...	ルールの変更...	ACHashRules...	ブロック	承認されて...	1	ste1_c28b91c...	root
2018-05-14 12:05:05		承認されていないソフトウェアの...	ルールの変更...	ACHashRules...	ブロック	承認されて...	1	ste1_a0721427...	root
2018-05-14 12:03:40		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	ste2_b1140330...	root
2018-05-14 12:03:25		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	ste1_b1140330...	root
2018-05-14 12:02:55		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	ste1_b1140330...	root
2018-05-14 12:02:31		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	ste2_18dae770...	root

[イベント]→[レポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント]には、コンピュータで実行された承認されていないソフトウェア、またはブロックルールにより実行されないようにした承認されていないソフトウェアがすべて表示されます。このリストは、期間および他の基準によってフィルタできます。

イベント (集約イベント以外) ごとに、[ルールの表示] をクリックすると、ルールの許可とブロックを切り替えることができます。Deep Security Agent 10.2以上には、同じイベントが繰り返し発生した場合にログの量を減らすためのイベント集約ロジックがあります。

アプリケーションコントロールで検出されるソフトウェア変更

すべてのファイルを監視する[変更監視](#)とは異なり、アプリケーションコントロールで初期インストーラの調査時と変更の監視時に確認されるのはソフトウェアファイルのみです。

ソフトウェアには次のものも含まれます。

- Windowsアプリケーション (.exe、.com、.dll、.sys)、Linuxライブラリ (.so)、およびその他のコンパイルされたバイナリやライブラリ
- Javaの.jarファイルと.classファイル、およびその他のコンパイルされたバイトコード
- PHP、Python、シェルスクリプト、およびその他の実行時に変換またはコンパイルされるWebアプリやスクリプト

- Windows PowerShellスクリプト、バッチファイル (.bat)、およびその他のWindows専用スクリプト (.wsf、.vbs、.js)

たとえば、WordPressとそのプラグイン、Apache、IIS、nginx、Adobe Acrobat、app.war、/usr/bin/sshは、いずれもソフトウェアとして検出されます。

アプリケーションコントロールは、ファイルの拡張子を確認してスクリプトかどうかを判定します。またLinuxでは、実行権限のあるファイルはスクリプトとみなされます。

注意: Windowsコンピュータでは、アプリケーションコントロールがローカルファイルシステム上の変更を追跡しますが、ネットワーク上の場所、CD/DVDドライブ、USBデバイスの変更は追跡しません。

アプリケーションコントロールはカーネル (Linuxコンピュータ) およびファイルシステムに統合されているため、ルートまたは管理者アカウントでインストールされたソフトウェアを含め、コンピュータ全体を監視する権限があります。監視対象は、ソフトウェアファイルに対するディスク上の書き込みアクティビティとソフトウェアの実行です。

Deep Security Agent 10と11におけるファイルの比較方法の相違点

Deep Security 10 Agentは、新規のソフトウェアやソフトウェアの変更を判定するために、最初にインストールされていたソフトウェアのSHA-256ハッシュ、ファイルサイズ、パス、およびファイル名を比較します (これらには「ファイルベース」のルールセットが使用されています)。Deep Security 11 (およびそれ以降の) Agentは、ファイルのSHA-256ハッシュおよびファイルサイズのみを比較します (これらには「ハッシュベース」のルールセットが使用されています)。Deep Security 11 (およびそれ以降の) Agentで作成されたルールでは、一意のハッシュおよびファイルサイズのみを比較するので、ソフトウェアファイルの名前変更または移動が実行された場合にも、ルールは引き続き適用されます。そのため、Deep Security 11 (およびそれ以降の) Agentを使用すると、処理の必要なソフトウェア変更の数が削減されます。

Deep Security 10 Agentは、Deep Security 11.0以降にアップグレードしない限り、引き続きファイルベースのルールセットを使用します。Agentをバージョン11.0以降にアップグレードすると、そのルールセットはハッシュベースのルールを使用するように変換されます。同じハッシュ値に対するファイルベースのルールが複数ある場合、それらのルールは1つのハッシュベースのルールに統合されます。統合されるルールが相互に競合する場合 (1つのルールがファイルをブロックし、もう1つがそのファイルを許可する場合)、新しいハッシュベースのルールは「許可」ルールになります。

アプリケーションコントロールの設定

警告: アプリケーションコントロールは、継続的にサーバを監視し、ソフトウェアの変更が生じるたびにイベントをログに記録します。これは、一部のWebサーバやメールサーバなど、自動的に変更されるソフトウェアを使用する環境や通常実行可能ファイルを作成する環境には向いていません。アプリケーションコントロールがお使いの環境に適しているかどうかを確認するには、"[アプリケーションコントロールで検出されるソフトウェア変更](#)" on [page 694](#)を参照してください。

アプリケーションコントロールの仕組みについては、"[アプリケーションコントロールによるソフトウェアのロックダウン](#)" on [page 688](#)を参照してください。

アプリケーションコントロールを有効にしてソフトウェア変更を監視するには、次の操作を実行します。

1. "[アプリケーションコントロールを有効にする](#)" below
2. "[新規および変更済みソフトウェアを監視する](#)" on [page 698](#)
3. "[変更の計画時にメンテナンスモードをオンにする](#)" on [page 701](#)

この記事では、アプリケーションコントロールを使用する際に注意する必要がある、"[アプリケーションコントロールのヒントと注意事項](#)" on [page 702](#)についても説明します。

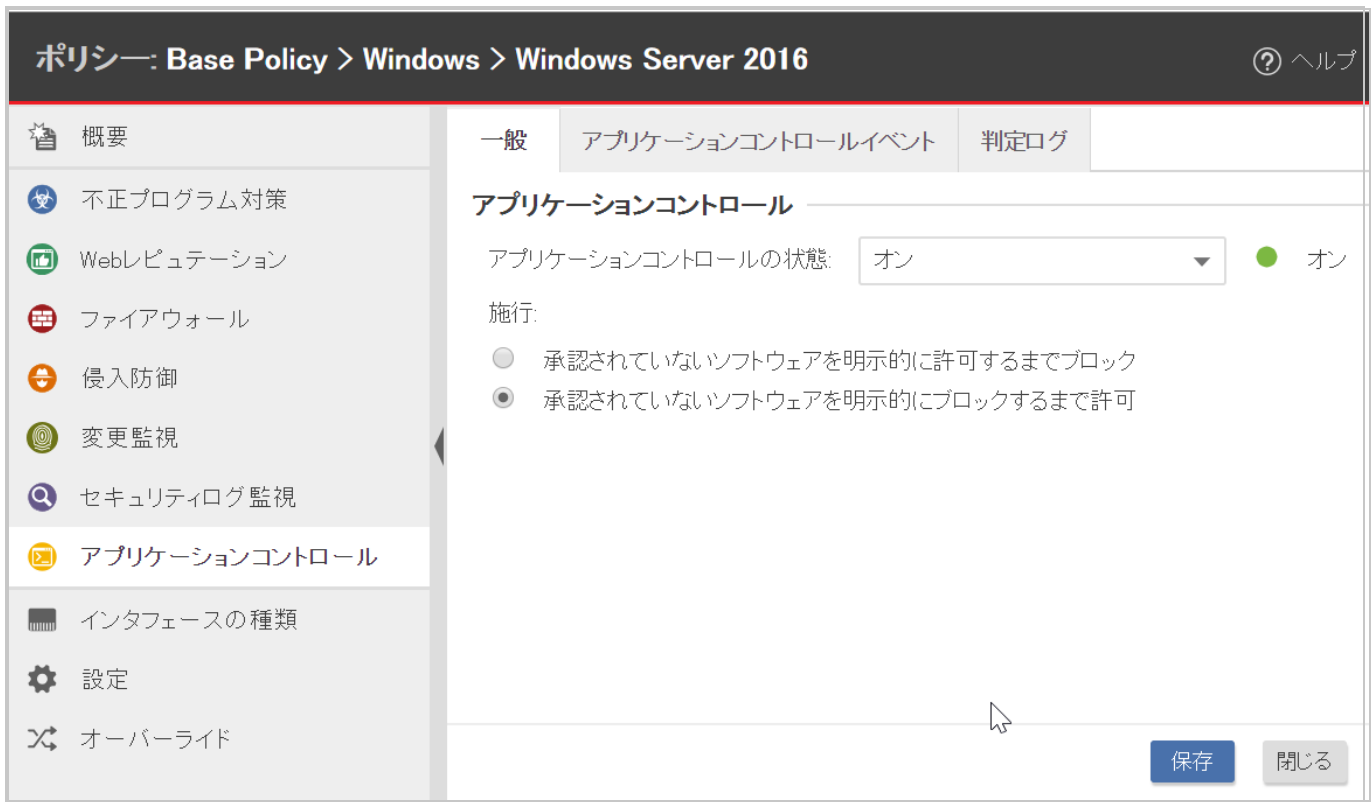
アプリケーションコントロールを有効にした後は、次のことを実行する方法について学ぶこともできます。

- "[アプリケーションコントロールルールセットの表示と変更](#)" on [page 709](#)
- "[大量のソフトウェア変更後にアプリケーションコントロールをリセットする](#)" on [page 713](#)
- "[アプリケーションコントロールイベントの監視](#)" on [page 705](#)
- "[共有ルールセットとグローバルルールセットを作成するためのAPIの使用](#)" on [page 714](#)

アプリケーションコントロールを有効にする

アプリケーションコントロールは、コンピュータの設定またはポリシーで有効にできます。

1. **コンピュータエディタまたはポリシーエディタ¹**を開き、[アプリケーションコントロール]→[一般] に移動します。
2. [アプリケーションコントロールの状態] を [オン] または [継承 (オン)] に設定します。
3. [施行] で、対象の保護状態を選択します。
 - 承認されていないソフトウェアを明示的に許可するまでブロック
 - 承認されていないソフトウェアを明示的にブロックするまで許可 (最初にアプリケーションコントロールを設定するときは、このオプションを選択することをお勧めします)
4. [保存] をクリックします。



次にDeep Security ManagerとAgentを接続すると、Agentにより検索が実行され、コンピュータにインストールされているすべてのソフトウェアのインベントリが生成されて、検出されたすべてのソフトウェアを許可するルールが作成されます。環境に応じて、この初期インベントリには15分以上かかることがあります。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

アプリケーションコントロールが予期したとおりに動作していることを確認するには、"[アプリケーションコントロールの有効化の確認](#)" on page 703の手順に従います。

新規および変更済みソフトウェアを監視する

保護対象コンピュータでインベントリの作成が完了した後は、追加または変更されたソフトウェアの実行可能ファイルは「ソフトウェア変更」として分類され、Deep Security Managerの[処理]画面に表示されます。承認されていないソフトウェアが実行されたり、実行の試みがブロックされたりすると、そのイベントは[イベントとレポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント]に表示されます。詳細については、"[アプリケーションコントロールイベント](#)" on page 1317を参照してください。

最初にアプリケーションコントロールを有効にした後は、[処理]画面に多くのソフトウェア変更が表示されることがあります。これは、通常の操作の過程で、許可されたソフトウェアが新しい実行可能ファイルを作成したり、ファイルの名前を変更したり、ファイルを移動した場合に起こります。ルールを追加してアプリケーションコントロールを調整するにつれて、表示されるソフトウェア変更は少なくなります。

すべてのコンピュータのすべてのソフトウェアの変更をすばやく確認し、許可またはブロックルールを作成するには、[処理] タブを使用します。

ヒント: 許可ルールやブロックルールの作成は、Deep Security APIを使用して自動化できます。詳細については、Deep Security Automation Centerにあるガイド [「Allow or block unrecognized software」](#) を参照してください。

1. Deep Security Managerで、[処理]に進みます。
2. 承認されていないソフトウェアの特定の検出情報だけを表示するには、いくつかの方法で情報をフィルタできます。

ヒント: 各コンピュータの各ソフトウェア変更を個別に評価する代わりに、この後で説明するフィルタを使用して問題のないことが分かっているソフトウェア変更を見つけ、一括で許可します。

The screenshot displays the Trend Micro Deep Security console interface. At the top, the title bar shows 'TREND MICRO Deep Security' and 'MasterAdmin'. The navigation menu includes 'ダッシュボード', '処理', 'アラート', 'イベントとレポート', 'コンピュータ', 'ポリシー', and '管理'. The main content area is titled 'アプリケーションコントロール: ソフトウェア変更' (Application Control: Software Change) with a dropdown menu set to '過去7日間' (Last 7 days). A search bar contains '172.16'. A graph shows '32 ファイル' (32 files) for the selected period. Below the graph, a list of software changes is shown, including 'saved_state, saved_state.tmp' and 'test1.sh, test2.sh'. The right sidebar displays file details for 'saved_state.tmp', including its path, size, and hashes.

表示されるソフトウェア変更の数を減らすには、次の操作を実行します。

- [アプリケーションコントロール: ソフトウェア変更] の横にあるドロップダウンリストから、[過去7日間] などの時間範囲を選択します。画面の上部付近にあるグラフのバーをクリックして、その期間の変更を表示することもできます。
- 左側の画面で、[コンピュータ] をクリックして個別のコンピュータまたはグループを選択するか、[スマートフォルダ] をクリックして特定のスマートフォルダに含まれるコンピュータのみを表示します ("スマートフォルダによるコンピュータの動的なグループ化" on page 1427を参照)。

注意: [コンピュータ] タブと異なり、[ソフトウェア変更] 画面には通常すべてのコンピュータが表示されることはありません。許可またはブロックルールがないソフトウェア変更がアプリケーションコントロールによって検出されたコンピュータのみが表示されます。

- 検索フィルタフィールドに検索語句と演算子を入力します。プロセスによる変更、ユーザによる変更、ホスト名、インストールパス、MD5、SHA1、SHA256などの属性を検索します。たとえば、信頼する特定のユーザが加えたすべての変更を検索し、[すべて許可] をクリックしてそのユーザのすべての変更を許可できます。または、

([メンテナンスモード](#)が有効になっていないときに) 組織全体に特定のソフトウェアアップデートがインストールされた場合は、ファイルのハッシュ値に従って画面をフィルタし、[すべて許可] をクリックして発生したすべての変更を許可します。

ヒント: ソフトウェア変更に関する詳細が右側の画面に表示されます。詳細のファイル名またはコンピュータ名をクリックして、検索フィルタに追加できます。

- [ファイル (ハッシュ) 別にグループ化] または [コンピュータ別にグループ化] を選択します。
3. [許可] または [ブロック] をクリックして、そのコンピュータに、そのソフトウェア用の許可またはブロックルールを追加します。許可するかブロックするかを判断するために詳細な情報が必要な場合は、ソフトウェア名をクリックし、右側の詳細パネルを使用します。

次にAgentがDeep Security Managerに接続すると、Agentが新しいルールを受け取りません。

変更の処理のヒント

- ほとんどの環境では、[承認されていないソフトウェアを明示的にブロックするまで許可] オプションを選択して、アプリケーションコントロールを最初に有効にしたときの初期設定でソフトウェア変更を許可し、[処理] 画面に表示された変更の許可およびブロックルールを追加することをお勧めします。最終的に、ソフトウェア変更の頻度が低下します。この時点で、初期設定でソフトウェア変更をブロックし、問題のないことが分かっているソフトウェアの許可ルールを作成することを検討できます。一部の組織では、引き続き初期設定で変更を許可し、ブロックする必要があるソフトウェアを [処理] 画面で監視することが好まれます。
- 承認されていないソフトウェアを最初に処理する代わりに、セキュリティイベントを評価することから始めることもできます。セキュリティイベントは、実行された (または実行が試みられた) 承認されていないソフトウェアを示します。セキュリティイベントの詳細については、"[アプリケーションコントロールイベントの監視](#)" on page 705を参照してください。
- 承認されていないファイルの実行が許可された場合に、そのまま許可を継続するときは、許可ルールを作成します。ファイルの実行が許可されるだけでなく、ファイルに対するイベントが記録されなくなるため、ノイズが低減され、重要なイベントを見つけやすくなります。
- 既知のファイルの実行がブロックされた場合は、コンピュータからそのファイルを駆除することを検討します (特に頻繁に発生する場合)。

- ソフトウェア変更は、発生したコンピュータごとに表示されることに注意してください。各コンピュータのソフトウェアを許可またはブロックする必要があります。
- ルールはコンピュータに割り当てられ、ポリシーには割り当てられません。たとえば、3台のコンピュータでhelloworld.pyが検出された場合、[すべて許可] または [すべてブロック] をクリックしても反映されるのはこの3台のコンピュータのみです。他のコンピュータは独自のルールセットを使用しているため、他のコンピュータでその後同じファイルが検出されても選択した処理は適用されません。
- 管理できるソフトウェアアップデートに関連する変更が表示された場合は、そのアップデートを実行するときにメンテナンスモード機能を使用します。"[変更の計画時にメンテナンスモードをオンにする](#)" [below](#)を参照してください。

変更の計画時にメンテナンスモードをオンにする

アプリケーションコントロールはパッチのインストール、ソフトウェアのアップグレード、またはWebアプリケーションの配信も検出します。承認されていないソフトウェアの処理方法の設定によっては、[処理] タブで許可ルールを作成するまでこれらのソフトウェアがブロックされることがあります。

インストールやメンテナンスの実行時に不要なダウンタイムやアラートを回避するには、アプリケーションコントロールをメンテナンス期間用のモードに切り替えます。メンテナンスモードが有効な場合、アプリケーションコントロールは引き続きソフトウェアをブロックするルールを適用しますが、新しいソフトウェアやアップデートされたソフトウェアを実行して自動的にコンピュータのインベントリに追加します。

ヒント: メンテナンスモードは、Deep Security APIを使用して自動化できます。詳細については、Deep Security Automation Centerにあるガイド [「Configure maintenance mode during upgrades」](#) を参照してください。

1. Deep Security Managerで、[コンピュータ] に進みます。
2. 1つ以上のコンピュータを選択し、[処理]→[メンテナンスモードをオンにする] をクリックします。
3. メンテナンス期間を選択します。

予定されているメンテナンス期間が終了した時点で、メンテナンスモードは自動的に無効になります。または、アップデートの完了時に手動でメンテナンスモードを無効にする場合は、[無期限] を選択します。

[ダッシュボード]の[アプリケーションコントロール - メンテナンスモードのステータス]ウィジェットに、コマンドが成功したかどうかが表示されます。

4. ソフトウェアをインストールまたはアップグレードします。
5. メンテナンスモードを手動で無効にするよう選択した場合、ソフトウェアの変更の検出を再び開始するにはメンテナンスモードを忘れずに無効にしてください。

アプリケーションコントロールのヒントと注意事項

- アプリケーションコントロールのパフォーマンスを高めるには、Windows Defenderの代わりにDeep Security不正プログラム対策を使用します。詳細については、"[Windows Server 2016へのDeep Security不正プログラム対策のインストール後のWindows Defenderの無効化](#)" on page 753を参照してください。
- バッチファイルまたはPowerShellスクリプトに対するブロックルールを作成する場合は、関連するインタープリタ (PowerShellスクリプトの場合はpowershell.exe、バッチファイルの場合はcmd.exe) の使用時に、このファイルをコピー、移動、または名前変更することはできません。
- 許可またはブロックルールを追加した場合、通常は次にAgentがDeep Security Managerに接続したときに、Agentにルールが送信されます。ルールセットのアップロードに失敗したことを示すエラーが表示された場合は、AgentとManagerまたはRelay間のネットワークデバイスによって、[ハートビートポート番号](#)または[Relayポート番号](#)の通信が許可されていることを確認します。
- ブロックルールが機能していることを確認するために、ブロックしたソフトウェアを実行してみます (Deep Security Agentによる変更の検出方法の詳細については、"[アプリケーションコントロールで検出されるソフトウェア変更](#)" on page 694を参照してください)。
- ブロックしたソフトウェアがインストールされたままの場合、アプリケーションコントロールは引き続きソフトウェアの実行をブロックするとアラートを表示し、ログに記録します。コンピュータの権限に関するエラーログを少なくし、攻撃対象領域を縮小するには、アプリケーションコントロールがブロックしているソフトウェアをアンインストールします。その後、関連するアラートを消去するには、[アラート]または[ダッシュボード]へ進み、そのアラートをクリックし、[アラートの消去]をクリックします。ただし、すべてのアラートを消去できるわけではありません。詳細については、"[事前定義アラート](#)" on page 1249を参照してください。
- コンピュータでのソフトウェアの変更が多すぎる場合、アプリケーションコントロールは引き続き既存のルールを適用しますが、パフォーマンス上の理由からそれ以上ソフトウェアの変更は検出されず、表示もされなくなります。この問題を解決するには、"[大量のソ](#)

[ソフトウェア変更後にアプリケーションコントロールをリセットする](#) on page 713を参照してください。

アプリケーションコントロールの有効化の確認

アプリケーションコントロールの概要については、"[アプリケーションコントロールによるソフトウェアのロックダウン](#)" on page 688を参照してください。初期設定の手順については、"[アプリケーションコントロールの設定](#)" on page 696を参照してください。

アプリケーションコントロールが有効化され、最初のソフトウェアインベントリ検索が完了すると、次の状態になります。

- [ステータス] が「オン」または「オン、承認されていないソフトウェアをブロック」になります。
- [コンピュータ] の [ステータス] が「アプリケーションコントロールルールセットの構築中」から「管理対象 (オンライン)」に変わります。
- [イベントとレポート]→[イベント]→[システムイベント] に、「アプリケーションコントロールルールセットの作成開始」および「アプリケーションコントロールルールセットの作成完了」が記録されます (ログが何も表示されない場合は、"[ログに記録するアプリ](#)

「[セッションコントロールイベントを選択する](#)」 on page 706を参照してください。

The screenshot shows the configuration page for a computer with ID `ec2-54-202-92-24.us-west-2.compute.amazonaws.com`. The left sidebar contains navigation options like '概要', '不正プログラム対策', 'Webレピュテーション', 'ファイアウォール', '侵入防御', '変更監視', 'セキュリティログ監視', and 'アプリケーションコントロール'. The main area has tabs for '一般', '処理', and 'システムイベント'. Under the '処理' tab, various security features are listed with their status:

機能	ステータス
不正プログラム対策	管理対象 (オンライン)
Webレピュテーション	オフ、インストールされていません、設定なし
ファイアウォール	オフ、インストールされていません
侵入防御	オフ、インストールされていません、ルールなし
変更監視	オフ、インストールされていません、ルールなし
セキュリティログ監視	オフ、インストールされていません、ルールなし
アプリケーションコントロール	オン

Below this table, there are buttons for 'ステータスの確認' and '警告/エラーのクリア'. At the bottom, the 'AWSアカウントのプロパティ' section shows account details like ID, instance ID, and region.

アプリケーションコントロールが機能していることを確認するには、次の手順に従います。

1. コンピュータに実行可能ファイルをコピーするか、プレーンテキストファイルに実行権限を追加して、そのファイルを実行してみます。

承認されていないソフトウェアに対する設定に応じて、ファイルがブロックまたは許可されます。アプリケーションコントロールで初期許可ルールの構築または共有ルールセットのダウンロードが完了している場合、変更が検出されると [処理] タブに表示され、この

タブで許可およびブロックルールを作成できます ("新規および変更済みソフトウェアを監視する" on page 698を参照)。また、アラートを設定していれば、承認されていないソフトウェアが検出されたときやアプリケーションコントロールによってソフトウェアの起動がブロックされたときにアラートも表示されます ("アプリケーションコントロールイベントの監視" below) を参照)。ソフトウェアの変更が存在しなくなるまで、または最も古いデータがデータベースから削除されるまで、イベントは保持されます。

2. テスト用ソフトウェアの許可またはブロックルールを追加して、もう一度実行してみます。今回は、許可またはブロックルールが適用されます。

ヒント: [承認されていないソフトウェアを明示的に許可するまでブロック] を選択したために、承認されていないソフトウェアが誤ってブロックされた場合は、アプリケーションコントロールイベントログの [理由] 列で原因のトラブルシューティングに役立つ情報を確認できます。

アプリケーションコントロールイベントの監視

アプリケーションコントロールの概要については、"[アプリケーションコントロールによるソフトウェアのロックダウン](#)" on page 688を参照してください。初期設定の手順については、"[アプリケーションコントロールの設定](#)" on page 696を参照してください。

初期設定では、アプリケーションコントロールを有効にすると、ソフトウェアの変更が発生したときやアプリケーションコントロールによってソフトウェアの実行がブロックされたときに、この機能によってイベントがログに記録されます。アプリケーションコントロールイベントは、[処理] 画面と [イベントとレポート] 画面に表示されます。設定されている場合は、[アラート] 画面にアラートが表示されます。

どのアプリケーションコントロールイベントログを記録し、どのアプリケーションコントロールイベントログを[外部SIEMシステムまたはSyslogサーバに転送する](#)かを設定できます。

コンピュータ上でのソフトウェア変更を監視するには、次の手順に従います。

1. "[ログに記録するアプリケーションコントロールイベントを選択する](#)" on the next page
2. "[アプリケーションコントロールイベントログを表示する](#)" on the next page
3. "[集約されたセキュリティイベントを解釈する](#)" on page 707
4. "[アプリケーションコントロールアラートを監視する](#)" on page 708

ログに記録するアプリケーションコントロールイベントを選択する

1. [管理]→[システム設定]→[システムイベント]に進みます。
2. イベント ID 7000 「アプリケーションコントロールセキュリティイベントのエクスポート」などのアプリケーションコントロールイベントにスクロールします。
3. そのタイプのイベントのイベントログを記録するには、[記録する]を選択します。

該当するイベントが発生すると、[イベントとレポート]→[イベント]→[システムイベント]にイベントが表示されます。ログは最大保持期間に達するまで記録されます。詳細については、"[Deep Securityのイベント](#)" on page 1116を参照してください。

注意: ここで設定するイベントは、[コンピュータ]→[詳細]→[アプリケーションコントロール]→[イベント]に表示されるイベントではありません。ここに表示されるイベントは常に記録されます。

4. イベントログをSIEMまたはSyslogサーバに転送するには、[転送する]を選択します。
5. 外部SIEMを使用する場合は、必要に応じて、対象となるアプリケーションコントロールイベントログのリストをロードし、実行する処理を指定します。アプリケーションコントロールイベントのリストについては、"[システムイベント](#)" on page 1271と"[アプリケーションコントロールイベント](#)" on page 1317を確認してください。

アプリケーションコントロールイベントログを表示する

アプリケーションコントロールは、システムイベントとセキュリティイベントを生成します。

- システムイベント: 設定変更やソフトウェアアップデートの履歴を提供する監査イベント。システムイベントを確認するには、[イベントとレポート]→[イベント]→[システムイベント]をクリックします。システムイベントの一覧については、"[システムイベント](#)" on page 1271を参照してください。
- セキュリティイベント: アプリケーションコントロールで承認されていないソフトウェアがブロックまたは許可される時や、ブロックルールによってソフトウェアがブロックされる時に、Agentで発生するイベント。セキュリティイベントを確認するには、[イベントとレポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント]の順にクリックします。一覧については、"[アプリケーションコントロールイベント](#)" on page 1317を参照してください。

集約されたセキュリティイベントを解釈する

Agentのハートビートに同一のセキュリティイベントの複数のインスタンスが含まれている場合、Deep Securityではセキュリティイベントログのイベントを集約します。イベントの集約によって、ログ内の項目数が減少するため、重要なイベントを見つけやすくなります。

- 一般的なケースとして、同一ファイルにイベントが発生した場合、ログにはファイル名と集約されたイベントが表示されます。たとえば、ハートビートにTest_6_file.shファイルに発生した「承認されていないソフトウェアの実行を許可」イベントの3つのインスタンスが含まれ、このイベントの他のインスタンスが含まれていない場合、Deep SecurityではTest_6_file.shファイルに対するこれらの3つのイベントが集約されます。
- イベントが多くのファイルに対して発生した場合、ログではルールのリンク、パス、ファイル名、およびユーザ名が省略されます。たとえば、ハートビートに複数の異なるファイルに発生した「承認されていないソフトウェアの実行を許可」イベントの21個のインスタンスが含まれている場合、Deep Securityではこの21個のイベントが単一のイベントに集約されますが、ルールのリンク、パス、ファイル名、およびユーザ名は含まれません。

集約されたイベントが複数のファイルに当てはまる場合、これらのイベントの他の発生情報は他のハートビートで報告されている可能性があります。ファイル名がわかっている他のイベントに対処すると、集約されたイベントは発生しなくなる可能性があります。

ログでは、集約されたイベントには特別なアイコンが使用され、[繰り返しカウント]列に集約されたイベント数が表示されます。

時刻	コンピュータ	イベント	ルール	ルールセット	処理	理由	繰り返しカウント	タグ	パス	ファイル	ユーザ名
2018-05-01 10:50:20		ソフトウェアの実行をルールでブ...	ルールの変更	ec2-54-202-9...	ブロック	ブロックルール	1		/dsaf-DSAF_...	libnumbers.so	root
2018-05-01 10:50:20		承認されていないソフトウェアの...	ルールの変更	なし	許可	なし	1		/dsaf-DSAF_...	main	root
2018-05-01 10:49:10		承認されていないソフトウェアの...	ルールの変更	なし	許可	なし	1		/dsaf-DSAF_...	libnumbers.so	root
2018-05-01 10:49:10		承認されていないソフトウェアの...	ルールの変更	なし	許可	なし	1		/dsaf-DSAF_...	main	root
2018-05-01 10:33:06		承認されていないソフトウェアの...	ルールの変更	ACHashRules...	ブロック	承認されてい...	1		/dsaf-DSAF_...	stg1_e88263ba...	root
2018-05-01 10:32:08		承認されていないソフトウェアの...	ルールの変更	ACHashRules...	ブロック	承認されてい...	3		/dsaf-DSAF_...	stg1_2541883...	root
2018-05-01 10:30:30		ソフトウェアの実行をルールでブ...	ルールの変更	ACHashRules...	ブロック	ブロックルール	1		/dsaf-DSAF_...	stg2_59bd28d8...	root
2018-05-01 10:30:16		ソフトウェアの実行をルールでブ...	ルールの変更	ACHashRules...	ブロック	ブロックルール	1		/dsaf-DSAF_...	stg1_59bd28d8...	root
2018-05-01 10:29:45		承認されていないソフトウェアの...	ルールの変更	ACHashRules...	許可	なし	1		/dsaf-DSAF_...	stg1_59bd28d8...	root
2018-05-01 10:21:51		ソフトウェアの実行をルールでブ...	ルールの変更	ACHashRules...	ブロック	ブロックルール	1		/dsaf-DSAF_...	stg1_c23b918b...	root
2018-05-01 10:21:20		承認されていないソフトウェアの...	ルールの変更	ACHashRules...	許可	なし	1		/dsaf-DSAF_...	stg1_c23b918b...	root
2018-05-01 10:20:03		ソフトウェアの実行をルールでブ...	ルールの変更	ec2-54-202-9...	ブロック	ブロックルール	1		/dsaf-DSAF_...	stg2_0e3c718...	root
2018-05-01 10:19:49		ソフトウェアの実行をルールでブ...	ルールの変更	ec2-54-202-9...	ブロック	ブロックルール	1		/dsaf-DSAF_...	stg1_0e3c718...	root
2018-05-01 10:19:18		承認されていないソフトウェアの...	ルールの変更	なし	許可	なし	1		/dsaf-DSAF_...	stg1_0e3c718...	root
2018-05-01 10:18:56		ソフトウェアの実行をルールでブ...	ルールの変更	ec2-54-202-9...	ブロック	ブロックルール	21		/dsaf-DSAF_...	stg2_7440182f...	root

アプリケーションコントロールアラートを監視する

どのアプリケーションコントロールイベントまたは重要度でアラートを生成するかを設定するには、[アラート] タブに進み、[アラートの設定] ボタンをクリックし、次にイベントを選択して [プロパティ] をダブルクリックします。詳細については、"[アラートの設定](#)" on page 1091 を参照してください。

アプリケーションコントロールイベントに対してアラートが有効になっていると、アプリケーションコントロールエンジンによって検出されたソフトウェアの変更と実行がブロックされたソフトウェアがすべて [アラート] タブに表示されます。[アラートステータス] ウィジェットを有効にした場合には、ダッシュボードにもアプリケーションコントロールアラートが表示されます。

The screenshot shows the Trend Micro Deep Security dashboard. The top navigation bar includes 'MasterAdmin', 'ヘルプ', 'サポート情報', and a search box. Below the navigation bar, there are tabs for 'ダッシュボード', '処理', 'アラート', 'イベントとレポート', 'コンピュータ', 'ポリシー', and '管理'. The main content area features a 'Default' tab and several filters: 'すべて', '24時間表示', 'すべてのコンピュータ', 'フィルタの適用', and 'ウィジェットの追加/削除...'. The 'アラートステータス' widget shows 1 Critical and 4 Warning alerts. The '最新のアラート' table lists the following alerts:

アラート	期間
ソフトウェアの実行をブロック-172...	0分
ソフトウェア変更を検出-172.16.8.61	3分
新しいパターンファイルアップデー...	19時間
保護モジュールライセンスが期限...	2日
メモリの重大しきい値の超過	2日

The 'コンピュータのステータス' widget displays a pie chart and a legend for computer status:

ステータス	数
重大	0
警告	0
管理対象	52
非管理対象	6

The 'ユーザ情報の概要' widget shows details for 'MasterAdmin':

- 役割: Full Access
- 最終ログオン: 2017-03-06 11:49
- 前回のログオン: 2017-03-03 17:15

どのコンピュータでメンテナンスモードが有効になっているかを監視するには、[ウィジェットの追加/削除] をクリックし、[アプリケーションコントロールメンテナンスモード] ウィジェットを有効にします。このウィジェットには、コンピュータのリストと各コンピュータで予定されているメンテナンス期間が表示されます。

アプリケーションコントロールルールセットの表示と変更

各コンピュータには独自のアプリケーションコントロールルールセットがあります。次の手順を実行します。

- ["アプリケーションコントロールルールセットを表示する"](#) [below](#)し、どのルールが含まれているかを確認します。

ヒント:最初にコンピュータのアプリケーションコントロールを有効にすると、コンピュータにインストールされているソフトウェアがコンピュータのインベントリに追加され、実行が許可されます。ただし、Deep Securityの従来のREST APIを使用しないかぎり、Deep Security Managerのインベントリに関連付けられたルールは表示されません (["共有ルールセットとグローバルルールセットを作成するためのAPIの使用"](#) [on page 714](#)を参照)。Deep Security Managerでは、コンピュータの許可ルールまたはブロックルールを作成するまで、コンピュータのルールセットは空です。

- ソフトウェアファイルが許可またはブロックされなくなった場合に、["アプリケーションコントロールルールの処理を変更する"](#) [on page 711](#)ことができます。
- ソフトウェアが削除され、元に戻る可能性が低い場合は、["個々のアプリケーションコントロールルールを削除する"](#) [on page 712](#)ことができます。
- ルールセットに関連付けられたコンピュータが削除されている場合は、["アプリケーションコントロールルールセットを削除する"](#) [on page 713](#)ことができます。

ヒント:特定のコンピュータで実行する必要のあるソフトウェアがアプリケーションコントロールによってブロックされていることがユーザから報告された場合は、そのコンピュータに対するブロックルールを取り消すことができます。[イベントとレポート]→[アプリケーションコントロールイベント]→[セキュリティイベント]の順に選択して、コンピュータを探して、ブロックイベントを見つけ、[ルールの表示]をクリックします。表示されたポップアップで、ブロックルールを許可ルールに変更できます。

アプリケーションコントロールルールセットを表示する

アプリケーションコントロールルールセットのリストを表示するには、[ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット]に移動します。

The screenshot shows the 'アプリケーションコントロールルールセット' (Application Control Rule Set) configuration page in the Trend Micro Deep Security console. The left sidebar shows the navigation menu with 'ポリシー' (Policy) selected, and 'アプリケーションコントロールルールセット' (Application Control Rule Set) highlighted under the 'ルール' (Rules) section. The main content area displays a table of rules.

名前	作成	前回のアップデート
ローカル (1)		
	2018-05-01 10:49	2018-05-01 10:49
共有 (17)		
ACHashRulesetTests_SHARED_...	2018-05-01 09:37	2018-05-01 09:37
ACHashRulesetTests_SHARED_...	2018-05-01 09:39	2018-05-01 09:39
ACHashRulesetTests_SHARED_...	2018-05-01 10:21	2018-05-01 10:29
ACHashRulesetTests_SHARED_...	2018-05-01 10:31	2018-05-01 10:33
ActionableEventsSecurityEvents...	2018-05-01 10:12	2018-05-01 10:13
ActionableEventsSecurityEvents...	2018-05-01 10:14	2018-05-01 10:14
ActionableEventsSecurityEvents...	2018-05-01 10:16	2018-05-01 10:16
ActionableEventsSecurityEvents...	2018-05-01 10:13	2018-05-01 10:14
ActionableEventsSecurityEvents...	2018-05-01 10:15	2018-05-01 10:16
BlockExtensionTestsPolicy_47d6...	2018-05-01 09:47	2018-05-01 09:47
PolicyWithLockdownTests_fd0c89...	2018-05-01 09:52	2018-05-01 09:52
PolicyWithoutLockdownTests_fd...	2018-05-01 09:51	2018-05-01 09:51
ReviewApplicationDriftTest-Poli...	2018-05-01 09:57	2018-05-01 09:58

At the bottom right of the console, there are notification buttons for 'アラート' (Alerts) with a count of 5 and '0'.

ルールセットに含まれるルールを確認するには、ルールセットをダブルクリックして [ルール] タブに移動します。[ルール] タブにはルールが関連付けられているソフトウェアファイルが表示され、許可ルールをブロックルールに変更したり、その逆に変更したりすることもできます ("アプリケーションコントロールルールの処理を変更する" on the next page を参照)。

セキュリティイベント

時刻	コンピュータ	イベント	ルール	ルールセット	処理	理由	繰り返し回数	ファイル	ユーザ名
2018-05-14 12:18:17		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	libnumbers.so	root
2018-05-14 12:18:17		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	man	root
2018-05-14 12:12:07		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	libnumbers.so	root
2018-05-14 12:12:07		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	man	root
2018-05-14 12:09:22		承認されていないソフトウェアの...	ルールの変更...	なし	ブロック	承認されてい...	1	ste1_d22e4778...	root
2018-05-14 12:08:29		承認されていないソフトウェアの...	ルールの変更...	なし	ブロック	承認されてい...	1	ste1_750de339...	root
2018-05-14 12:06:03		承認されていないソフトウェアの...	ルールの変更...	ACHashRules...	ブロック	承認されてい...	1	ste1_c28b691c...	root
2018-05-14 12:05:05		承認されていないソフトウェアの...	ルールの変更...	ACHashRules...	ブロック	承認されてい...	1	ste1_a0721427...	root
2018-05-14 12:03:40		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	ste2_b1140330...	root
2018-05-14 12:03:25		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	ste1_b1140330...	root
2018-05-14 12:02:55		承認されていないソフトウェアの...	ルールの変更...	なし	許可	なし	1	ste1_b1140330...	root
2018-05-14 12:02:31		ソフトウェアの実行をルールでブ...	ルールの変更...	ec2-35-162-1...	ブロック	ブロックルール	1	ste2_18dae70...	root

[イベントとレポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント]には、コンピュータ上で実行されているか、アクティブに実行がブロックされているすべての承認されていないソフトウェアが表示されます。このリストは、期間および他の基準によってフィルタできます。詳細については、"[アプリケーションコントロールイベント](#)" on [page 1317](#)を参照してください。

イベント (集約イベント以外) ごとに、[ルールの表示] をクリックすると、ルールの許可とブロックを切り替えることができます。

Deep Security Agent 10.2以上には、同じイベントが繰り返し発生した場合にログの量を減らすためのイベント集約ロジックがあります。 ("[集約されたセキュリティイベントを解釈する](#)" on [page 707](#)を参照してください)。

アプリケーションコントロールルールの処理を変更する

以前にブロックしたソフトウェアを許可 (または以前に許可したソフトウェアをブロック) する場合は、該当するルールの処理を編集します。ソフトウェアがアプリケーションコントロールで認識されないようにルールを取り消す必要がある場合 (処理を変更するだけでなく、ルール自体を削除する場合) は、"[個々のアプリケーションコントロールルールを削除する](#)" on the [next page](#)を参照してください。

1. [ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット]の順に選択します。
2. 変更するルールを含むルールセットをダブルクリックして選択します。
3. 表示されたポップアップ画面で、[ルール] タブを選択します。
4. ブロック (または許可) されたソフトウェアに絞り込む場合は、[アプリケーションコントロールルール]の横にあるメニューで、[処理別] または [パス別] を選択して類似するルールをグループ化します。また、検索を使用してリストをフィルタすることもできます。

処理を変更するソフトウェアファイルについて、ファイル名やパスが異なる複数のルールがある場合は、[ファイル名別] または [パス別] を選択して関連するルールをグループ化します。

ACTION	HASH	FILE SIZE (B...	LAST CHANGE BY	LAST CHANGED
Allow	CDEFF41012D3C71FD3DD903B6D4BA0FFA24649115A2EB06E3FC9DDB83EFF7C88	93,258	MasterAdmin	February 1, 2019 07:40
Allow	49381F8DE40E2D2287807FB38D612CCF44D8215BBE9A99C39660D3E5C17A4DAB	92,971	MasterAdmin	February 1, 2019 07:40
Allow	620C6B9FC167162057F7C208D88BFD2F4D9B0ACE9FE926F29BFD3281A761B3311	344,742,846	MasterAdmin	February 7, 2019 05:43

5. 許可またはブロックするソフトウェアに対応する行を探します。
6. [処理] 列で、許可するかブロックするかを設定を変更し、[OK] をクリックします。

AgentからDeep Security Managerへの次回接続時に、ルールがアップデートされ、バージョン番号が上がります。

個々のアプリケーションコントロールルールを削除する

作成したルールを取り消す場合は、[ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット]の順に移動し、そのルールを含むルールセットをダブルクリックして、[ルール] タブに移動し、ルールを選択して [削除] をクリックします。

次のことに注意してください。

- ルールが不要になった場合は、それらを削除することでルールセットのサイズを削減することができます。これにより、RAMとCPUの使用量が削減され、パフォーマンスが向上します。
- ルールを削除すると、そのソフトウェアはアプリケーションコントロールで認識されなくなります。ソフトウェアが再度インストールされると、[処理] タブに再び表示されます。
- ソフトウェアアップデートが不安定な場合やダウングレードが必要になる可能性がある場合は、テストが完了するまで前のソフトウェアバージョンへのロールバックを許可するルールを残しておきます。
- 古いルールを確認するには、[ポリシー]→[ルール]→[アプリケーションコントロールルールセット]の順に選択し、[列] をクリックします。[前回の变更日期] を選択して [OK] をクリックし、その列のヘッダをクリックすると、日付順にソートできます。

アプリケーションコントロールルールセットを削除する

ルールセットに関連付けられたコンピュータがもう存在しない場合など、アプリケーションコントロールルールセットがもう使用されていない場合は、削除できます。

ルールセットを削除するには、[ポリシー]→[ルール]→[アプリケーションコントロールルールセット]の順に選択し、ルールセットをクリックして選択してから [削除] をクリックします。

大量のソフトウェア変更後にアプリケーションコントロールをリセットする

アプリケーションコントロールの概要については、"[アプリケーションコントロールによるソフトウェアのロックダウン](#)" on page 688を参照してください。

アプリケーションコントロールは、ソフトウェアが頻繁に変更されるワークステーションまたはサーバではなく、頻繁にはアップデートされない安定したサーバで使用することを想定しています。

変更が多すぎると、古いルールを削除しないかぎり、大量のルールセットが生成されて多くのRAMが消費されます。承認されたソフトウェアのアップデート時にメンテナンスモードを使用しない場合は、変更が多すぎると、管理者が変更ごとに許可ルールを手動で作成しなければならないため、作業負荷の増加にもつながります。

承認されていないソフトウェアの変更数が上限を超えると、アプリケーションコントロールはコンピュータのすべてのソフトウェア変更の検出と表示を停止します。この停止は、ルール

セットが大きくなりすぎた場合に発生する可能性のあるメモリ不足やディスク容量のエラーを防ぐことを目的としています。

停止した場合は、アラート(「未解決のソフトウェア変更数の上限」)とイベントログ(「未解決のソフトウェア変更数の上限に達しました」)によりDeep Security Managerから通知されます。ソフトウェアの変更の検出を継続するには、問題を解決する必要があります。

1. コンピュータのプロセスとセキュリティイベントを調べ、コンピュータが攻撃を受けていないことを確認します。攻撃を受けていないかがわからない場合や十分な時間が無い場合、最も安全かつ迅速な方法は、バックアップまたは仮想マシンスナップショットからシステムを復元することです。

警告: 承認されていないソフトウェア(ゼロデイの不正プログラムを含む)があってそれを削除しなかった場合、アプリケーションコントロールのリセット後そのソフトウェアを無視され、[処理] タブに表示されなくなります。そのソフトウェアのプロセスがすでに実行されてRAMに存在する場合、コンピュータを再起動しないかぎり、このソフトウェアに関するイベントはログに記録されず、アラートも生成されません。

2. コンピュータで自動アップデート(ブラウザ、Adobe Reader、またはyumによる自動アップデートなど)を含むソフトウェアアップデートを実行していた場合は、アップデートを無効にするか、アプリケーションコントロールのメンテナンスモードを有効にした場合にのみアップデートが実行されるようにスケジュールを設定してください("変更の計画時にメンテナンスモードをオンにする" on page 701を参照)。
3. アプリケーションコントロールをリセットします。リセットするために、**コンピュータエディタ**¹でアプリケーションコントロールを無効にします。Agentでアプリケーションコントロールの無効化が確認され、エラーステータスがクリアされたら、アプリケーションコントロールを再び有効にします。エージェントは、新しいソフトウェアインベントリリストを生成します。

共有ルールセットとグローバルルールセットを作成するためのAPIの使用

アプリケーションコントロールの概要については、"[アプリケーションコントロールによるソフトウェアのロックダウン](#)" on page 688を参照してください。初期設定の手順については、"[アプリケーションコントロールの設定](#)" on page 696を参照してください。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

[自動化センター](#)でDeep Security Manager APIを使用すると、共有ルールセットとグローバルルールを作成できます。1種類のルールセットを使用することも、組み合わせて使用することもできます。詳細については、[共有ルールセットの作成](#) および [グローバルルールの追加](#)を参照してください。

- ローカルルールセット:コンピュータのソフトウェアインベントリの一部として、またはメンテナンスモードで追加されたルールは、保護対象コンピュータにのみ保存され、Deep Security Managerでは表示されません。Deep Security Managerで設定するルールの許可またはブロックは、Agentに送信され、両方の場所に保存されます。Agentはインベントリ情報をManagerに転送しないため、ローカルルールセットは共有ルールセットよりも優れたパフォーマンスを発揮します。

Deep Security 10 Agentは、新規のソフトウェアやソフトウェアの変更を判定するために、最初にインストールされていたソフトウェアのSHA-256ハッシュ、ファイルサイズ、パス、およびファイル名を比較します(これらには「ファイルベース」のローカルルールセットが使用されています)。Deep Security 11 (またはそれ以降の) Agentは、ファイルのSHA-256ハッシュおよびファイルサイズのみを比較します(これらには「ハッシュベース」のローカルルールセットが使用されています)。Deep Security 11 (またはそれ以降の) Agentで作成されたルールでは、一意のハッシュおよびファイルサイズのみを比較するので、ソフトウェアファイルの名前変更または移動が実行された場合にも、ルールは引き続き適用されます。そのため、Deep Security 11 (またはそれ以降の) Agentを使用すると、処理の必要なソフトウェア変更の数が削減されます。Deep Security 10 Agentは、Deep Security 11以降にアップグレードしない限り、引き続きファイルベースのローカルルールセットを使用します。Agentをバージョン11以降にアップグレードすると、そのローカルルールセットはハッシュベースのルールを使用するように変換されます。

注意: 同じハッシュ値に対するファイルベースのルールが複数ある場合、それらのルールは1つのハッシュベースのルールに統合されます。統合されるルールが相互に競合する場合(1つのルールがファイルをブロックし、もう1つがそのファイルを許可する場合)、新しいハッシュベースのルールは「許可」ルールになります。

- 共有ルールセット:すべてのルールデータをAgentとManagerの両方に同期します(有効な場合はRelayも対象)。これにより、ネットワークとディスクの使用量が増加します。ただし、初期インベントリ検索またはメンテナンスモードのルールを確認する必要がある場合や、設定が同一でなければならない多数のコンピュータで構成されるサーバファームを管理する場合は、共有ルールセットを使用する方が業務を簡素化できることがあります。共有ルールセットは、同じ構成のLAMP Webサーバで構成されるサーバプールや、複数仮想マシンでオートスケーリンググループを構成している場合などに便利です。管理作業の負荷も軽減できます。

警告: [承認されていないソフトウェアを明示的に許可するまでブロック] が有効で、コンピュータが単に類似しているが同一ではない場合は、共有ルールセットを使用しないでください。最初のコンピュータのルールセットに含まれていない他のコンピュータのすべてのソフトウェアがブロックされてしまいます。重要なファイルが含まれている場合、OSが破損する可能性があります。OSが破損すると、再インストール、バックアップの復元、またはOSの復旧モードの使用が必要になる可能性があります。

Deep Security 11.1以降を使用して新しい共有ルールセットを作成すると、ハッシュベースのルール（ファイルのハッシュとサイズのみを比較するルール）のみを含めることができます。Deep Security 11.0以前を使用して共有ルールセットを作成した場合は、ファイルベースのルール（ファイルの名前、パス、サイズ、およびハッシュを比較するルール）が含まれます。共有ルールセットを使用するすべてのAgentがDeep Security Agent 11.0以降にアップグレードされるまで、古い共有ルールセットでは引き続きファイルベースのルールが使用されます。すべてのAgentがバージョン11.0以降にアップグレードされると、ハッシュベースのルールを使用するように共有ルールセットが変換されます。

警告: ルールセットを使用するすべてのAgentがバージョン11.0以降である場合を除き、新しい共有ルールセットを作成しないでください。新しい共有ルールセットはハッシュベースのルールセットであり、10.3以前のAgentとの互換性はありません。10.3以前のAgentでサポートされているのは、ファイルベースのルールセットのみです。

注意: 同じハッシュ値に対するファイルベースのルールが複数ある場合、それらのルールは1つのハッシュベースのルールに統合されます。統合されるルールが相互に競合する場合（1つのルールがファイルをブロックし、もう1つがそのファイルを許可する場合）、新しいハッシュベースのルールは「許可」ルールになります。

共有ルールを作成するには、オートメーションセンターで [共有ルールセット](#) を作成を参照してください。

- **グローバルルール:** 共有ルールセットと同様に、グローバルルールはマネージャによってエージェントに配信されます（リレーが有効な場合は）。これにより、ネットワークとディスクの使用量が増加します。ただし、これらのルールセットはグローバルであるため、各ポリシーでの選択の手間を省くことができます。グローバルルールは、Deep Security Managerに表示されるルールセットの一部ではありません。グローバルルールにはブロックルールのみを含めることができ、ルールは許可しません。

グローバルルールには、Deep Security エージェント10.2以降が必要です。Managerはそれより古いAgentにはグローバルルールセットを送信しません。グローバルルールセットは、他のすべてのアプリケーションコントロールルールよりも優先されます。また、アプリケーションコントロールが有効になっているすべてのコンピュータに適用されます。グローバルルールのルールは、ファイルのSHA-256ハッシュに基づいています。ソフトウェアファイルのハッシュは一意的のため、ファイルパス、ポリシー、コンピュータグループに関係なく、またアプリケーションコントロールによって以前にソフトウェアが検出されているかどうかに関係なく、特定のソフトウェアをあらゆる場所でブロックできます。

注意: マルチテナント展開では、各テナントにグローバルルールが個別に割り当てられます。すべてのテナントに対してソフトウェアをブロックするには、各テナントに同一のグローバルルールを作成します。

共有ルールを作成するには、オートメーションセンターで [グローバルルール](#) を追加を参照してください。

このトピックの内容:

- ["共有ルールセットを作成する" below](#)
- ["共有許可およびブロックルールからコンピュータ固有の許可およびブロックルールに切り替える" on the next page](#)
- ["Relayを介してアプリケーションコントロール共有ルールセットをインストールする" on page 719](#)
- ["Relayと共有ルールセットを使用する際の注意事項" on page 721](#)

共有ルールセットを作成する

APIを使用して、共有の許可ルールまたはブロックルールを作成し、ルールセットを他のコンピュータに適用できます。これは、同一のコンピュータが複数ある場合 (Webサーバファームで負荷を分散している場合など) に便利です。共有ルールセットはインベントリが完全に一致するコンピュータにのみ適用する必要があります。

1. APIを使用して、コンピュータの共有の許可ルールとブロックルールを作成します。詳細については、[共有ルールセット](#)の作成を参照してください。共有ルールセットを配信する前に内容を確認する場合は、["アプリケーションコントロールルールセットの表示と変更" on page 709](#)を参照してください。

2. **コンピュータエディタまたはポリシーエディタ**¹で、[アプリケーションコントロール]に進みます。
3. [ルールセット] で、[設定を継承] が選択されていないことを確認してから、[共有ルールセットを使用] を選択します。使用する共有ルールセットを指定します。

注意: これらの設定は、APIを使用して作成した共有ルールセットがない場合は表示されません。共有ルールセットを作成していない場合、または初期設定をそのまま使用する場合は、各コンピュータには独自の許可およびブロックルールがローカルに使用されます。ローカルルールに対する変更は他のコンピュータには反映されません。

4. [保存] をクリックします。

コンピュータのDeep Security Agentが次回Deep Security Managerに接続するときに、Agentによってルールが適用されます。

ルールセットのアップロードに失敗したことを示すエラーが表示された場合は、AgentとManagerまたはRelay間のネットワークデバイスによって、[ハートビートポート番号](#)または[Relayポート番号](#)の通信が許可されていることを確認します。

共有許可およびブロックルールからコンピュータ固有の許可およびブロックルールに切り替える

コンピュータで共有許可またはブロックルールを使用している場合は、ローカルルールを使用するように変更できます。アプリケーションコントロールをはじめて有効にしたときと同様に、ファイルシステムに現在インストールされているすべてのソフトウェアが検索され、初期ルールセットが作成されます。

警告: この手順を開始する前に、適切なソフトウェアのみが現在インストールされていることを確認してください。ルールセットを再構築すると、安全性が確認されていないソフトウェアや不正プログラムも含め、現在インストールされているすべてのソフトウェアが許可されます。インストールされているソフトウェアを把握していない場合は、クリーンインストールを実施し、その後でアプリケーションコントロールを有効にするのが最も安全な方法です。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

以下の手順は、特定のコンピュータのAgentでローカルルールセットを使用するように設定する手順です。すべてのコンピュータでローカルルールを使用する場合は、代わりに [ポリシー] タブで設定を編集します。

1. **コンピュータエディタ**¹で、[アプリケーションコントロール] に進みます。
2. [ルールセット] で、[設定を継承] が選択されている場合は解除し、[最初はインストールされているソフトウェアに基づいてローカルルールセットを使用] を選択します。
3. [保存] をクリックします。

変更を確認するには、AgentとDeep Security Managerとの次回接続時に、[アプリケーションコントロールルールセットの構築に関するイベントログ](#)を確認します。

Relayを介してアプリケーションコントロール共有ルールセットをインストールする

アプリケーションコントロールルールセットを作成または変更するたびに、使用するすべてのコンピュータに配布する必要があります。共有ルールセットはローカルルールセットよりも大きくなります。また、共有ルールセットはさまざまなサーバにも適用されることがあります。ルールセットをManagerから同時に直接ダウンロードすると、負荷が大きくなり、パフォーマンスが低下する可能性があります。グローバルルールセットの注意事項も同じです。

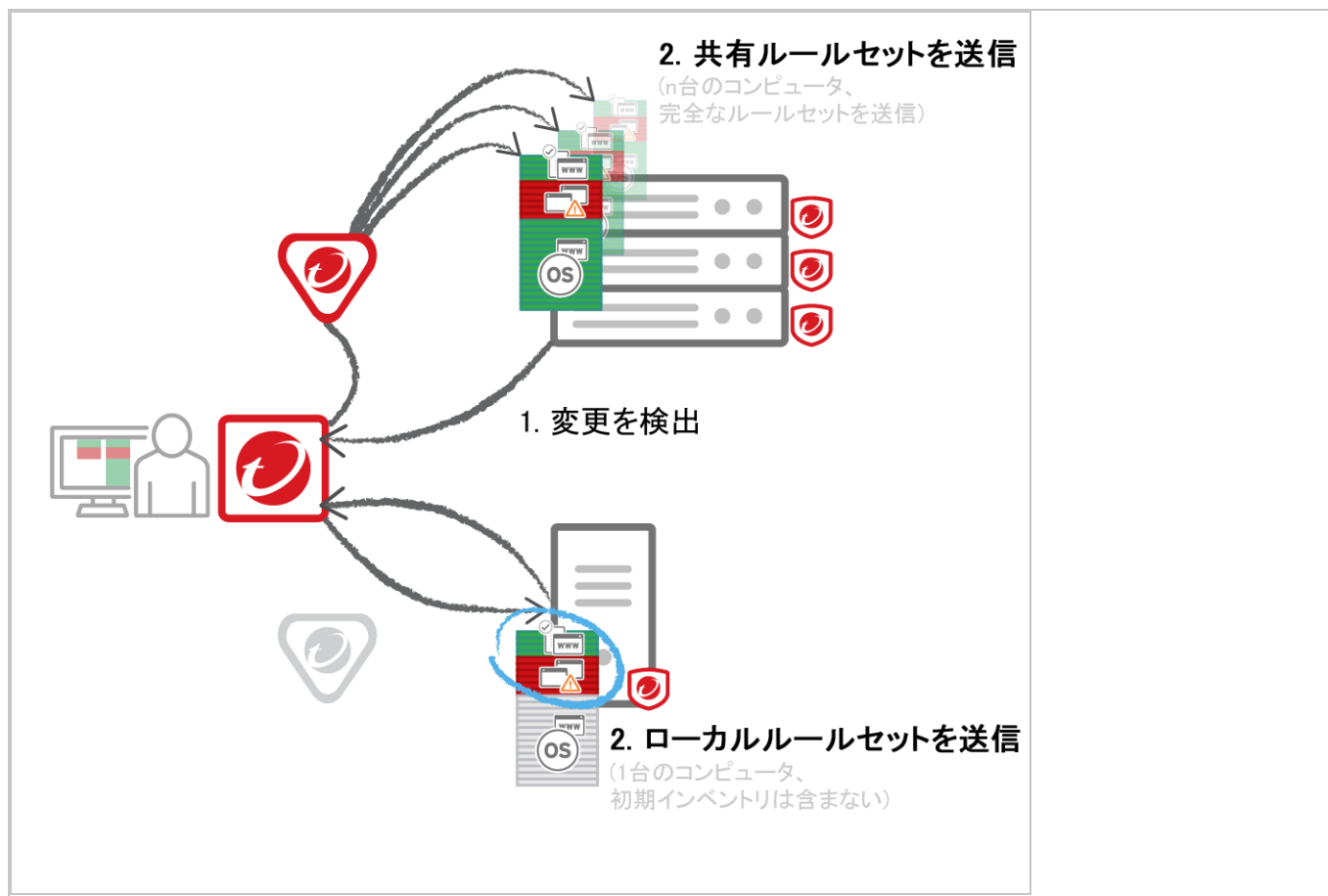
Deep Security Relayを使用すると、この問題を解決できます。(Relayの設定の詳細については、「["Relayによるセキュリティとソフトウェアのアップデートの配布" on page 438](#)」を参照してください。)

マルチテナント環境を使用しているかどうかによって、手順が異なります。

単一テナント環境

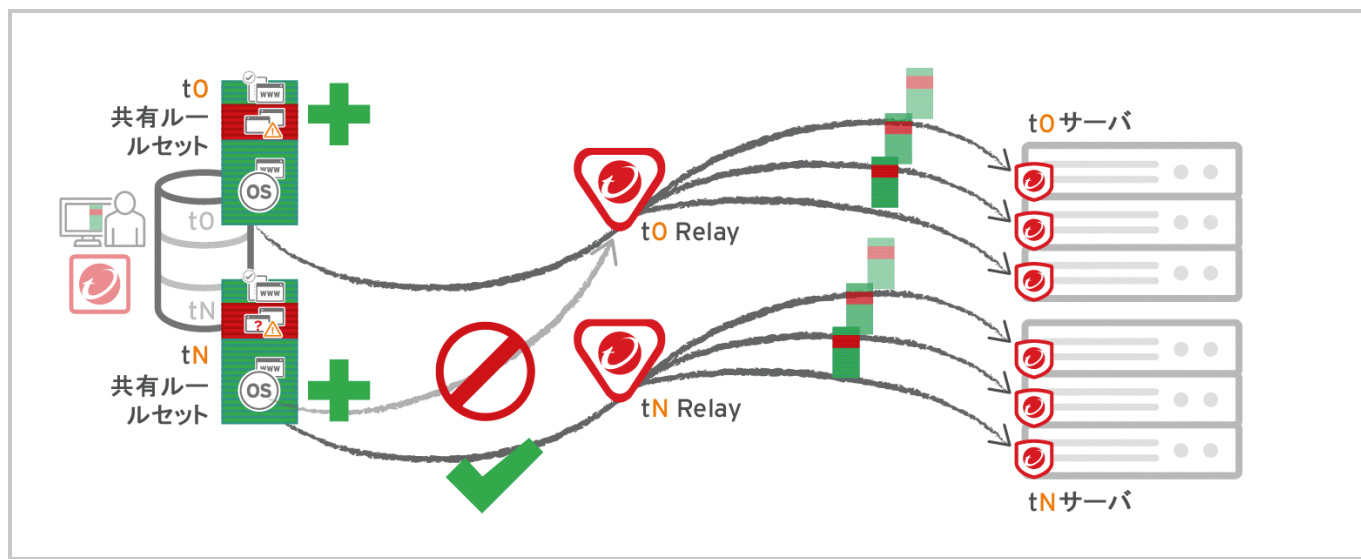
[管理]→[システム設定]→[詳細] の順に選択し、[アプリケーションコントロールルールセットをRelayから提供する] を選択します。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。



マルチテナント環境

プライマリテナント (t0) は他のテナント (tN) の設定にアクセスできないため、t0 RelayにはtN アプリケーションコントロールルールセットが設定されません。他のテナント (tN) は独自の [Relayグループ](#)を作成してから [アプリケーションコントロールルールセットをRelayから提供する] を選択する必要があります。



Relayと共有ルールセットを使用する際の注意事項

Relayを使用する前に、Relayに使用環境との互換性があることを確認してください。以前にダウンロードされて現在有効になっているルールセットがAgentにない場合、Agentが新しいアプリケーションコントロールルールを受け取らないと、コンピュータがアプリケーションコントロールによって保護されることはありません。アプリケーションコントロールルールセットのダウンロードに失敗した場合は、ルールセットダウンロード失敗イベントが、ManagerおよびAgentで記録されます。

- プロキシを使用してAgentをManagerに接続する場合は、Relayを使用する必要があります。

注意: Deep Security Agent 10.0以前では、プロキシ経由でのRelayへの接続がサポートされていませんでした。プロキシが原因でルールセットダウンロードに失敗した場合、およびAgentがRelayまたはManagerにアクセスするためのプロキシを必要とする場合は、次のいずれかを実行する必要があります。

- [Agentソフトウェアをアップデート](#)して、[プロキシを設定する](#)。
 - プロキシをバイパスする。
 - Relayを追加してから、[アプリケーションコントロールルールセットをRelayから提供する]を選択する。
- 共有ルールセットまたはグローバルルールセットを使用している場合は、Relayを使用するとパフォーマンスが向上します。

- ローカルルールセットを使用している場合は、Relayを使用するとパフォーマンスが低下する可能性があります。
- プライマリ以外のテナント (tN) が初期設定のプライマリ (t0) Relayグループを使用する場合は、マルチテナント設定でRelayを使用しないでください。

不正プログラムの防止

ヒント: 不正プログラム対策機能の紹介や推奨設定方法についての情報は、次のWebサイトでまとめて確認できます。環境の構築を始める前に参照すると、動作不調のリスク軽減および安定性の向上に役立てることができます。

<https://success.trendmicro.com/jp/solution/000286756>

Deep Security不正プログラム対策モジュールには、不正プログラム、ウイルス、トロイの木馬、スパイウェアなどのファイルベースの脅威からAgentコンピュータをリアルタイムに保護する機能と、必要に応じて保護する機能があります。この不正プログラム対策モジュールでは、脅威を特定するために、ローカルハードドライブ上のファイルを包括的な脅威データベースに対して照合します。また、圧縮や既知の攻撃コードなど、特定の特性がないかについても確認します。

脅威データベースの一部はTrend Microサーバにホストされたり、パターンファイルとしてローカルに保存されます。Deep Security Agentは、最新の脅威からも保護できるよう、不正プログラム対策パターンファイルとアップデートを定期的にダウンロードします。

注意: Deep Security Agentを新規にインストールした場合、アップデートサーバに接続して不正プログラム対策パターンファイルとアップデートをダウンロードするまで、不正プログラム対策保護は有効になりません。Deep Security Agentのインストール後に、Deep Security Relayまたはトレンドマイクロのアップデートサーバと通信できることを確認してください。

不正プログラム対策モジュールでは、脅威を排除しつつ、システムパフォーマンスへの影響は最小限に抑えます。不正なファイルは、駆除、削除、または隔離できます。特定した脅威に関連付けられているプロセスを終了したり、他のシステムオブジェクトを削除することもできます。

不正プログラム対策モジュールをオンにして設定するには、"[不正プログラム対策の有効化と設定](#)" on page 730を参照してください。

- ["不正プログラム検索の種類" below](#)
- ["不正プログラム検索設定" on page 725](#)
- ["不正プログラムイベント" on page 725](#)
- ["スマートスキャン" on page 725](#)
- ["機械学習型検索" on page 726](#)
- ["Connected Threat Defense" on page 727](#)
- ["不正プログラム検索の種類" below](#)

不正プログラム検索の種類

不正プログラム対策モジュールでは、さまざまな種類の検索を実行します。["実行する検索の種類を選択する" on page 731](#)も参照してください。

リアルタイム検索

受信、開く、ダウンロード、コピー、編集などの処理が行われるたびに、そのファイルにセキュリティ上のリスクがないかが検索されます。セキュリティ上のリスクが検出されなかった場合、ファイルは現在の場所にそのまま残され、ユーザはファイルにアクセスできます。セキュリティ上のリスクが検出された場合、感染ファイルの名前と具体的なセキュリティ上のリスクの内容を示す通知メッセージが表示されます。

リアルタイム検索は、[スケジュール] オプションで別の期間を設定した場合を除き、継続的に有効になります。

ヒント: リアルタイム検索は、ファイルサーバでファイルのバックアップが予約されているときなど、パフォーマンスへの影響が大きいときを避けて実行するように設定できます。

この検索は、不正プログラム対策モジュールでサポートされるすべてのプラットフォームで実行できます。

手動検索

コンピュータ上のすべてのプロセスとファイルを対象にフルシステム検索が実行されます。検索に要する時間は、検索するファイル数と、コンピュータのハードウェアリソースに応じて異なります。手動検索はクイック検索より時間がかかります。

手動検索は、[不正プログラムのフル検索] をクリックしたときに実行されます。

この検索は、不正プログラム対策モジュールでサポートされるすべてのプラットフォームで実行できます。

予約検索

設定した日時に自動的に実行されます。予約検索を使用して日々の検索を自動化することで、検索をより効率的に管理できます。

予約検索は、予約タスク ("[Deep Security予約タスクの設定](#)" on page 479を参照) を使用して [コンピュータの不正プログラムを検索] タスクを作成したときに指定した日時に実行されません。

この検索は、不正プログラム対策モジュールでサポートされるすべてのプラットフォームで実行できます。

クイック検索

コンピュータの重大なシステム領域で、現在アクティブな脅威の検索のみが実行されます。クイック検索では、現在アクティブな不正プログラムが検索されますが、活動のない、または保存されている感染ファイルを検索するためにファイルが詳細に検索されることはありません。大容量のドライブでは、フル検索よりも短時間で終了します。クイック検索は設定できません。

クイック検索は、[不正プログラムのクイック検索] をクリックしたときに実行されます。

注意: クイック検索を実行できるのは、Windowsコンピュータのみです。

検索されるオブジェクトと順序

次の表は、検索の種類ごとに、検索されるオブジェクトと検索の順序を示しています。

対象	フル検索 (手動または予約)	クイック検索
ドライバ	1	1
トロイの木馬	2	2
プロセスイメージ	3	3
メモリ	4	4

対象	フル検索 (手動または予約)	クイック検索
ブートセクタ	5	-
ファイル	6	5
スパイウェア	7	6

不正プログラム検索設定

不正プログラム検索設定は、不正プログラム検索の動作を制御する一連のオプションです。ポリシーを使用して不正プログラム対策を設定したり、特定のコンピュータに対して不正プログラム対策を設定するときは、使用する不正プログラム検索設定を選択します。不正プログラム検索設定は複数作成でき、コンピュータグループによって検索要件が異なる場合はポリシーの異なる設定を使用できます。

リアルタイム検索、手動検索、および予約検索では、すべて不正プログラム検索設定を使用します。Deep Securityでは、検索の種類ごとに不正プログラム検索の初期設定が用意されています。これらの検索設定は、セキュリティポリシーの初期設定に使用されます。検索の初期設定をそのまま使用することも、変更することも、独自の設定を作成することもできます。

注意: クイック検索は設定できないため、不正プログラム検索設定を使用しません。

検索の対象または対象外となるファイルやディレクトリ、またコンピュータで不正プログラムが検出された場合の処理 (駆除、隔離、削除など) を指定できます。

詳細については、"[不正プログラム検索の設定](#)" on page 733を参照してください。

不正プログラムイベント

Deep Securityで不正プログラムが検出されると、イベントログに表示されるイベントがトリガされます。イベントログでは、イベントに関する情報を確認したり、誤判定の場合のファイルの例外を作成したりできます。また、実際には安全なファイルを復元することもできます。 ("[不正プログラム対策イベント](#)" on page 1319と"[不正プログラムの処理](#)" on page 778を参照。)

スマートスキャン

スマートスキャンでは、トレンドマイクロのサーバに保存されている脅威シグニチャが使用されます。スマートスキャンには次のメリットがあります。

- セキュリティステータスの検索をクラウドベースで高速かつリアルタイムに実行
- 脅威からの保護にかかる合計時間を削減
- パターンファイルのアップデート時に使用されるネットワーク帯域幅を削減 (パターン定義のアップデートの大半は、クラウドで保持され、多数のコンピュータへの配信は不要)
- 企業全体へのパターン展開のコストとオーバーヘッドを削減
- コンピュータにおけるカーネルのメモリ消費を削減 (メモリ消費量の増加を最小限に抑制)

スマートスキャンを使用すると、まず、ローカルで保持しているパターンファイルにより検索が行われます。そこでファイルの危険性を評価できなかった場合は、ローカルのSmart Protection Serverに接続します。ローカルのSmart Protection Serverでも危険性を評価できなかった場合は、トレンドマイクロのGlobal Smart Protectionサービスに接続します。この機能の詳細については、"[Deep SecurityのSmart Protection](#)" on page 774を参照してください。

機械学習型検索

Deep Securityは、機械学習型検索により、未知の脅威とゼロデイ攻撃に対する不正プログラム対策保護を強化します。トレンドマイクロの機械学習型検索では、デジタルDNAフィンガープリント、APIマッピング、その他のファイル機能を使用して、高度な機械学習技術により脅威情報を関連付け、詳細なファイル分析を実行することで新たなセキュリティリスクを検出します。

機械学習型検索は、フィッシングやスパイフィッシングなどの手法を用いた標的型攻撃によるセキュリティ侵害に対する保護に効果的です。これらのケースでは、特定の環境を標的に設計された不正プログラムが従来の不正プログラム検索の手法をすり抜ける場合があります。

Deep Securityはリアルタイムスキャン中に不明なファイルや感染率の低いファイルを検出すると、高度な脅威検索エンジン (ATSE) を使用してファイルを検索し、ファイルの機能を抽出します。このレポートは、Trend Micro Smart Protection Networkの機械学習型検索エンジンに送信されます。機械学習型検索は、不正プログラムモデリングを使用してサンプルを不正プログラムモデルと比較し、脅威の可能性スコアを割り当て、ファイルに含まれる可能性がある不正プログラムの種類を特定します。

ファイルが脅威として認識された場合、Deep Securityはファイルからの脅威の駆除、ファイルの隔離、またはファイルの削除を実行し、脅威がネットワーク全体に広がり続けることを防ぎます。

機械学習型検索の使用方法の詳細については、"[機械学習型検索を使用した脅威の検出](#)" on page 756を参照してください。

Connected Threat Defense

Connected Threat Defenseは、Deep Securityとトレンドマイクロのサンドボックス技術であるDeep Discovery Analyzerの間の接続を設定することで、新しい脅威にする不正プログラム対策保護を強化します。詳細については、"[Connected Threat Defenseを使用した脅威の検出](#)" on page 758を参照してください。

不正プログラムの種類

不正プログラム対策モジュールは、多数のファイルベースの脅威から保護します。"[特定の種類の不正プログラムを検索する](#)" on page 736と"[不正プログラムの処理方法を設定する](#)" on page 745も参照してください。

ウイルス

ウイルスは、ファイルに不正コードを挿入することによって感染します。通常は、感染したファイルを開くと不正なコードが自動的に実行され、他のファイルを感染させるだけでなく、ペイロードが配信されます。次に、一般的なウイルスをいくつか示します。

- COMおよびEXE感染型ウイルス: 一般的に.COMや.EXEの拡張子が付いている、DOSおよびWindows実行可能ファイルに感染します。
- マクロウイルス: 不正マクロを挿入することで、Microsoft Officeファイルを感染させます。
- システム領域感染型ウイルス: OSを起動させるために必要な情報が格納されているハードディスクドライブの領域に感染します。

不正プログラム対策モジュールでは、感染ファイルを特定して駆除するために、さまざまな技術を使用しています。最もよく行われる方法は、ファイルの感染に使用される実際の不正コードを検出し、感染ファイルからこのコードを取り除くことです。その他にも、感染する可能性のあるファイルへの変更を規制する方法や、不審な変更が適用される場合にファイルをバックアップする方法などがあります。

トロイの木馬

一部の不正プログラムは、その他のファイルにコードを挿入することによって拡散する方法を採りません。代わりに別の方法を探ったり、別の影響を及ぼします。

- トロイの木馬: トロイの木馬の神話のように、ファイルを開いたときに実行されてシステムに感染する不正プログラムファイル。
- バックドア: ポート番号を開いて権限のないリモートユーザに感染システムへのアクセスを許可する不正プログラムアプリケーション。
- ワーム: ネットワークを使用してシステム間で伝播する不正プログラム。ワームは人目を引くメールメッセージ、インスタントメッセージ、または共有ファイルを介したソーシャルエンジニアリングを利用して伝播します。また、アクセス可能なネットワーク共有に自身をコピーし、脆弱性を突いて別のコンピュータに広がります。
- ネットワークウイルス: ファイルベースではない、メモリまたはパケット上のみに存在する不正プログラム。不正プログラム対策ではネットワークウイルスを検出または削除できません。
- ルートキット: OSのコンポーネントの呼び出しを操作するファイルベースの不正プログラム。監視やセキュリティソフトウェアなどのアプリケーションでは、ファイルのリスト作成や実行中のプロセスの特定など、非常に基本的な機能を呼び出す必要があります。これらの呼び出しを操作することによって、ルートキットは自身の存在や、その他の不正プログラムの存在を隠すことができます。

パッカー

パッカーは圧縮され暗号化された実行可能プログラムです。不正プログラムの作者は、検出を免れるために、既存の不正プログラムを何重にも圧縮または暗号化することがあります。不正プログラム対策は、実行可能ファイル内に不正プログラムに関連付けられた圧縮パターンがないか検索します。

スパイウェア/グレーウェア

スパイウェアおよびグレーウェアは、別のシステムに送信するための情報や、別のアプリケーションで収集された情報を収集するアプリケーションおよびコンポーネントです。スパイウェア/グレーウェアの検出では、不正と思われる動作だけでなく、リモート監視のような合法的な目的に使用されるアプリケーションまで検出されることがあります。スパイウェア/グレーウェアアプリケーションの中で、既知の不正プログラムチャンネルを通して配布されるものなど、もともと不正な性質を帯びているものは、一般にスパイウェア/グレーウェアではなく「トロイの木馬」として検出されます。

スパイウェアおよびグレーウェアアプリケーションは、通常、次のように分類されます。

- スパイウェア: 個人情報を収集および送信する目的でコンピュータにインストールされたソフトウェア。

- **ダイヤラー:**不正プログラムであるダイヤラーは、接続の設定先を変更して、ユーザの予期しない料金を発生させるように設計されています。ダイヤラーの中には、個人情報を送信したり、不正プログラムソフトウェアをダウンロードしたりするものもあります。
- **ハッキングツール:**コンピュータシステムへの不正アクセスを支援するために設計されたプログラムまたはプログラムのセット。
- **アドウェア:** 広告を自動的に再生、表示、またはダウンロードするソフトウェアパッケージ。
- **Cookie:** Webブラウザによって保存されるテキストファイル。Cookieには認証情報やサイトの設定など、Webサイトに関するデータが含まれています。Cookieは実行可能ファイルではないため感染することはありませんが、スパイウェアとして使用される可能性があります。合法的なWebサイトから送信されたCookieも、不正な目的に使用されることがあります。
- **キーロガー:** ユーザのキー入力を記録して、パスワードやその他の秘密情報を盗むソフトウェア。キーロガーの中には、リモートシステムにログを送信するものがあります。

グレーウェアの定義

スパイウェアのようなアプリケーションの中には、押しつけがましい動作を示すものの、不正ではないとみなされるものがあります。たとえば、市販のリモート制御および監視アプリケーションの中には、システムイベントを追跡および収集して、これらのイベントに関する情報を別のシステムに送信するものがあります。システム管理者などのユーザが自ら、これらの合法的なアプリケーションをインストールしている場合があります。これらのアプリケーションを「グレーウェア」と言います。

不正プログラム対策モジュールでは、グレーウェアの不正使用を防止するためにグレーウェアを検出します。ただし、検出されたアプリケーションを「承認」して、実行を許可することができます。

Cookie

Cookieは、Webブラウザに保存されるテキストファイルで、HTTP要求のたびにWebサーバに返されます。Cookieには認証情報や設定が保存されていますが、感染サーバがからの持続型攻撃の場合、それらに紛れてSQLインジェクションやXSSなどの攻撃コードが含まれている可能性があります。

その他の脅威

その他の脅威は、どのタイプにも分類されない不正プログラムなどです。このカテゴリには、偽の通知を表示したり、画面の動作を操作したりする、一般に実害のないジョークプログラムが含まれます。

潜在的な不正プログラム

潜在的な不正プログラムとは、疑わしいが、特定の不正プログラムの変異形として分類できないファイルのことです。トレンドマイクロでは、ファイルの詳細な分析についてサポート担当者にお問い合わせいただくことをお勧めします。初期設定では、これらの検出結果がログに記録され、ファイルは分析用に匿名でトレンドマイクロに送信されます。

不正プログラム対策の有効化と設定

ヒント: 不正プログラム対策機能の紹介や推奨設定方法についての情報は、次のWebサイトでまとめて確認できます。環境の構築を始める前に参照すると、動作不調のリスク軽減および安定性の向上に役立てることができます。

<https://success.trendmicro.com/jp/solution/000286756>

不正プログラム対策を使用するには、次の基本手順を実行します。

1. "不正プログラム対策モジュールをオンにする" on the next page.
2. "実行する検索の種類を選択する" on the next page.
3. "検索除外を設定する" on the next page
4. "最新の脅威に対応できるようにDeep Securityを最新の状態に保つ" on page 732

この手順を実行したら、"不正プログラム検索の設定" on page 733を確認し、不正プログラム対策検索の動作を設定します。

ヒント: 不正プログラム対策設定のほとんどは、各コンピュータで個別に設定するか、またはポリシーで設定して複数のコンピュータ(すべてのWindows 2008 Serverなど)に適用できます。管理を容易にするために、可能なかぎり個々のコンピュータではなくポリシーで設定を行ってください。詳細については、"ポリシー、継承、およびオーバーライド" on page 587を参照してください。

ヒント: 不正プログラム対策の設定によって、CPUとRAMの使用率は変化します。Deep Security Agentでの不正プログラム対策のパフォーマンスを最適化するには、"[不正プログラム対策のパフォーマンスのヒント](#)" on page 750を参照してください。

不正プログラム対策機能の概要については、"[不正プログラムの防止](#)" on page 722を参照してください。

不正プログラム対策モジュールをオンにする

1. [ポリシー]に移動します。
2. 不正プログラム対策を有効にするポリシーをダブルクリックします。
3. [不正プログラム対策]→[一般]の順に選択します。
4. [不正プログラム対策のステータス]で、[オン]を選択します。
5. [保存]をクリックします。

実行する検索の種類を選択する

不正プログラム対策をオンにしたら、Deep Securityで実行する検索の種類を指定する必要があります ("[不正プログラム検索の種類](#)" on page 723を参照)。

1. [ポリシー]に移動します。
2. 設定するポリシーをダブルクリックします。
3. [不正プログラム対策]>[一般]の順にクリックします。
4. 検索の各種類を有効または無効にします。
 - a. 初期設定を使用して検索を実行するには、[初期設定]を選択します。
 - b. カスタマイズ可能な不正プログラム検索設定を使用して検索を実行するには、不正プログラム検索設定を選択します。
 - c. 検索を無効にするには、不正プログラム検索設定で[設定なし]を選択します。
5. [保存]をクリックします。

ヒント:トレンドマイクロでは、Deep Securityで保護するすべてのサーバについて、週に1回は予約検索を実行するように設定することを推奨します。これは、予約タスクを使用して実行できます ("[Deep Security予約タスクの設定](#)" on page 479を参照してください)。

検索除外を設定する

Deep Securityの不正プログラム検索では、検索時間を短縮してコンピューティングリソースの使用を最小限に抑えるために、すべての種類の検索から除外するフォルダ、ファイル、および

ファイルの種類を指定することができます。また、Windowsサーバで実行するリアルタイムの不正プログラム検索からプロセスイメージファイルを除外することもできます。

これらの除外項目を指定するには、不正プログラム検索設定エディタの [検索除外] タブで除外リストを選択します。"[検索対象ファイルを指定する](#)" on page 738を参照してください。

ヒント: Deep Securityの不正プログラム対策保護を有効にするとパフォーマンスが低下する場合、検索除外を使用して特定のフォルダやファイルを検索対象から除外すると改善できることがあります。

最新の脅威に対応できるようにDeep Securityを最新の状態に保つ

Deep Security Agentを新たなウイルスや攻撃コードに常に対応できる状態に維持するためには、トレンドマイクロから直接、あるいはRelay経由で間接的に、最新のソフトウェアおよびセキュリティアップデートパッケージをダウンロードする必要があります。これらのパッケージには、脅威の定義とパターンファイルが含まれています。トレンドマイクロからセキュリティアップデートを取得し、他のAgentおよびApplianceに配布する場合は、Relay有効化済みAgentを使用します。Relay有効化済みAgentを使用します。Relay有効化済みAgentはRelayグループに編成されていて、Relayグループの管理および設定はDeep Security Managerで行います。

1. [管理]→[システム設定]→[アップデート]の順に選択します。
2. Deep Securityがトレンドマイクロからセキュリティアップデートを取得できるように設定します。Relay有効化済みAgentが少なくとも1つあり、該当するAgentおよびApplianceに割り当てられていることを確認します。
Deep Security AgentがRelayかどうかを判断するには、コンピュータの横の [プレビュー] をクリックします。



3. [管理]→[予約タスク]の順に選択します。
4. 利用可能なセキュリティアップデートとソフトウェアアップデートの両方を定期的にダウンロードする予約タスクがあることを確認します。

不正プログラム検索の設定

ヒント: 不正プログラム対策機能の紹介や推奨設定方法についての情報は、次のWebサイトでまとめて確認できます。環境の構築を始める前に参照すると、動作不調のリスク軽減および安定性の向上に役立てることができます。

<https://success.trendmicro.com/jp/solution/000286756>

不正プログラム検索設定は保存して再利用可能な設定で、ポリシーまたはコンピュータに不正プログラム対策を設定する場合に適用できます。この設定には、Deep Securityで実行する不正プログラム検索の種類と検索対象のファイルを指定します。一部のポリシーのプロパティも、不正プログラム検索の動作に影響を与えます。

- "不正プログラム検索設定を作成または編集する" on the next page
- "特定の種類の不正プログラムを検索する" on page 736
- "検索対象ファイルを指定する" on page 738

- ["リアルタイム検索を実行するタイミングを指定する" on page 745](#)
- ["不正プログラムの処理方法を設定する" on page 745](#)
- ["ファイルのハッシュダイジェストにより不正プログラムファイルを特定する" on page 749](#)
- ["コンピュータで通知を設定する" on page 749](#)

Deep Securityの[ベストプラクティスガイド](#)にも、不正プログラム検索の推奨設定が記載されています。

ヒント: 不正プログラム対策の設定によって、CPUとRAMの使用率は変化します。Deep Security Agentでの不正プログラム対策のパフォーマンスを最適化するには、["不正プログラム対策のパフォーマンスのヒント" on page 750](#)を参照してください。

不正プログラム検索設定を作成または編集する

リアルタイム、手動、または予約検索の動作を制御するために、不正プログラム検索設定を作成または編集します(詳細については、["不正プログラム検索設定" on page 725](#)を参照してください)。必要に応じて、複数の不正プログラム検索設定を作成できます。

- 作成した不正プログラム検索設定は、ポリシーまたはコンピュータの検索と関連付けることができます (["実行する検索の種類を選択する" on page 731](#)を参照してください)。
- ポリシーまたはコンピュータが使用している不正プログラム検索設定を編集すると、この変更は設定に関連付けられている検索に影響します。

ヒント: 既存の設定に類似する不正プログラム検索設定を作成するには、既存の設定を複製して編集します。

制御する検索の種類に応じて、2種類の不正プログラム検索設定を作成できます (["不正プログラム検索の種類" on page 723](#)を参照してください)。

- リアルタイム検索の設定: リアルタイム検索を制御します。[アクセス拒否] などの一部の処理は、リアルタイム検索の設定でのみ使用可能です。
- 手動/予約検索の設定: 手動検索または予約検索を制御します。[CPU使用率] などの一部のオプションは、手動/予約検索の設定でのみ使用可能です。

Deep Securityは、検索の種類ごとに不正プログラム検索の初期設定を提供します。

1. [ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] に移動します。
2. 検索設定を作成するには、[新規]→[新規の不正プログラムのリアルタイム検索設定] または [新規の不正プログラムの手動/予約検索設定] をクリックします。
 - a. 検索設定を識別する名前を入力します。この名前は、ポリシーで不正プログラム検索を設定するときにリストに表示されます。
 - b. (オプション) この設定の使用例の説明を入力します。
3. 既存の検索設定を表示して編集するには、その検索設定を選択して [プロパティ] をクリックします。
4. 検索設定を複製するには、その検索設定を選択して [複製] をクリックします。

ヒント: 不正プログラム検索設定を使用するポリシーとコンピュータを確認するには、プロパティの [割り当て対象] タブをご覧ください。

不正プログラム検索をテストする

以降の不正プログラム対策の設定手順に進む前に、リアルタイム検索および手動/予約検索をテストし、それらが正しく動作することを確認します。

リアルタイム検索のテスト:

1. リアルタイム検索が有効で、設定が選択されていることを確認します。
2. [EICARサイト](#) に移動し、不正プログラム対策のテストファイルをダウンロードします。この標準ファイルは、リアルタイム検索の不正プログラム対策機能をテストします。このファイルが隔離されればテストは成功です。
3. Deep Security Managerで、[イベントとレポート]→[不正プログラム対策イベント] の順に選択し、EICARファイルの検出が記録されていることを確認します。検出が記録されていれば、不正プログラム対策のリアルタイム検索は正常に機能しています。

手動/予約検索のテスト:

注意: 手動/予約検索のテストを開始する前に、リアルタイム検索が無効になっていることを確認します。

1. [管理] を選択します。
2. [予定タスク]→[新規] の順にクリックします。
3. ダウンロードメニューから [コンピュータの不正プログラムを検索] を選択し、実行間隔を選択します。必要な指定を行い、検索の設定を完了します。
4. [EICARサイト](#) に移動し、不正プログラム対策のテストファイルをダウンロードします。この標準ファイルは、手動/予約検索の不正プログラム対策機能をテストします。
5. 予約検索を選択して、[今すぐタスクを実行] をクリックします。このテストファイルが隔離されればテストは成功です。

6. Deep Security Managerで、[イベントとレポート]→[不正プログラム対策イベント]の順に選択し、EICARファイルの検出が記録されていることを確認します。検出が記録されていれば、不正プログラム対策の手動/予約検索は正常に機能しています。

特定の種類の不正プログラムを検索する

- ["スパイウェア/グレーウェアを検索する" below](#)
- ["圧縮済み実行可能ファイルを検索する \(リアルタイム検索のみ\)" below](#)
- ["プロセスメモリを検索する \(リアルタイム検索のみ\)" on the next page](#)
- ["圧縮ファイルを検索する" on the next page](#)
- ["埋め込みのMicrosoft Officeオブジェクトを検索する" on the next page](#)

関連項目:

- ["挙動監視による不正プログラム/ランサムウェア検索の強化" on page 767](#)
- ["Connected Threat Defenseを使用した脅威の検出" on page 758](#)

スパイウェア/グレーウェアを検索する

スパイウェアおよびグレーウェア対策を有効にすると、不審なファイルの検出時に、スパイウェア検索エンジンによってこれらのファイルが隔離されます。

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般] タブで、[スパイウェア/グレーウェア対策を有効にする]を選択します。
3. [OK] をクリックします。

スパイウェア検索エンジンで無視する必要があるファイルを特定するには、["不正プログラム対策の例外の作成" on page 785](#)を参照してください。

圧縮済み実行可能ファイルを検索する (リアルタイム検索のみ)

ウイルスは、リアルタイム圧縮アルゴリズムを使用して、ウイルスフィルタを回避しようとすることがあります。IntelliTrap機能は、リアルタイムの圧縮済み実行可能ファイルを遮断し、他の不正プログラムの特性とファイルを組み合わせます。

注意: IntelliTrapはそのようなファイルをセキュリティ上の危険として特定するため、IntelliTrapを有効にすると、安全なファイルを (削除や駆除ではなく) 隔離したり、間違っ
てブロックする場合があります(["不正プログラムの処理方法を設定する" on page 745](#)を参照してください)。ユーザがリアルタイムで圧縮した実行可能ファイルを頻繁にやり取りする場合

は、IntelliTrapを無効にしてください。IntelliTrapは、ウイルス検索エンジン、IntelliTrapパターンファイル、およびIntelliTrap除外パターンファイルを使用します。

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般] タブで、[IntelliTrapを有効にする] を選択します。
3. [OK] をクリックします。

プロセスメモリを検索する (リアルタイム検索のみ)

リアルタイムでプロセスメモリを監視し、Trend Micro Smart Protection Networkと連携した追加のチェックを実行することにより、不審なプロセスが既知の不正なプロセスであるかどうかを判別します。プロセスが不正である場合、プロセスは強制終了されます。詳細については、"[Deep SecurityのSmart Protection](#)" on page 774を参照してください。

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般] タブで、[プロセスメモリ内の不正プログラムを検索する] を選択します。
3. [OK] をクリックします。

圧縮ファイルを検索する

圧縮ファイルを解凍し、コンテンツに不正プログラムが含まれていないか検索します。検索を有効にするときに、解凍するファイルの最大サイズと最大数を指定します (大きなファイルはパフォーマンスに影響を及ぼすことがあります)。また、圧縮ファイル内に存在する圧縮ファイルを検索できるように、検査する圧縮レベルも指定します。圧縮レベル1は、単一の圧縮ファイルです。レベル2は、ファイル内の圧縮ファイルです。最大6の圧縮レベルを検索できますが、レベルが高くなるとパフォーマンスに影響を及ぼす可能性があります。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[圧縮ファイルの検索] を選択します。
3. 解凍するコンテンツファイルの最大サイズ (MB)、検索する圧縮レベル、解凍する最大ファイル数を指定します。
4. [OK] をクリックします。

埋め込みのMicrosoft Officeオブジェクトを検索する

Microsoft Officeの特定のバージョンでは、Object Linking and Embedding (OLE) を使用してOfficeファイルにファイルやその他のオブジェクトを挿入します。これらの埋め込みオブジェクトには、不正なコードが含まれている場合があります。

他のオブジェクトに埋め込まれているオブジェクトを検出するために、検索するOLE層の数を指定します。パフォーマンスへの影響を軽減するため、各ファイル内の埋め込みオブジェクトの層をいくつかだけ検索できます。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[埋め込みのMicrosoft Officeオブジェクトを検索する] を選択します。
3. 検索するOLE層の数を指定します。
4. [OK] をクリックします。

検索対象ファイルを指定する

不正プログラムを検索するファイルを指定するには、検索に含めるファイルとディレクトリを指定してから、これらのファイルとディレクトリのうち、検索から除外するものを指定します。ネットワークディレクトリも検索できます。

- ["検索対象" below](#)
- ["検索除外" on the next page](#)
- ["ネットワークディレクトリを検索する \(リアルタイム検索のみ\)" on page 745](#)

検索対象

検索するディレクトリと、ディレクトリ内の検索するファイルも指定します。

検索するディレクトリを指定するには、すべてのディレクトリまたはディレクトリのリストを指定できます。ディレクトリリストでは、特定の構文に含まれるパターンを使用して、検索するディレクトリを指定します(["ディレクトリリストの構文" on page 741](#)を参照してください)。

検索するファイルを指定するには、次のいずれかのオプションを使用します。

- すべてのファイル
- IntelliScanによって識別されるファイルタイプ。IntelliScanでは、感染しやすいファイルの種類 (.zipや.exeなど) のみを検索します。IntelliScanでは、ファイルの種類はファイル拡張子から判断するのではなく、ファイルのヘッダや内容を読み取ってそのファイルが検索対象かどうかを決定します。すべてのファイルを検索する場合と比較して、IntelliScanでは検索するファイル数が減少しパフォーマンスが向上します。
- 指定したリストに含まれているファイル名の拡張子を持つファイル: ファイル拡張子リストでは、特定の構文に含まれるパターンを使用します(["ファイル拡張子リストの構文" on page 744](#)を参照してください)。

1. 不正プログラム検索設定のプロパティを開きます。
2. [検索対象] タブをクリックします。
3. 検索するディレクトリを指定するには、[すべてのディレクトリ] または [ディレクトリリスト] を選択します。
4. [ディレクトリリスト] を選択した場合は、ドロップダウンメニューから既存のリストを選択するか、[新規] を選択して新しいリストを作成します。
5. 検索するファイルを指定するには、[すべてのファイル]、[トレンドマイクロの推奨設定で検索されるファイルタイプ]、または [ファイル拡張子リスト] のいずれかを選択します。
6. [ファイル拡張子リスト] を選択した場合は、ドロップダウンメニューから既存のリストを選択するか、[新規] を選択して新しいリストを作成します。
7. [OK] をクリックします。

検索除外

検索対象からディレクトリ、ファイル、およびファイル拡張子を除外します。リアルタイム検索の場合（ Deep Security Virtual Appliance で実行する場合を除く）、プロセスイメージファイルも検索から除外できます。

除外するファイルとフォルダの例：

- Microsoft Exchange サーバの不正プログラム検索設定を作成する場合は、SMEX 隔離フォルダを除外して、不正プログラムであることがすでに確認されているファイルの再検索を回避する必要があります。
- Deep Security Manager で使用されているデータベースサーバ上で不正プログラム検索を実行する場合は、データディレクトリを除外します。Deep Security Manager でウイルスが含まれている可能性のある侵入防御データを取り込み、格納する際に、Deep Security Agent による隔離が実行され、データベースの破損を引き起こす場合があります。
- サイズの大きい VMware イメージがある場合は、パフォーマンスの問題が発生した場合は、これらのイメージが格納されているディレクトリを除外します。

ディレクトリ、ファイル、プロセスイメージファイルを除外するには、除外する項目を特定するためにパターンを使用するリストを作成します。

1. 不正プログラム検索設定のプロパティを開きます。
2. [検索除外] タブをクリックします。
3. 検索から除外するディレクトリを指定します。
 - a. [ディレクトリリスト] を選択します。
 - b. ディレクトリリストを選択するか、[新規] を選択して新しいリストを作成します ("[ディレクトリリストの構文](#)" on page 741 を参照してください)。
 - c. ディレクトリリストを作成した場合は、ディレクトリリストで選択します。

- 同様に、検索から除外するファイルリスト、ファイル拡張子リスト、プロセスイメージファイルを指定します("ファイルリストの構文" on page 742、"ファイル拡張子リストの構文" on page 744、および"プロセスイメージファイルリストの構文 (リアルタイム検索のみ)" on page 744を参照してください)。
- [OK] をクリックします。

注意:

Deep Security Agentが対象ファイルの種類を特定できない場合、不正プログラム対策エンジンは、そのファイルをメモリにロードして、自己解凍型ファイルかどうかを判断します。大量のファイルがメモリにロードされると、検索エンジンのパフォーマンスに影響する可能性があります。特定のサイズを超えるファイルを除外するには、次の Deep Security Managerコマンドを使用します。

```
dsm_c -action changesetting -name  
com.trendmicro.ds.antimalware:settings.configuration.maxSelfExtractR  
TScanSizeMB -value 512
```

上記の例では、対象ファイルをロードするためのファイルサイズ制限が512MBに設定されています。検索エンジンは、設定値を超えるファイルをメモリに追加せず、直接検索します。この設定を配信するには、Deep Security Managerでコマンドを実行した後に、対象のDeep Security Agentにポリシーを送信する必要があります。

ファイル除外のテスト

以降の不正プログラム対策の設定手順に進む前に、ファイル除外をテストし、それらが正しく動作することを確認します。

注意: 開始する前に、リアルタイム検索が有効で、設定が選択されていることを確認します。

- [ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] に移動します。
- [新規]→[新規の不正プログラムのリアルタイム検索設定] の順にクリックします。
- [検索除外] タブに移動し、ディレクトリリストから [新規] を選択します。
- ディレクトリリストに名前を付けます。
- [ディレクトリ] で、検索から除外するディレクトリのパスを指定します。たとえば、「c:\Test Folder\」と指定します。[OK] をクリックします。
- [一般] タブで、手動検索に名前を付け、[OK] をクリックします。
- [EICARサイト](#) に移動し、不正プログラム対策のテストファイルをダウンロードします。前の手順で指定したフォルダにファイルを保存します。このファイルが不正プログラム対策モジュールによって検出されずにそのまま保存されればテストは成功です。

ディレクトリリストの構文

注意: ディレクトリリスト項目では、WindowsとLinuxの両方の命名規則をサポートするため、スラッシュ (/) とバックスラッシュ (\) の区別はありません。

検索除外	形式	説明	例
ディレクトリ	DIRECTORY\	指定したディレクトリとそのすべてのサブディレクトリにあるファイルをすべて除外します。	C:\Program Files\ 「Program Files」ディレクトリとそのすべてのサブディレクトリにあるファイルをすべて除外します。
ワイルドカード (*) を使用したディレクトリ	DIRECTORY*\	指定されたサブディレクトリと、そこに含まれるファイルを除き、すべてのサブディレクトリを除外します。	C:\abc*\ 「abc」のすべてのサブディレクトリにあるファイルをすべて除外します。ただし、「abc」ディレクトリにあるファイルは除外しません。 C:\abc\wx*z\ 一致： C:\abc\wxz\ C:\abc\wx123z\ 一致しない： C:\abc\wxz C:\abc\wx123z C:\abc*wx\ 一致： C:\abc\wx\ C:\abc\123wx\ が一致しません： C:\abc\wx C:\abc\123wx
ワイルドカード (*) を使用したディレクトリ	ディレクトリ*\	一致する名前を持つ任意のサブディレクトリを除外します。ただし、そのディレクトリにあるファイルおよび任意のサブディレクトリは除外しません。	C:\Program Files\サブディレクトリ名*\ 「SubDirName」で始まるフォルダ名を持つすべてのサブディレクトリを除外します。C:\Program Files\またはその他のサブディレクトリにあるすべてのファイルを除外しません。

検索除外	形式	説明	例
環境変数	<code>\${ENV VAR}</code>	環境変数によって定義されているすべてのファイルとサブディレクトリを除外します。Virtual Applianceの場合は、環境変数の値のペアをポリシーエディタまたはコンピュータエディタの [設定]→[一般]→[環境変数のオーバーライド] で定義する必要があります。	<code>\${windir}</code> 変数が「c:\windows」に変換された場合、「c:\windows」とそのすべてのサブディレクトリにあるファイルをすべて除外します。
コメント	<code>DIRECTORY #コメント</code>	除外の定義にコメントを追加します。	<code>c:\abc #Exclude the abc directory</code>

ファイルリストの構文

検索除外	形式	説明	例
ファイル	FILE	場所やディレクトリに関係なく、指定したファイル名を持つすべてのファイルを除外します。	<code>abc.doc</code> すべてのディレクトリで「abc.doc」という名前のファイルをすべて除外します。「abc.exe」は除外しません。
ファイルパス	FILEPATH	ファイルパスで指定された単一のファイルを除外します。	<code>C:\Documents\abc.doc</code> 「Documents」ディレクトリの「abc.doc」という名前のファイルのみ除外します。
ワイルドカード (*) を使用したファイルパス	FILEPATH	ファイルパスで指定されたすべてのファイルを除外します。	<code>C:\Documents\abc.co*</code> (Windows Agentプラットフォームのみ)「Documents」ディレクトリにある、ファイル名が「abc」で拡張子が「.co」で始まるファイルを除外します。
ファイル名はワイルドカード (*) です	FILEPATH*	パス内のすべてのファイルを除外しますが、指定されていないサブディレクトリ内のファイルは除外しません	<code>C:\Documents*</code> ディレクトリC:\Documents\にあるすべてのファイルを除外します。 <code>C:\Documents\SubDirName*</code> フォルダ名が「SubDirName」で始まるサブディレクトリ内のすべてのファイルを除外します。 C:\Documents\またはその他のサブディレクトリにあるすべてのファイルを除外しません。 <code>C:\Documents**</code> C:\Documents下のすべての直接サブディレクトリ内のすべて

検索除外	形式	説明	例
ワイルドカード (*) を使用したファイル	FILE*	ファイル名のパターンに一致するすべてのファイルを除外します。	<p>のファイルを除外します。以降のサブディレクトリにあるファイルは除外しません。</p> <p><i>abc*.exe</i> 接頭語が「abc」で拡張子が「.exe」のファイルを含めます。</p> <p><i>*.db</i> 対象: 123.db abc.db 対象外: 123db 123.abd cbc.dba</p> <p><i>*db</i> 対象: 123.db 123db ac.db acdb db 対象外: db123</p> <p><i>wxy*.db</i> 対象: wxy.db wxy123.db 対象外: wxydb</p>
ワイルドカード (*) を使用したファイル	FILE.EXT*	ファイルの拡張子のパターンに一致するすべてのファイルを除外します。	<p><i>abc.v*</i> ファイル名が「abc」で拡張子が「.v」で始まるファイルを除外します。</p> <p><i>abc.*pp</i> 対象: abc.pp abc.app 対象外: wxy.app</p> <p><i>abc.a*p</i> 対象:</p>

検索除外	形式	説明	例
			abc.ap abc.a123p 対象外: abc.pp abc.* 対象: abc.123 abc.xyz 対象外: wxy.123
ワイルドカード(*)を使用したファイル	FILE*.EXT*	ファイル名と拡張子のパターンに一致するすべてのファイルを除外します。	a*c.a*p 対象: ac.ap a123c.ap ac.a456p a123c.a456p 対象外: ad.aa
環境変数	\${ENV VAR}	`\${ENV VAR}` の形式を使用した環境変数で指定されるファイルを除外します。環境変数は、ポリシーエディタまたはコンピュータエディタの [設定]→[一般]→[環境変数のオーバーライド] で定義またはオーバーライドできます。	\${myDBFile} 「myDBFile」 ファイルを除外します。
コメント	FILEPATH # コメント	除外の定義にコメントを追加します。	C:\Documents\abc.doc #This is a comment

ファイル拡張子リストの構文

検索除外	形式	説明	例
ファイル拡張子	EXT	一致する拡張子を持つすべてのファイルと一致します。	doc すべてのディレクトリの「.doc」という拡張子を持つすべてのファイルと一致します。
コメント	EXT # コメント	除外の定義にコメントを追加します。	doc #This a comment

プロセスイメージファイルリストの構文 (リアルタイム検索のみ):

検索除外	形式	説明	例
ファイルパス	FILEPATH	ファイルパスで指定されたプロセスイメージファイルを除外します。	C:\abc\file.exe 「abc」ディレクトリの「file.exe」という名前のファイルのみ除外します。

ネットワークディレクトリを検索する (リアルタイム検索のみ)

Network File System (NFS)、Server Message Block (SMB)、またはCommon Internet File System (CIFS) に存在するネットワーク共有内およびマッピングされているネットワークドライブ内のファイルやフォルダを検索する場合は、[ネットワークディレクトリ検索を有効にする]を選択します。このオプションはリアルタイム検索でのみ使用できます。

注意: GVFS (GNOMEデスクトップで利用できる仮想ファイルシステム) を通じて「~/gvfs」でアクセスされるリソースは、ネットワークドライブではなくローカルリソースとして扱われます。

注意: Windows上でネットワークフォルダをスキャンする場合、ウイルスが検出された場合、エージェントは、いくつかの「きれいな失敗」(失敗を削除)表示される場合がありますイベント。

リアルタイム検索を実行するタイミングを指定する

ファイルの読み取り時、書き込み時、またはそのどちらでもファイルを検索するかを選択します。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[リアルタイム検索] プロパティのオプションを1つ選択します。
3. [OK] をクリックします。

不正プログラムの処理方法を設定する

不正プログラムが検出されたときのDeep Securityの動作を設定します。

- ["不正プログラム修復処理をカスタマイズする" below](#)
- ["不正プログラム検出のアラートを生成する" on page 748](#)
- ["NSXセキュリティタグを適用する" on page 748](#)

不正プログラム修復処理をカスタマイズする

Deep Securityで不正プログラムが検出されると、修復処理が実行されファイルが処理されません。不正プログラムが見つかった場合、Deep Securityが実行できる処理には次の5つがあります。

- 放置: 感染ファイルに何も行わず、そのファイルへのフルアクセスを許可する(不正プログラム対策イベントは依然として記録されます。)

注意: 修復処理の [放置] は、潜在的なウイルスに対しては絶対に使用しないでください。

- 駆除: ファイルへのフルアクセスを許可する前に、感染ファイルを駆除します。駆除できないファイルは、隔離されます。
- 削除: Linuxでは、感染ファイルはバックアップされずに削除されます。Windowsでは、感染ファイルはバックアップされてから削除されます。Windowsのバックアップファイルは、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル]で[表示および復元](#)できます。
- アクセス拒否: この検索処理はリアルタイム検索中にのみ実行されます。Deep Securityは、感染ファイルを開いたり実行しようとしたりする動きを検出すると、すぐにその処理をブロックします。感染ファイルは変更されずにそのままバックアップされます。アクセス拒否の処理がトリガされると、感染ファイルは元の場所に留まります。

注意: リアルタイム検索がに設定されているときには是正処置 拒否アクセス を使用しないでください。書き込み中。書き込み中が選択されている場合、ファイルが書き込まれるとファイルが検索され、拒否アクセスの処理は無効になります。

- 隔離: コンピュータまたはVirtual Appliance上の隔離ディレクトリに感染ファイルを移動します。隔離ファイルは、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル]で[表示および復元](#)できます。

注意: 同じ不正プログラムであっても、Linuxでは「隔離」とマークされ、Windowsでは「削除」とマークされる場合があります。どちらの場合でも、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル]でファイルを[表示および復元](#)できます。

注意: Windowsでは、感染した非圧縮ファイルは隔離されます (.txtファイルなど)。一方、感染した圧縮ファイルは削除されます (.zipファイルなど)。Windowsでは、隔離ファイルと削除ファイル両方のバックアップがあり、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル]でそれらを[表示および復元](#)できません。

Linuxでは、圧縮ファイルであれ非圧縮ファイルであれ、すべての感染ファイルは隔離され、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル]で[表示および復元](#)できます。

不正プログラム検索設定の修復処理は、ほとんどの状況に対応できるように初期設定されています。ただし、Deep Securityで不正プログラムが検出された際に実行する処理はカスタマイズ可能です。トレンドマイクロの推奨処理を使用することも、脆弱性の種類ごとに処理を指定することもできます。

トレンドマイクロの推奨処理は、不正プログラムの各カテゴリ用に最適化された一連の定義済みのクリーンアップ処理です。個々の検出を適切に処理するため、トレンドマイクロの推奨処理での処理は随時調整されます。 ("[トレンドマイクロの推奨処理](#)" [below](#)を参照してください)。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[修復処理] に対して [カスタム] を選択します。
3. 実行する処理を指定します。
 - a. [トレンドマイクロ推奨の修復処理から実行する処理を決定するには、\[トレンドマイクロの推奨処理を使用\]](#) を選択します。
 - b. 脆弱性の種類ごとに処理を指定するには、[\[カスタム処理を使用\]](#) を選択してから、使用する処理を選択します。
4. 潜在的な不正プログラムに対して実行する処理を指定します。
5. [OK] をクリックします。

トレンドマイクロの推奨処理

次の表は、トレンドマイクロの推奨処理を選択した場合に実行される処理の一覧です。

不正プログラムの種類	処理
"ウイルス" on page 727	駆除 。ウイルスを駆除できない場合は、 deleted (Windows) または quarantined (LinuxまたはSolaris) です。この動作には例外があります。LinuxまたはSolarisのクライアントで、「ウイルスの種類」のウイルスが見つかった場合、 へのアクセスは感染ファイルに対して で拒否されます。
"トロイの木馬" on page 727	隔離
"パッカー" on page 728	隔離
"スパイウェア/グレーウェア" on page 728	隔離
CVE攻撃コード	隔離

不正プログラムの種類	処理
アグレッシブ検出ルール	放置 (この設定では、より多くの問題が検出されますが、誤判定も増えるため、初期設定の処理はイベントの発生です)。
"Cookie" on page 729	削除 (リアルタイム検索には適用されません)。
"その他の脅威" on page 730	<p>駆除</p> <p>脅威を駆除できない場合は、次のように処理されます。</p> <ul style="list-style-type: none"> Windowsでは、感染ファイルは削除されますが、必要に応じて、確認および復元することができます。 LinuxまたはSolaris上で へのアクセスが から感染ファイルに拒否されました <p>また、LinuxまたはSolarisのエージェントでは、「Joke」タイプのウイルスが検出された場合、ウイルスはただちに隔離されます。駆除は行われません。</p>
"潜在的な不正プログラム" on page 730	トレンドマイクロの推奨処理

注意: AgentでアップデートサーバまたはRelayからウイルスパターンファイルのアップデートをダウンロードすると、それに応じてトレンドマイクロの推奨処理が変わることがあります。

CVE攻撃コードおよびアグレッシブ検出ルールの詳細については、"[Connected Threat Defenseで使用する不正プログラム検索設定を作成する](#)" on page 763を参照してください。

不正プログラム検出のアラートを生成する

Deep Securityによる不正プログラムの検出時に、アラートを生成できます。

- 不正プログラム検索設定のプロパティを開きます。
- [一般] タブで、[アラート] に対して [この不正プログラム検索設定でイベントが記録されたときにアラートを発令する] を選択します。
- [OK] をクリックします。

NSXセキュリティタグを適用する

Deep Securityでは、不正プログラムの脅威が検出された際に、保護対象の仮想マシンにNSXセキュリティタグを適用できます。詳細については、"[NSXセキュリティタグを適用するように不](#)

[正プログラム対策を設定する](#) on page 366を参照してください。

ファイルのハッシュダイジェストにより不正プログラムファイルを特定する

Deep Securityでは、不正プログラムファイルのハッシュ値を計算して、[イベントとレポート]→[イベント]→[不正プログラム対策イベント] 画面に表示できます。一部の不正プログラムには複数の異なる名前が使用されていることがあるため、不正プログラムを一意に識別するハッシュ値が役立ちます。ハッシュ値は、他のソースでその不正プログラムに関する情報を確認する場合に使用できます。

1. 設定するポリシーエディタまたはコンピュータエディタを開きます。
2. [不正プログラム対策]→[詳細] の順にクリックします。
3. [ファイルハッシュ計算] で、[初期設定] または [継承] チェックボックスをオフにします (ルートポリシーの場合は [初期設定] が表示され、子ポリシーの場合は [継承] が表示されます)。

注意: [継承] チェックボックスがオンになっている場合、ファイルハッシュ設定は現在のポリシーの親ポリシーから継承されます。

注意: [初期設定] チェックボックスがオンになっている場合、Deep Securityはハッシュ値を計算しません。

4. [すべての不正プログラム対策イベントのハッシュ値を計算する (SHA1は初期設定で計算)] を選択します。
5. 初期設定では、Deep SecurityはSHA-1ハッシュ値を生成します。追加のハッシュ値を生成するには、[MD5]または[SHA256]、あるいはその両方を選択します。
6. ハッシュ値を計算する不正プログラムファイルの最大サイズを変更することもできます。初期設定では128MBを超えるファイルはスキップされますが、この値を64~512MBの任意の値に変更できます。

コンピュータで通知を設定する

WindowsベースのAgentでは、不正プログラム対策モジュールおよびWebレピュテーションモジュールに関連するDeep Securityの実行が必要な処理を警告する通知メッセージが画面に表示されることがあります。たとえば、「A reboot is required for Anti-Malware cleanup task」というメッセージが表示されることがあります。ダイアログボックスで [OK] をクリックしてメッセージを消去する必要があります。

このような通知を表示しないようにするには、次のように設定します。

1. **コンピュータエディタまたはポリシーエディタ¹**に移動します。
2. 左側にある [設定] をクリックします。
3. [一般] タブで、[通知] セクションまでスクロールします。
4. [ホストのすべてのポップアップ通知を抑制] を [はい] に設定します。オフにしても、メッセージはDeep Security Managerのアラートやイベントとして表示されます。Notifierの詳細については、"[Deep Security Notifier](#)" on page 578を参照してください。

不正プログラム対策のパフォーマンスのヒント

Deep Security Agentでのシステムリソースの使用を改善するには、パフォーマンスに関連する次の設定をベストプラクティスに従って最適化します。

関連項目:

- "[不正プログラム対策の例外の作成](#)" on page 785
- "[ファイルのハッシュダイジェストにより不正プログラムファイルを特定する](#)" on the [previous page](#)
- "[NSXセキュリティタグの設定](#)" on page 365

ディスク使用量を最小限に抑える

検出した不正プログラムファイルを保存するために適切なディスク容量を確保します。確保した容量は、物理コンピュータ、仮想マシン、Deep Security Virtual Applianceを含むすべてのコンピュータにグローバルに適用されます。この設定は、ポリシーレベルおよびコンピュータレベルでオーバーライドできます。

ヒント: 検出ファイルを保存するための十分な空き領域がない場合は、アラートが発令されません。

1. 設定するポリシーエディタまたはコンピュータエディタを開きます。
2. [不正プログラム対策]→[詳細] の順にクリックします。
3. [検出ファイル] の [初期設定] をクリアします。
4. [検出ファイルの保存に使用される最大ディスク容量] ボックスに使用するディスク容量を指定します。
5. [保存] をクリックします。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Deep Security Virtual Applianceを使用して仮想マシンを保護している場合は、保護対象の仮想マシンからのすべての検出ファイルがVirtual Applianceに格納されます。そのため、Virtual Appliance上で検出ファイル用のディスク容量を増やす必要があります。

["Virtual Applianceの検索キャッシュ" on page 899](#)も参照してください。

CPU使用率を最適化する

- データベース、Microsoft Exchange検出ファイル、ネットワーク共有など、一般に安全であることがわかっていてI/Oが高いファイルをリアルタイム検索から除外します (Windowsの場合は、[procmon](#)を使用してI/Oの高いファイルを検出できます)。"[検索除外" on page 739](#)を参照してください。
- ネットワークディレクトリは検索しないでください。"[ネットワークディレクトリを検索する \(リアルタイム検索のみ\)" on page 745](#)を参照してください。
- コンピュータとTrend Micro Smart Protection NetworkまたはSmart Protection Serverとのネットワーク接続が不安定である場合は、[スマートスキャン]を使用しないでください。"[Deep SecurityのSmart Protection" on page 774](#)を参照してください。
- [CPU使用率]を [中] (推奨、ファイル検索の間に一時停止) または [低] (ファイル検索の間に「中」よりも長い時間一時停止) に設定して、不正プログラム検索がCPUに与える影響を軽減します。
 - a. 不正プログラム検索設定のプロパティを開きます。
 - b. [詳細] タブで、検索を実行中の [CPU使用率] を選択します。
 - c. [OK] をクリックします。
- CPUリソースに空きが出た場合に検索を実行する予約タスクを作成します。"[Deep Security予約タスクの設定" on page 479](#)を参照してください。
- [仮想マシンの検索キャッシュ] で、[リアルタイム検索キャッシュの設定] を選択します。検索を頻繁に実行しない場合は、[期限] を引き上げます (頻繁な検索を回避します)。"[Virtual Applianceの検索キャッシュ" on page 899](#)を参照してください。
- すべてのコンピュータではなく1台のVirtual ApplianceのCPUだけが消費されるように、Agentレスの配信を使用します。"[Agentレスによる保護またはコンバインモードの保護の選択" on page 315](#)を参照してください。
- [検索するファイルの最大サイズ]、[ファイルを解凍する最大圧縮レイヤ]、[解凍した個別ファイルの最大サイズ]、[解凍するファイルの最大数]、および [検索するOLE層] の値を引き下げるか、低い初期設定値のままにします。"[特定の種類の不正プログラムを検索する" on page 736](#)を参照してください。

警告: ほとんどの不正プログラムはサイズが小さく、ネストされた圧縮ファイルは不正プログラムであることを示唆しています。ただし、大きなファイルを検索から除外した場合、一部の不正プログラムが検出されないリスクがわずかながら生じます。このリスクは、変更監視などの他の機能で軽減できます。以下を参照してください。

- 手動検索および予約検索ではマルチスレッド処理を使用します (リアルタイム検索では、初期設定でマルチスレッド処理が使用されます)。マルチスレッド処理は、マルチスレッド機能をサポートしているシステムでのみ効果があります。この設定を適用するには、有効にした後にコンピュータを再起動します。

注意: 次の場合はマルチスレッド処理を有効にしないでください。

- リソースに限りがある場合 (CPUバウンドのタスクなど)
- リソースを保持するオペレータを1つに限定する場合 (IOバウンドのタスクなど)

- a. [ポリシー] をクリックします。
- b. マルチスレッド処理を有効にするポリシーをダブルクリックして開きます。
- c. [不正プログラム対策]→[詳細] の順にクリックします。
- d. [不正プログラム検索用のリソース割り当て] セクションで、[はい] を選択します。
- e. マルチスレッド処理を有効にしたコンピュータを再起動して、この設定を有効にします。

注意: マルチスレッド処理を有効にすると、コンピュータの他のプロセスに使用できるCPUコアの数が一時的に少なくなることがあります。

RAM使用率を最適化する

- [検索するファイルの最大サイズ]、[ファイルを解凍する最大圧縮レイヤ]、[解凍した個別ファイルの最大サイズ]、[解凍するファイルの最大数]、および [検索するOLE層] の値を引き下げるか、低い初期設定値のままにします。"[特定の種類の不正プログラムを検索する](#)" on page 736を参照してください。

警告: ほとんどの不正プログラムはサイズが小さく、ネストされた圧縮ファイルは不正プログラムであることを示唆しています。ただし、大きなファイルを検索から除外した場合、一部の不正プログラムが検出されないリスクがわずかながら生じます。このリスクは、変更監視などの他の機能で軽減できます。"[変更監視の設定](#)" on page 887を参照してください。

- Agentレスの配信を使用します (すべてのコンピュータではなく1台のVirtual ApplianceのRAMだけが消費されます)。"Agentレスによる保護またはコンバインモードの保護の選択" on page 315を参照してください。

Windows Server 2016へのDeep Security不正プログラム対策のインストール後のWindows Defenderの無効化

Windows Server 2016にDeep Security 10.0 Agentの不正プログラム対策モジュールをインストールすると、AgentはWindows Defenderを自動的に無効にしますが、Windows Defenderサービスに関連するすべてのWindowsプロセスが無効になるわけではありません。そのためには、Deep Security不正プログラム対策モジュールのインストール後にWindows Server 2016を再起動する必要があります。Deep Security Agentは、再起動のタイミングを通知するためにWindowsメッセージを表示します。

注意: Agentはコンピュータの警告イベント (「不正プログラム対策保護を完了するためにコンピュータの再起動が必要」) をDeep Security Managerに通知します。このイベントは表示され続けるため、管理者が手動で消去する必要があります。

Windows Defenderが無効の状態です不正プログラム対策モジュールをインストールする

Deep Securityの不正プログラム対策モジュールのインストール前にWindows Defenderを無効にすると、Deep Security AgentにWindowsの再起動メッセージは表示されません。ただし、Deep Securityの不正プログラム対策機能を正しく機能させるには、Windows Server 2016を再起動する必要があります。

Virtual Applianceの検索キャッシュ

検索キャッシュは、仮想マシンの不正プログラム対策および変更監視の検索を最大限に効率化する目的で、Virtual Applianceによって使用されます。検索キャッシュによって、大規模なVMware環境で、複数の仮想マシンから同じ内容を検索する必要性がなくなるため、検索の効率が向上します。検索キャッシュには、Deep Security保護モジュールによって検索されたファイルとその他の検索対象のリストが格納されます。仮想マシン上の検索対象と過去の検索対象が同じであることが確認された場合、その対象はVirtual Applianceによって再度検索されません。エンティティが同じであるかどうかを確認するために使用される属性は、作成時刻、変更時刻、ファイルサイズ、およびファイル名です。リアルタイム検索キャッシュの場合、Deep Securityはファイルの内容の一部を読み取り、2つのファイルが同じであるかどうかを確認しま

す。ファイルの更新シーケンス番号 (USN、Windowsのみ) を使用するオプション設定もありますが、その設定はクローン作成された仮想マシン以外には使用しないでください。

検索キャッシュによって、クローン作成された仮想マシン間または類似した仮想マシン間で検索結果が共有されるため、変更監視が効率化されます。

後続の検索の速度が向上するため、クローン作成された仮想マシンまたは類似した仮想マシンでの不正プログラムの検索が効率化されます。

また、クローン作成された仮想マシンまたは類似した仮想マシンの起動プロセス検索とアプリケーションアクセス検索の速度が向上するため、不正プログラムのリアルタイム検索が強化されます。

検索キャッシュ設定

検索キャッシュ設定は、有効期限、更新シーケンス番号 (USN)、除外するファイル、含めるファイルなどを指定する設定の集まりです。

注意: 同じ検索キャッシュ設定を使用する仮想マシン間では、同じ検索キャッシュが共有されます。

既存の検索キャッシュ設定のリストを表示するには、[管理]→[システム設定]→[詳細]→[検索キャッシュ設定]の順に進み、[検索キャッシュ設定の表示]をクリックします。Deep Securityには、事前に設定された検索キャッシュの初期設定がいくつか用意されています。これらの設定は、保護する仮想マシンのプロパティと実行する検索の種類に応じて、Virtual Applianceによって自動的に実装されます。

[期限]では、個々のエントリを検索キャッシュに保存する期間を指定します。推奨される初期設定は、手動/予約による不正プログラム検索で1日、不正プログラムのリアルタイム検索で15分、変更監視の検索で1日です。

[USNの使用 (Windowsのみ)]では、Windows NTFSの更新シーケンス番号を使用するかどうかを指定します。更新シーケンス番号は、個々のファイルへの変更を記録するための番号です。このオプションは、クローン作成された仮想マシンにのみ設定してください。

[含めるファイル]と[除外するファイル]では、検索キャッシュに含める、または検索キャッシュから除外するファイルの正規表現パターンとリストを指定します。検索対象のファイルは、まず含めるリストに対して照合されます。

個々のファイルとフォルダは名前でも識別できます。また、ワイルドカード (「*」および「?」) を使用して、1つの正規表現で複数のファイルや場所を参照することもできます(ゼロ個以上の任意の文字を表すには「*」を、任意の1文字を表すには「?」を使用します)。

注意: 含めるリストと除外リストによって、ファイルの検索に検索キャッシュを使用するかどうかが決まります。ただし、これらのリストを使用することによって、ファイルを従来の方法で検索できなくなるわけではありません。

不正プログラム検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ¹**を開き、[不正プログラム対策]→[詳細]→[仮想マシンの検索キャッシュ]の順に進みます。ここで、不正プログラムのリアルタイム検索に使用する検索キャッシュ設定と、手動/予約検索に使用する検索キャッシュ設定を選択できます。

変更監視の検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ²**を開き、[変更監視]→[詳細]→[仮想マシンの検索キャッシュ]の順に進みます。

検索キャッシュの管理設定

検索キャッシュの管理設定では、検索キャッシュの実行に関する設定ではなく、Virtual Applianceによる検索キャッシュの管理方法を指定します。そのため、検索キャッシュの管理設定は、検索キャッシュ設定と別になっています。検索キャッシュの管理設定は、ポリシーレベルで制御されます。検索キャッシュの管理設定を表示するには、**ポリシーエディタ³**を開き、[設定]→[一般]→[Virtual Appliance]の順に進みます。

同時検索の最大数: Virtual Applianceによって同時に実行される検索の数を指定します。推奨される数は5です。この数が10を超えると、検索のパフォーマンスが低下する可能性があります。検索要求はVirtual Applianceで処理待ちの状態となり、到着順に実行されます。この設定は、手動/予約検索にのみ適用されます。

不正プログラムの手動検索キャッシュの最大エントリ数: 不正プログラムの手動検索または予約検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100 MBです。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

³ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

不正プログラムのリアルタイム検索キャッシュの最大エントリ数: 不正プログラムのリアルタイム検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100MBです。

変更監視の検索キャッシュの最大エントリ数: 変更監視のベースラインデータに含めるエンティティの最大数を指定します。エンティティが20万個の場合、使用されるメモリは約100MBです。

初期設定を変更する場合の考慮事項

検索キャッシュは、同じファイルを再度検索しないことを目的としています。Deep Securityでは、同じファイルであるかどうかを確認するために、すべてのファイルの内容全体を調べることはありません。設定によっては、Deep SecurityでファイルのUSN値をチェックすることもできますが、リアルタイム検索中は、ファイルの内容の一部を読み取り、通常はそのファイル属性を調べることによって、同じファイルであるかどうかを確認します。不正プログラムがファイルに変更を加えた後、それらのファイル属性を変更前の状態に復元することは困難ですが、不可能ではありません。

Deep Securityでは、初期設定でキャッシュの有効期限を短くすることによって、この潜在的な脆弱性を軽減しています。セキュリティを強化するために、キャッシュの有効期限をさらに短くしたり、USNを使用することもできますが、これによってパフォーマンスの向上率が低下したり、より大きなキャッシュの設定が必要になることがあります。特定の仮想マシンに最高レベルのセキュリティを提供し、他から切り離して検索結果を共有しないようにするには、該当する仮想マシン専用のポリシーを作成して、それらが別のゾーンで管理されるようにします。この方法は、異なる部門または組織間で同じインフラストラクチャを共有する場合に適しています(マルチテナントのDeep Security Managerを使用している場合は、この設定が自動的に各テナントに適用されます)。

VDI環境など、ESXiホストあたりのゲスト仮想マシン数が非常に多い場合は、検索中のディスクI/OとCPU使用率を監視してください。検索に時間がかかりすぎる場合は、キャッシュのサイズを増やすか、パフォーマンスが改善されるまで検索キャッシュの管理設定を調整します。キャッシュのサイズを増やす場合は、Deep Security Virtual Applianceシステムメモリの調整も必要になることがあります。

機械学習型検索を使用した脅威の検出

注意: 機械学習型検索はDeep Security Agent 11.0以降でサポートされています。この機能をサポートするプラットフォームの詳細については、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。

機械学習型検索を使用して、不明または感染率の低い不正プログラムを検出します(詳細については、"[機械学習型検索](#)" on page 726参照してください)。

機械学習型検索では、高度な脅威検索エンジン (ATSE) を使用して、ファイルの特徴を抽出し、Trend Micro Smart Protection Network上の機械学習型検索エンジンにレポートを送信します。機械学習型検索を有効にするには、次の手順を実行します。

1. "[インターネットに接続されていることを確認する](#)" below
2. "[機械学習型検索を有効にする](#)" below

すべての不正プログラム検出と同様に、機械学習型検索では不正プログラムが検出されると、イベントがログに記録されます("[Deep Securityのイベント](#)" on page 1116を参照してください)。誤検出の場合の例外も作成できます("[不正プログラム対策の例外の作成](#)" on page 785を参照してください)。

インターネットに接続されていることを確認する

機械学習型検索では、Global Censusサービス、Good File Reputationサービス、および機械学習型検索サービスにアクセスする必要があります。これらのサービスは、Trend Micro Smart Protection Networkにホストされています。Deep Security AgentまたはVirtual Applianceが直接インターネットにアクセスできない場合は、"[インターネットにアクセスできないエージェントを設定する](#)" on page 413を参照して、この問題を回避してください。

機械学習型検索を有効にする

機械学習型検索は、ポリシーまたは個々のコンピュータに適用されるリアルタイム検索設定の一環として設定されます("[不正プログラム検索の設定](#)" on page 733を参照してください)。検索設定を行ったら、ポリシーまたはコンピュータに適用します。

注意: 機械学習型検索では、リアルタイム検索で検索対象に設定されたファイルおよびディレクトリのみが保護されます。"[検索対象ファイルを指定する](#)" on page 738を参照してください。

次の設定は、Windowsコンピュータのリアルタイム検索設定にのみ適用できます。

1. [ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] に移動します。
2. 設定するリアルタイム検索設定を選択して、[詳細] をクリックします。

必要に応じて、新しいリアルタイム検索設定も作成できます。

3. [一般] タブの [機械学習型検索] で、[機械学習型検索の有効化] を選択します。

4. [OK] をクリックします。
5. 検索設定を適用するポリシーまたはコンピュータのエディタを開いて、[不正プログラム対策]→[一般] の順に選択します。
6. [不正プログラム対策のステータス] が [オン] または [継承 (オン)] になっていることを確認します。
7. [リアルタイム検索] セクションで、不正プログラム検索設定を選択します。
8. [保存] をクリックします。

Connected Threat Defenseを使用した脅威の検出

今日のデータセンターでは、フィッシングやスパイフィッシングなどの手法を用いた標的型攻撃によるセキュリティ侵害が増えています。これらのケースでは、不正プログラム作成者は特定の環境を標的にした不正プログラムを作成することによって、従来の不正プログラム Scanner を回避します。Deep Security の Connected Threat Defense 機能は、新しい脅威に対する不正プログラム対策保護を強化します。

注意: FIPS モードが有効な場合、Connected Threat Defense は使用できません。"[FIPS 140-2 のサポート](#)" on page 1457 を参照してください。

このトピックの内容:

- ["Connected Threat Defense の仕組み"](#) on the next page
- ["Connected Threat Defense の前提条件を確認する"](#) on the next page
- ["Deep Discovery Analyzer への接続をセットアップする"](#) on page 760
- ["Trend Micro Apex Central への接続をセットアップする"](#) on page 762
- ["Connected Threat Defense で使用する不正プログラム検索設定を作成する"](#) on page 763
- ["コンピュータで Connected Threat Defense を有効にする"](#) on page 764
- ["分析のためにファイルを Deep Discovery へ手動で送信する"](#) on page 765
- ["誤ったアラームを引き起こしたファイルを許可する"](#) on page 765
- ["不審なファイルに対する検索処理を設定する"](#) on page 765
- ["Deep Security で不審オブジェクトリストをアップデートする"](#) on page 766
- ["マルチテナント環境で Connected Threat Defense を設定する"](#) on page 766
- ["サポートされているファイルタイプ"](#) on page 766

不正プログラム対策モジュールの概要については、"[不正プログラムの防止](#)" on page 722を参照してください。

Connected Threat Defenseの仕組み

1. すべてのコンポーネントが適切に設定されている場合、Deep Security Agentはヒューリスティック検出を使用して、保護されているコンピュータ上のファイルを分析し、それらが不審なファイルであるかどうかを判断します。
2. 必要に応じて、Deep SecurityからDeep Discovery Analyzerへ手動または自動で不審なファイルを送信できます。Deep Discovery Analyzerは、受け取ったファイルをサンドボックス(分離され、保護されている仮想環境)で実行して挙動を検証します。
3. Deep Security Managerが、Deep Discovery Analyzerからサンドボックス分析の結果を受け取ります。

注意: サンドボックス分析レポートが保護を提供するわけではなく、Deep Discovery分析に関する情報が記載されているだけにすぎません。保護を実行するためには、Apex Centralへの接続が必要です。このレポートは、Deep Discovery Analyzerから15分ごとに取得されます。

4. Deep Discovery Analyzerが分析結果をApex Centralにプッシュします。Apex Centralでは、分析に基づいてファイルに対する処理を指定できます。処理が指定されると、「不審オブジェクトリスト」と呼ばれる新しい脅威のリストが作成またはアップデートされます。Deep Discovery InspectorやDeep Discovery Email Inspectorなどの他のトレンドマイクロ製品もApex Centralに接続してこのリストをアップデートできます。
5. 必要に応じて、Deep Security ManagerでApex Centralから不審オブジェクトリストを取得し、Deep Security Agentに送信するように設定できます。

Connected Threat Defenseの前提条件を確認する

Deep SecurityをDeep Discoveryに接続する前に、環境が次の要件を満たしていることを確認してください。

- Deep Security Managerがインストールされ、Deep Security AgentまたはDeep Security Agentによって保護されたコンピュータ、あるいはその両方が設定されている。

オプション:

- Deep Discovery Analyzer 5.5がインストールされ、サンドボックス仮想マシンがプロビジョニングされている。

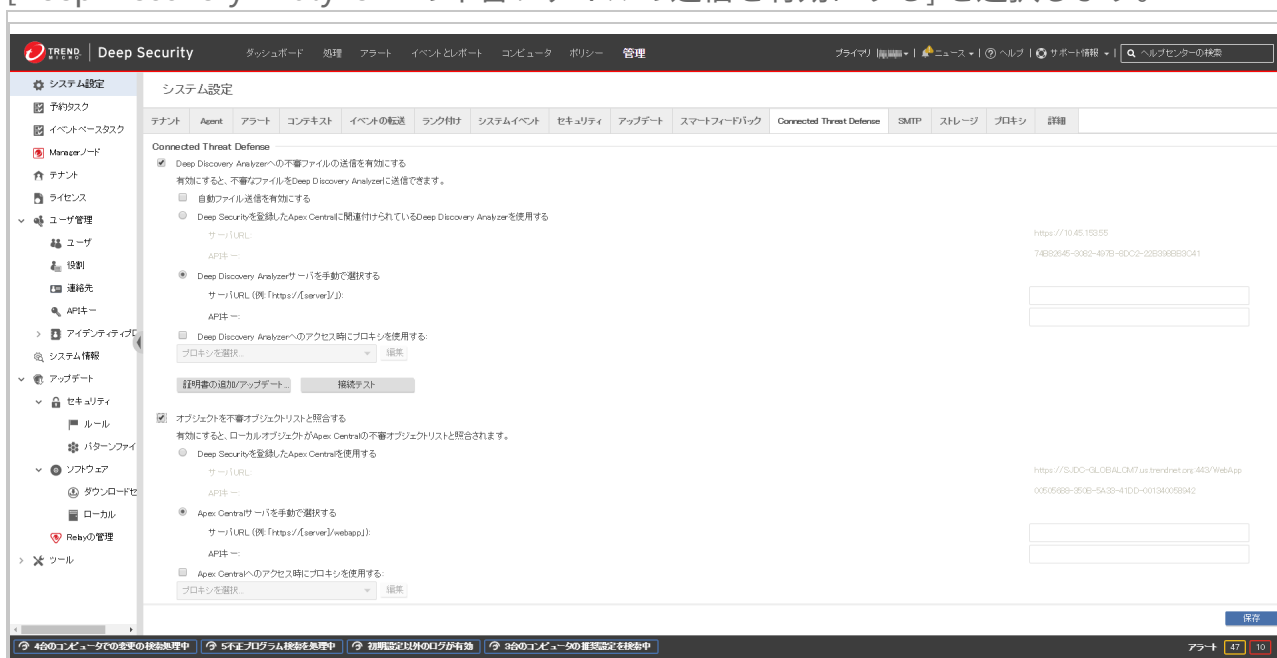
- Trend Micro Apex Central 2019以降がインストールされている。
- Apex Centralの管理対象サーバにDeep Discovery Analyzerが追加されている。詳細については、Apex Centralのドキュメントを参照してください。

Deep Discovery Analyzerへの接続をセットアップする

Deep Security ManagerからDeep Discovery Analyzerに分析用の不審なファイルを送信する場合は、接続を設定する必要があります。

Apex CentralがすでにDeep Securityを管理している場合:

1. Deep Security Managerで、[管理]→[システム設定]→[Connected Threat Defense]に進みます。
2. [Deep Discovery Analyzerへの不審ファイルの送信を有効にする]を選択します。



3. Deep Security Managerでファイルを自動的にDeep Discovery Analyzerに送信するには、[自動ファイル送信を有効にする]を選択します。

注意: Deep Discovery Analyzerへの自動送信は15分ごとに発生し、1回の送信で最大100個のファイルが送信されます。

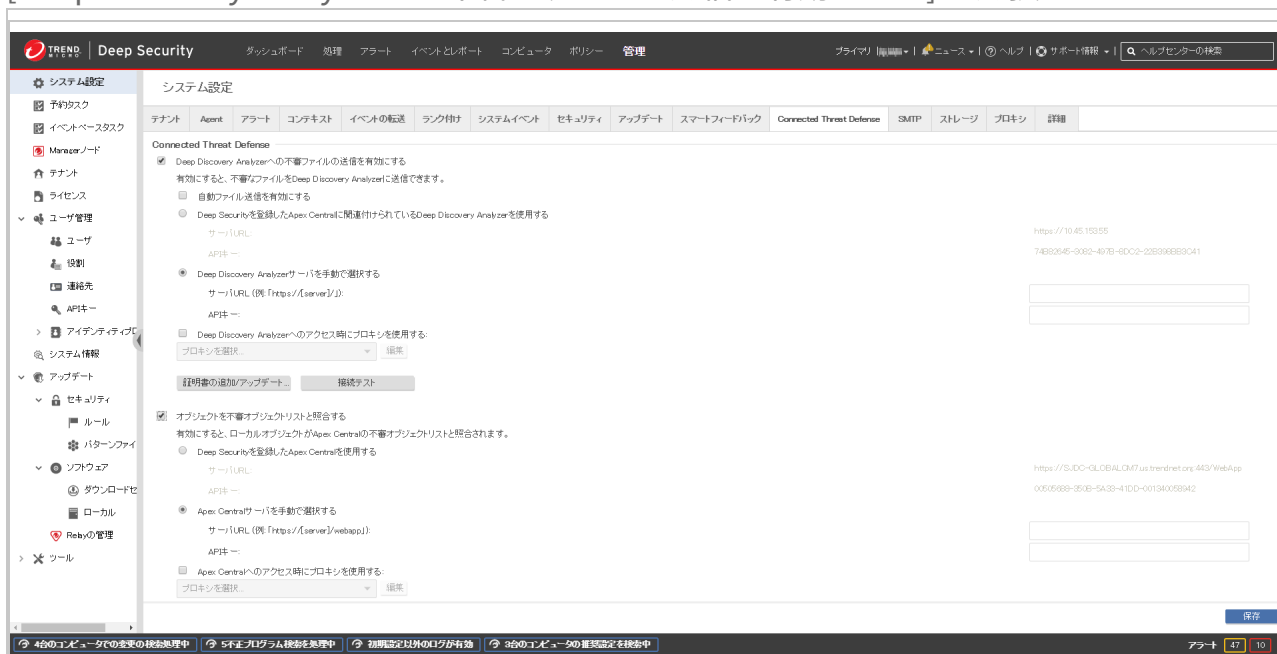
4. [Deep Securityを登録したApex Centralに関連付けられているDeep Discovery Analyzerを使用する]を選択します。
5. [接続テスト]をクリックします。証明書が見つからないかまたは無効であるためにDeep Securityが接続できないというエラーが表示される場合は、[証明書の追加/アップデート]

をクリックし、正しいDeep Discovery Analyzer証明書にアップデートします。

6. [保存] をクリックします。

Apex CentralがまだDeep Securityを管理していない場合:

1. Deep Discovery Analyzerで、[ヘルプ]→[バージョン情報] に進み、サーバURLとAPIキーを確認します。これらの値は後で必要になるため、テキストファイルにコピーしてください。
2. Deep Security Managerで、[管理]→[システム設定]→[Connected Threat Defense] に進みます。
3. [Deep Discovery Analyzerへの不審ファイルの送信を有効にする] を選択します。



4. Deep Security Managerでファイルを自動的にDeep Discovery Analyzerに送信するには、[自動ファイル送信を有効にする] を選択します。

注意: Deep Discovery Analyzerへの自動送信は15分ごとに発生し、1回の送信で最大100個のファイルが送信されます。

5. [Deep Discovery Analyzerサーバを手動で選択する] を選択し、手順1で確認したサーバURLとAPIキーを入力します。
6. [接続テスト] をクリックします。証明書が見つからないかまたは無効であるためにDeep Securityが接続できないというエラーが表示される場合は、[証明書の追加/アップデート] をクリックし、正しいDeep Discovery Analyzer証明書にアップデートします。
7. [保存] をクリックします。

Trend Micro Apex Centralへの接続をセットアップする

以下の設定を行うと、Deep Security ManagerでApex Centralから不審オブジェクトリストを取得し、保護されているコンピュータで共有して、ローカルオブジェクトをApex Centralの不審オブジェクトリストと照合できるようになります。

Apex CentralがすでにDeep Securityを管理している場合に接続をセットアップする

1. Deep Security Managerで、[管理]→[システム設定]→[Connected Threat Defense]に進みます。
2. [オブジェクトを不審オブジェクトリストと照合する]を選択します。



3. [Deep Securityを登録したApex Centralを使用する]を選択します。このオプションを利用できない場合、Apex CentralがまだDeep Securityを管理していないため、代わりに **"Apex CentralがまだDeep Securityを管理していない場合に接続をセットアップする"** on the next pageの手順に従う必要があります。
4. [接続テスト]をクリックします。証明書が見つからないかまたは無効であるためにDeep Securityで接続できないというエラーが表示される場合は、[証明書の追加/アップデート]をクリックし、正しいApex Central証明書にアップデートします。
5. [保存]をクリックします。

Apex CentralがまだDeep Securityを管理していない場合に接続をセットアップする

1. Trend Micro Apex Centralで、[Administration]→[Managed Servers]→[Server Registration]→[]の順に選択します。



2. [サーバの種類]の[]ドロップダウンメニューからDeep Securityを選択します。
3. Deep SecurityをApex Centralサーバに登録するには、[Add]をクリックします。

注意: Deep Securityの登録に必要な サービスURL および APIキー は、管理下の製品として追加されてから10分以内に自動的に転送されます。

Connected Threat Defenseで使用する不正プログラム検索設定を作成する

以下の設定を行うと、Deep Securityで不審なファイルを検出してバックアップし、詳細な分析のため自動的にDeep Discovery Analyzerに送信できるようになります。

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定]の順に選択します。
2. 新しい検索設定を作成するか、または既存の設定を編集します。
3. [一般] タブの [ドキュメントの脆弱性対策] で、[ドキュメントの脆弱性を突いた攻撃コードを検索する] を選択し、次のいずれかのオプションを選択します。
 - 既知の脆弱性に対する攻撃コードのみを検索する: 既知の重大な脆弱性のみを検出します。CVE攻撃コードの脆弱性タイプはこのオプションに関連付けられています ("[不正プログラム修復処理をカスタマイズする](#)" on page 745を参照してください)。

- 既知の脆弱性に対する攻撃に加え、未知の攻撃コードも積極的に検索する: より多くの問題が検出されますが、誤判定も増えます。不審なファイルを検出してDeep Discovery Analyzerに送信する場合は、このオプションを選択する必要があります。アグレッシブ検出ルールの脆弱性タイプはこのオプションに関連付けられています("不正プログラム修復処理をカスタマイズする" on page 745を参照してください)。
4. "不正プログラム検索の設定" on page 733の説明に従って、他の不正プログラム検索オプションを設定します。

コンピュータでConnected Threat Defenseを有効にする

Connected Threat Defenseは、ポリシーで有効にすることも、コンピュータごとに有効にすることもできます。

1. **コンピュータエディタまたはポリシーエディタ**¹で、[不正プログラム対策]→[一般]の順に選択します。
2. [不正プログラム対策のステータス]が[オン]または[継承(オン)]であることを確認します。
3. [一般]タブには、[リアルタイム検索]、[手動検索]、および[予約検索]の各セクションがあります。それぞれの検索の種類については、"**不正プログラム対策の有効化と設定**" on page 730を参照してください。該当するセクションで、[不正プログラム検索設定]リストから上記の手順で作成した検索設定を選択します。
4. [Connected Threat Defense]タブに移動し、必要に応じて以下の設定を調整します。
 - Deep SecurityからDeep Discovery Analyzerに不審なファイルを送信する場合は、[サンドボックス分析]の下にあるオプションを[はい]または[継承(はい)]に設定します。
 - Deep SecurityとApex Central間の接続がセットアップされており、Apex Centralの不審オブジェクトリストを使用して不正なファイルを検出する場合は、[不審オブジェクトリスト]の下にある[Apex Centralの不審オブジェクトリストを使用する]を[はい]または[継承(はい)]に設定します。
5. [保存]をクリックします。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

分析のためにファイルをDeep Discoveryへ手動で送信する

[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル] 画面に表示されるファイルを手動で送信できます。

1. 送信するファイルを選択し、[分析] ボタンをクリックします。
2. 表示されるウィザードの手順に従います。
3. ファイルが送信された後に、[検出ファイル] 画面の [送信ステータス] 列で分析の進捗状況を確認できます。
4. 分析が完了すると、[送信ステータス] 列が「レポートの準備完了」になります。[レポートの準備完了] リンクをクリックすると、詳細を確認できます。

誤ったアラームを引き起こしたファイルを許可する

[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル] 画面で不正プログラムと判定されたファイルが不正プログラムでないことがわかっている場合は、**コンピュータエディタまたはポリシーエディタ**¹の [不正プログラム対策]→[詳細] タブで [ドキュメントの脆弱性対策ルールの例外] リストに追加できます。

ファイルを許可するには、ファイルを右クリックして [許可] をクリックし、表示されるウィザードの手順に従います。

不審なファイルに対する検索処理を設定する

Apex Centralコンソールで不審オブジェクトリストを表示し、不審なオブジェクトが検出された場合に実行する処理 (ログ、ブロック、または隔離) を設定できます (.)の設定の詳細については、[不審オブジェクトリスト管理](#)を参照してください。Apex Centralから不審オブジェクトリストを取得するようにDeep Security Managerを設定している場合、Deep Securityで不審なオブジェクトが検出されると、指定した処理がDeep Securityで実行されます。

注意: Deep Securityでは、ファイルが不審なオブジェクトがサポートされます。Webレピュテーション保護モジュールがTrend Micro Smart Protection Serverを使用するように設定されている場合、URL不審オブジェクトもサポートされます。IPが不審なオブジェクトとドメインが不審なオブジェクトはサポートされません。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Deep Securityで不審オブジェクトリストをアップデートする

Apex Centralで不審なオブジェクトの分析が完了し、ファイルに対する処理を設定した後、Deep SecurityでApex Centralの不審オブジェクトリストを使用してコンピュータを保護できます。Deep Security Managerで手動で不審ファイルリストをアップデートするには、[管理]→[アップデート]→[セキュリティ]に進み、[不審オブジェクトリストのアップデート]列の項目を使用して最新のリストを取得し、保護されたコンピュータに送信します。アップデートされたリストがないかを定期的に確認する予約タスクを作成することもできます ("[Deep Security予約タスクの設定](#)" on page 479を参照してください)。

注意: Apex Centralにおける不審オブジェクトの初期設定は「ログ」です。この初期設定は、必要に応じて「隔離」または「ブロック」に変更できます。

Deep Securityで不審オブジェクトリストがアップデートされ、指定した処理でコンピュータポリシーがアップデートされた後、Deep Security Agentで該当するコンピュータが確認され、保護されたコンピュータ上で同じファイルが再び検出された場合に常に同じ処理が実行されるようになります。

マルチテナント環境でConnected Threat Defenseを設定する

マルチテナント環境では、プライマリテナント (t0) のDeep Discovery AnalyzerおよびApex Centralの設定を他のテナントと共有するかどうかを選択できます。[管理]→[システム設定]→[テナント]→[プライマリテナントのTrend Micro Apex CentralおよびDeep Discovery Analyzerサーバの設定の使用をテナントに許可]で設定します。

- この設定が有効になっている場合、テナントで [管理]→[システム設定]→[Connected Threat Defense] に移動すると、[初期サーバ設定を使用する] チェックボックスが表示されます。このチェックボックスをオンにすると、プライマリテナントの設定が使用されます。[初期サーバ設定を使用する] チェックボックスがオフの場合は、各テナントでConnected Threat Defenseの設定を独自に設定できます。
- この設定が無効になっている場合、テナントでConnected Threat Defenseを使用するには、Apex CentralおよびDeep Discovery Analyzerを各テナントで独自に設定する必要があります。

サポートされているファイルタイプ

Deep Securityでは、次のファイルタイプをDeep Discovery Analyzerに送信できます。

- doc - Microsoft Word文書
- docx - Microsoft Office Word 2007文書
- gul - JungUm Global文書
- hwp - Hancm Hangul Word Processor (HWP) 文書
- hwpX - Hancm Hangul Word Processor 2014 (HWPX) 文書
- jar - JavaアプレットJavaアプリケーション
- js - JavaScriptファイル
- jse - JavaScriptエンコード済みスクリプトファイル
- jtd - JustSystems一太郎ドキュメント
- lnk - Microsoft Windowsシェルバイナリ形式リンクショートカット
- mov - Apple QuickTimeメディア
- pdf - Adobeポータブルドキュメントフォーマット (PDF)
- ppt - Microsoft PowerPointプレゼンテーション
- pptx - Microsoft Office PowerPoint 2007プレゼンテーション
- ps1 - Microsoft Windows PowerShellスクリプトファイル
- rtf - Microsoftリッチテキスト形式 (RTF) 文書
- swf - Adobe Shockwave Flashファイル
- vbe - Visual Basicエンコード済みスクリプトファイル
- vbs - Visual Basicスクリプトファイル
- xls - Microsoft Excel表計算ファイル
- .xlsx - Microsoft Office Excel 2007表計算ファイル
- xml - Microsoft Office 2003 XMLファイル

挙動監視による不正プログラム/ランサムウェア検索の強化

Deep Securityには、Deep Security Agentで保護されているWindowsコンピュータに適用することで、不正プログラムとランサムウェアの検出率と駆除率の向上を実現するセキュリティ設定が用意されています。この設定を適用すると、パターンファイルとの照合による不正プログラムの検出にとどまらず、パターンファイルにまだ追加されていない新たな不正プログラムを含んでいる可能性がある不審なファイル (ゼロデイ攻撃) も特定できます。

このトピックの内容:

- ["強化された検索で実現される保護" below](#)
- ["強化された検索を有効にする方法" below](#)
- ["強化された検索で問題が検出された場合の動作" on page 770](#)
- ["Agentをインターネットに直接接続できない場合の対処" on page 774](#)

不正プログラム対策モジュールの概要については、["不正プログラムの防止" on page 722](#)を参照してください。

強化された検索で実現される保護

脅威の検出: 不正プログラムの中には、検出を逃れるために、システムファイルや既知のインストール済みソフトウェアに関連するファイルを変更しようとするものがあります。不正プログラムは正規のファイルに代わって動作するため、多くの場合このような変更が表面化することはありません。Deep Securityでは、システムファイルとインストール済みソフトウェアを監視して、不正な変更を検出して未然に防ぐことができます。

攻撃コード対策: 不正プログラムの作成者は、不正なコードをユーザモードのプロセスにフックすることで、信頼されたプロセスに特権でアクセスし、不審なアクティビティを隠します。また、DLLインジェクションを通じてユーザプロセスにコードを挿入し、エスカレートされた特権でAPIを呼び出します。さらに、不正なペイロードを挿入してメモリ内でコードの実行をトリガする方法で、ソフトウェアのセキュリティホールに対して攻撃を仕掛けることもあります。Deep Securityの攻撃コード対策機能は、通常とは異なる操作を実行している可能性があるプロセスがないかを監視します。Deep Securityでは、Data Execution Prevention (DEP)、Structured Exception Handling Overwrite Protection (SEHOP)、ヒープスプレー防止などの複数のメカニズムを使用して、プロセスへの感染を判断し、プロセスを終了してさらなる感染を防止します。

拡張されたランサムウェア対策: ランサムウェアは最近ますます巧妙になり、標的を絞り込んだものが増えています。ほとんどの組織では、不正プログラム対策を含むセキュリティポリシーをエンドポイントに適用しており、既知のランサムウェア亜種には対応しています。ただし、新たな亜種の発生を検出して防止するには不十分です。Deep Securityが提供するランサムウェア対策機能は、不正な暗号化や変更からドキュメントを保護します。また、暗号化されたファイルのコピーを作成可能なデータ復元エンジンも組み込まれているため、ファイルがランサムウェアプロセスで暗号化された場合にも復元できる可能性が高くなります。

強化された検索を有効にする方法

強化された検索は、ポリシーまたは個々のコンピュータに適用する不正プログラム対策設定の一部として設定します。不正プログラム対策保護の設定に関する全般的な情報については、["不](#)

[正プログラム対策の有効化と設定](#) on page 730を参照してください。

注意: この設定は、Deep Security Agentで保護されているWindowsコンピュータにのみ適用できます。

警告: 強化された検索は、負荷の高いアプリケーションを実行しているAgentコンピュータのパフォーマンスに影響する可能性があります。強化された検索が有効なDeep Security Agentをインストールする前に、"[不正プログラム対策のパフォーマンスのヒント](#)" on page 750を確認することをお勧めします。

最初に、不正プログラムのリアルタイム検索設定で、強化された検索を有効にします。

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定]の順に選択します。
2. 既存のリアルタイム検索設定をダブルクリックして編集します (不正プログラム検索設定の詳細については、"[不正プログラム検索の設定](#)" on page 733を参照してください)。
3. [一般] タブで以下のオプションを選択します。
 - 不審なアクティビティ/不正な変更 (ランサムウェアを含む) を検出する:前述した脅威の検出、攻撃コード対策、ランサムウェア検出の各機能を有効にします。
 - ランサムウェアによって暗号化されたファイルをバックアップおよび復元する:このオプションを選択すると、ファイルの暗号化がランサムウェアプロセスによるものである場合に備えて、暗号化されたファイルのバックアップコピーが作成されます。
4. [OK] をクリックします。

注意: 初期設定では、リアルタイム検索はすべてのディレクトリを検索するように設定されます。この設定をディレクトリリストの検索に変更すると、強化された検索が想定どおりに機能しない場合があります。たとえば、[検索対象ディレクトリ]を「Folder1」に設定した場合にFolder1でランサムウェアが発生すると、Folder1の外部にあるファイルがランサムウェアによって暗号化された場合、ランサムウェアが検出されない可能性があります。

次に、不正プログラム検索設定をポリシーまたは個々のコンピュータに適用します。

1. **コンピュータエディタまたはポリシーエディタ**¹で、[不正プログラム対策]→[一般]の順に選択します。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

2. [不正プログラム対策のステータス] が [オン] または [継承 (オン)] であることを確認します。
3. [一般] タブには、[リアルタイム検索]、[手動検索]、[予約検索] の各セクションがあります。該当するセクションで、[不正プログラム検索設定] リストから上記の手順で作成した検索設定を選択します。
4. [保存] をクリックします。

強化された検索で問題が検出された場合の動作

有効になっている強化された検索の設定に一致するアクティビティやファイルが検出されると、イベントがログに記録されます ([イベントとレポート]→[イベント]→[不正プログラム対策イベント]) の順に選択するとイベントのリストを表示できます)。このイベントは [主要なウイルスの種類] 列に「不審なアクティビティ」または「不正な変更」として記録され、[対象] 列と [対象の種類] 列に詳細が表示されます。

Deep Securityでは強化された検索の設定に関連するさまざまなチェックが実施され、問題を検出したチェックの種類に基づいて処理が実行されます。実行される処理は、「アクセス拒否」、「終了」、または不審なオブジェクトの「駆除」です。実行される処理はDeep Securityによって決定され、「駆除」以外の処理は変更できません。

- アクセス拒否: 不審なファイルをオープンまたは実行しようとする挙動を検知すると、ただちにその操作をブロックして不正プログラム対策イベントを記録します。
- 終了: 不審な操作を実行したプロセスを終了し、不正プログラム対策イベントを記録します。
- 駆除: 不正プログラム検索設定をチェックし、[処理] タブでトロイの木馬に対して指定されている処理を実行します。トロイの木馬ファイルに対して実行される処理に関連して、1つ以上のイベントが追加で生成されます。

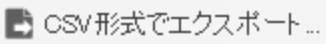



時刻	コンピュータ	感染ファイル	不正プログラム	検索の種類	実行された処理	主要なウイルスの種類	対象	対象の種類
2017-04-10 18:15:14		c:\adc\yadc1.exe	HEU_AEGIS_CRYPT	リアルタイム	終了	不正な変更	複数	ファイルシステム
2017-04-10 18:19:13		C:\test\PolicyID657SelfProp...	TM_MALWARE_BEHAVI...	リアルタイム	駆除	不審なアクティビティ	C:\test\trend...	ファイルシステム

イベントをダブルクリックすると詳細が表示されます。

一般	タグ
一般情報	
コンピュータ:	172.16.122.66
送信元:	Agent
不正プログラム情報	
検出時刻:	2016-08-16 16:31:54
不正プログラム:	TM_MALWARE_BEHAVIOR
感染ファイル:	C:\BM\PolicyID856>CreateProcessPacked.exe
検索の種類:	リアルタイム
実行された処理:	終了
理由:	Default Real-Time Scan Configuration
主要なウイルスの種類:	不審なアクティビティ
挙動監視情報	
対象:	C:\test\trendmicro\594\pit\terminate.exe
対象の種類:	プロセス
<div style="display: flex; justify-content: space-between; align-items: center;"> < 戻る 次へ > 閉じる </div>	

ランサムウェアに関連するイベントの場合は、[対象ファイル] タブが追加で表示されます。

一般	対象ファイル	タグ
一般情報		
コンピュータ:	172.16.122.66	
送信元:	Agent	
不正プログラム情報		
検出時刻:	2016-08-16 14:48:36	
不正プログラム:	HEU_AEGIS_CRYPT	
感染ファイル:	c:\adc\adc1.exe	
検索の種類:	リアルタイム	
実行された処理:	終了	
理由:	Default Real-Time Scan Configuration	
主要なウイルスの種類:	不正な変更	
挙動監視情報		
対象:	複数	
対象の種類:	ファイルシステム	
<p>< 戻る 次へ > 閉じる</p>		

一般	対象ファイル	タグ
対象ファイル情報		
		
攻撃プログラム ▲	対象	復元結果
 c%adc%adc1.exe	c%adc#normalfile#1.zip	成功
 c%adc%adc1.exe	c%adc#normalfile#2.zip	成功
 c%adc%adc1.exe	c%adc#normalfile#3.zip	成功
<input type="button" value="戻る"/> <input type="button" value="次へ"/>		<input type="button" value="閉じる"/>

特定されたファイルを調べて無害であることが判明した場合は、イベントを右クリックして[許可]をクリックし、コンピュータまたはポリシーの検索除外リストにそのファイルを追加します。検索除外リストは、ポリシーエディタまたはコンピュータエディタで [不正プログラム対策]→[詳細]→[挙動監視保護の例外] の順に選択して確認できます。

Agentをインターネットに直接接続できない場合の対処

このトピックで説明した強化された検索機能は、Global Census ServerとGood File Reputation Serviceでファイルをチェックするため、インターネットへのアクセスを必要とします。Deep Security Agentがインターネットに直接アクセスできない場合は、"[インターネットにアクセスできない エージェントを設定する](#)" on page 413で回避策について参照してください。

Deep SecurityのSmart Protection

不正プログラム対策モジュールおよびWebレピュテーションモジュールでは、コンピュータおよびワークロードをSmart Protection Networkで統合できます。システムレベルで設定されるスマートフィードバックにより、Smart Protection Networkに継続的にフィードバックを提供できます。

トレンドマイクロのSmart Protection Networkの詳細については、[「Smart Protection Network」](#)を参照してください。

このトピックの内容:

- "[不正プログラム対策とSmart Protection](#)" below
- "[WebレピュテーションとSmart Protection](#)" on page 777
- "[スマートフィードバック](#)" on page 777

また、AWSでの配置手順については「[AWSでのSmart Protection Serverの配置](#)」を、サーバの手動配置の手順については[Smart Protection Serverのドキュメント](#)を参照してください。

不正プログラム対策とSmart Protection

- [スマートスキャンの利点](#)
- "[スマートスキャンを有効にする](#)" on the next page
- "[ファイルレピュテーションサービス用のSmart Protection Server](#)" on page 776

スマートスキャンの利点

スマートスキャンには、次の機能と利点があります。

- クラウドでのリアルタイムのセキュリティステータス検索機能を提供します。
- 新たな脅威に対する保護の提供にかかる全体的な時間を短縮します。

- パターンファイルのアップデート中に消費されるネットワーク帯域幅を削減します。パターン定義のアップデートの大部分はクラウドに配信するだけでよく、多くのエンドポイントに配信する必要はありません。
- 企業全体のパターン配信に関連するコストとオーバーヘッドを削減します。

スマートスキャンを有効にする

スマートスキャンは不正プログラム対策モジュールで使用できます。トレンドマイクロの [Smart Protection Network](#) を利用してローカルのパターンファイルのサイズを抑え、AgentとApplianceで必要なアップデートのサイズおよび数を削減します。スマートスキャンが有効になっている場合、Agentは不正プログラムパターンファイルの完全バージョンではなく、より小さなサイズのバージョンをSmart Protection Serverからダウンロードします。このサイズの小さいパターンファイルは、ファイルが「安全を確認済み」か「危険の可能性あり」かを迅速に特定します。「危険の可能性あり」とみなされたファイルは、Trend Micro Smart Protection Serverに保管されている大容量の完全なパターンファイルと照合され、危険の有無が確実に判定されます。

スマートスキャンが有効になっていない場合、Relay Agentは不正プログラムの完全なパターンファイルをSmart Protection Serverからダウンロードしてローカルで使用する必要があります。パターンファイルは、セキュリティアップデートの予約タスク実行時にのみアップデートされます。パターンファイルは通常1日1回アップデートされてAgentにダウンロードされ、サイズは約120MBです。

注意: Trend Micro Smart Protection NetworkのグローバルのURLに対して安定した接続を確立できることを確認します (URLのリストについては"[ポート番号、URL、およびIPアドレス](#)" on page 190を参照してください)。ファイアウォール、プロキシ、またはAWSセキュリティグループによって接続がブロックされる場合、または接続が不安定な場合は、不正プログラム対策のパフォーマンスが低下します。

1. [ポリシー] に移動します。
2. ポリシーをダブルクリックします。
3. [不正プログラム対策]→[Smart Protection] の順に選択します。
4. [スマートスキャン] セクションで、次のいずれかを実行します。
 - [継承] を選択します (親ポリシーでスマートスキャンが有効になっている場合)
 - [継承] の選択を解除し、[オン] または [Deep Security Agentはオン、Virtual Applianceはオフ] を選択します。
5. [保存] をクリックします。

注意: スマートスキャンを使用するように設定されたコンピュータでは、不正プログラム対策パターン全体がローカルにダウンロードされることはありません。したがって、このコンピュータ上で不正プログラム対策ライセンスの有効期限が切れた場合は、スマートスキャンをオフにしても、不正プログラムの検索にローカルパターンは使用されません。これは、不正プログラム対策パターンがローカルに存在しないためです。

ファイルレピュテーションサービス用のSmart Protection Server

ファイルレピュテーションサービス用のSmart Protection Serverは不正プログラム対策モジュールで利用できます。スマートスキャンで必要なファイルレピュテーション情報を提供します。

ファイルレピュテーションサービス用のSmart Protection Serverを編集するには

1. [コンピュータ] または [ポリシー] → [不正プログラム対策] → [Smart Protection] の順に選択します。
2. トレンドマイクロのSmart Protection Serverに直接接続するか、ローカルにインストールされた1つ以上のSmart Protection Serverに接続するかを選択できます。
3. AgentとSmart Protection Networkとの通信にプロキシを使用する場合は、Smart Protection Network専用のプロキシサーバを作成することをお勧めします。使用可能なプロキシ一覧の表示および編集は、[管理] → [システム設定] 画面の [プロキシ] タブで行えます。プロキシプロトコルの詳細については、"[Deep Securityでサポートされるプロキシプロトコル](#)" on page 421を参照してください。

注意: プロキシの選択後、そのプロキシを使用しているAgentをすべて再起動する必要があります。

4. コンピュータがドメインに参加していない場合にGlobal Smart Protectionサービスを使用するには、[ドメインに参加していない場合はGlobal Smart Protectionサービスに接続(Windowsのみ)] オプションを選択します。コンピュータがドメインコントローラに接続できない場合は、ドメインに参加していないとみなされます(このオプションはWindows Agentでのみ使用できます)。

注意: Smart Protection Serverをローカルにインストールしている場合、Smart Protection Server自体に問題が発生した場合に通知が表示されるよう、少なくとも1台のコンピュータでこのオプションを [はい] に設定する必要があります。

5. コンピュータからSmart Protection Serverへの接続が失われたときにエラーイベントとアラートを生成するには、[Smart Protection Serverへの接続の警告] を設定します。

WebレピュテーションとSmart Protection

Webレピュテーション用のSmart Protection Serverは、Webレピュテーションモジュールに必要なWebレピュテーション情報を提供します。

Webレピュテーションサービス用のSmart Protection Serverを編集するには

1. [コンピュータ] または[ポリシー]→[不正プログラム対策]→[Smart Protection] の順に選択します。
2. トレンドマイクロのSmart Protection Serverに直接接続するか、ローカルにインストールされた1つ以上のSmart Protection Serverに接続するかを選択できます。
3. AgentとSmart Protection Networkとの通信にプロキシを使用する場合は、Smart Protection Network専用のプロキシサーバを作成することをお勧めします。使用可能なプロキシ一覧の表示および編集は、[管理]→[システム設定] 画面の [プロキシ] タブで行えます。プロキシプロトコルの詳細については、"[Deep Securityでサポートされるプロキシプロトコル](#)" on page 421を参照してください。

注意: プロキシの選択後、そのプロキシを使用しているAgentをすべて再起動する必要があります。

4. コンピュータがドメインに参加していない場合にGlobal Smart Protectionサービスを使用するには、[ドメインに参加していない場合はGlobal Smart Protectionサービスに接続(Windowsのみ)] オプションを選択します。コンピュータがドメインコントローラに接続できない場合は、ドメインに参加していないとみなされます(このオプションはWindows Agentでのみ使用できます)。

注意: Smart Protection Serverをローカルにインストールしている場合、Smart Protection Server自体に問題が発生した場合に通知が表示されるよう、少なくとも1台のコンピュータでこのオプションを [はい] に設定する必要があります。

5. コンピュータからSmart Protection Serverへの接続が失われたときにエラーイベントとアラートを生成するには、[Smart Protection Serverへの接続の警告] を設定します。

スマートフィードバック

トレンドマイクロスマートフィードバックは、トレンドマイクロ製品と、24時間体制の脅威リサーチセンターおよび技術部門との間に継続的な通信を提供します。スマートフィードバックでは、脅威に関する膨大なデータの共有とリアルタイム分析を行うTrend Micro Smart Protection Networkの一部として製品が機能します。この相互接続により、毎日発生する何千もの新しい脅威とその変種/亜種の分析、特定、および阻止を、これまでにない速さで実行できます。

トレンドマイクロスマートフィードバックは、Deep Security Managerのシステム設定として有効にできます。スマートフィードバックを有効にすると、匿名の脅威情報がSmart Protection Networkと共有されるため、トレンドマイクロは新しい脅威を迅速に特定し、対処することができます。初期設定では、スマートフィードバックは有効になっています。[管理]→[システム設定]→[スマートフィードバック]に移動すると、この設定を無効にしたり、調整したりできます。

注意: スマートフィードバックでは、[管理]→[システム設定]→[プロキシ] タブの [プロキシサーバの使用] で選択したAgent、Appliance、およびRelay (セキュリティアップデート) プロキシが使用されます。

不正プログラムの処理

不正プログラム対策モジュールによって検出された不正プログラムを処理するには、次のタスクを実行します。

- ["検出した不正プログラムの確認と復元" below](#)
- ["不正プログラム対策の例外の作成" on page 785](#)
- ["保護対象のLinuxインスタンスにおける不正プログラム対策のデバッグログレベルの引き上げ" on page 788](#)

["不正プログラム検出のアラートを生成する" on page 748](#)も参照してください。

不正プログラム対策モジュールの概要については、["不正プログラムの防止" on page 722](#)を参照してください。

検出した不正プログラムの確認と復元

検出ファイルとは、不正プログラムであるか不正プログラムを含むことが検出されたため、暗号化されて特殊なフォルダに移されたファイルのことです。感染ファイルを表示して復元できるかどうかは、不正プログラム対策設定と、感染ファイルが検出されたOSによって異なります。

- Windows Agentでは、["不正プログラム修復処理をカスタマイズする" on page 745](#)されたファイルを表示して復元できます。
- Linux Agentでは、隔離されたファイルのみを表示して復元できます。

このページのトピック:

- ["検出ファイルのリストを参照する" below](#)
- ["検出ファイル进行处理する" on the next page](#)
- ["検出ファイルを検索する" on page 781](#)
- ["検出ファイルを復元する" on page 782](#)
- ["検出ファイルを手動で復元する" on page 785](#)

不正プログラム検出時に生成されるイベントの詳細については、["不正プログラム対策イベント" on page 1319](#)を参照してください。

検出ファイルのリストを参照する

[イベントとレポート] 画面に検出ファイルのリストが表示されます。ここで、検出ファイルの詳細を確認できます。

1. [イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル] の順にクリックします。
2. ファイルの詳細を確認するには、ファイルを選択して [表示] をクリックします。

検出ファイルのリストには、次の情報が表示されます。

- 感染ファイル: 感染ファイルの名前と特定のセキュリティ上のリスクを表示します。
- 不正プログラム: 感染した不正プログラムを表示します。
- コンピュータ: 感染の疑いがあるコンピュータ名を表示します。




[詳細] 画面には次の情報が表示されます。

- 検出時刻: 感染コンピュータで感染が検出された日時。
- 感染ファイル: 感染ファイルの名前。
- ファイルのSHA-1: ファイルのSHA-1ハッシュ。
- 不正プログラム: 検出された不正プログラムの名前。
- 検索の種類: 不正プログラムを検出した検索の種類 (リアルタイム検索、予約検索、または手動検索のいずれか)。
- 実行された処理: 不正プログラムが検出されたときにDeep Securityが実行した処理の結果。
- コンピュータ: このファイルが検出されたコンピュータ (コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- コンテナ名: 不正プログラムが検出されたDockerコンテナの名前。

- コンテナID: 不正プログラムが検出されたDockerコンテナのID。
- コンテナイメージ名: 不正プログラムが検出されたDockerコンテナのイメージ名。

検出ファイル进行处理する

[検出ファイル] 画面では、検出ファイルに関連するタスクを管理できます。メニューバーまたは右クリックのコンテキストメニューで、次のことを実行できます。

-  復元 検出ファイルを元の場所および条件に復元する。
-  ダウンロード 検出ファイルをコンピュータまたはVirtual Applianceから任意の場所にダウンロードする。
-  分析 コンピュータまたはVirtual Applianceからの検出ファイルを分析する。
-  削除 1つ以上の検出ファイルをコンピュータまたはVirtual Applianceから削除する。
-  エクスポート 検出ファイルの情報 (ファイル自体ではない) をCSVファイルにエクスポートする。
-  表示 検出ファイルの詳細を表示する。
-  コンピュータの詳細 不正プログラムが検出されたコンピュータの画面を表示する。
-  不正プログラム対策イベントの表示 この検出ファイルに関連する不正プログラム対策イベントを表示する。
-  列の追加/削除 [追加]/[削除] をクリックして列を追加または削除する。
-  検索 特定の検出ファイルを検索する。

注意:

検出ファイルは、次のような場合にDeep Security Virtual Applianceから自動的に削除されません。

- vMotionによって仮想マシンが別のESXiホストに移動された場合。その仮想マシンに関連付けられている検出ファイルがVirtual Applianceから削除されます。
- 仮想マシンがDeep Security Managerから無効化された場合。その仮想マシンに関連付けられている検出ファイルがVirtual Applianceから削除されます。
- Deep Security Virtual ApplianceがDeep Security Managerから無効化された場合。そのVirtual Applianceに保存されているすべての検出ファイルが削除されます。

- Deep Security Virtual ApplianceがvCenterから削除された場合。そのVirtual Applianceに保存されているすべての検出ファイルも削除されます。

検出ファイルを検索する

- [期間] ドロップダウンメニューを使用すると、特定の期間内で検出されたファイルのみを表示できます。
- [コンピュータ] ドロップダウンメニューを使用すると、コンピュータグループまたはコンピュータポリシー別にファイルを表示できます。
- [このページを検索]→[詳細検索を開く]をクリックすると、詳細検索オプションの表示を切り替えることができます。

隔離ファイル		グループ化しない ▼
期間:	過去10時間	
コンピュータ:	すべてのコンピュータ	
検索:	感染ファイル	次の文字列を含む

詳細検索には、検出ファイルのフィルタリングに使用する検索条件が1つ以上含まれます。各条件は、次の項目から構成される論理文になります。

- ファイルの種類 (感染ファイルまたは不正プログラム) や感染したコンピュータなど、フィルタ対象の検出ファイルの特性
- 演算子:
 - 次の文字列を含む: 選択した列の入力内容に検索文字列が含まれる。
 - 次の文字列を含まない: 選択した列の入力内容に検索文字列が含まれない。
 - 次の文字列に等しい: 選択した列の入力内容と検索文字列が完全に一致する。
 - 次の文字列に等しくない: 選択した列の入力内容が検索文字列と一致しない。
 - 次のリストに含まれる: 選択した列の入力内容がカンマ区切りで入力された検索文字列1つと完全に一致する。
 - 次のリストに含まれない: 選択した列の入力内容がカンマ区切りで入力されたどの検索文字列とも一致しない。
- 値

条件を追加するには、最上部の条件の右側にある「プラス」ボタン (+) をクリックします。検索するには、検索ボタン (環状矢印) をクリックします。

注意: 検索では大文字と小文字は区別されません。

検出ファイルを復元する

ファイルの検索除外を作成する

ファイルを元の場所に復元する前に、検索除外を作成して、そのファイルがコンピュータに復元されたときにDeep Securityによってただちに再検出されないようにする必要があります。

注意: 以下の手順は個々のコンピュータ上でファイルの検索除外を作成する方法を示していますが、同じ設定変更をポリシーレベルで行うこともできます。

1. [コンピュータ] 画面を開き、[不正プログラム対策]→[検出ファイル] に進み、検出ファイルをダブルクリックしてそのプロパティを表示します。
2. ファイルの正確な名前と元の場所を書き留めます。
3. [コンピュータ] 画面を表示したまま、[不正プログラム対策]→[一般] に進み、有効になっている各不正プログラム検索の横にある [編集] ボタンをクリックし、[不正プログラム検

設定] プロパティ画面を開きます。

コンピュータ: WIN-LLH6SSRG4KK

概要 | 不正プログラム対策 | Webレピュテーション | ファイアウォール | 侵入防御 | 変更監視 | セキュリティログ監視 | アプリケーション制御 | インタフェース | 設定 | アップデート | オーバーライド

一般 | Smart Protection | 詳細 | 隔離ファイル | イベント

不正プログラム対策

設定: 継承(オン)

ステータス: ● オン,リアルタイム

リアルタイム検索

継承

不正プログラム検索設定: Default Real-Time Scan Configuration

スケジュール: Every Day All Day

手動検索

継承

不正プログラム検索設定: Default Manual Scan Configuration

予約検索

継承

不正プログラム検索設定: Default Scheduled Scan Configuration

不正プログラム検索

不正プログラムの前回の手動検索: なし

不正プログラムの前回の予約検索: なし

不正プログラムのクイック検索 | 不正プログラムのフル検索

4. [不正プログラム検索設定] プロパティ画面で、[検索除外] タブをクリックします。
5. [検索除外] エリアで、[ファイルリスト] を選択します。次に、[編集] をクリック (ファイルリストがすでに選択されている場合) するか、メニューから[新規] を選択します (新しいファイルリストを作成する場合)。

6. [ファイルリスト] プロパティ画面で、復元するファイルのパスと名前を入力します。[OK] をクリックして [ファイルリスト] プロパティ画面を閉じます。

一般 **割り当て対象**

一般情報

名前:

説明:

ファイル: (1行あたり1つのファイル)

C:\Documents\testfile.doc

サポートされている形式

備考 [プロセスイメージファイルリスト] で認識されるのはフルパスのみで、それ以外の形式は無視されます。

ファイル:

ファイル	例: testfile.doc
ファイルパス	例: C:\Documents\testfile.doc

ワイルドカード (*) 付きファイル:

ファイル*	例: MyApp*.vApp
ファイル 拡張子*	例: MyApp.v*

環境変数:

\${ENV.VAR}	例: \${myDBFile}
-------------	-----------------

コメント:

ファイルパス #コメント	例: C:\temp\file.txt #除外します
--------------	----------------------------

7. [OK] をクリックして [不正プログラム検索設定] プロパティ画面を閉じます。
8. すべての [不正プログラム検索設定] の編集が終わった後、[コンピュータ] 画面で [保存] をクリックし、変更を保存します。これでファイルを復元する準備ができました。

ファイルを復元する

1. [コンピュータ] 画面を表示したまま、[不正プログラム対策]→[検出ファイル] タブに進みます。
2. 検出ファイルを右クリックして [処理]→[復元] を選択し、ウィザードの手順に従います。

これでファイルが元の場所に復元されます。

検出ファイルを手動で復元する

検出ファイルを手動で復元するには、そのファイルをコンピュータにダウンロードします。[検出ファイル] ウィザードに、管理ユーティリティへのリンクが表示されます。このユーティリティを使用して、ファイルの復号、検査、および復元を行うことができます。検出ファイル復号ユーティリティを使用してファイルを復号し、元の場所に戻します。

復号ユーティリティは、Deep Security Managerのルートディレクトリの下に「util」フォルダにあるzipファイル (QFAdminUtil_win32.zip) 内にあります。圧縮ファイルには、同じ機能を持つ2つのユーティリティが含まれています。QDecrypt.exeとQDecrypt.comです。QDecrypt.exeを実行するとファイルを開く画面が呼び出され、復号するファイルを選択できます。QDecrypt.comは次のオプションを持つコマンドラインユーティリティです。

- /h, --help: このヘルプメッセージを表示
- --verbose: 詳細なログメッセージを生成
- /i, --in=<str>:復号する検出ファイル。<str> は検出ファイルの名前です。
- /o, --out=<str>:復号したファイルの出力。<str> は復号されたファイルに付けられる名前です。

注意: このユーティリティは、Windows 32ビットおよびWindowsの64ビットシステムでサポートされています。

不正プログラム対策の例外の作成

不正プログラムと同じ特徴があると、不正ではないファイルが不正プログラムに誤って識別される場合があります。安全なことがわかっていて、不正プログラムに識別されてしまう場合は、そのファイルの例外を作成できます。例外を作成すると、Deep Securityでこのファイルが検索されても、イベントはトリガされません。

不正プログラム対策モジュールの概要については、"[不正プログラムの防止](#)" on page 722を参照してください。

注意: リアルタイム、手動、および予約検索でファイルを除外することもできます。"[検索対象ファイルを指定する](#)" on page 738を参照してください。

次の不正プログラムおよび不正プログラム検索の種類について、例外を作成できます。

- 機械学習型検索 (詳細については、"[機械学習型検索を使用した脅威の検出](#)" on page 756を参照)。
- ドキュメントの脆弱性対策の検索 (詳細については、"[Connected Threat Defenseを使用した脅威の検出](#)" on page 758を参照)。
- スパイウェア/グレーウェアの検索 (詳細については、"[スパイウェア/グレーウェアを検索する](#)" on page 736を参照)。
- 挙動監視保護 (詳細については、"[挙動監視による不正プログラム/ランサムウェア検索の強化](#)" on page 767を参照)。

Deep Securityでは、ポリシーおよびコンピュータプロパティに不正プログラム検索のそれぞれの種類について、例外のリストを保持しています。

1. 例外のリストを表示するには、ポリシーまたはコンピュータのエディタを開きます。
2. [不正プログラム対策]→[詳細] の順にクリックします。
例外は、[許可するスパイウェア/グレーウェア]、[ドキュメントの脆弱性対策ルールの例外]、[機械学習型検索の検出除外対象]、および [挙動監視保護の例外] セクションに一覧表示されます。

"[検索除外の推奨設定](#)" on the next pageも参照してください。

不正プログラム対策イベントから例外を作成する

ファイルが不正プログラムとして識別されると、Deep Securityでは不正プログラム対策イベントが生成されます。ファイルが安全だとわかっている場合は、イベントレポートからそのファイルの例外を作成できます。

1. [イベントとレポート]→[イベント]→[不正プログラム対策イベント] の順にクリックして、不正プログラム検出イベントを特定します。
2. 該当するイベントを右クリックします。
3. [許可] を選択します。

不正プログラム対策の例外を手動で作成する

スパイウェア/グレーウェア、ドキュメントの脆弱性対策ルール、機械学習型検索、および挙動監視の例外について、不正プログラム対策の例外を手動で作成できます。例外を追加するに

は、検索によって生成された不正プログラム対策イベントの特定の情報が必要です。不正プログラムまたは検索の種類によって、次の情報が必要になります。

- スパイウェア/グレーウェア: [不正プログラム] フィールドの値 (SPY_CCFR_CPP_TEST.A など)
 - ドキュメントの脆弱性対策ルール: [不正プログラム] フィールドの値 (HEUR_OLEP.EXE など)
 - 機械学習型検索: [ファイルのSHA-1] フィールドのファイルのSHA1ダイジェスト (3395856CE81F2B7382DEE72602F798B642F14140 など)
 - 挙動監視: プロセスイメージパス (C:\test.exe など)
1. [イベントとレポート]→[イベント]→[不正プログラム対策イベント] の順にクリックして、不正プログラムの識別に必要なフィールド値をコピーします。
 2. 例外を作成するポリシーまたはコンピュータのエディタを開きます。
 3. [不正プログラム対策]→[詳細] の順にクリックします。
 4. [許可するスパイウェア/グレーウェア]、[ドキュメントの脆弱性対策ルールの例外]、[機械学習型検索の検出除外対象]、または [挙動監視保護の例外] セクションのテキストボックスにイベントの情報を入力します。
 5. [追加] をクリックします。

スパイウェア/グレーウェアの例外の処理方法

スパイウェアが検出された場合、検索を制御する不正プログラム検索設定に基づいて、不正プログラムは即座に駆除、隔離、または削除されます。スパイウェア/グレーウェアイベントの例外を作成後、ファイルの復元が必要な場合があります ("[検出ファイルを復元する](#)" on [page 782](#)を参照してください)。

または、一時的に処理を [放置] に設定した上でスパイウェア/グレーウェアを検索すると、スパイウェア/グレーウェア検出がすべて [不正プログラム対策イベント] 画面に記録されても、駆除、隔離、または削除は実行されません。これにより、検出されたスパイウェア/グレーウェアの例外を作成できます。例外リストの安全性が高くなったら、処理を [駆除]、[隔離]、または [削除] モードに設定できます。

処理の設定の詳細については、"[不正プログラムの処理方法を設定する](#)" on [page 745](#)を参照してください。

検索除外の推奨設定

検索除外については、トレンドマイクロやその他のベンダが包括的な詳しい情報を提供しています。ここでは、検索除外の推奨設定の一部について、その概要を紹介します。

- 不正プログラムであることがすでに確認されているファイルが再検索されないように、隔離フォルダ (Microsoft Windows Exchange ServerのSMEXなど) を除外します。
- 検索を実行するとデータベースのパフォーマンスに影響することがあるため、大規模なデータベースやデータベースファイル (dsm.mdfやdsm.ldfなど) を除外します。データベースファイルを検索する必要がある場合は、ピーク時を避けてデータベースを検索する予約タスクを作成します。Microsoft SQL Serverデータベースは動的であるため、ディレクトリおよびバックアップフォルダを検索リストから除外します。

Windowsの場合:

```
${ProgramFiles}\Microsoft SQL Server\MSSQL\Data\
```

```
${Windir}\WINNT\Cluster\ # (SQLクラスタリングを使用している場合)
```

```
Q:\ # (SQLクラスタリングを使用している場合)
```

Linuxの場合:

```
/var/lib/mysql/ # (マシンでこのパスがMySQLのデータの保存先として設定されている場合)
```

```
/mnt/volume-mysql/ # (マシンでこのパスがMySQLのデータの保存先として設定されている場合)
```

Windowsサーバでの検索ファイルの除外については、Microsoftが公開している[ウイルス対策除外リスト](#)を参考にしてください。

保護対象のLinuxインスタンスにおける不正プログラム対策のデバッグログレベルの引き上げ

Linuxオペレーティングシステムを使用している場合、不正プログラム対策 (AM) に関連した問題を診断するために使用するAMデバッグログのレベルを変更することができます。

不正プログラム対策のデバッグログは、テクニカルサポート向けの診断パッケージに自動的に追加されます。

診断パッケージの作成については、"[診断パッケージとログの作成](#)" on page 1573を参照してください。

不正プログラム対策のデバッグログレベルを上げるには、Linuxインスタンスのシェルでスーパーユーザとして次のコマンドを入力します。

```
killall -USR1 ds_am
```

このコマンドはレベルを1つ上げます。初期設定のレベルは6、最大レベルは8です。

不正プログラム対策のデバッグログレベルを下げるには、Linuxインスタンスのシェルでスーパーユーザとして次のコマンドを入力します。

```
killall -USR2 ds_am
```

このコマンドはレベルを1つ下げます。最小レベルは0です。

注意: Linuxディストリビューションでkillallを使用していない場合は、pkillコマンドを代わりに使用できます。

侵入防御を使用した攻撃のブロックをブロックする

侵入防御 モジュールは、SQLインジェクション攻撃、クロスサイトスクリプティング攻撃、およびその他のWebアプリケーションの脆弱性に対する脆弱性攻撃からコンピュータを保護します。

アプリケーションまたはOSの既知の脆弱性に対してパッチが利用できない場合、侵入防御ルールは、この脆弱性を悪用しようとしているトラフィックをインターセプトできます。また、ネットワークにアクセスする不正なソフトウェアを特定し、ネットワークにアクセスするアプリケーションに対する可視性および制御性を向上します。このため、脆弱性を修正するパッチがリリースされ、テストされて配信されるまでコンピュータが保護されます。

Skypeなどのファイル共有およびメッセージングソフトウェアだけでなく、SQLインジェクションやクロスサイトスクリプティングなどの脆弱性を持つWebアプリケーション (XSS) も利用できます。このように、侵入防御 は、軽量Webアプリケーションファイアウォール (WAF) としても使用できます。

侵入防御を有効にして設定するには、"[侵入防御の設定](#)" on page 793を参照してください。

侵入防御 ルール

侵入防御 ルールは、ネットワークパケットのペイロードセッションおよびアプリケーション層 (DNS、HTTP、SSL、およびSMTP)、など) と比較される一連の条件と、それらの上位層プロトコルに基づくパケットの順序を定義します。

ヒント: ファイアウォールルールはパケットのネットワーク層とトランスポート層 (IP、TCP、UDPなど) を確認します。

Deep Security Agentがネットワークトラフィックを検索してトラフィックがルール的一致条件を満たすと、Agentはそのトラフィックを予想される攻撃または確認済みの攻撃とみなし、ルールに応じて次のいずれかの処理を実行します。

- パケットの完全な破棄
- 接続のリセット

侵入防御ルールはポリシーとコンピュータに割り当てられます。このため、使用するポリシーに基づいてコンピュータのグループにルールセットを適用し、必要に応じてポリシーをオーバーライドできます("ポリシー、継承、およびオーバーライド" on page 587を参照してください)。

ルールの機能に影響を与える方法については、"[侵入防御ルールの設定](#)" on page 801。

アプリケーションの種類

アプリケーションの種類では、関連付けられているアプリケーションごとにルールを整理します。また、通信に使用されるプロトコルやポート番号などのように必要に応じてルールが参照できるプロパティ値を格納できます。一部のアプリケーションの種類には、設定可能なプロパティがあります。たとえば、Database Microsoft SQLのアプリケーションの種類には、Microsoft SQL Serverに関連付けられているルールが含まれます。このアプリケーションの種類を設定すると、データベースへの接続に使用するポートを指定できます。

詳細については、"[アプリケーションの種類](#)" on page 821を参照してください。

ルールアップデート

Trend Micro は、アプリケーションの脆弱性に対する 侵入防御ルールを作成します。セキュリティアップデートには、新しいルールまたはアップデートされたルール、およびアプリケーションの種類を含めることができます。ルールがすでにポリシーに割り当てられていて、割り当てられたルールが依存するルールがアップデートに含まれる場合は、アップデートされたルールを自動的に割り当てるように選択できます。

ヒント: 侵入防御ルールには、保護対象とする脆弱性に関する情報が含まれています。

侵入防御ルールはDeep Security Managerで直接編集できません。ただし、一部のルールは設定可能であり、設定が必要なルールもあります ("[設定オプションを設定する \(トレンドマイクロのルールのみ\)](#)" on page 806参照してください)。

推奨設定の検索

推奨検索を使用して、ポリシーとコンピュータに割り当てる 侵入防御 ルールを検出できます。
("推奨設定の検索の管理と実行" on page 592を参照してください)。

動作モードを使用してルールをテストする

侵入防御 は、[検出]または[防御]モードで動作します。

- の検出： 侵入防御 では、一致するトラフィックを検出してイベントを生成するためにルールを使用しますが、トラフィックはブロックしません。検出モードは、侵入防御ルールが正規のトラフィックに干渉しないことをテストする場合に便利です。
- Prevent： 侵入防御 では、ルールを使用して一致するトラフィックを検出し、イベントを生成し、トラフィックをブロックして攻撃を防止します。

新しい 侵入防御 ルールを最初に適用する場合は、Detectモードを使用して、誤って通常のトラフィックをブロックしないことを確認します (誤検出).誤判定が発生しないことを確認できた時点で、防御モードを使用して、ルールを適用して攻撃をブロックできます ("検出モードで侵入防御を有効にする" on page 794 および "予防モードに切り替える" on page 799 .)

ヒント: Detectモードで 侵入防御 を使用すると同様に、Deep Security ネットワークエンジンはテスト目的でタップモードで実行できます。タップモードでは、侵入防御 はルールマッチングトラフィックを検出してイベントを生成しますが、トラフィックはブロックしません。また、タップモードは、ファイアウォール および Webレピュテーション モジュールにも影響します。検出モードを使用すると、侵入防御ルールを個別にテストできます。タップモードをファイアウォール ルールのテストに使用すると同じ方法で、侵入防御でタップモードを使用します。"ファイアウォールルールを配信前にテストする" on page 836を参照してください。

ルールの動作モードをオーバーライドする

個々のルールで[検出]モードを選択することで、コンピュータまたはポリシーレベルで[防止モード]の動作を選択して優先させることができます。ポリシーまたはコンピュータに適用される新しい 侵入防御 ルールをテストする場合に便利です。たとえば、防御モードで侵入防御が機能するようにポリシーが設定されている場合、ルールを[検出]モードに設定することで、個々のルールの防御モードの動作を回避できます。そのルールの場合にのみ、侵入防御 はトラ

フィックをログに記録し、ポリシーの動作モードをオーバーライドしない他のルールを適用します。 ("[ルールの動作モードをオーバーライドする](#)" on page 808を参照してください)。

注意: コンピュータまたはポリシーレベルでの防御モードは、矛盾するルール設定で上書きできますが、[検出]モードにはできません。コンピュータまたはポリシーレベルで[検出]モードを選択すると、ルール設定に関係なく検出モードの動作が適用されます。

トレンドマイクロが用意している一部のルールは、初期設定で検出モードを使用します。たとえば、メールクライアントルールでは、一般的に[検出]モードが使用されます。これは、予防モードでは、すべてのメールのダウンロードがブロックされるためです。一部のルールは、条件が多数回、または一定期間中に一定回数発生した場合にのみアラートをトリガします。これらのルールは、条件が再度発生した場合にのみ、不審な挙動を示すトラフィックに適用され、その条件が1回発生しただけでは異常とはみなされません。

警告:

設定が必要なルールは、正規のトラフィックをブロックしたりネットワークサービスを中断することがないようにするには、設定が完了するまで検出モードのままにします。ルールを防御モードに切り替えるのは、設定とテストの完了後にします。

侵入防御 イベント

初期設定では、Deep Security Managerは、Deep Security**エージェントおよびアプライアンス**¹ から ファイアウォール および 侵入防御 イベントログをすべてのハートビートで収集します。イベントログは、Deep Security Managerによって収集された後、設定された一定の期間保持されます。初期設定値は1週間です ("[ログとイベントの保存に関するベストプラクティス](#)" on page 1122を参照してください)。必要に応じて、個々のルールにイベントログを設定できます ("[ルールにイベントログを設定する](#)" on page 805を参照してください)。

イベントにタグを付けると、イベントをソートしやすくなります。イベントには、手動でタグを付けることも、自動でタグを付けることもできます。また、自動タグ付け機能を使用し、複数のイベントをグループ化してラベルを付けることもできます。イベントのタグ付けの詳細については、"[イベントを識別およびグループ化するためのタグの適用](#)" on page 1129を参照してください。

¹Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

安全な接続のサポート

侵入防御 モジュールでは、セキュリティで保護された接続でパケットを検査できます。"[SSL またはTLSトラフィックの検査](#)" on page 823を参照してください。

コンテキスト

コンテキストは、コンピュータのネットワーク環境に応じてさまざまなセキュリティポリシーを実装する有効な方法です。一般的には、コンテキストが使用されるポリシーを作成して、さまざまなファイアウォールルールと侵入防御ルールをコンピュータ（通常はモバイルラップトップ）に適用します。このルールは、そのコンピュータが社内にあるか離れているかによって異なります。

コンピュータの場所を決定するには、コンピュータがどのようにドメインコントローラと接続されているかコンテキストで検証します。詳細については、"[ポリシーで使用するコンテキストの定義](#)" on page 680を参照してください。

インタフェースのタグ付け

ファイアウォール または 侵入防御 ルールを特定のインタフェースに割り当てる必要がある場合にインタフェースの種類を使用できます。複数のネットワークインタフェースがあるコンピュータの場合初期設定では、ファイアウォールルールと侵入防御ルールはコンピュータ上のすべてのインタフェースに割り当てられます。たとえば、ワイヤレスネットワークインタフェースにのみ特別なルールを適用する場合、インタフェースの種類を使用します。詳細については、"[複数のインタフェースに対してポリシーを設定する](#)" on page 603を参照してください。

侵入防御の設定

侵入防御モジュールを有効にし、[Detect]モードを使用してネットワークトラフィックの攻撃を監視します。侵入防御ルールの割り当て方法に問題がなければ、防御モードに切り替えてください。

1. "[検出モードで侵入防御を有効にする](#)" on the next page
2. "[侵入防御のテスト](#)" on page 796
3. "[推奨ルールを適用する](#)" on page 797
4. "[システムを監視する](#)" on page 798
5. "[パケットまたはシステムのエラーに対して「Fail-Open」を有効にする](#)" on page 799

6. ["予防モードに切り替える" on page 799](#)
7. ["個々のルールについてのベストプラクティスを実装する" on page 799](#)
8. ["NSXセキュリティタグを適用する" on page 800](#)

注意: IPSの設定によって、CPUとRAMの使用率は変化します。Deep Security エージェントでIPSのパフォーマンスを最適化するには、["侵入防御のパフォーマンスに関するヒント" on page 832](#)のパフォーマンスに関するヒントを参照してください。

侵入防御モジュールの概要については、["侵入防御を使用した攻撃のブロックをブロックする" on page 789](#)を使用した攻撃のブロックの試みを参照してください。

検出モードで侵入防御を有効にする

Intrusion Preventionを有効にし、[Detect]モードを使用して監視します。適切なポリシーを使用して侵入防御を設定し、対象コンピュータに影響を与えます。個々のコンピュータを設定することもできます。

1. **コンピュータエディタまたはポリシーエディタ¹**で、[侵入防御]→[一般]に進みます。
2. [設定]で、[オン] または [継承 (オン)] を選択します。

コンピュータ: [検索欄] ヘルプ

概要 | 不正プログラム対策 | Webレピュテーション | ファイアウォール | **侵入防御** | 変更監視 | セキュリティログ監視 | アプリケーションコント | インタフェース | 設定 | アップデート | オーバーライド

一般 | 詳細 | 侵入防御イベント

侵入防御
 設定: オン
 ステータス: ● アプリケーションの種類のポートリストの誤った設定
 侵入防御の動作
 防御
 検出

コンテナの保護
 コンテナのネットワークトラフィックの検索: 継承 (はい)

現在割り当てられている侵入防御ルール

すべて ▼

割り当て/割り当て解除... | プロパティ... | エクスポート ▼ | アプリケーションの種類... | 列...

名前	アプリケーションの種類	優先度	重要度	モード	種類	カテゴリ	CVE	CVSSスコ...
1000128 - HTTP Protocol Deco...	Web Server Common	1 - 低	● 重大	防御	スマート	Webアプリケーション...	CVE-2004-1...	10.0
1000552 - Generic Cross Site S...	Web Application Common	1 - 低	● 重大	防御	スマート	Webアプリケーション...	CVE-2005-3...	10.0
1000608 - Generic SQL Injectio...	Web Application Common	1 - 低	● 重大	防御	スマート	Webアプリケーション...	CVE-2000-1...	10.0
1003304 - Identified Remote FIL...	Web Application Common	2 - 標準	● 重大	検出のみ	スマート	Webアプリケーション...	CVE-2018-1...	10.0

推奨設定
 現在のステータス: 4個の侵入防御ルールが割り当てられています
 前回の推奨設定の検索: なし
 ⓘ 推奨設定の検索結果なし
 侵入防御の推奨設定を自動的に適用 (可能な場合): 継承 (はい) ▼
 推奨設定の検索 | 推奨設定の検索のキャンセル | 推奨設定をクリア
 保存 | 閉じる

3. [侵入防御の動作] では、[検出] を選択します。
4. Deep Security Agent 11.1以前では、ホストコンピュータのネットワークインタフェースを通過してコンテナに向かうトラフィックが侵入防御モジュールによって監視されます。Deep Security Agent 11.2以降では、コンテナ間のトラフィックを監視することもできます。[コンテナのネットワークトラフィックの検索] 設定が [はい] に設定されている場合、コンテナとホストの両方を通過するトラフィックがDeep Securityによって検索されま

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

す。[いいえ]に設定されている場合、Deep Securityで検索されるのは、ホストネットワークインタフェースを通過するトラフィックだけです。

5. [保存] をクリックします。

ヒント: 動作を設定できない場合は、[ネットワークエンジンモード]が[タップ]に設定されている可能性があります ("ファイアウォールルールを配信前にテストする" on page 836) を参照してください。

より細かい制御を行うには、侵入防御ルールを割り当てるときに、グローバル動作モードを無効にして、防止または検出のいずれかに特定のルールを設定できます。 ("ルールの動作モードをオーバーライドする" on page 808を参照してください)。

侵入防御のテスト

侵入防御モジュールが正常に動作していることをテストしてから、次の手順に進んでください。

1. Agentベースの配信がある場合は、コンピュータのAgentが実行中であることを確認します。Agentレスの配信の場合は、Deep Security Virtual Applianceが正常に実行していることを確認します。
2. Webレピュテーションモジュールの電源を切ります。Deep Security Managerで[Computers]をクリックし、侵入防御をテストするコンピュータをダブルクリックします。コンピュータのダイアログボックスで[Webレピュテーション]をクリックし、[オフ]を選択します。Webレピュテーションは現在無効になっており、侵入防御機能に干渉することはありません。
3. 不正なトラフィックがブロックされることを確認します。引き続き、コンピュータのダイアログボックスで[侵入防御]をクリックし、[一般] タブで [防御] を選択します(影付き表示されている場合は、[設定] ドロップダウンリストを [継承 (オン)] に設定します)。
4. EICARテストポリシーを割り当てます。引き続き、コンピュータのダイアログボックスで[侵入防御]をクリックします。[割り当て/割り当て解除] をクリックします。1005924. を検索します。[1005924 - Restrict Download of EICAR Test File Over HTTP] ポリシーが表示されます。チェックボックスをオンにして、[OK] をクリックします。これで、ポリシーがコンピュータに割り当てられました。
5. EICARファイルをダウンロードしてください (侵入防御が適切に実行されている場合は実行できません)。Windowsの場合は、: <http://files.trendmicro.com/products/eicar-file/eicar.com>のリンクをクリックしてください。Linuxの場合は次のコマンドを入力します。curl -O http://files.trendmicro.com/products/eicar-file/eicar.com
6. コンピュータの侵入防御イベントを確認します。引き続き、コンピュータのダイアログボックスで[侵入防御]→[侵入防御イベント] をクリックします。[イベントの取得] をク

リックすると、前回のハートビート以降に発生したイベントが表示されます。[理由] が [1005924 - Restrict Download of EICAR Test File Over HTTP] となっているイベントが表示されます。このイベントが発生すると、侵入防御が機能していることを示します。

7. 変更を元に戻し、システムを以前の状態に戻します。Webレピュテーションモジュールをオンにし(オフにした場合)、[防御] または [検出] オプションをリセットして、コンピュータからEICARポリシーを削除します。

推奨ルールを適用する

パフォーマンスを最大化するには、ポリシーとコンピュータで必要な侵入防御ルールのみを割り当てます。推奨検索を使用して、適切なルールのリストを取得できます。

注意: 推奨設定の検索は特定のコンピュータに対して実行されますが、この推奨設定はコンピュータが使用するポリシーに割り当てることができます。

詳細については、"[推奨設定の検索の管理と実行](#)" on page 592を参照してください。

1. 検索するコンピュータのプロパティを開きます。"[推奨設定の検索を手動で実行する](#)" on page 597の説明に従って推奨設定の検索を実行します。

注意: Deep Securityを "[推奨設定を自動的に適用する](#)" on page 598 検索結果を自動的に実装します。

2. ルールを割り当てるポリシーを開き、"[検索結果を確認して手動でルールを割り当てる](#)" on page 599の説明に従ってルールの割り当てを実行します。

名前	優先度	重要度	モード	種類	カテゴリ	CVE	CVSSスコア	前回のアップ...
Application Control For Download Manager (1)								
1004902 - Application Control F...	2 - 標準	● 重大	検出のみ	スマート	アプリケーション制御	なし	なし	2015-09-08
Application Control For File Sharing (18)								
1001109 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2010-03-19
1002471 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2010-03-19
1002472 - Application Control F...	2 - 標準	● 重大	検出のみ	スマート	アプリケーション制御	なし	なし	2014-03-26
1002473 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2008-12-08
1003368 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2010-03-19
1003647 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2008-12-08
1003651 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2011-08-24
1003652 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2010-03-19
1003655 - Application Control F...	2 - 標準	● 重大	検出のみ	スマート	アプリケーション制御	なし	なし	2014-06-11
1003656 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2010-03-19
1003682 - Application Control F...	2 - 標準	● 重大	検出のみ	スマート	アプリケーション制御	なし	なし	2014-06-11
1003882 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2010-03-19
1004575 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2011-02-23
1004706 - Application Control F...	2 - 標準	● 高	検出のみ	スマート	アプリケーション制御	なし	なし	2011-06-29
1004707 - Application Control F...	2 - 標準	● 重大	検出のみ	スマート	アプリケーション制御	なし	なし	2015-06-24

ヒント: 自動および定期的に割り当てられた侵入防御ルールを微調整するには、推奨検索をスケジュールできます。"[Deep Security予約タスクの設定](#)" on page 479を参照してください。

システムを監視する

侵入防御ルールを適用した後、システムパフォーマンスと侵入防御イベントログを監視します。

システムパフォーマンスを監視する

CPU、RAM、およびネットワークの使用量を監視して、システムのパフォーマンスが許容範囲に収まっていることを確認します。パフォーマンスが許容範囲を超えて低下している場合は、

パフォーマンスを改善するために一部の設定や環境を変更します ("侵入防御のパフォーマンスに関するヒント" on page 832.)を参照してください。

侵入防御イベントを確認する

侵入防御イベントを監視して、ルールが正規のネットワークトラフィックに一致しないようにします。ルールで誤判定が発生している場合は、ルールの割り当てを解除できます("ルールを割り当てる/ルールの割り当てを解除する" on page 804を参照してください)。

侵入防御イベントを表示するには、[イベント] [&レポート] [] → [侵入防御イベント] [] の順にクリックします。

パケットまたはシステムのエラーに対して「Fail-Open」を有効にする

侵入防御モジュールには、侵入防御ルールを適用する前にパケットをブロックするネットワークエンジンが含まれています。これにより、サービスおよびアプリケーションでダウンタイムやパフォーマンスの問題が発生することがあります。この動作を変更し、システムまたは内部パケットエラーの発生時にパケットの通過を許可できます。詳細については、"「Fail-Open」の動作を有効にする" on page 838を参照してください。

予防モードに切り替える

侵入防御で誤検出が見つからないことが確認されたら、防御モードで侵入防御を使用するようにポリシーを設定し、ルールが適用され、関連するイベントがログに記録されるようにします。

1. **コンピュータエディタまたはポリシーエディタ**¹で、[侵入防御] → [一般] に進みます。
2. [侵入防御の動作] では、[防御] を選択します。
3. [保存] をクリックします。

個々のルールについてのベストプラクティスを実装する

HTTPプロトコルデコードルール

HTTPプロトコルデコードルールは、アプリケーションの種類「Web Server Common」の中で最も重要なルールです。このルールは、他のルールによってHTTPトラフィックが検査され

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

る前にHTTPトラフィックをデコードします。また、このルールを使用して、デコードプロセスの各種のコンポーネントを制御することもできます。

このルールは、このルールを必要とするいずれかの「Web Application Common」ルールまたは「Web Server Common」ルールを使用する場合には必須です。他のルールでこのルールが必要とされる場合、Deep Security Managerはこのルールを自動的に割り当てます。Webアプリケーションは1つ1つ異なるため、設定変更が必要かどうかを判断するために、このルールを使用するポリシーは一定期間検出モードで実行してから保護モードに切り替える必要があります。

無効な文字のリストは、しばしば変更が必要です。

このルールとその調整方法の詳細については、次の製品Q&Aを参照してください。

- <https://success.trendmicro.com/jp/solution/1120027>
- <https://success.trendmicro.com/jp/solution/1311120>

クロスサイトスクリプティングルールと汎用的なSQLインジェクションルール

アプリケーション層への攻撃として最も代表的なものに、SQLインジェクションとクロスサイトスクリプティング (XSS) があります。クロスサイトスクリプティングルールとSQLインジェクションルールは初期設定で攻撃の大半を阻止しますが、特定のリソースが誤判定を引き起こす場合はその破棄のしきい値の調整が必要になることがあります。

この2つのルールは、どちらもWebサーバに合わせてカスタム設定が必要なスマートフィルタです。Webアプリケーション脆弱性Scannerからの情報がある場合は、保護を適用する際に利用することをお勧めします。たとえば、login.aspページのユーザ名フィールドがSQLインジェクションに対して脆弱な場合は、破棄のしきい値を低くしてそのパラメータを監視するようにSQLインジェクションルールを設定してください。

詳細については、<https://success.trendmicro.com/solution/1098159>を参照してください。

NSXセキュリティタグを適用する

NSXセキュリティタグを適用する

Deep Securityでは、侵入防御ルールがトリガされた際に、保護対象の仮想マシンにNSXセキュリティタグを適用できます。詳細については、"[NSXセキュリティタグを適用するように侵入防御を設定する](#)" on page 367を参照してください。

侵入防御ルールの設定

次のタスクを実行して、侵入防御ルールを設定および使用します。

- "侵入防御ルールのリストを表示する" [below](#)
- "侵入防御ルールに関する情報を表示する" [on the next page](#)
- "関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ)" [on page 804](#)
- "ルールを割り当てる/ルールの割り当てを解除する" [on page 804](#)
- "アップデートされた必須ルールを自動割り当てする" [on page 805](#)
- "ルールにイベントログを設定する" [on page 805](#)
- "アラートを生成する" [on page 806](#)
- "設定オプションを設定する (トレンドマイクロのルールのみ)" [on page 806](#)
- "有効な時間を予約する" [on page 807](#)
- "推奨設定から除外する" [on page 808](#)
- "ルールのコンテキストを設定する" [on page 808](#)
- "ルールの動作モードをオーバーライドする" [on page 808](#)
- "ルールおよびアプリケーションの種類の設定をオーバーライドする" [on page 809](#)
- "ルールをエクスポート/インポートする" [on page 810](#)
- "SQLインジェクション防御ルールの設定" [on page 810](#)

侵入防御モジュールの概要については、"[侵入防御を使用した攻撃のブロックをブロックする](#)" [on page 789](#)を参照してください。

侵入防御ルールのリストを表示する

[ポリシー] 画面には侵入防御ルールのリストが表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。このリストでは、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールのリストでもTippingPointルールIDを表示できます。

リストを確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

侵入防御ルールに関する情報を表示する

侵入防御ルールのプロパティには、ルールおよび防御対象の攻撃コードに関する情報が含まれます。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。

一般情報

- 名前: 侵入防御ルールの名前。
- 説明: 侵入防御ルールの説明。
- 最小Agent/Applianceバージョン: この侵入防御ルールのサポートに必要なDeep Security **Agent/Appliance**¹の最小バージョン。

詳細

[新規] () または [プロパティ] () をクリックして、[侵入防御ルールプロパティ] 画面を表示します。

注意: [設定] タブを確認します。トレンドマイクロが提供する侵入防御ルールは、Deep Security Managerを使用して直接編集することはできません。その代わりに、侵入防御ルールに設定が必要な場合や設定が可能な場合は、[設定] タブの設定オプションを使用します。ユーザ自身で作成したカスタム侵入防御ルールは、[ルール] タブが表示され、直接編集可能です。

侵入防御ルールのリストを表示する

[ポリシー] 画面には侵入防御ルールのリストが表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。このリストでは、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

¹Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールのリストでもTippingPointルールIDを表示できます。

リストを確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

一般情報

- **アプリケーションの種類:**この侵入防御ルールが分類されているアプリケーションの種類。

ヒント:このパネルでアプリケーションの種類を編集できます。ここでアプリケーションの種類を編集すると、そのアプリケーションの種類を使用するすべてのセキュリティコンポーネントに対して変更内容が適用されます。

- **優先度:** ルールの優先度。優先度の低いルールよりも優先度の高いルールが優先的に適用されます。
- **重要度:**ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、侵入防御ルールのリストを表示するときにソート条件として使用できます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します ([管理]→[システム設定]→[ランク付け] を参照してください)。
- **CVSSスコア:**[脆弱性情報データベース](#)に基づいた、脆弱性の重要度の基準。

ID (トレンドマイクロのルールのみ)

- **種類:** [スマート] (1つ以上の既知または不明なゼロデイの脆弱性)、[攻撃コード] (通常、署名ベースの攻撃コード) または [脆弱性] (1つ以上の攻撃コードが存在する可能性のある特定の脆弱性) のいずれかになります。
- **発行日:** ルールがリリースされた日付。ダウンロードされた日付ではありません。
- **前回のアップデート:** ローカルで、またはセキュリティアップデートのダウンロード中に、ルールが変更された前回の日時。
- **識別子:** ルールに一意のIDタグ。

関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ)

トレンドマイクロのルールには、ルールで防御する脆弱性に関する情報が含まれます。適用可能な場合は、共通脆弱性評価システム (CVSS) が表示されます(この評価システムの詳細は、[脆弱性情報データベース](#)のCVSSページを参照してください)。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [脆弱性] タブをクリックします。

ルールを割り当てる/ルールの割り当てを解除する

Agent検索時に侵入防御ルールを適用するには、該当するポリシーとコンピュータに割り当てます。脆弱性にパッチが適用されたため、ルールが必要でなくなった場合は、ルールを割り当て解除できます。

コンピュータエディタ¹で侵入防御ルールの割り当てを解除できない場合、そのルールがポリシーに割り当てられている可能性があります。ポリシーレベルで割り当てられたルールを削除するには**ポリシーエディタ**²を使用する必要があり、コンピュータレベルでは削除できません。

ポリシーに対する変更は、そのポリシーを使用するすべてのコンピュータに反映されます。たとえば、ポリシーからルールを割り当て解除すると、そのポリシーで保護しているすべてのコンピュータからルールが削除されます。継続してこのルールを他のコンピュータに適用するには、そのグループのコンピュータ用に新しいポリシーを作成します。 ("[ポリシー、継承、およびオーバーライド](#)" on page 587を参照してください)。

ヒント: ルールが割り当てられたポリシーとコンピュータを確認するには、ルールプロパティの [割り当て対象] タブをご覧ください。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

2. [侵入防御]→[一般] の順にクリックします。
ポリシーに割り当てられているルールの一覧は、[現在割り当てられている侵入防御ルール] リストに表示されます。
3. [現在割り当てられている侵入防御ルール] で、[割り当て/割り当て解除] をクリックします。
4. ルールを割り当てるには、ルールの横にあるチェックボックスをオンにします。
5. ルールの割り当てを解除するには、ルールの横にあるチェックボックスをオフにします。
6. [OK] をクリックします。

アップデートされた必須ルールを自動割り当てする

セキュリティアップデートには、セカンダリ侵入防御ルールの割り当てが必要な新規またはアップデートされたアプリケーションの種類および侵入防御ルールが含まれている場合があります。Deep Securityでは必要に応じて、これらのルールを自動割り当てできます。ポリシーまたはコンピュータプロパティで、次のように自動割り当てを有効化できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御]→[詳細] を順にクリックします。
3. 自動割り当てを有効にするには、[ルールアップデート] 領域で [はい] を選択します。
4. [OK] をクリックします。

ルールにイベントログを設定する

ルールのイベントをログに記録するか、ログにパケットデータを含めるかどうかを設定します。

注意: Deep Securityの侵入防御イベントで、パケットデータにX-Forwarded-Forヘッダが含まれている場合は、このヘッダを表示できます。このヘッダの情報は、Deep Security Agentをロードバランサまたはプロキシの背後に配置している場合に役立ちます。X-Forwarded-Forヘッダデータは、イベントの [プロパティ] 画面に表示されます。ヘッダデータを含めるには、ログにパケットデータを追加します。また、ルール1006540 [X-Forwarded-For HTTPヘッダのログを有効にする] も割り当てる必要があります。

ルールがイベントをトリガするたびにすべてのパケットデータを記録するのは現実的ではないので、Deep Securityでは、一定時間内でイベントが最初に発生したときのデータのみを記録します。初期設定時間は5分ですが、ポリシーの [ネットワークエンジンの詳細設定] の [1つのパケットデータのみをログに記録する期間] プロパティを使用して期間を変更できます。(「[ネットワークエンジンの詳細オプション](#)」を参照してください)。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" on page 809を参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [一般] タブで、[イベント] 領域に移動し、次のように必要なオプションを選択します。
 - ルールのログを無効化するには、[イベントログの無効化]を選択します。
 - パケットが破棄またはブロックされた場合にイベントのログを記録するには、[パケット破棄時にイベントを生成]を選択します。
 - ログエントリにパケットデータを含めるには、[常にパケットデータを含める]を選択します。
 - ルールで検出されたパケットの前後のパケットをログに記録するには、[デバッグモードを有効にする]を選択します。サポート担当者から指示があった場合のみデバッグモードを使用します。

また、ログにパケットデータを含めるには、ルールを割り当てるポリシーで次のように、ルールによるパケットデータの取得を許可する必要があります。

1. [ポリシー] 画面で、ルールを割り当てたポリシーを開きます。
2. [侵入防御]→[詳細] を順にクリックします。
3. [イベントデータ] 領域で [はい] を選択します。

アラートを生成する

侵入防御ルールがイベントをトリガした場合にアラートを生成します。


次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" on page 809を参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [オプション] タブをクリックして[アラート] 領域で [オン] を選択します。
4. [OK] をクリックします。

設定オプションを設定する (トレンドマイクロのルールのみ)

トレンドマイクロの侵入防御ルールの一部には、ヘッダ長、HTTPに許可される拡張子、Cookie長など、1つ以上の設定オプションがあります。オプションには設定が必要なものもあ

ります。必要なオプションを設定せずにルールを割り当てると、アラートが生成され、必要なオプションについての情報が表示されます。(これは、セキュリティアップデートによってダウンロードされ自動的に適用されたルールにも適用されます)。


設定オプションのある侵入防御ルールは、[侵入防御ルール] リストでルールのアイコンに小さなギアマークが付きます .

注意: 独自のカスタム侵入防御ルールには、[ルール] タブがあり、ルールを編集できます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" on page 809を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [設定] タブをクリックします。
4. プロパティを設定して [OK] をクリックします。

有効な時間を予約する

侵入防御ルールが有効な時間を予約します。予約された時間のみ有効になる侵入防御ルールは、[侵入防御ルール] 画面でルールのアイコンに小さな時計マークが付きます .

注意: Agentベースの保護では、スケジュールで保護対象のエンドポイントと同じタイムゾーンが使用されます。Agentレスによる保護では、Deep Security Virtual Applianceと同じタイムゾーンが使用されます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" on page 809を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [スケジュール] 領域で [新規] を選択するか、頻度を選択します。
5. 必要に応じてスケジュールを編集します。
6. [OK] をクリックします。

推奨設定から除外する

推奨設定検索のルール推奨設定から侵入防御ルールを除外します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" [on the next page](#)を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [推奨設定オプション] 領域で [推奨設定から除外] を選択します。
5. [OK] をクリックします。

ルールのコンテキストを設定する

ルールが適用されるコンテキストを設定します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" [on the next page](#)を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [コンテキスト] 領域で [新規] を選択するか、コンテキストを選択します。
5. 必要に応じてコンテキストを編集します。
6. [OK] をクリックします。

ルールの動作モードをオーバーライドする

新しいルールをテストする場合は、侵入防御ルールの動作モードを [検出] に設定します。[検出] モードでは、ルールは「検出のみ:」という言葉で始まるログエントリを作成しますが、トラフィックに干渉しません。侵入防御ルールには [検出] モードでのみ動作するものがあります。これらのルールについては、動作モードを変更できません。

注意: ルールのログを無効にすると、動作モードに関係なく、ルールのアクティビティはログに記録されません。

動作モードの詳細については、"[動作モードを使用してルールをテストする](#)" on page 791を参照してください。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"[ルールおよびアプリケーションの種類の設定をオーバーライドする](#)" [below](#)を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [検出のみ] を選択します。

ルールおよびアプリケーションの種類の設定をオーバーライドする

コンピュータエディタとポリシーエディタ¹で、侵入防御ルールを編集して、ポリシーまたはコンピュータのコンテキストのみで変更を適用できます。グローバルに変更が適用されるようにルールを編集して、ルールが割り当てられた他のポリシーおよびコンピュータで変更を有効にすることもできます。同様に、1つのポリシー/コンピュータ、またはグローバルにアプリケーションの種類を設定できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御] をクリックします。
3. ルールを編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
 - プロパティ: そのポリシーのみのルールを編集します。
 - プロパティ (グローバル): グローバルに (すべてのポリシーとコンピュータに対して) ルールを編集します。
4. ルールのアプリケーションの種類を編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
 - アプリケーションの種類プロパティ: そのポリシーのみのアプリケーションの種類を編集します。
 - アプリケーションの種類プロパティ (グローバル): グローバルに (すべてのポリシーとコンピュータに対して) アプリケーションの種類を編集します。
5. [OK] をクリックします。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ヒント: ルールを選択して [プロパティ] をクリックした場合は、編集中のポリシーのみでルールを編集します。

注意: 1つのポートを割り当てできるアプリケーションの種類は8個までです。9個以上割り当てると、そのルールは該当するポートで機能しません。

ルールをエクスポート/インポートする

1つ以上の侵入防御ルールをXMLまたはCSVファイルにエクスポートしたり、XMLファイルからルールをインポートできます。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. 1つ以上のルールをエクスポートするには、[エクスポート]→[選択したアイテムをCSV形式でエクスポート] または [エクスポート]→[選択したアイテムをXML形式でエクスポート] を順にクリックします。
3. すべてのルールをエクスポートするには、[エクスポート]→[CSV形式でエクスポート] または [エクスポート]→[XML形式でエクスポート] を順にクリックします。
4. ルールをインポートするには、[新規]→[ファイルからインポート] を順にクリックして、ウィザードの指示に従います。

SQLインジェクション防御ルールの設定

Deep Securityの侵入防御モジュールには、SQLインジェクション攻撃を検出するルールが搭載されており、その特徴に応じて接続を破棄するか、ログに記録します。このルールは [1000608 - Generic SQL Injection Prevention] と呼ばれており、組織のニーズに合うように設定できます。たとえば、ルールの感度を変更するには、破棄のしきい値を変更します。

The screenshot shows the 'Deep Security' interface with the 'ポリシー' (Policies) section selected. Under 'ルール' (Rules), '侵入防御ルール' (Intrusion Detection Rules) is chosen. The main area displays a table of intrusion detection rules. The rule '1000608 - Generic SQL Injection Prevention' is highlighted with a red box. The table columns are: 名前 (Name), 優先度 (Priority), 重要度 (Severity), モード (Mode), 種類 (Type), カテゴリ (Category), and CVE. The rule's priority is '1 - 低' (Low) and its severity is '重大' (Critical).

名前	優先度	重要度	モード	種類	カテゴリ	CVE
Web Application Common (1)						
1000608 - Generic SQL Injection Prevention	1 - 低	重大	防御	スマート	Webアプリケーション...	CVE-2000...

この記事のトピック:

- ["SQLインジェクション攻撃とは" below](#)
- ["SQLインジェクション攻撃に共通する文字および文字列" below](#)
- ["Generic SQL Injection Preventionルールの仕組み" on page 813](#)
- ["ルールおよび評価システムの実例" on page 814](#)
- ["Generic SQL Injection Preventionルールを設定する" on page 817](#)
- ["文字エンコードのガイドライン" on page 819](#)

SQLインジェクション攻撃とは

SQLインジェクション攻撃 (またはSQLフィッシング攻撃) はデータ駆動型アプリケーションの攻撃方法で、攻撃者の入力フィールドにはSQL文が分割して含まれます。新規に生成された不正なSQLコマンドがWebサイトからデータベースに渡され、実行されます。このコマンドによって、攻撃者はデータベース内の情報の読み取り、追加、削除、または変更ができます。

SQLインジェクション攻撃に共通する文字および文字列

以下は一般的に使用される文字および文字列の例です。このリストは一部です。

- ('
- %27
- \x22
- %22
- char
- ;
- ascii
- %3B
- %2B
- --
- %2D%2D
- /*
- %2F%2A
- */
- %2A%2F
- substring

- drop table
- drop+table
- insert into
- insert+into
- version(
- values
- group by
- group+by
- create table
- create+table
- delete
- update
- bulk insert
- bulk+insert
- load_file
- shutdown
- union
- having
- select
- declare
- exec
- and
- or
- like
- @@hostname
- @@tmpdir
- is null
- is+null
- is not null
- is+not+null
- %3D

- CONCAT
- %40%40basedir
- version%28,user(
- user%28,system_user(
- (,%28,)
- %29
- @
- %40
- cast

Generic SQL Injection Preventionルールの仕組み

Generic SQL Injection Preventionルールは、評価システムを使用してSQLインジェクション攻撃を検出します。ルールは次のように動作します。

1. アプリケーションからDeep Security Agentにパケットが到着し、分析されます。
2. Generic SQL Injection Preventionルールでは、パケットを検査して以下の表に示す文字列があるかどうかを確認します。文字列はカンマで区切られ、10個のグループに分類されています。
3. 文字列が見つかった場合、スコアが次のように計算されます。
 - 1つの文字列が見つかった場合は、そのグループのスコアが合計スコアになります。
 - 複数の文字列が異なるグループで見つかった場合は、それらのグループのスコアが合計されます。
 - 複数の文字列が同じグループで見つかった場合、そのグループのスコアは1度だけ加算されます。
詳細については、"[ルールおよび評価システムの実例](#)" on the next pageを参照してください。
4. 合計スコアを使用して、Deep Securityは接続を中断するか、ログに記録するかを決定します。合計スコアが破棄のしきい値スコアを超えた場合、接続は中断されます。ログしきい値スコアを超えた場合は、ログに記録されます。

注意: Trend Microによってルールが頻繁にアップデートされるため、以下の表の文字列はDeep Security Managerで使用するものと完全には一致しない場合があります。

注意: この表内の「\w」は、「この後に英数字以外の文字が続く」ことを示します。

グループ	スコア
drop table,drop+table,insert into,insert+into,values\W,create table,create+table,delete\W,update\W,bulk insert,bulk+insert,shutdown\W,from\W	2
declare\W,select\W	2
cast\W,exec\W,load_file	2
union\W,group by,group+by,order by,order+by,having\W	2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W	1
--,%2D%2D,/*,%2F%2A,*/*,%2A%2F	1
',%27,\x22,%22,char\W	1
;%3B	1
%2B,CONCAT\W	1
%3D	1
(,%28,)%29,@,%40	1
ascii,substring	1
version(,version%28,user(,user%28,system_user(,system_user%28,database(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,%40%40tmpdir,@@datadir,%40%40datadir	2

ルールおよび評価システムの実例

次に、スコアの集計方法とシナリオごとの処理方法の例を示します。

例1: トラフィックのログ記録と破棄が発生

次のルール設定 (グループのスコアはコロン (「:」) の後にあります) を使用すると仮定します。

```
drop table,drop+table,insert into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W,select\W:2
cast\W,exec\W,load_file:2
union\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--, %2D%2D, /*, %2F%2A, */ , %2A%2F:1
', %27, \x22, %22, char\W:1
;, %3B:1
%2B, CONCAT\W:1
%3D:1
(, %28, ), %29, @, %40:1
ascii, substring:1
version(, version%28, user(, user%28, system_user(, system_user%28, databas
(, database%28, @@hostname, %40%40hostname, @@basedir, %40%40basedir, @@tmpdir, %
40%40tmpdir, @@datadir,
%40%40datadir:2

Log Threshold:3
Drop Threshold: 4
```

ここで、次の攻撃文字列が発生したとします。

```
productID=BB10735166+UNION/**/+SELECT+FROM+user
```

次の集計をして、合計スコアは5 (2+1+0+2) になります。

- 文字列UNION/は4番目のグループに一致するためスコアは2。
- 文字列/**は6番目のグループに一致するためスコアは1。
- 文字列*/は6番目のグループに一致するためスコアは0 (6番目のグループのスコアは加算済み)。
- 文字列SELECT+は2番目のグループに一致するためスコアは2。

合計スコアは5で、ログが生成され、トラフィックは破棄されます。

例2: トラフィックのログ/破棄が発生しない

次のルール設定 (select\W文字列は、union\Wと同じ行に変更しました) を使用すると仮定します。

```
drop table,drop+table,insert into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W:2
cast\W,exec\W,load_file:2
union\W,select\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--, %2D%2D, /*, %2F%2A, */ , %2A%2F:1
', %27, \x22, %22, char\W:1
;, %3B:1
%2B, CONCAT\W:1
%3D:1
(, %28, ), %29, @, %40:1
ascii, substring:1
version(, version%28, user(, user%28, system_user(, system_user%28, databas
(, database%28, @@hostname, %40%40hostname, @@basedir, %40%40basedir, @@tmpdir,
%40%40tmpdir, @@datadir, %40%40datadir:2

Log Threshold:3
Drop Threshold: 4
```

ここで、次の攻撃文字列が発生したとします。

```
productID=BB10735166+UNION/**/+SELECT+FROM+user
```

次の集計をして、合計スコアは3 (2+1+0+0) になります。

- 文字列UNION/は4番目のグループに一致するためスコアは2。
- 文字列/*は6番目のグループに一致するためスコアは1。
- 文字列*/は6番目のグループに一致するためスコアは0 (6番目のグループのスコアは加算済み)。
- 文字列SELECT+は4番目のグループに一致するためスコアは0 (4番目のグループのスコアは加算済み)。

合計スコアは3で、ログは生成されず、トラフィックは破棄されません。ログや破棄が発生するには、スコアがしきい値を超える必要があります。

Generic SQL Injection Preventionルールを設定する

Generic SQL Injection Preventionルールを組織のニーズに合うように設定できます。設定可能なオプションを次の図に示します。

Generic SQL Injection Preventionのプロパティ - Internet Explorer

一般 脆弱性 詳細 **設定** オプション 割り当て対象

設定オプション

SQL Injection Patterns. One group per line separated by '\n'. The score for the group is at the end of the line after ':'. For '%' use %x2c and for '"' use %x22. The Maximum number of groups is 32.
eg. script, object, embed:2

drop table,drop+table,insert into,insert+into,values¥W,create table,create+table,delete¥W,update¥W,bulk insert,bulk+insert.shutdown¥W,from¥W?

Drop Threshold (if the score exceeds this value, the connection will be dropped): 4

Log Threshold (if the score exceeds this value, a log will be generated): 4

Max distance between matches (if this many characters go by without seeing a pattern in any group, the score is reset to 0): 35

Note: If Log Threshold is greater or equal to Drop Threshold then only Drop events will be generated. In the default configuration both are equal.

Pages (resource) with a non-default score to drop on. The score for each resource is at the end of the line after ':'. eg. /index.html:5 (One per line)

Form parameters with a non-default score to drop on. Each line begins with the resource name followed by the resource parameters separated by a ':'. The score for each parameter is set at the end of the parameter after '='. eg. /index.html:userid=5,passwd=7 (One per line)

ルールの表示...

OK キャンセル 適用

ルールを設定するには、次の手順に従います。

1. Deep Security Managerにログインします。
2. 画面上部の [ポリシー] をクリックします。
3. 右側にある検索ボックスにGeneric SQL Injection Preventionの番号IDの「1000608」を入力します。Enterキーを押します。メイン画面にルールが表示されます。
4. ルールをダブルクリックします。

5. [設定] タブをクリックします。画面上部のテキストボックスにSQLインジェクションパターンが表示されます。
6. カスタマイズをまだしていない場合は、このSQLインジェクションパターンを最新のバージョンにアップデートします。最新のパターンにアップデートするには、[詳細] タブに移動し、[Default SQL Pattern] 見出しの下のテキストをコピーし、[設定] タブの [SQL Injection Patterns] テキストボックスに貼り付けます。これで、トレンドマイクロの最新のパターンを使用できます。
7. 次のようにフィールドを編集します。
 - SQL Injection Patterns: SQLインジェクション攻撃に使用する文字と文字列のリストを指定します。文字と文字列はグループ化されており、スコアが割り当てられています。文字列を追加または変更する場合は、適切なエンコードを使用してください。詳細については、以下の["文字エンコードのガイドライン" on the next page](#)を参照してください。
 - Drop Threshold: 破棄スコアを指定します。このしきい値をスコアを超えると、接続は中断されます。(スコアがDrop Thresholdと一致した場合、接続は維持されます)。初期設定は4です。
 - Log Threshold: ログスコアを指定します。このしきい値をスコアを超えると、接続のログが記録されます(スコアがLog Thresholdと一致した場合、ログは記録されません)。初期設定は4です。
 - Max distance between matches: スコアを0にリセットする場合の一致の最大間隔をバイト数で指定します。初期設定は35です。
 - **注意:** 通常のしきい値では超過してしまう可能性があるページやフィールドのオーバーライドを作成する場合は、次の2つのオプションの使用を検討します。
 - Pages (resource) with a non-default score to drop on: 特定のリソースについては [Drop Threshold] をオーバーライドできます。たとえば、[Drop Threshold] は4ですが、アンケートページでは破棄スコアを8にする場合は、`/example/questionnaire.html:8`を指定します。この設定では、接続が中断される場合、`/example/questionnaire.html`には8より高いスコアが必要になりますが、その他すべてのリソースでは4より高いスコアで中断されます。リソースは1行に1つ指定します。
 - Form parameters with a non-default score to drop on: [Drop Threshold] または [Pages (resource) with a non-default score to drop on] フィールドで定義したしきい値を特定のフォームフィールドについてはオーバーライドできます。たとえば、[Drop Threshold] スコアは4ですが、ユーザ名フィールドについては破棄スコアを高くして10にする場合は、`/example/login.html:username=10`を指定します。ここ

で、`/example/login.html`はユーザ名フィールドが表示されるページのパスと名前に置き換え、`username`はアプリケーションで使用するユーザ名フィールドに置き換えます。この設定では、接続が中断される場合、ユーザ名フィールドではスコアが10より高くなる必要がありますが、ページ自体では4を超えると中断されます。フォームフィールドは1行に1つ指定します。

注意: [Log Threshold] は、[Pages (resource) with a non-default score to drop on] や [Form parameters with a non-default score to drop on] フィールドによる接続の中断時には有効になりません。たとえば、Form parametersフィールドを`/example/login.html:username=10`に設定していて、usernameフィールドのスコアが11の場合は、接続は中断されますが、このイベントのログは記録されません。

8. [OK] をクリックします。

これでGeneric SQL Injection Preventionルールの設定が完了しました。

文字エンコードのガイドライン

Generic SQL Injection Preventionルールに文字列の変更または追加をする場合は、適切にエンコードする必要があります。たとえば、パターン内で引用符「`'`」を使用する場合は、「`\x22`」を入力する必要があります。

以下の表に、文字とそのエンコード後の値、および拡張パターンを表現する場合に使用する文字クラスを示します。

入力する文字列	エンコードする文字
<code>\a</code> <code>\A</code>	英字 (a~z A~Z) 英字以外の文字 例: <code>delete\a</code> は「 <code>delete</code> 」の後に英字が続く」ことを意味します
<code>\w</code> <code>\W</code>	英数字 (a~z A~Z 0~9) 英数字以外の文字 例: <code>delete\w</code> は「 <code>delete</code> 」の後に英数字以外の文字が続く」ことを意味します

入力する文字列	エンコードする文字
\d \D	数字 (0～9) 数字以外の文字 例: delete\dは「delete」の後に数字 (0～9) が続く」ことを意味します
\s \S	空白文字 空白文字以外の文字 [\r,\n,\t,0x32] 例: delete\sは「delete」の後に空白以外の文字が続く」ことを意味します
\p \P	句読文字、上記以外の印字可能なASCII文字 句読文字以外の文字 例: delete\pは「delete」の後に句読文字または印字可能なASCII文字が続く」ことを意味します
\c \C	制御文字 (ASCIIの32番より前または127番以降、空白文字は含まない) 制御文字以外の文字
\.	任意
\xDD	16進数のバイト0xDD
\x2c	カンマ文字 (,)
\x22	2重引用符 (")
\\	エスケープされたバックスラッシュ (\)
	エスケープされたパイプ ()
xx xx xx...	16進数パイプ (バイトシーケンス)


アプリケーションの種類

アプリケーションの種類で定義されるアプリケーションは、トラフィックの方向、使用しているプロトコル、およびトラフィックが通過するポート番号によって識別されます。アプリケーションの種類は、共通の目的がある侵入防御ルールをグループ化する場合に役立ちます。ルールグループによって、侵入防御ルールセットを選択してコンピュータに割り当てる処理が簡略化されます。たとえば、Oracle Report ServerへのHTTPトラフィックの保護に必要な侵入防御ルールセットを検討してみます。「Web Server Common」および「Web Server Oracle Report Server」のアプリケーションの種類でルールを選択して、IISサーバ専用のルールをなど、必要のないルールを除外するだけです。

アプリケーションの種類の一覧を表示する

アプリケーションの種類の一覧を開きます。ここでは、既存のアプリケーションの種類のプロパティ表示の他、設定、エクスポート、および複製ができます。XMLまたはCSVファイルにエクスポートできます。XMLファイルをインポートできます。アプリケーションの種類の新規作成と削除もできます。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. [アプリケーションの種類]をクリックします。
3. コマンドをアプリケーションの種類に適用するには、種類を選択して、該当するボタンをクリックします。

ヒント: 設定可能なプロパティがあるアプリケーションの種類にはギアアイコンが表示されます。 

["ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 809](#)も参照してください。

一般情報

アプリケーションの種類の名前と説明です。[最小Agent/Applianceバージョン]は、このアプリケーションの種類をサポートするのに必要なDeep Security **Agent/Appliance**¹のバージョンを示します。

¹Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

接続

- 方向: 通信を開始する方向。つまり、2つのコンピュータ間で接続を確立する最初のパケットの方向です。たとえば、Webブラウザのアプリケーションの種類を定義する場合、これは通信を確立するための最初のパケットをサーバに送信するWebブラウザであるため、[送信]を選択します(サーバからブラウザに流れるトラフィックを調査する場合も同じです)。特定のアプリケーションの種類に関連付けられた侵入防御ルールは、いずれかの方向に流れる個々のパケットを調査するために作成できます。
- プロトコル: このアプリケーションの種類に適用されるプロトコル。
- ポート: このアプリケーションの種類が監視するポート(トラフィックが例外的に許可されているポートは含まれません)。

設定

[設定] タブには、アプリケーションの種類に関連付けられた侵入防御ルールの処理を制御するオプションが表示されます。たとえば、種類が「Web Server Common」のアプリケーションには「Monitor responses from Web Server」オプションがあります。このオプションの選択を解除すると、アプリケーションの種類に関連付けられた侵入防御ルールでは、応答トラフィックが検査されません。

オプション

[オプション] タブの項目は、Deep Security Managerがアプリケーションの種類を使用および適用する方法を制御します。たとえば、ほとんどのアプリケーションの種類には、そのアプリケーションを推奨設定の検索から除外するためのオプションがあります。つまり、[推奨設定から除外] オプションを選択すると、推奨設定の検索では、対象のアプリケーションが検出された場合でも、このアプリケーションの種類およびアプリケーションの種類に関連付けられた侵入防御ルールがコンピュータに推奨されません。

割り当て対象

[割り当て対象] タブには、アプリケーションの種類に関連付けられた侵入防御ルールが一覧表示されます。

SSLまたはTLSトラフィックの検査

侵入防御 モジュールでは、保護対象コンピュータの1つまたは複数のインタフェースで、特定のクレデンシャルとポートのペアに対してSSL検査を設定できます。

注意: 圧縮トラフィックまたはDeep Securityネットワークエンジンがタップモードで動作している場合、SSL検査はサポートされません。インラインモードまたはタップモードでの操作の詳細については、"[ネットワークエンジン設定](#)" on page 612を参照してください。

資格情報は、PKCS#12またはPEM形式でインポートできます。資格情報ファイルには、秘密鍵が含まれている必要があります。Windowsコンピュータでは、CryptoAPIを直接使用できません。

侵入防御 モジュールの概要については、"[侵入防御を使用した攻撃のブロックをブロックする](#)" on page 789を参照してください。

このトピックの内容:

- "[SSLインスペクションを設定する](#)" below
- "[ポート設定を変更する](#)" on the next page
- "[トラフィックがPerfect Forward Secrecy \(PFS\)で暗号化されている場合に侵入防御を使用する](#)" on page 825
- "[サポートされている暗号化スイート](#)" on page 826
- "[サポートされているプロトコル](#)" on page 827

SSLインスペクションを設定する

1. Deep Security Managerで、設定するコンピュータを選択し、[詳細] をクリックしてコンピュータエディタを開きます。
2. コンピュータエディタの左側の画面で、[侵入防御]→[詳細]→[SSL設定の表示] の順にクリックし、[SSL設定の表示] をクリックして [SSL設定] 画面を開きます。
3. [新規] をクリックして、SSL設定ウィザードを開きます。
4. このコンピュータで設定を適用するインタフェースを指定します。
 - このコンピュータのすべてのインタフェースに適用するには、[すべてのインタフェース] を選択します。
 - 特定のインタフェースに適用するには、[特定のインタフェース] を選択します。
5. [ポート] または [ポートリスト] を選択してリストを選択し、[次へ] をクリックします。

6. [IP選択] 画面で、[すべてのIP] を選択するか、SSLインスペクションを実行する [特定のIP] を指定し、[次へ] をクリックします。
7. [資格情報] 画面で、資格情報を指定する方法を選択します。
 - 今すぐ資格情報をアップロードします
 - 資格情報はコンピュータにあります

注意: 資格情報ファイルには、秘密鍵が含まれている必要があります。

8. 今すぐ資格情報をアップロードするオプションを選択する場合、資格情報の種類、格納場所、および必要に応じてパスワードを入力します。

資格情報がコンピュータにある場合、資格情報の詳細を指定します。

- コンピュータに格納されているPEMまたはPKCS#12資格情報形式を使用する場合は、その資格情報ファイルの格納場所と必要に応じてファイルのパスワードを入力します。
- Windows CryptoAPI資格情報を使用する場合は、コンピュータで見つかった資格情報のリストから対象の資格情報を選択します。

9. この設定の名前と説明を入力します。
10. 概要を確認して、SSL設定ウィザードを閉じます。設定操作の概要を読んで、[完了] をクリックしてウィザードを閉じます。

ポート設定を変更する

コンピュータのポート設定を変更して、クライアントがSSL対応ポートで適切な 侵入防御 フィルタを実行していることを確認します。加えた変更は、Agentコンピュータ上の特定のアプリケーションの種類 (Webサーバ共通など) に適用されます。この変更は、他のコンピュータ上のアプリケーションの種類には影響しません。

1. このコンピュータに適用されている 侵入防御 ルールのリストを表示するには、コンピュータの[詳細]画面の[侵入防御ルール]の順に選択します。
2. ルールを [アプリケーションの種類] 別にソートし、「Webサーバ共通」のアプリケーションの種類を探します(同様のアプリケーションの種類に対しても、これらの変更を加えることができます)。
3. アプリケーションの種類のルールを右クリックし、[アプリケーションの種類プロパティ] をクリックします。
4. 継承された「HTTP」ポートリストをオーバーライドして、SSLの設定時に定義したポートとポート80をこのポートリストに追加します。ポートはカンマ区切りの値として入力

します。たとえば、SSLの設定でポート9090を使用する場合は、「9090, 80」と入力します。

5. パフォーマンスを向上させるために、[設定] タブで、[継承] と [Webサーバからの応答を監視] の選択を解除します。
6. [OK] をクリックして画面を閉じます。

トラフィックがPerfect Forward Secrecy (PFS)で暗号化されている場合に侵入防御を使用する

Perfect Forward Secrecy (PFS) を使用することで、仮に後でサーバの秘密鍵が侵害された場合に復号できない通信チャネルを作成できます。Perfect Forward Secrecyの目的はセッションが終了した後に復号できなくすることなので、侵入防御モジュールによるSSLインスペクションもできなくなります。

この問題を回避するには、次の手順を実行することをお勧めします。

1. インターネットとロードバランサ (またはリバースプロキシ) の間のTLSトラフィックに Perfect Forward Secrecyを使用します。
2. ロードバランサ (またはリバースプロキシ) でPerfect Forward Secrecyセッションを終了します。
3. ロードバランサ (またはリバースプロキシ) とWebサーバまたはアプリケーションサーバ間のトラフィックに非PFS暗号スイート (["サポートされている暗号化スイート" on the next page](#) を参照) を使用して、サーバ上の 侵入防御 モジュールがTLSを復号化できるようにします。セッションを検査し、それらを検査します。
4. Perfect Forward Secrecyを使用しないアプリケーションサーバポートのトラフィックをWebサーバに制限します。

Diffie-Hellman暗号化の特別な注意事項

Perfect Forward Secrecyは、Diffie-Hellman鍵交換アルゴリズムに依存しています。初期設定でDiffie-Hellmanが使用されるWebサーバでは、SSLインスペクションが正常に動作しない場合があります。そのため、サーバの設定ファイルを確認して、Webサーバとロードバランサ (またはリバースプロキシ) の間のTLSトラフィックに対してDiffie-Hellman暗号化を無効にすることが重要です。ApacheサーバでDiffie-Hellmanを無効にするには、次の手順を実行します。

1. サーバの設定ファイルを開きます。Webサーバ設定ファイルのファイル名と場所は、OS およびディストリビューションによって異なります。たとえば、次のようなパスになります。

- RHELの初期インストールの場合: `/etc/httpd/conf.d/ssl.conf`
- Red Hat Linux上のApache 2.2.2の場合: `/apache2/conf/extra/httpd-ssl.conf`

2. 設定ファイル内で、「SSLCipherSuite」変数を探します。
3. 「!DH:!EDH:!ADH:」をこれらのフィールドに追加します (この文字列がまだ表示されていない場合)。(「!」:この暗号化をApacheで「使用しない」ように指定するものです)。
4. たとえば、Apache設定ファイルの暗号化スイートを次のように編集します。

SSLCipherSuite

```
!DH:!EDH:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

詳細については、ApacheドキュメントのSSLCipherSuiteに関する箇所を参照してください。
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslcipherSuite.

サポートされている暗号化スイート

16進値	OpenSSL名	IANA名	NSS名
0x00,0x04	RC4-MD5	TLS_RSA_WITH_RC4_128_MD5	SSL_RSA_WITH_RC4_128_MD5
0x00,0x05	RC4-SHA	TLS_RSA_WITH_RC4_128_SHA	SSL_RSA_WITH_RC4_128_SHA
0x00,0x09	DES-CBC-SHA	TLS_RSA_WITH_DES_CBC_SHA	SSL_RSA_WITH_DES_CBC_SHA
0x00,0x0A	DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSL_RSA_WITH_3DES_EDE_CBC_SHA
0x00,0x2F	AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA
0x00,0x35	AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA	TLS_RSA_WITH_AES_256_CBC_SHA
0x00,0x3C	AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256

16進値	OpenSSL名	IANA名	NSS名
0x00,0x3D	AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
0x00,0x41	CAMELLIA128-SHA	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
0x00,0x84	CAMELLIA256-SHA	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
0x00,0xBA	CAMELLIA128-SHA256	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
0x00,0xC0	非実装	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256

サポートされているプロトコル

次のプロトコルがサポートされます。

- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

回避技術対策の設定

回避技術対策の設定では、分析を回避しようとする異常なパケットに対するネットワークエンジンによる処理を管理します。回避技術対策の設定は、ポリシーまたは個々のコンピュータで設定されます。セキュリティモード設定は、侵入防御がパケットをどの程度厳密に分析するかを管理し、次のいずれかの値に設定できます。

- 標準: 誤検出が発生しないように侵入防御ルールの回避を防ぎます。これが初期設定値です。

- 厳格: 標準モードよりも厳密なチェックが行われますが、誤検出が発生する場合があります。厳密モードは侵入テストに役立ちますが、通常の状態下では有効にしないでください。
- カスタム: [カスタム] を選択すると、追加設定が可能になり、問題のあるパケットのでの処理方法を指定できます。この設定では、許可 (Deep Securityはパケットをシステムに送信します)、ログ記録のみ ([許可] と同じ処理をしますが、イベントをログに記録しません)、拒否 (Deep Securityはパケットを破棄し、イベントをログに記録します)、または拒否 (ログに記録しない) ([拒否] と同じ処理を行います、イベントをログに記録しません) を選ぶことができます (TCP PAWSウィンドウでは上記のオプションは選べません)。

注意: Deep Security 10.1以前のバージョンでモードを「カスタム」に変更した場合は、回避技術対策設定のすべての初期設定値が「拒否」に設定されていました。これにより、ブロックイベントが大幅に増加しました。Deep Security 10.2では、初期設定のカスタム値が次の表のように変更されています。

設定	説明	標準値	厳格値	初期設定のカスタム値 (10.2より前)	初期設定のカスタム値 (10.2以降)
無効なTCPタイムスタンプ	TCPタイムスタンプが古い場合の処理	無視とログ (ログのみと同じ機能)	拒否 (ログに記録)	拒否 (ログに記録)	無視とログ (ログのみと同じ機能)
TCP PAWSウィンドウ	パケットにはタイムスタンプが付加されている場合があります。パケットのタイムスタンプが、それ以前に受信したタイムスタンプよりも古い場合、不審なタイムスタンプが使用されている可能性があります。タイムスタンプの差異についての許容度は、OSによって異なります。Windowsシステムの場合	Linux Agentの場合は1、それ以外の場合	Linux Agentの場合は1、それ以外の場合	0	Linux Agentの場合は1、それ以外の場合

設定	説明	標準値	厳格値	初期設定のカスタム値 (10.2より前)	初期設定のカスタム値 (10.2以降)
	合、0を選択してください (パケットのタイムスタンプが、それ以前のパケットと同じ、もしくは新しい場合、システムがパケットを受容します)。Linuxシステムの場合は、1を選択してください (パケットのタイムスタンプの古さが、それ以前のパケットより最大で1秒未満の場合、システムがパケットを受容します)。	は0	は0		は0
TCPタイムスタンプ (PAWS: Protection Against Wrapped Sequence) の値がゼロ	TCPタイムスタンプがゼロの場合の処理	Linux Agent または NDIS5 の場合は拒否、それ以外の場合は許可	Linux Agent または NDIS5 の場合は拒否、それ以外の場合は許可	拒否 (ログに記録)	Linux Agent または NDIS5 の場合は拒否、それ以外の場合は許可
フラグメント化されたパケット	パケットがフラグメント化されている場合の処理	許可	許可	拒否 (ログに記録)	許可
TCPゼロフラグ	パケットにゼロフラグが設定されている場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに)	拒否 (ログに記録)

設定	説明	標準値	厳格値	初期設定のカスタム値 (10.2より前)	初期設定のカスタム値 (10.2以降)
				記録)	
TCP輻輳フラグ	パケットに輻輳フラグが設定されている場合の処理	許可	許可	拒否 (ログに記録)	許可
TCP緊急フラグ	パケットに緊急フラグが設定されている場合の処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可
TCP SYN FINフラグ	パケットにSYNおよびFINフラグが設定されている場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP SYN RSTフラグ	パケットにSYNおよびRSTフラグが設定されている場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP RST FINフラグ	パケットにRSTおよびFINフラグが設定されている場合の処理	拒否 (ログ	拒否 (ログ	拒否	拒否 (ログ

設定	説明	標準値	厳格値	初期設定のカスタム値 (10.2より前)	初期設定のカスタム値 (10.2以降)
		に記録)	に記録)	(ログに記録)	に記録)
TCP SYNパケット (データあり)	パケットにSYNフラグが設定されていて、かつデータが含まれる場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP Split Handshake	SYNへの応答としてSYNACKではなくSYNを受信した場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
識別できないTCPセッション上のRSTパケット	識別できないTCPセッション上のRSTパケットに対する処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可
識別できないTCPセッション上のFINパケット	識別できないTCPセッション上のFINパケットに対する処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可

設定	説明	標準値	厳格値	初期設定のカスタム値 (10.2より前)	初期設定のカスタム値 (10.2以降)
識別できないTCPセッション上の送信パケット	識別できないTCPセッション上の送信パケットに対する処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可
回避再送	複製または重複したデータを含むパケットに対する処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可
TCPチェックサム	無効なチェックサムを含むパケットに対する処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可

侵入防御のパフォーマンスに関するヒント

Deep Security Agentのシステムリソースの使用状況を改善するには、次に示すパフォーマンス関連の設定を最適化します。

侵入防御モジュールの概要については、"[侵入防御を使用した攻撃のブロックをブロックする](#)" [on page 789](#)を参照してください。

システムリソース	パフォーマンスに影響する設定
CPU使用率	<ul style="list-style-type: none"> • パケットが破棄またブロックされたときにイベントがログに記録されません。パケットの変更をログに記録すると、多くのログエントリが作成される可能性があります。 ("ルールにイベントログを設定する" on page 805を参照してください)。 • トラブルシューティング中にのみイベントログにパケットデータを含めます ("ルールにイベントログを設定する" on page 805を参照してください)。 • コンピュータのOSとアプリケーションに適用される侵入防御ルールを割り当てます。該当する脆弱性およびルールを検出するための推奨設定の検索の使用については、 "推奨設定の検索の管理と実行" on page 592を参照してください。 • 割り当てるルール数を300以下にします。
ネットワーク使用量またはスループット	<ul style="list-style-type: none"> • パケットが破棄またブロックされたときにイベントがログに記録されません。パケットの変更をログに記録すると、多くのログエントリが作成される可能性があります。 ("ルールにイベントログを設定する" on page 805を参照してください)。 • トラブルシューティング中にのみイベントログにパケットデータを含めます ("ルールにイベントログを設定する" on page 805を参照してください)。 • 特にポリシーに多数の署名が適用されている場合はWebサーバから応答を監視しないでください。 <ul style="list-style-type: none"> a. [ポリシー]→[侵入防御ルール] の順にクリックします。 b. アプリケーションの種類「Web Server Common」のルールを右クリックし、[アプリケーションの種類プロパティ] をクリックします。 c. [設定] タブで、[継承] と [Webサーバからの応答を監視] の選択を解除します。
ディスク使用量	<ul style="list-style-type: none"> • トラブルシューティング中にのみイベントログにパケットデータを含めます ("ルールにイベントログを設定する" on page 805を参照してください)。

設定パッケージの最大サイズ

Agentに大量の侵入防御ルールを割り当てている場合、設定パッケージのサイズが最大許容サイズを超えることがあります。許容サイズを超えると、Agentのステータスが「Agentの設定パッケージが大きすぎる」に変わり、イベントメッセージ「設定パッケージが大きすぎる」が表示されます。

注意: 32ビットのWindowsプラットフォームでは、使用できるカーネルメモリが小さいため、設定制限が20MBまでになっています。他のプラットフォームでは、制限は32MBです。

パフォーマンス上の理由から、1台のコンピュータに割り当てる侵入防御ルールは350未満にしてください。必要なルールの数を最小限にするために、コンピュータのOSとインストールされているサードパーティのソフトウェアに、使用可能なすべてのパッチが適用されていることを確認してください。

1. 使用可能なパッチをコンピュータのOSに適用します。
2. 使用可能なパッチをインストールされているすべてのサードパーティのソフトウェアに適用します。
3. 推奨設定の検索で推奨されている侵入防御ルールのみを適用します。コンピュータからすべてのルール、または割り当ての解除が推奨されている割り当て済みポリシーを削除します("推奨設定の検索の管理と実行" on page 592を参照してください)。
4. ポリシーレベルで侵入防御を管理していて、設定パッケージがまだ大きすぎる場合は、次のいずれかの方法で侵入防御を設定します。
 - ポリシー内のすべてのサーバが同じOSとアプリケーションを持つように、ポリシーを細分化します。
 - コンピュータのルールが自動的に追加および削除されるように、侵入防御をサーバレベルで管理します。

侵入防御をサーバレベルで管理するには、次の手順に従います。

1. コンピュータに割り当てられているポリシーをエディタで開きます。
2. [侵入防御]→[一般]の順にクリックします。
3. [推奨設定] セクションで、[侵入防御の推奨設定を自動的に適用 (可能な場合)] を [はい] に設定します。
4. ポリシーからすべての侵入防御ルールを削除します。
5. コンピュータで推奨設定の検索を実行します。

ファイアウォールを使用したエンドポイントトラフィックの制御

ファイアウォールモジュールは、受信/送信トラフィックの双方向のステートフルインスペクションを提供します。ファイアウォールルールでは、そのトラフィックの個々のパケットに対して実行する処理を定義します。パケットは、すべてのIPベースのプロトコルとフレームタイプで、IPアドレスとMACアドレス、ポートとパケットフラグを使ってフィルタできます。ファイアウォールモジュールはまた、DoS攻撃を防ぎ、攻撃の予兆検索を検出して防ぐのにも役立ちます。

ファイアウォールを有効にして設定するには、"[Deep Securityファイアウォールの設定](#)" on the next pageを参照してください。

ファイアウォールルール

ファイアウォールルールでは、優先度の順に示した次のいずれかの処理によってトラフィックを処理できます。

- バイパス
- ログ記録のみ
- 強制的に許可
- 拒否 (ログに記録)
- 許可

また、ルールには4 (優先度が最も高い) ~ 0 (優先度が最も低い) の優先度があります。特定の優先度内では、上記のルール処理の種類における優先度に基づいた順序で処理されます。つまり、他のファイアウォールの設定時と異なり、Deep Securityファイアウォールでは割り当て順に関係なくルールが処理されます。

ルールの優先度と処理で処理順序が決まる仕組みの詳細については、「"[ファイアウォールルールの処理と優先度](#)" on page 858」を参照してください。

ファイアウォールルールの作成方法の詳細については、"[ファイアウォールルールの作成](#)" on page 850を参照してください。

注意: ルールを作成するときは、配信する前に、ファイアウォールモジュールのタップモードとインラインモードを使用して必ずテストしてください。この方法の詳細については、

["Deep Securityファイアウォールの設定" below](#)の「ファイアウォールルールを配信前にテストする」セクションを参照してください。

Deep Securityファイアウォールの設定

Deep Securityのファイアウォールは非常に柔軟なファイアウォールで、制限の多い厳格な設定にすることも、少ない寛容な設定にすることもできます。侵入防御やWebレピュテーションモジュールと同様に、ファイアウォールモジュールもインラインまたはタップモードの2つのモードで実行できます。ファイアウォールルールをタップモードでテストし、すべてが正しく動作することを確認してからインラインモードに切り替えることを推奨します。

ファイアウォールの設定と管理は慎重に行う必要があります、すべての環境に合うルールセットは存在しません。ルールの作成を開始する前にファイアウォールの処理と優先度を理解しておく必要があります。許可ルールを作成する場合、定義されていない対象がすべて默示的に拒否されるため、特に注意が必要です。

このトピックの内容:

- ["ファイアウォールルールを配信前にテストする" below](#)
- ["「Fail-Open」の動作を有効にする" on page 838](#)
- ["ファイアウォールをオンにする" on page 840](#)
- ["初期設定のファイアウォールルール" on page 840](#)
- ["厳格または寛容なファイアウォール設計" on page 842](#)
- ["ファイアウォールルールの処理" on page 843](#)
- ["ファイアウォールルールの優先度" on page 844](#)
- ["推奨されるファイアウォールポリシールール" on page 845](#)
- ["ファイアウォールルールをテストする" on page 845](#)
- ["攻撃の予兆検索" on page 846](#)
- ["ステートフルインスペクション" on page 848](#)
- ["例" on page 848](#)
- ["重要事項" on page 849](#)

ファイアウォールルールを配信前にテストする

ファイアウォールモジュール (および侵入防御モジュール、Webレピュテーションモジュール) には、パケットをブロックするか許可するかを決定するDeep Securityネットワークエンジンが

含まれます。ファイアウォールモジュールと侵入防御モジュールの場合、ネットワークエンジンはパケットのサニティチェックを実行し、ファイアウォールと侵入防御のルールを各パケットが通過することも確認します。ネットワークエンジンは次の2つのモードで動作します。

- **タップモード:** パケットストリームは変更されません。ファイアウォールまたは侵入防御モジュールが有効になっている場合、トラフィックはこれらによって処理されます。ただし、問題が検出されてもパケットや接続が拒否されることはありません。タップモードでは、Deep Securityはイベントのレコードを提供する以外の保護は提供しません。
- **インラインモード:** パケットストリームがDeep Securityネットワークエンジンを直接流れます。すべてのルールは、プロトコルスタックの上位に伝わる前にネットワークトラフィックに適用されます。

配信前はルールの処理を [ログ記録のみ] に設定し、タップモードかインラインモードのいずれかでファイアウォールルールをテストすることが重要です。これにより、トラフィックに対するルールの影響を、処理を実行することなくプレビューできます。配信前にルールをテストしない場合、トラフィックがすべてブロックされ、コンピュータにアクセスできなくなる可能性があります。

タップモードでテストする

タップモードでは、トラフィックのフローを妨げることなくファイアウォールルールをテストできます。

1. Deep Security Managerの [コンピュータ] または [ポリシー] に移動します。
2. コンピュータ (またはポリシー) を右クリックして [詳細] を選択し、**コンピュータエディタまたはポリシーエディタ¹**を開きます。
3. [設定]→[詳細]→[ネットワークエンジンモード] の順に選択します。
4. リストから [タップ] を選択し、[保存] をクリックします。
5. ルールを作成し、[OK] をクリックします。ルールを確認するには、[イベントとレポート]→[イベント]→[ファイアウォールイベント] に移動します。

注意: タップモードではルールの処理を [ログ記録のみ] に設定する必要はありません。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ファイアウォールルールの結果に問題がない場合は、**コンピュータエディタまたはポリシーエディタ**¹に戻ってドロップダウンリストから [インライン] を選択し、[保存] をクリックします。

インラインモードでテストする

多くの場合、トラフィックを妨げることなくファイアウォールルールをテストするにはタップモードが良い方法となります。しかし、ルールの処理を [ログ記録のみ] に設定すると、インラインモードでもルールをテストできます。この方法ではトラフィック分析の実際のプロセスが発生し、パケットのブロックや拒否などの処理を実行する必要がありません。

1. Deep Security Managerの [コンピュータ] または [ポリシー] に移動します。
2. コンピュータ (またはポリシー) を右クリックして [詳細] を選択し、**コンピュータエディタまたはポリシーエディタ**²を開きます。
3. [設定]→[詳細]→[ネットワークエンジンモード] の順に選択します。
4. ドロップダウンメニューから [インライン] を選択し、[保存] をクリックします。
5. ルールを作成するときは、処理を [ログ記録のみ] に設定しておきます。
6. ルールを確認するには、[イベントとレポート]→[イベント]→[ファイアウォールイベント] に移動します。

ファイアウォールルールの結果に問題がない場合は、処理を [ログ記録のみ] から任意の処理に変更し、[OK] をクリックします。

「Fail-Open」の動作を有効にする

ケースによっては、ファイアウォールルール (または侵入防御ルール) を適用する前にネットワークエンジンがパケットをブロックすることがあります。初期設定では、ネットワークエンジンは次の場合にパケットをブロックします。

- AgentまたはVirtual Applianceにメモリ不足などのシステム上の問題がある。
- パケットのサニティチェックでエラーが発生する。

この「Fail-Closed」動作により、高度なセキュリティが提供されます。AgentまたはVirtual Applianceが正常に機能していないときもサイバー攻撃がネットワークに侵入することはできず、不正と思われるパケットから保護できます。「Fail-Closed」の問題は、Agentまたは

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Virtual Applianceの問題によってサービスおよびアプリケーションが利用できなくなる場合があります。また、パケットのサニティチェックの誤判定が多いために大量のパケットが必要以上にドロップされ、パフォーマンスの問題が発生することもあります。

サービス可用性に関して懸念がある場合は、以下の手順に従って、システムエラーやパケットチェックエラーの場合にもパケットの通過を許可する(「Fail-Open」にする)ように初期設定の動作を変更できます。

1. Deep Security Managerの [コンピュータ] または [ポリシー] に移動します。
2. コンピュータ (またはポリシー) を右クリックして [詳細] を選択し、**コンピュータエディタまたはポリシーエディタ¹**を開きます。
3. 左側にある [設定] をクリックします。
4. [詳細] タブをクリックします。
5. [ネットワークエンジン設定] で、[エラー発生時の処理] を次のように設定します。
6. Deep Securityネットワークエンジンで問題が発生した場合 (メモリ不足エラー、割り当てメモリエラー、ネットワークエンジンの Deep Packet Inspection (DPI) デコードエラーなど) のパケットの通過を許可するには、[ネットワークエンジンのシステムエラー] を [Fail-Open] に設定します。ここで、Fail-Openの使用を検討するのは、高負荷やリソース不足によりAgentまたはVirtual Applianceでネットワーク例外が頻繁に発生する場合適です。「Fail-Open」を使用すると、ネットワークエンジンはパケットの通過を許可し、ルールのチェックを実行せず、イベントをログに記録します。AgentまたはVirtual Applianceに問題がある場合でも、サービスとアプリケーションは利用し続けることができます。
7. ネットワークエンジンのパケットのサニティチェックでエラーとなるパケットの通過を許可するには、[ネットワークパケットのサニティチェックエラー] を [Fail-Open] に設定します。パケットのサニティチェックの例としては、ファイアウォールのサニティチェック、ネットワーク層2、3、または4の属性チェック、TCP状態チェックなどがあります。ここで、Fail-Openの使用を検討するのは、サニティチェックを通過する「良好な」パケットでのみルールチェックを実行する場合です。Fail-Openを使用すると、ネットワークエンジンはエラーパケットの通過を許可し、ルールのチェックを実行せず、イベントをログに記録します。
8. [保存] をクリックします。

これで、システムまたはパケットチェックエラーに対するFail-Open動作が有効になります。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ファイアウォールをオンにする

コンピュータでファイアウォール機能を有効にするには、次の手順に従います。

1. **コンピュータエディタまたはポリシーエディタ**¹で、[ファイアウォール]→[一般]の順に選択します。
2. Deep Security Agent 11.1以前では、ホストコンピュータのネットワークインタフェースを通過してコンテナに向かうトラフィックがファイアウォールモジュールによって監視されます。Deep Security Agent 11.2以降では、コンテナ間のトラフィックを監視することもできます。[コンテナのネットワークトラフィックの検索]設定が[はい]に設定されている場合、コンテナとホストの両方を通過するトラフィックがDeep Securityによって検索されます。[いいえ]に設定されている場合、Deep Securityで検索されるのは、ホストネットワークインタフェースを通過するトラフィックだけです。
3. [オン]を選択し、[保存]をクリックします。

初期設定のファイアウォールルール

初期設定では、Deep Securityに組み込みのポリシーに送信ルールは割り当てられていませんが、受信ルールは割り当てられています。各ポリシーに割り当てられた初期設定の受信ルールは、該当するオペレーティングシステムポリシーで[ファイアウォール]タブを選択して確認できます。次の例は、Windows 10 Desktopポリシーに初期設定で割り当てられているファイアウォールルールを示しています。これらのファイアウォールルールは環境のニーズに合わせて設定できますが、すぐに始められるようにいくつかの初期設定ルールがあらかじめ用意されています。

ヒント: システムパフォーマンスへの影響を最小限に抑えるには、300件より多くファイアウォールルールを割り当てないようにします。また、ファイアウォールルールへの変更をそのルールの[説明]フィールドに記録することも推奨します。より簡単にファイアウォールをメンテナンスするために、ルールを作成または削除した日付とその理由を記録してください。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

コンピュータ:

概要

不正プログラム対策

Webレピュテーション

ファイアウォール

侵入防御

変更監視

セキュリティログ監視

アプリケーションコント

インターフェース

設定

アップデート

オーバーライド

一般 インタフェース制限 攻撃の予兆 詳細 ファイアウォールイベント

ファイアウォール

設定: 継承 (オン) ▼

ステータス: ● オン, 8 ルール

ファイアウォールステートフル設定

グローバル (すべてのインタフェース)

Ethernet - 00:50:56:9E:CF:82 (DHCP)

ポート検索

前回のポートの検索: なし

検索されたポート: なし

オープンポート: なし

オープンポートの検索
ポート検索のキャンセル

コンテナの保護

コンテナのネットワークトラフィックの検索:

割り当てられたファイアウォールルール

割り当て/割り当て解除...
プロパティ...
エクスポート ▼
列...

名前 ^	処理の種類	優先度	方向	フレーム...
Allow ICMP fragmentation pack...	強制的に許可	2 - 標準	受信	IP
Allow solicited ICMP replies	許可	0 - 最低	受信	IP
Allow solicited TCP/UDP replies	許可	0 - 最低	受信	IP

Deep Security Managerのトラフィックに関するバイパスルールの初期設定

Deep Security Managerは、Deep Security Agentを実行しているコンピュータでAgentがハートビートに使用する待機ポート番号を開く優先度4のバイパスルールを自動的に実装します。このルールは優先度4なので、他の拒否ルールよりも先に適用されます。また、バイパスルールなので、トラフィックの障害が発生することはありません。なお、このバイパスルールは内部的に作成されるため、ファイアウォールルールの一覧には明示的に表示されません。

ただし、このルールでは、任意のIPアドレスと任意のMACアドレスからのトラフィックが許可されます。Deep Security Agentの待機ポートのセキュリティを強化するには、このポート用により厳しいバイパスルールを作成します。新しいカスタムルールが以下の設定になっていれば、Agentはこのルールで初期設定のDeep Security Managerトラフィックルールをオーバーライドします。

- 優先度: 4 (最高)
- パケット方向: 受信
- フレームの種類: IP
- プロトコル: TCP
- パケット送信先ポート: [Agentのハートビートの待機ポート](#)

初期設定のルールをカスタムルールに置き換えるには、カスタムルールに上記のパラメータが必要です。ルールのパケット送信元として、実際のDeep Security ManagerのIPアドレスまたはMACアドレスを使用するのが理想です。

厳格または寛容なファイアウォール設計

一般に、ファイアウォールポリシーは、2つの設計戦略のどちらかに基づいています。つまり、明示的に拒否されていないかぎりすべてのサービスを許可するか、明示的に許可されていないかぎりすべてのサービスを拒否するかのいずれかです。どちらのタイプのファイアウォールを実装するか決定しておくことを推奨します。これにより、ルールの作成とメンテナンスにかかる管理の手間を削減できます。

厳格なファイアウォール

厳格なファイアウォールは、セキュリティの観点から推奨されます。初期設定ではすべてのトラフィックがブロックされ、明示的に許可されたトラフィックだけが許可されます。計画しているファイアウォールの主な目的が不正なアクセスをブロックすることであれば、接続を許可するのではなく制限することを重視する必要があります。厳格なファイアウォールはメンテナ

ンスが比較的容易であり、安全性にも優れています。許可ルールを使用して、ファイアウォールを通過する特定のトラフィックだけを許可し、他はすべて拒否します。

注意: 送信の許可ルールを1つ割り当てると同時に、送信ファイアウォールが制限モードで稼働します。これは受信ファイアウォールの場合も同じです。受信の許可ルールを1つ割り当てると同時に、受信ファイアウォールが制限モードで稼働します。

寛容なファイアウォール

寛容なファイアウォールは、初期設定ですべてのトラフィックを許可し、設定されている拒否ファイアウォールルールに基づいて既知の不正なポート/プロトコルのみをブロックします。寛容なファイアウォールは実装は容易ですが、提供されるセキュリティは最小限であり、複雑なルールが必要です。拒否ルールを使用して、トラフィックを明示的にブロックします。

ファイアウォールルールの処理

ファイアウォールは、以下の処理を実行するように設定できます。

警告: 受信ルールのみを割り当てると、送信トラフィックはすべて許可されます。送信許可ルールを1つ割り当てると、送信ファイアウォールは制限モードで稼働します。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていないかぎり、常に許可されます。

許可	<p>ルールと一致するトラフィックの通過を明示的に許可し、その他のトラフィックは黙示的に拒否します。</p> <p>注意: [許可] の処理は定義されていないトラフィックをすべて黙示的に拒否するため、この処理は慎重に使用する必要があります。関連するルールを正しく定義せずに許可ルールを作成すると、許可ルールで許可したトラフィックを除き、すべてのトラフィックがブロックされる可能性があります。許可ルールで明示的に許可されていないトラフィックは破棄され、ポリシーで「未許可」のファイアウォールイベントとして記録されます。</p>
バイパス	<p>ファイアウォールと侵入防御分析の両方のバイパスをトラフィックに許可します。バイパスルールは常にペアで (受信トラフィックと送信トラフィックの両方に対して) 作成する必要があります。バイパスルールは、IP、ポート、トラフィックの方向、プロトコルに基づいて設定できます。</p>

	バイパスルールは、ネットワーク負荷の高いプロトコルや、信頼済みソースからのトラフィックのために設計されたものです。
拒否	ルールと一致するトラフィックを明示的にブロックします。
強制的に許可	強制的に許可ルールに一致したパケットは通過しますが、この場合でも侵入防御によるフィルタリングは行われます。イベントはログに記録されません。 UDPおよびICMPトラフィックには、この種類のファイアウォールルール処理を使用する必要があります。
ログのみ	トラフィックがルールに一致した場合、ログに記録されます。その他の処理は実行されません。

ファイアウォールルールの作成方法の詳細については、「["ファイアウォールルールの作成" on page 850](#)」を参照してください。

ファイアウォールルールの優先度

ルールの優先度によって、フィルタが適用される順序が決定します。優先度の低いルールよりも優先度の高いルールが優先的に適用されます。同じ優先度の処理が複数存在する場合のルールの優先度は、「バイパス」、「強制的に許可」、「拒否」の順になります。ただし、より高い優先度が適用された拒否処理は、より低い優先度が適用されたバイパス処理よりも優先されます。ルールの優先度と処理で処理順序が決まる仕組みの詳細については、「["ファイアウォールルールの処理と優先度" on page 858](#)」を参照してください。

ファイアウォールルールの管理を簡略化するには、特定の処理に対して所定の優先度を固定します。たとえば、バイパスを使用するルールには初期設定の優先度3を、強制的に許可ルールには優先度2を、拒否ルールには優先度1を適用します。こうすることで、ルールの競合を削減できます。

許可ルール

許可ルールに適用できる優先度は0のみです。これは、より高い優先度の強制的に許可ルールおよび拒否ルールがすべて適用された後で許可ルールが処理されるようにするためです。許可ルールを使用してトラフィックを黙示的に拒否するときにはこの点に注意してください(許可ルールに一致しないトラフィックはすべて拒否されます)。こうすることで、拒否ルールを割り当てると、割り当てられている既存のすべての許可ルールよりも拒否ルールが優先されます。

強制的に許可ルール

強制的に許可ルールは、常に許可する必要があるトラフィック (アドレス解決プロトコル (ARP) など) に推奨されるルールで、同じまたはより高い優先度の拒否ルールに対してのみ機能します。たとえば、10.0.0.0/8サブネットから許可ポート番号へのアクセスを禁止する優先度3の拒否ルールがあり、ホスト10.102.12.56にこのポート番号へのアクセスを許可したいとします。この場合、優先度3の拒否ルールに対して優先度3または4の強制的に許可ルールを作成する必要があります。あるパケットがこのルールに該当するとそのアクセスはただちに許可され、優先度の低いルールは以降このアクセスを処理できなくなります。

バイパスルール

バイパスルールは、ファイアウォールエンジンと Deep Packet Inspection (DPI) エンジンの両方をバイパスすることをパケットに許可する特別なルールです。このルールは優先度4に設定し、ペアで作成する必要があります (各トラフィック方向に対して1つ)。

推奨されるファイアウォールポリシールール

すべてのファイアウォールポリシーに対して以下のルールを必須にすることを推奨します。

- ARP: コンピュータへの受信ARP要求を許可し、コンピュータがMACアドレスのクエリに応答できるようにします。このルールを割り当てないと、ネットワーク上のデバイスはホストにMACアドレスで照会できず、ホストにネットワークからアクセスできなくなります。
- Allow solicited TCP/UDP replies: コンピュータが、送信したTCP接続やUDPのメッセージへの応答を受信できるようにします。これは、TCPとUDPのステートフルファイアウォール設定と連携します。
- Allow solicited ICMP replies: コンピュータが、送信したICMPメッセージへの応答を受信できるようにします。これは、ICMPのステートフルファイアウォール設定と連携します。
- DNS Server: DNSサーバが受信DNSクエリを受け取ることができるようにします。
- Remote Access RDP: コンピュータがリモートデスクトップ接続を受け入れることができるようにします。
- Remote Access SSH: コンピュータがSSH接続を受け入れることができるようにします。

ファイアウォールルールをテストする

以降のファイアウォール設定手順に進む前に、推奨されるファイアウォールルールをテストし、それらが正しく動作することを確認します。

次の手順でRemote Access SSHルールをテストします。

1. コンピュータに対するSSH接続の確立を試みます。ファイアウォールが有効でも、Remote Access SSHルールが有効になっていないと、接続は拒否されます。[イベントとレポート]→[ファイアウォールイベント]の順に選択し、拒否されたイベントを表示します。
2. **コンピュータエディタまたはポリシーエディタ**¹で [ファイアウォール] に移動します。[割り当てられたファイアウォールルール] で [割り当て/割り当て解除] をクリックします。
3. Remote Access SSHを検索してそのルールを有効にします。[OK] をクリックし、[保存] をクリックします。
4. コンピュータに対するSSH接続の確立を試みます。接続が許可されます。

次の手順でRemote Access RDPルールをテストします。

1. コンピュータに対するRDP接続の確立を試みます。ファイアウォールが有効でも、Remote Access RDPルールが有効になっていないと、接続は拒否されます。[イベントとレポート]→[ファイアウォール] イベントの順に選択し、拒否されたイベントを表示します。
2. **コンピュータエディタまたはポリシーエディタ**²で [ファイアウォール] に移動します。[割り当てられたファイアウォールルール] で [割り当て/割り当て解除] をクリックします。
3. Remote Access RDPを検索してそのルールを有効にします。[OK] をクリックし、[保存] をクリックします。
4. コンピュータに対するRDP接続の確立を試みます。接続が許可されます。

攻撃の予兆検索

攻撃の予兆検索を検出するようにファイアウォールを設定し、一時的に送信元IPからのトラフィックをブロックして攻撃の防止を図ることができます。攻撃が検出されると、一時的に送信元IPからのトラフィックをAgentおよびApplianceでブロックするように設定できます。ポリシーまたはコンピュータエディタの [ファイアウォール]→[攻撃の予兆] タブにある [トラフィックのブロック] リストを使用し、時間 (分数) を設定してください。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- OSのフィンガープリント調査: AgentまたはApplianceはコンピュータのOSを見つけようとする動作を検出します。
- ネットワークまたはポートの検索: AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしていることを検出した場合、ネットワークまたはポート検索をレポートします。通常、AgentまたはApplianceのコンピュータは、コンピュータ自身宛てのトラフィックのみを監視するため、ポート検索が最も一般的に検出されます。コンピュータまたはポート検索の検出で使用される統計的な分析方法は「TAPS」アルゴリズムから導出されたもので、2006年にIPCCCで発表された「Connectionless Port Scan Detection on the Backbone」で提案されました。
- TCP Null検索: AgentまたはApplianceはフラグが付いていないパッケージを検出します。
- TCP SYNFIN検索: AgentまたはApplianceはSYNフラグおよびFINフラグの付いたパケットのみを検出します。
- TCP Xmas検索: AgentまたはApplianceは、FINフラグ、URGフラグ、およびPSHフラグの付いたパケット、または値0xFF (想定されるすべてのフラグ) を含むパケットを検出します。

攻撃の種類ごとに、オプション [DSMにただちに通知] を選択することにより、アラートがトリガされるDeep Security Managerに情報を送信するようAgentまたはApplianceを設定できます。このオプションを有効にするには、ポリシー/コンピュータエディタ→設定→一般→通信方向で、クライアントまたはアプライアンスが開始した、またはアプライアンスが開始した、または双方向の通信用にクライアントとアプライアンスを設定する必要があります。この設定を有効にすると、AgentまたはApplianceは、攻撃や調査を検出後ただちにDeep Security Managerに対してハートビートを送信します。

注意: 攻撃の予兆の保護を有効にする場合は、ポリシーまたはコンピュータエディタの [ファイアウォール]→[一般] タブで、ファイアウォールおよびステートフルインスペクションも有効にする必要があります。また、ポリシーまたはコンピュータエディタの [ファイアウォール]→[詳細] タブで、[「ポリシーの許可外」のパケットのファイアウォールイベントを生成] 設定も有効にする必要があります。これにより、攻撃の予兆に必要なファイアウォールイベントが生成されるようになります。

注意: 攻撃の予兆の検出では、1つ以上のアクティブなファイアウォールルールがAgentのポリシーに割り当てられている必要があります。

攻撃の予兆警告に対応する方法の詳細については、"[警告: 攻撃の予兆の検出](#)" on page 1374を参照してください。

ステートフルインスペクション

Deep Securityファイアウォールがオンのときは、ファイアウォールステートフル設定メカニズムを有効にする必要があります。このメカニズムでは、トラフィック履歴との関連における各パケット、TCPおよびIPヘッダ値の正当性、およびTCP接続状態の推移が分析されます。UDPやICMPなどのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実装されます。

パケットは、ステートフルメカニズムによって次のように処理されます。

1. 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
2. パケットを調べて、既存の接続に属しているかどうか判断されます。
3. TCPヘッダの正当性(シーケンス番号、フラグの組み合わせなど)が調査されます。

ステートフルTCP、ICMP、またはUDPプロトコルが指定された初期設定が有効で、要請された応答だけが許可されている場合、Deep Securityのファイアウォールステートフル設定によってDoSなどの攻撃から防御できます。UDPステートフルオプションが有効な場合は、UDPサーバ(DHCPなど)の実行時に強制的に許可を使用する必要があります。Deep Security AgentにDNSサーバまたはWINSサーバが設定されていない場合は、NetBIOSに対して、受信のUDPポート137を強制的に許可するルールが必要になることがあります。

ステートフルログは、ICMPまたはUDPプロトコルで必要でない限り無効にする必要があります。

例

Webサーバ用の単純なファイアウォールポリシーを作成する方法の例を示します。

1. オプションが有効になっているグローバルなファイアウォールステートフル設定を使用して、TCP、UDP、およびICMPのステートフルインスペクションを有効にします。
2. ワークステーションからの要求に対するTCPおよびUDPの応答を許可するファイアウォールルールを追加します。そのためには、受信許可ルールを作成し、プロトコルセットを[TCP+UDP]に設定し、[指定フラグ]の下にある[選択以外]と[SYN]をオンにします。この時点で、ワークステーションのユーザからの要求に回答するTCPとUDPのパケットだけがポリシーによって許可されます。たとえば、手順1で有効にしたステートフル分析オプションと連動してこのルールを使用すると、コンピュータのユーザはDNS検索(UDP経由)やHTTP(TCP)経由のWeb閲覧ができるようになります。
3. ワークステーションからの要求にICMP応答を許可するファイアウォールルールを追加します。そのためには、プロトコルを[ICMP]に設定した受信許可ルールを作成し、[任意のフラグ]チェックボックスをオンにします。このコンピュータのユーザは別のワークス

テーションにpingを送信して応答を受信できますが、他のユーザはこのコンピュータにpingを送信できなくなります。

4. [指定フラグ] セクションの [SYN] チェックボックスをオンにして、受信TCPトラフィックをポート80およびポート443に対して許可するファイアウォールルールを追加します。外部ユーザがこのコンピュータのWebサーバにアクセスできるようになります。

この時点で、他の受信トラフィックをすべて拒否するコンピュータで、承諾されたTCP、UDP、およびICMP応答とWebサーバへの外部アクセスを許可する基本的なファイアウォールポリシーが設定されます。

拒否ルールおよび強制的に許可ルールの処理を使用してこのポリシーをさらに詳細に定義する方法の例について、ネットワーク内の他のコンピュータからのトラフィックを制限する方法を考察します。たとえば、内部ユーザに対してはこのコンピュータのWebサーバへのアクセスを許可し、DMZにあるコンピュータからのアクセスは拒否するものとします。この場合、DMZのIP範囲にあるサーバからのアクセスを禁止する拒否ルールを追加することによって設定が可能になります。

5. 送信元IP 10.0.0.0/24 (DMZ内のコンピュータに割り当てられたIP範囲) を使用して、受信TCPトラフィック用に拒否ルールを追加します。このルールでは、DMZ内にあるコンピュータからこのコンピュータへのトラフィックをすべて拒否します。

ただし、このポリシーをさらに詳細に定義するとDMZ内にあるメールサーバからの受信トラフィックを許可できます。

6. 送信元IP 10.0.0.100からの受信TCPトラフィックに強制的に許可ルールを使用します。この強制的に許可ルールは、前の手順で作成した拒否ルールをオーバーライドして、DMZ内にあるコンピュータからのトラフィックを許可します。

重要事項

- すべてのトラフィックは、まずファイアウォールルールと照合されてからステートフルインスペクションエンジンで分析されます。トラフィックがファイアウォールルールを通過した場合は、ステートフルインスペクションエンジンによって分析されます (ステートフルインスペクションがファイアウォールステートフル設定で有効になっているものとします)。
- 許可ルールは暗黙の拒否ルールを含んでいます。許可ルールで指定されていないトラフィックは自動的に破棄されます。このルールには他の種類のフレームのトラフィックが含まれるため、他のフレームの種類の必要なトラフィックを許可するルールを含める必要

があります。たとえば、静的ARPテーブルを使用していない場合にはARPトラフィックを許可するルールを忘れずに含める必要があります。

- UDPのステートフルインスペクションが有効になっている場合は、強制的に許可ルールを使用して未承諾のUDPトラフィックを許可する必要があります。たとえば、UDPステートフルインスペクションがDNSサーバで有効になっている場合に、サーバが受信DNS要求を受け入れるように、強制的に許可ルールをポート53に設定する必要があります。
- ICMPのステートフルインスペクションが有効になっている場合は、強制的に許可ルールを使用して未承諾のICMPトラフィックを許可する必要があります。たとえば、外部のping要求を許可する場合は、ICMPタイプ3 (エコー要求) を強制的に許可するルールが必要です。
- 強制的に許可の処理は、同じ優先度のコンテキスト内でのみ切り札として機能します。
- テスト環境でよく見られるようにDNSまたはWINSサーバが設定されていない場合は、受信のUDPポート137を強制的に許可するルールがNetBIOS (Windows共有) に必要となることがあります。

注意: 新しいファイアウォールポリシーのトラブルシューティング時には、まず**AgentまたはAppliance¹**にあるファイアウォールルールのログを確認してください。ファイアウォールルールのログには、拒否されているトラフィックを判断するために必要な情報がすべて含まれており、必要に応じてポリシーをさらに詳細に設定できます。

ファイアウォールルールの作成

ファイアウォールルールは、個々のパケットの制御情報を確認し、定義された条件に従ってブロックまたは許可します。ファイアウォールルールは、ポリシー、または直接コンピュータに割り当てることができます。

注意: ここでは、ファイアウォールルールの作成方法を具体的に説明します。ファイアウォールモジュールの設定方法については、"[Deep Securityファイアウォールの設定](#)" on page 836を参照してください。

新しいファイアウォールルールを作成するには、次の手順を実行する必要があります。

¹Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

1. "新しいルールを追加する" below。
2. "ルールの動作とプロトコルを選択する" below。
3. "パケットの送信元と送信先を選択する" on page 854。

ファイアウォールルールを作成したら、次の方法も学習できます。

- "ルールイベントとアラートを設定する" on page 855
- "ルールのスケジュールを設定する" on page 855
- "ルールが割り当てられているポリシーとコンピュータを確認する" on page 856
- "ルールにコンテキストを割り当てる" on page 856

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[ファイアウォールルール] ページで新しいファイアウォールルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新規ファイアウォールルール] の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存のルールをコピーして変更します。[ファイアウォールルール] リストで、該当のルールを右クリックし、[複製] をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ] をクリックします。

ルールの動作とプロトコルを選択する

1. ルールの [名前] と [説明] を入力します。

ヒント: ファイアウォールルールへの変更をそのルールの [説明] フィールドに記録することを推奨します。ファイアウォールのメンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールがパケットに対して実行する [処理] を選択します。次の5つの処理のいずれかを選択できます。

注意: 1つのパケットに適用されるのは、1つのルール処理だけです。同じ優先度のルールが複数ある場合は、下記の優先順序で適用されます。

- トラフィックにファイアウォールのバイパスを許可できます。バイパスルールにより、トラフィックはファイアウォールと侵入防御エンジンを可能な限り早く通過できます。バイパスルールは、フィルタリングを望まないマルチメディア系プロトコルを使用するトラフィックや、信頼済みソースからのトラフィックに対して使用します。

ヒント: ポリシーで信頼済みソース用のバイパスルールを作成して使用方法の例については、"[信頼済みトラフィックに対するファイアウォールのバイパス許可](#)" [on page 857](#)を参照してください。

注意: バイパスルールは単一方向です。トラフィックの各方向に対して明確なルールが必要です。

ヒント: 次の設定を使用して、バイパスルールで最大のスループットパフォーマンスを達成できます。

- 優先度: 最高
 - フレームの種類: IP
 - プロトコル: TCP、UDP、またはその他のIPプロトコル (「任意」オプションは使用しないでください)
 - 送信元および送信先のIPおよびMAC: すべて「任意」
 - プロトコルがTCPまたはUDPでトラフィックの方向が「受信」の場合は、送信先ポートを「任意」ではなく1つ以上指定する必要がある、送信元ポートを「任意」にする必要があります。
 - プロトコルがTCPまたはUDPでトラフィックの方向が「送信」の場合は、送信元ポートを「任意」ではなく1つ以上指定する必要がある、送信先ポートを「任意」にする必要があります。
 - スケジュール: なし
- ログ記録のみが可能です。この処理では、ログにエントリは作成されますが、トラフィックは処理されません。
 - 定義済みのトラフィックを強制的に許可できます (他のトラフィックを除外することなく、このルールによって定義されたトラフィックを許可できます)。
 - トラフィックの拒否が可能です (このルールによって定義されたトラフィックを拒否します)。
 - トラフィックの許可が可能です (このフィルタによって定義されたトラフィックを例外的に許可します)。

注意: コンピュータに有効な許可ルールがない場合、拒否ルールでブロックされていないかぎり、すべてのトラフィックが許可されます。許可ルールを1つ作成したら、許可ルールの条件を満たしていないかぎり、その他すべてのトラフィックがブロックされます。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていない限り、常に許可されます。

3. ルールの [優先度] を選択します。優先度により、ルールが適用される順序を決定します。ルール処理に「強制的に許可」、「拒否」、または「バイパス」を選択した場合は、0 (最低) から4 (最高) の優先度を設定できます。優先度を設定すると、ルール処理を組み合わせ、階層型のルール効果を実現できます。

注意: ログのみルールでの優先度は4のみ設定でき、許可ルールでは0のみが設定できません。

注意: 優先度の低いルールよりも優先度の高いルールが優先的に適用されます。たとえば、ポート80の受信を強制的に許可する優先度2のルールが適用されるより前に、ポート80の受信を拒否する優先度3のルールが適用され、パケットを破棄します。

処理と優先度の関係の詳細については、"[ファイアウォールルールの処理と優先度](#)" on [page 858](#)を参照してください。

4. [パケットの方向] を選択します。このルールを受信 (ネットワークからコンピュータ) または送信 (コンピュータからネットワーク) トラフィックのどちらに適用するかを選択します。

注意: 個々のファイアウォールルールは、単一のトラフィック方向にのみ適用されます。特定の種類のトラフィックに対しては、受信および送信ファイアウォールルールをペアで作成する必要があります。

5. イーサネットの [フレームの種類] を選択します。「フレーム」とはイーサネットフレームを指し、フレームで送信されるデータは、使用可能なプロトコルによって指定されます。フレームの種類として「その他」を選択する場合は、[フレーム番号](#)を指定する必要があります。
6. **注意:** [IP] は、IPv4とIPv6両方をサポートしています。[IPv4] または [IPv6] を個別に選択することもできます。

注意: LinuxのAgentは、フレームの種類がIPまたはARPの packetsのみ確認します。その他のフレームの種類のパケットは許可されます。Virtual Applianceにはこのような制限事項はありません。保護する仮想マシンのOSに関係なく、すべてのフレームの種類を確認できます。

フレームの種類としてインターネットプロトコル (IP) を選択した場合は、トランスポートの [プロトコル] を選択する必要があります。プロトコルとして「その他」を選択する場合は、[プロトコル番号](#)も指定する必要があります。

パケットの送信元と送信先を選択する

[IP] アドレスと [MAC] アドレスの組み合わせを選択し、フレームの種類で使用できる場合は、パケット送信元およびパケット送信先の [ポート] および [指定フラグ] を選択します。

ヒント: 以前に作成した[IP](#)、[MAC](#)、または[ポート](#)リストを使用できます。

サポートされているIPベースのフレームの種類は次のとおりです。

	IP	MAC	ポート	フラグ
任意	✓	✓		
ICMP	✓	✓		✓
ICMPV6	✓	✓		✓
IGMP	✓	✓		
GGP	✓	✓		
TCP	✓	✓	✓	✓
PUP	✓	✓		
UDP	✓	✓	✓	
IDP	✓	✓		
ND	✓	✓		

	IP	MAC	ポート	フラグ
RAW	✓	✓		
TCP+UDP	✓	✓	✓	✓

注意: ARPおよびREVARPのフレームの種類では、パケットの送信元と送信先としてMACアドレスの使用のみがサポートされています。

[任意のフラグ] を選択することも、以下のフラグを個別に選択することもできます。

- URG
- ACK
- PSH
- RST
- SYN
- FIN

ルールイベントとアラートを設定する

ファイアウォールルールがトリガされると、Deep Security Managerでイベントがログに記録され、パケットデータが記録されます。

注意: 「許可」、「強制的に許可」、および「バイパス」処理を使用するルールは、イベントのログを記録しません。

アラート

イベントのログを記録した場合に、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション] をクリックしてから、[このルールによってイベントが記録された場合にアラート] を選択します。

注意: アラートをトリガするように設定できるのは、処理が [拒否] または [ログ記録のみ] に設定されているファイアウォールルールのみです

ルールのスケジュールを設定する

予約された時間のみファイアウォールルールを有効化するかどうかを選択します。

その方法の詳細については、"[ルールに適用するスケジュールの定義](#)" on page 687を参照してください。

ルールにコンテキストを割り当てる

ルールコンテキストを使用すると、さまざまなネットワーク環境に独自のファイアウォールルールを設定できます。コンテキストは一般的に、オンサイトとオフサイトのノートパソコンで異なるルールを有効にするために使用されます。

コンテキストの作成方法については、"[ポリシーで使用するコンテキストの定義](#)" on page 680を参照してください。

ヒント: コンテキストを使用してファイアウォールルールを実装するポリシーの例については、「Windows Mobile ラップトップ」ポリシーのプロパティを参照してください。

ルールが割り当てられているポリシーとコンピュータを確認する

ファイアウォールルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべてのファイアウォールルールを、.csvまたは.xmlファイルにエクスポートするには、[エクスポート] をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[ファイアウォールルール] リストで該当のルールを右クリックしてから、[削除]→[OK] の順にクリックします。

注意: 1台以上のコンピュータに割り当てられたファイアウォールルール、またはポリシーの一部であるファイアウォールルールは削除できません。

信頼済みトラフィックに対するファイアウォールのバイパス許可

信頼済みトラフィックに対してファイアウォールのバイパスを許可するようにDeep Securityを設定できます。

この設定の基本手順は次のとおりです。

1. "信頼済みトラフィックのソースの新しいIPリストを作成する" [below](#)
2. "IPリストを使用して信頼済みトラフィックの受信用と送信用のファイアウォールルールを作成する" [below](#)
3. "信頼済みトラフィックが通過するコンピュータで使用されているポリシーにファイアウォールルールを割り当てる" [on the next page](#)

ファイアウォールルールをポリシーに割り当てると、IPリストに登録された信頼済みソースからのトラフィックが許可され、それらのトラフィックについてはステータスの問題や脆弱性の有無が検索されなくなります。

信頼済みトラフィックのソースの新しいIPリストを作成する

1. [ポリシー] をクリックします。
2. 左側の画面で [リスト] → [IPリスト] の順にクリックします。
3. [新規] → [新規IPリスト] の順にクリックします。
4. IPリストの名前を入力します。
5. 信頼済みソースのIPアドレスを、1行に1つずつ [IP] ボックスに貼り付けます。
6. [OK] をクリックします。

IPリストを使用して信頼済みトラフィックの受信用と送信用のファイアウォールルールを作成する

1. [ポリシー] をクリックします。
2. 左側の画面で [ルール] をクリックします。
3. [ファイアウォールルール] → [新規] → [新規ファイアウォールルール] の順にクリックします。
4. 次の値を使用して、信頼済みトラフィックの受信用のファイアウォールルールを作成します。

名前:	信頼済みトラフィック名 - 受信方向のバイパス
処理:	バイパス

プロトコル:	任意
パケット送信元:	IPリスト (前の手順で作成したIPリストを選択)

5. 次の値を使用して、信頼済みトラフィックの送信用のファイアウォールルールを作成します。

名前:	信頼済みトラフィック名 - 送信方向のバイパス
処理:	バイパス
プロトコル:	任意
パケット送信先:	IPリスト (前の手順で作成したIPリストを選択)

信頼済みトラフィックが通過するコンピュータで使用されているポリシーにファイアウォールルールを割り当てる

1. [ポリシー] をクリックします。
2. 左側の画面で [ポリシー] をクリックします。
3. ポリシーをダブルクリックしてプロパティ画面を開きます。
4. ポリシーのプロパティの左側の画面で [ファイアウォール] をクリックします。
5. [割り当て/割り当て解除] をクリックします。
6. 左上のリストにすべてのファイアウォールルールが表示されていることを確認します。
7. 検索ウィンドウを使用し、作成したルールを探して選択します。
8. [OK] をクリックします。
9. 信頼済みトラフィックが通過する各コンピュータについて上記の手順を繰り返します。

ファイアウォールルールの処理と優先度

このトピックの内容:

- ["ファイアウォールルールの処理" below](#)
- ["ファイアウォールルールのシーケンス" on page 861](#)
- ["各ファイアウォールルールの関係" on page 863](#)
- ["ルール優先度" on page 865](#)
- ["ルール処理およびルール優先度を集約する" on page 865](#)

ファイアウォールルールの処理

ファイアウォールルールでは、次の処理が可能です。

- 許可: ルールと一致するトラフィックの通過を明示的に許可し、その他のトラフィックは黙示的に拒否します。
- バイパス: ファイアウォールと侵入防御分析の両方のバイパスをトラフィックに許可します。この設定は、ネットワーク負荷の高いプロトコルや信頼済みソースからのトラフィックに対して使用します。バイパスルールは、IP、ポート、トラフィックの方向、プロトコルに基づいて設定できます。
- 拒否: ルールと一致するトラフィックを明示的にブロックします。
- 強制的に許可: 他のルールで拒否されるトラフィックを強制的に許可します。

注意: 強制的に許可ルールで許可されるトラフィックは、侵入防御モジュールによる分析の対象となります。

- ログ記録のみ: トラフィックはログに記録されるだけです。その他の処理は実行されません。

許可ルールの詳細

許可ルールには、次の2つの機能があります。

1. 明示的に許可されているトラフィックを許可
2. その他のトラフィックを黙示的に拒否

注意: 許可ルールで明示的に許可されていないトラフィックは破棄され、「ポリシーで未許可」のファイアウォールイベントとして記録されます。

一般的に適用される許可ルールは、次のとおりです。

- ARP:受信ARPトラフィックを許可します。
- Allow solicited TCP/UDP replies:コンピュータが、送信したTCPやUDPのメッセージへの応答を受信できるようにします。これは、TCPとUDPのステートフル設定と連携します。
- Allow solicited ICMP replies:コンピュータが、送信したICMPメッセージへの応答を受信できるようにします。これは、ICMPのステートフル設定と連携します。

バイパスルールの詳細

バイパスルールは、ネットワーク負荷の高いプロトコルや信頼済みソースからのトラフィック対象に設計されています。ファイアウォールや侵入防御モジュールによるフィルタリングが必要とされず、望まれてもいないためです。

バイパスルールの条件と一致するパケットは、次のように処理されます。

- ステートフル設定の条件の対象にならない。
- ファイアウォールと侵入防御分析の両方をバイパスする。

バイパスされるトラフィックにはステートフルインスペクションが適用されないため、一方のトラフィックがバイパスされても、逆方向の応答は自動的にバイパスされません。受信トラフィック用と送信トラフィック用のバイパスルールは、必ずペアで作成および適用する必要があります。

注意: バイパスルールのイベントは記録されません。この動作は変更できません。

ヒント: Deep Security Managerで、Deep Security Agentによって保護されているリモートデータベースを使用した場合、Deep Security Managerによって侵入防御ルールがデータベースに保存されるときに、侵入防御に関連するアラームが誤って発生する可能性があります。これは、ルール自体の内容が誤って攻撃と認識されることが原因です。この問題を回避するには、Deep Security Managerからデータベースへのトラフィックに対してバイパスルールを作成します。

注意: バイパスルールを割り当てることで、該当の通信に対してはファイアウォールおよび侵入防御による保護が行われなくなります。通信のパフォーマンスが低下することが業務に与えるリスクと、該当の通信に対して保護が行われなくなるリスクを評価し、通信のパフォーマンスを優先することが必要と判断した場合にご使用ください。

Deep Security Managerのトラフィックに関するバイパスルールの初期設定

Deep Security Managerは、Agentのハートビートの待機ポート上で受信TCPトラフィックを許可する優先度4のバイパスルールを、Deep Security Agentを実行しているコンピュータに自動的に実装します ("[ハートビートを設定する](#)" on page 400を参照してください)。このルールは優先度4なので、他の拒否ルールよりも先に適用されます。また、バイパスルールなので、トラフィックの障害が発生することはありません。なお、このバイパスルールは内部的に作成されるため、ファイアウォールルールの一覧には明示的に表示されません。

ただし、このルールでは、任意のIPアドレスと任意のMACアドレスからのトラフィックが許可されます。このポートでのAgentのセキュリティを強化するには、このポート用に、より厳しいバイパスルールを作成します。新しいカスタムルールを次のように設定すれば、Agentでは初期設定のDeep Security Managerトラフィックルールよりもカスタムルールが優先されません。

- 優先度:4 (最高)
- パケット方向: 受信

- フレームの種類:IP
- プロトコル:TCP
- パケット送信先ポート: Managerからのハートビートを待機するAgentのポート番号

初期設定のルールをカスタムルールに置き換えるには、カスタムルールに上記のパラメータが必要です。ルールのパケット送信元として、実際のDeep Security ManagerのIPアドレスまたはMACアドレスを使用するのが理想です。

強制的に許可ルールの詳細

強制的に許可オプションでは、拒否処理の対象となるトラフィックの一部を除外します。他の処理との関係を下に示します。強制的に許可ルールは、バイパスルールと同じ効果があります。ただし、バイパスルールとは異なり、この処理によってファイアウォールを通過するトラフィックは侵入防御モジュールによる監視の対象となります。強制的に許可ルールの処理は、基本的なネットワークサービスがDSAコンピュータとの通信を確保するのに便利です。一般に、強制的に許可ルールは、許可ルールと一緒に使用して、許可および拒否ルールで禁止されているトラフィックの一部を許可します。また、ICMPおよびUDPステートフルが有効になっている際に、未承諾のICMPおよびUDPトラフィックを許可するように強制的に許可ルールを設定する必要があります。

注意: 複数ノード構成で複数のDeep Security Managerを使用する場合は、それらのサーバのIPリストを定義し、そのリストを使用してDeep Security Managerトラフィックのカスタムルールを作成すると便利です。

ファイアウォールルールのシーケンス

コンピュータに届くパケットは、ファイアウォールルール、ファイアウォールステートフル設定条件、および侵入防御ルールの順に処理されます。

受信および送信でファイアウォールルールが適用される順序は次のとおりです。

1. 優先度4 (最高) のファイアウォールルール
 - a. バイパス
 - b. ログ記録のみ (ログ記録のみルールは優先度4 (最高) にのみ割り当て可能)
 - c. 強制的に許可
 - d. 拒否
2. 優先度3 (高) のファイアウォールルール
 - a. バイパス
 - b. 強制的に許可

- c. 拒否 (ログに記録)
- 3. 優先度2 (標準) のファイアウォールルール
 - a. バイパス
 - b. 強制的に許可
 - c. 拒否 (ログに記録)
- 4. 優先度1 (低) のファイアウォールルール
 - a. バイパス
 - b. 強制的に許可
 - c. 拒否 (ログに記録)
- 5. 優先度0 (最低) のファイアウォールルール
 - a. バイパス
 - b. 強制的に許可
 - c. 拒否 (ログに記録)
 - d. 許可 (許可ルールは優先度0 (最低) にのみ割り当て可能)

注意: コンピュータに有効な許可ルールがない場合、拒否ルールでブロックされていないかぎり、すべてのトラフィックが許可されます。許可ルールを1つ作成したら、許可ルールの条件を満たしていないかぎり、その他すべてのトラフィックがブロックされます。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていない限り、常に許可されます。

同じ優先度のコンテキスト内では、拒否ルールが許可ルールをオーバーライドし、強制的に許可ルールが拒否ルールをオーバーライドします。ルールの優先度システムを使用すると、優先度の低い強制的に許可ルールを、優先度の高い拒否ルールでオーバーライドできます。

強制的に許可ルールを使用して[受信DNSクエリ](#)をすべて許可するDNSサーバ用のポリシーを例に考えてみます。強制的に許可ルールよりも優先度の高い拒否ルールを作成し、この公開サーバへのアクセスを禁止する必要がある特定範囲のIPアドレスを指定します。

優先度に基づいたルール設定によって、ルールを適用する順序を設定できます。拒否ルールに最も高い優先度を設定し、同じ優先度の強制的に許可ルールがない場合、拒否ルールに一致するパケットはすべて自動的に破棄されて残りのルールは無視されます。反対に、強制的に許可ルールに最も高い優先度が設定されている場合、強制的に許可ルールに一致する受信パケットは他のルールに対して確認されることなくすべて自動的に許可されます。

ログに関する注意

バイパスルールはイベントを生成しません。この設定は変更できません。

ログのみルールは、対象のパケットが、次のいずれかのルールによって、それ以降に停止されない場合にのみイベントを生成します。

- 拒否ルール
- そのパケットを除外する許可ルール

この2つのルールのいずれかがパケットを停止する場合は、ログのみルールではなくこれらのルールによって、イベントが生成されます。以降のルールでパケットを停止しない場合は、ログのみルールがエントリを生成します。

各ファイアウォールルールの関係

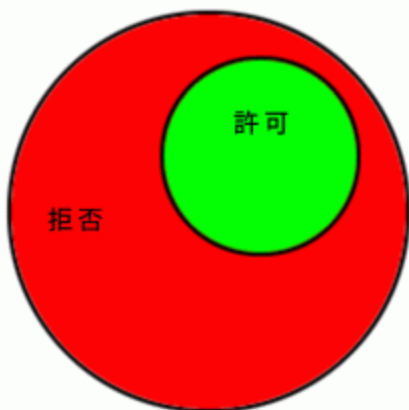
Deep Securityファイアウォールルールには、ルール処理とルール優先度があります。この2つのプロパティを同時に使用することによって、非常に柔軟で強力なルール設定を作成できます。他のファイアウォールで使用されているルール設定では実行順にルールを定義する必要がありますが、それとは異なり、Deep Securityファイアウォールルールは、ルール処理とルール優先度に基づいて決定論的な順序で実行されます。これは、定義された順序や割り当てられた順序とは無関係です。

ルール処理

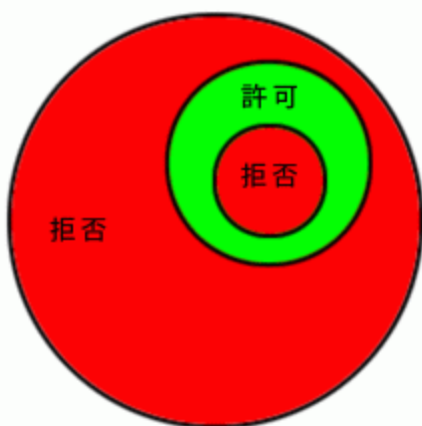
各ルールには、以下の5つのルール処理のいずれかを設定できます。

1. バイパス: パケットがバイパスルールに一致した場合は、同じ優先度の他のルールにかかわらずファイアウォールと侵入防御エンジンを通過します。
2. ログ記録のみ: パケットがログ記録のみルールに一致した場合は、通過してイベントがログ記録されます。
3. 強制的に許可: パケットが強制的に許可ルールに一致した場合は、同じ優先度の他のルールにかかわらず通過します。
4. 拒否: パケットが拒否ルールに一致した場合は、破棄されます。
5. 許可: パケットが許可ルールに一致した場合は、通過します。許可ルールのいずれにも一致していないトラフィックはすべて拒否されます。

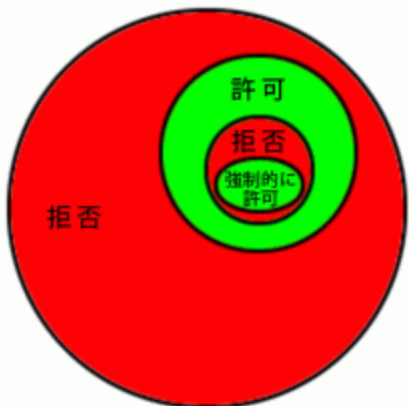
許可ルールを実装すると、許可ルールに一致しないその他すべてのトラフィックが拒否されます。



拒否ルールを許可ルールに優先して適用すると、特定の種類のトラフィックをブロックすることができます。



強制的に許可ルールを拒否トラフィックに適用すると、例外のみ通過させることができます。



ルール優先度

拒否および強制的に許可のルール処理を5つの優先度のいずれかで定義できます。これにより、許可されるトラフィックを許可ルールのセットでさらに細かく定義できます。ルールは、最高 (優先度4) から最低 (優先度0) の順に実行されます。特定の優先度内では、ルール処理 (強制的に許可、拒否、許可、ログのみ) に基づいた順序で処理されます。

優先度のコンテキストによって、ユーザは拒否および強制的に許可の組み合わせを使用してトラフィック管理をさらに詳細に定義することが可能になります。同じ優先度のコンテキスト内では、拒否ルールによって許可ルールを無効にし、また、強制的に許可ルールによって拒否ルールを無効にすることもできます。

注意: 許可のルール処理は優先度0でのみ動作し、ログのみのルール処理は優先度4でのみ動作します。

ルール処理およびルール優先度を集約する

ルールは、最高 (優先度4) から最低 (優先度0) の順に実行されます。特定の優先度内では、ルール処理に基づいた順序で処理されます。同じ優先度のルールが処理される順序は次のとおりです。

- バイパス
- ログのみ
- 強制的に許可
- 拒否
- 許可

注意: 許可のルール処理は優先度0でのみ動作し、ログのみのルール処理は優先度4でのみ動作します。

注意: 強制的に許可ルールと拒否ルールが同等の優先度の場合、強制的に許可ルールが拒否ルールよりも優先されるので、強制的に許可ルールと一致するトラフィックが許可されません。

ファイアウォールの設定

[ファイアウォール] モジュールは、双方向のステートフルなファイアウォール保護を提供します。DoS攻撃を阻止し、すべてのIPベースのプロトコルとフレームタイプに対応するほか、ポート、IPアドレス、およびMACアドレスをフィルタリングします。

コンピュータエディタとポリシーエディタ¹の [ファイアウォール] セクションには、タブで区切られた次のセクションがあります。

- ["一般" below](#)
- ["インターフェース制限" on page 868](#)
- ["攻撃の予兆" on page 869](#)
- ["詳細" on page 871](#)
- ["イベント" on page 871](#)

一般

ファイアウォール

ファイアウォールのオン/オフ状態を親ポリシーから継承したり、設定をローカルでロックするようにこのポリシーまたはコンピュータを設定できます。

ファイアウォールステートフル設定

このポリシーに適用するファイアウォールステートフル設定を選択します。上記のポリシーに対して複数のインターフェースを定義した場合は、各インターフェースに対して個別に設定することができます。ステートフル設定作成の詳細については、["ステートフルファイアウォールの設定の定義" on page 878](#)を参照してください。

ポート検索 (コンピュータエディタのみ)

前回のポートの検索: Deep Security Managerがこのコンピュータ上で前回ポート検索を実行した日時。

検索されたポート: 直近のポート検索で検索されたポート。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

オープンポート: ローカルコンピュータのIPアドレスの下に、オープンポートのリストが表示されます。

[オープンポートの検索] ボタンと [ポート検索のキャンセル] ボタンを使用して、このコンピュータのポート検索を開始またはキャンセルできます。Deep Security Managerは、**コンピュータエディタまたはポリシーエディタ**¹の [設定]→[一般]→[オープンポート]→[検索するポート] で指定したポートの範囲を検索します。

注意: また、検索対象として設定したポートの他に、[AgentまたはApplianceがDeep Security Managerからのハートビート接続を待機するポート番号](#)も検索します。

割り当てられたファイアウォールルール

このポリシーまたはコンピュータで有効になっているファイアウォールルールを表示します。ファイアウォールルールを追加または削除するには、[割り当て/割り当て解除] をクリックします。使用可能なすべてのファイアウォールルールが表示され、ルールを選択したり選択を解除したりできます。

コンピュータエディタまたはポリシーエディタ²画面では、ファイアウォールルールを編集して、編集中のルールにのみローカルに適用することも、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容をグローバルに適用することもできます。

ルールをローカルに編集するには、ルールを右クリックして [プロパティ] をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)] をクリックします。

ファイアウォールルール作成については、"[ファイアウォールルールの作成](#)" on page 850を参照してください。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

インタフェース制限

インタフェース制限

インタフェース制限の有効/無効状態を親ポリシーから継承したり、設定をローカルでロックするようにこのポリシーまたはコンピュータを設定できます。

警告: インタフェース制限を有効にする前に、インタフェースパターンを適切な順序で設定し、必要な文字列パターンをすべて追加し、不要なパターンは削除してください。優先度が最も高いパターンのインタフェースのみが、トラフィックの転送を許可されます。それ以外のインタフェース (リスト内にある残りのパターンのいずれかと一致するインタフェース) は、「制限」されます。制限されたインタフェースは、ファイアウォールの [許可] ルールを使用して特定のトラフィックを許可しないかぎり、すべてのトラフィックをブロックします。

インタフェースパターン

インタフェース制限が有効な場合、ファイアウォールでは、ローカルコンピュータのインタフェース名が、正規表現パターンと照合されます。

注意: Deep Securityは、POSIX基本正規表現を使用してインタフェース名を照合します。基本的なPOSIX正規表現の詳細については、https://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03を参照してください。

優先度が最も高いパターンのインタフェースのみが、トラフィックの転送を許可されます。それ以外のインタフェース (リスト内にある残りのパターンのいずれかと一致するインタフェース) は、「制限」されます。制限されたインタフェースは、ファイアウォールの [許可] ルールを使用して特定のトラフィックを許可しないかぎり、すべてのトラフィックをブロックします。

[1つのアクティブインタフェースに制限] を選択すると、優先度が最も高いパターンのインタフェースが複数見つかった場合でも、1つのインタフェースからのトラフィックのみ許可されます。

攻撃の予兆

攻撃の予兆検索

[攻撃の予兆] 画面では、コンピュータのトラフィック分析を有効にして設定することができます。この機能により、標的型攻撃の前段階として脆弱性を見つけるために使用されることの多い「予兆」を特検出することができます。

注意: Reconnaissance 検索は、TAPモードでは機能しません。Reconnaissance 検索は、IPv4トラフィックでしか検出できません。

- 攻撃の予兆の検出の有効化: 攻撃の予兆の検出のオン/オフを切り替えできます。
- 検出を実行するコンピュータ/ネットワーク: 保護するIPをリストから選択します。既存のIPリストから選択します(このIPリストは、[ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] 画面を使用して作成できます)。
- 検出を実行しないIPリスト: 無視するコンピュータとネットワークをIPリストセットから選択します(上で述べたように、このIPリストは、[ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] 画面を使用して作成できます)。

注意: 攻撃の予兆の保護を有効にする場合は、**コンピュータエディタまたはポリシーエディタ**¹の [ファイアウォール]→[一般] タブで、ファイアウォールおよびステートフルインスペクションも有効にする必要があります。また、**コンピュータエディタまたはポリシーエディタ**²の [ファイアウォール]→[詳細] タブで、[「ポリシーの許可外」のパケットのファイアウォールイベントを生成] 設定も有効にする必要があります。これにより、攻撃の予兆に必要なファイアウォールイベントが生成されるようになります。

攻撃の種類ごとに、Deep Security Managerに情報を送信するよう**AgentまたはAppliance**³を設定し、Managerでアラートをトリガできます。また、アラートのトリガ時にメール通知を送

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

³Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

信するようにDeep Security Managerを設定できます([管理]→[システム設定]→[アラート]を参照してください。アラートは、「ネットワークまたはポートの検索」、「OSのフィンガープリント調査」、「TCP Null検索」、「TCP SYNFIN検索」、および「TCP Xmas検索」です)。このオプションには [DSMにただちに通知] を選択してください。

注意: [DSMにただちに通知] オプションを動作させるには、AgentおよびApplianceの通信方法を [Agent/Applianceから開始] または [双方向] に設定する必要があります (**コンピュータエディタまたはポリシーエディタ**¹の [設定]→[一般])。設定が有効になると、AgentまたはApplianceは、攻撃や調査を検出後ただちにDeep Security Managerに対してハートビートを開始します。

攻撃が検出されると、一時的に送信元IPからのトラフィックをAgentおよびApplianceでブロックするように設定できます。[トラフィックのブロック] リストを使用して分数を設定します。

- OSのフィンガープリント調査: AgentまたはApplianceは、コンピュータOSを検出しようとする動作を検出します。
- ネットワークまたはポートの検索: AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしていることを検出した場合、ネットワークまたはポート検索をレポートします。通常、AgentまたはApplianceのコンピュータは、コンピュータ自身宛てのトラフィックのみを監視するため、ポート検索が最も一般的に検出されます。コンピュータまたはポート検索の検出で使用される統計的な分析方法は「TAPS」アルゴリズムから導出されたもので、2006年にIPCCCで発表された「Connectionless Port Scan Detection on the Backbone」で提案されました。
- TCP Null検索: AgentまたはApplianceはフラグが付いていないパッケージを検出します。
- TCP SYNFIN検索: AgentまたはApplianceはSYNフラグおよびFINフラグの付いたパケットのみ検出します。
- TCP Xmas検索: AgentまたはApplianceは、FINフラグ、URGフラグ、およびPSHフラグの付いたパケット、または値0xFF (想定されるすべてのフラグ) を含むパケットを検出します。

注意: 「ネットワークまたはポートの検索」は、他の攻撃の予兆と違って単一のパケットでは確認できず、Deep Securityでトラフィックを一定期間監視する必要があります。AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしている

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ことを検出した場合、コンピュータまたはポート検索をレポートします。ポートスキャンがはるかに検出されたプローブの最も一般的なタイプですので、通常はエージェントまたはアプライアンスのコンピュータは、自身宛てのトラフィックが表示されます。ただし、コンピュータがルータまたはブリッジとして動作している場合は、多数の他のコンピュータ宛てのトラフィックを監視して、AgentまたはApplianceがコンピュータ検索 (サブネット全体でポート80が開いているコンピュータを検索するなど) を検出できます。

こうした検索を検出するには数分かかります。これは、AgentまたはApplianceが接続の失敗を追跡して、比較的短い期間に単一のコンピュータからの異常な数の接続の失敗があることを確認する必要があるためです。

注意: Windowsコンピュータでブラウザアプリケーションを使用してDeep Security Agentを実行している場合、切断された接続からの残存トラフィックが原因で、攻撃予兆の誤検索 (偽陽性) が報告されることがあります。

攻撃の予兆警告に対応する方法の詳細については、"[警告: 攻撃の予兆の検出](#)" on page 1374を参照してください。

詳細

イベント

「ポリシーで未許可」の packets に対して、イベントを生成するかどうかを設定します。これらは、[許可] ファイアウォールルールで明確に許可されていないため、ブロックされている packets です。このオプションを [はい] に設定すると、有効なファイアウォールルールに応じて、大量のイベントが生成される場合があります。

イベント

ファイアウォールイベントは、Deep Security Managerのメイン画面と同じように表示されますが、表示される内容はこのポリシーまたは特定のコンピュータに関するイベントのみです。

Oracle RACでのファイアウォール設定

Deep Securityでは次の構成がサポートされます。

- SUSE Linux Enterprise Server 11 SP3とOracle RAC 12c Release 1 (v12.1.0.2.0)
- Red Hat Linux Enterprise Server 6.6とOracle RAC 12c Release 1 (v12.1.0.2.0)

- Red Hat Linux Enterprise Server 7.0とOracle RAC 12c Release 1 (v12.1.0.2)

初期設定のLinux Server Deep SecurityポリシーはOracle RAC環境に対応していますが、ファイアウォールの設定だけは例外です。RACノード間の通信チャンネルが複雑であるため、ファイアウォールが原因でRACノードが仮想NICの作成やNICの検索に失敗することがあります。このため、一部のノードでOracle Clusterwareが起動しなくなります。ファイアウォールを無効にするか、ファイアウォールの設定をカスタマイズすることができます。

ノード間の接続を許可するルールを追加する

1. Deep Security Managerで、[ポリシー] タブに進みます。
2. [Linux Server] ポリシーを右クリックし、[複製] をクリックします。
3. 新しく作成された [Linux Server_2] ポリシーをクリックし、[詳細] をクリックします。
4. このポリシーに新しい名前 (「Oracle RAC」 など) を付け、[保存] をクリックします。
5. [ファイアウォール] をクリックします。
6. [割り当て/割り当て解除] をクリックします。
7. [新規]→[新規ファイアウォールルール] の順にクリックします。
8. [一般情報] で、[名前] に「Oracleノードとの通信を許可」などのわかりやすい名前を指定します。[処理] を「強制的に許可」に設定し、[プロトコル] を「任意」に設定します。
9. [パケット送信元] で、[MAC] を「MACリスト」に設定します。表示された [MACリストの選択] 画面で、[新規] を選択します。[新規MACリストのプロパティ] ダイアログボックスが表示されます。
10. MACリストに「Oracle RAC MACリスト」などの名前を付けます。[MAC:(1行あたり1つのMAC)] に、すべてのOracleノードが使用しているすべてのMACアドレスを追加します (プライベートNICとパブリックNIC両方のMACを含む)。追加したら [OK] をクリックします。
11. [パケット送信先] で、[MAC] を「MACリスト」に設定します。表示された [MACリストの選択] 画面で、手順10で作成したMACリストを選択し、[OK] をクリックします。
12. ポリシーの [ファイアウォールルール] リストで、新しいルールが選択されていることを確認して [OK] をクリックし、[保存] をクリックします。

UDPポート42424を許可するルールを追加する

上記の手順に従って、UDPポート42424を許可する新しいルールを追加します。この[ポート番号](#)は、Cluster Synchronization Serviceデーモン (CSSD)、Oracle Grid Interprocess Communicationデーモン (GIPCD)、およびOracle HA Servicesデーモン (OHASD) で使用されます。

注意: 上記の手順で作成したMACリストでは、このルールに対応できない可能性があります。Oracle RACにはこのルールが必要です。

一般	オプション	割り当て対象
一般情報		
名前:	新規ファイアウォールルール	
説明:		
処理:	強制的に許可 ▼	
優先度:	0 - 最低 ▼	
パケット方向:	受信 ▼	
フレームの種類:	IP ▼	<input type="checkbox"/> 選択以外
プロトコル:	UDP ▼	<input type="checkbox"/> 選択以外
パケット送信元		
IP:	任意 ▼	<input type="checkbox"/> 選択以外
MAC:	任意 ▼	<input type="checkbox"/> 選択以外
ポート:	任意 ▼	<input type="checkbox"/> 選択以外
パケット送信先		
IP:	任意 ▼	<input type="checkbox"/> 選択以外
MAC:	任意 ▼	<input type="checkbox"/> 選択以外
ポート:	ポート: ▼	<input type="checkbox"/> 選択以外
		42424
		OK
		キャンセル

その他のRAC関連パケットを許可する

Oracle RACは、フレームの種類がC08Aおよび0ACBのパケットを大量に送信します。これらのパケットをブロックすると、予期しない動作が発生する可能性があります。

- TCPポート6200を許可する: [パケット送信元] および [パケット送信先] の [IP] フィールドにRACノードのパブリックIPアドレスを追加し、送信先ポートを6200に設定します。この[ポート番号](#)は、Oracle Notification Services (ONS) で使用されます。このポートは設定可能です。システムで6200以外のポートに設定されている場合は、正しいポート番号を設定してください。

一般	オプション	割り当て対象
一般情報		
名前:	RAC_TCP 6200_suse	
説明:		
処理:	許可	
優先度:	0 - 最低	
パケット方向:	受信	
フレームの種類:	P	<input type="checkbox"/> 選択以外
プロトコル:	TCP	<input type="checkbox"/> 選択以外
パケット送信元		
IP:	任意	<input type="checkbox"/> 選択以外
MAC:	任意	<input type="checkbox"/> 選択以外
ポート:	ポート:	6200 <input type="checkbox"/> 選択以外
		OK キャンセル

- フレームの種類COA8を許可する:[フレームの種類]を「その他」、[フレーム番号]を「COA8」に設定したルールを追加します。

一般	オプション	割り当て対象
一般情報		
名前:	RAC_COA8	
説明:	<div style="border: 1px solid gray; height: 100px;"></div>	
処理:	許可 ▼	
優先度:	0 - 最低 ▼	
パケット方向:	受信 ▼	
フレームの種類:	その他: ▼	フレーム番号: CA08
プロトコル:	任意 ▼	<input type="checkbox"/> 選択以外
		<input type="checkbox"/> 選択以外
		OK キャンセル

- フレームの種類0ACBを許可する:[フレームの種類]を「その他」、[フレーム番号]を「0ACB」に設定したルールを追加します。
- フレームの種類0AC9を許可する:[フレームの種類]を「その他」、[フレーム番号]を「0AC9」に設定したルールを追加します。

- IGMPプロトコルを許可する:[プロトコル]を「IGMP」に設定したルールを追加します。

The screenshot shows a configuration window for a rule. The tabs at the top are '一般' (General), 'オプション' (Options), and '割り当て対象' (Target), with '割り当て対象' being the active tab. Under the '一般情報' (General Information) section, the following fields are visible:

- 名前 (Name): RAC_allow_IGMP
- 説明 (Description): [Empty text area]
- 処理 (Action): 許可 (Allow)
- 優先度 (Priority): 0 - 最低 (0 - Lowest)
- パケット方向 (Packet Direction): 受信 (Inbound)
- フレームの種類 (Frame Type): IP
- プロトコル (Protocol): IGMP

At the bottom right, there are two checkboxes: '選択以外' (None) for the frame type and '選択以外' (None) for the protocol. At the bottom center, there are 'OK' and 'キャンセル' (Cancel) buttons.

特定のポートを許可するファイアウォールルールを追加する必要があるRAC関連コンポーネントがシステムに含まれているかどうかは、次のリンクで確認してください。

<https://docs.oracle.com/database/121/RILIN/ports.htm#RILIN1178>

Oracle SQL Serverルールが割り当てられていることを確認する

Linux Serverポリシーに「Oracle SQL Server」ファイアウォールルールが割り当てられていることを確認します。このルールは、Deep Securityで事前に定義されている、ポート1521を許可するファイアウォールルールです。

回避技術対策の設定が「標準」に設定されていることを確認する

Linux Serverポリシーのプロパティでは、[設定]→[ネットワークエンジン]→[回避技術対策の設定]は初期設定で「標準」に設定されています。この設定が「厳格」に設定されていると、RACデータベースの応答が非常に遅くなります。



ステートフルファイアウォールの設定の定義

Deep Securityのステートフルファイアウォール設定メカニズムでは、トラフィック履歴との関連における各パケット、TCPおよびIPヘッダ値の正当性、およびTCP接続状態の推移が分析されます。UDPやICMPなどのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実装されます。パケットは、ステートフルメカニズムによって次のように処理されます。

1. 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
2. パケットを調べて、既存の接続に属しているかどうか判断されます。
3. TCPヘッダの正当性 (シーケンス番号、フラグの組み合わせなど) が調査されます。

新しいステートフル設定を作成するには、次の手順に従います。

1. ["ステートフル設定を追加する" on the next page](#)
2. ["ステートフル設定情報を入力する" on the next page.](#)
3. ["パケットインスペクションオプションを選択する" on the next page.](#)

ステートフル設定の後は、次の操作について説明します。

- ["ステートフル設定が割り当てられたポリシーとコンピュータを表示する" on page 883](#)
- ["ステートフル設定をエクスポートする" on page 883](#)

- ["ステートフル設定を削除する" on page 883](#)

ステートフル設定を追加する

[ポリシー]→[共通オブジェクト]→[その他]→[ファイアウォールステートフル設定] でステートフル設定を定義する方法には次の3つがあります。

- 新しい設定を作成します。[新規]→[新規ファイアウォールステートフル設定] の順にクリックします。
- XMLファイルから設定をインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存の設定をコピーして変更します。[ファイアウォールステートフル設定] リストの設定を右クリックして、[複製] をクリックします。新しい設定を編集するには、その設定を選択し、[プロパティ] をクリックします。

ステートフル設定情報を入力する

設定の [名前] と [説明] を入力します。

パケットインスペクションオプションを選択する

IP、TCP、UDPおよびICMPパケットインスペクションのオプションを定義し、アクティブまたはパッシブFTPを有効化できます。

IPパケットインスペクション

[一般] タブで [フラグメント化されたすべての受信パケットを拒否する] を選択し、フラグメント化されたパケットをすべて破棄します。破棄されたパケットはフラグメント化分析をバイパスして、「IP fragmented packet」というログエントリが生成されます。全長がIPヘッダの長さよりも短いパケットはログに記録されずに破棄されます。

警告: 攻撃者は、ファイアウォールルールをバイパスするために、フラグメント化されたパケットを作成して送信する場合があります。

注意: 初期設定では、ファイアウォールエンジンは、フラグメント化されたパケットに対して一連のチェックを実行します。これは初期設定の動作で、変更することはできません。次のような特徴を持つパケットは、破棄されます。

- フラグメントのフラグ/オフセットが無効: IPヘッダ内のDFフラグまたはMFフラグのいずれかが1に設定されている、またはヘッダ内に含まれるDFフラグが1に設定されており、オフセット値が0以外に設定されているとき、パケットは破棄されます。
- 最初のフラグメントが最小サイズ未満: MFフラグが1に設定されていて、オフセット値が0、合計の長さが (最大組み合わせヘッダ長である) 120バイトよりも短い場合、パケットは破棄されます。
- IPフラグメントが範囲を超えている: 合計パケット長と組み合わされたオフセットフラグの値が最大データグラム長である65,535バイトを超えた場合、パケットは破棄されません。
- IPフラグメントのオフセットが小さすぎる: 60バイトよりも小さい値を持つ0以外のオフセットフラグがある場合、パケットは破棄されます。

TCPパケットインスペクション

[TCP] タブで有効化するオプションを次の中から選択します。

- CWR、ECEフラグを含むTCPパケットを拒否する: これらのフラグは、ネットワーク輻輳時に設定されます。

注意: RFC 3168では、ECN (Explicit Congestion Notification) に使用する予約済みフィールドの6ビットのうち2ビットを、次のように定義しています。

- ビット8から15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
- TCPヘッダフラグのビット名参照:
 - ビット8: CWR (Congestion Window Reduced) [RFC3168]
 - ビット9: ECE (ECN-Echo) [RFC3168]

警告: パケットの自動転送 (特にDoS攻撃によって生成されたものなど) によって、これらのフラグが設定されたパケットが作成されることがよくあります。

- TCPステートフルインスペクションを有効にする: TCPレベルでのステートフルインスペクションを有効にします。ステートフルTCPインスペクションを有効にすると、次のオプションが利用可能です。
 - TCPステートフルログを有効にする: TCPステートフルインスペクションイベントがログに記録されます。

- 単一コンピュータからの受信接続数の上限: 単一コンピュータからの接続数を制限すると、DoS攻撃の影響を低減できます。
- 単一コンピュータへの送信接続数の上限: 単一コンピュータへの送信接続数を制限すると、Nimdaなどのワームの影響を大幅に低減できます。
- 単一コンピュータからのハーフオープン接続数の上限: この制限を設定すると、SYNフラッドなどのDoS攻撃から保護できます。ほとんどのサーバでは、ハーフオープン接続を終了するためにタイムアウトが設定されています。この値を設定することにより、ハーフオープン接続が重大な問題にならないようにします。SYN-SENT (リモート) エントリが指定された制限に達した場合、その特定のコンピュータからの後続のTCPパケットは破棄されます。

注意: 単一コンピュータからのオープン接続を許可する数を決定する際に、使用している種類のプロトコルで妥当と考えられる単一コンピュータからのハーフオープン接続数と、輻輳を引き起こすことなくシステムが維持できる単一コンピュータからのハーフオープン接続数との間の数を選択します。

- すでに確認されたパケット数が次を超過したときにACKストーム防御を有効にする: このオプションを設定して、ACKストーム攻撃が発生した場合のイベントを記録します。
 - ACKストームが検出されたときに接続を中断する: このオプションを設定して、攻撃が検出された場合に接続を切断するようにします。

注意: ACKストーム保護オプションはDeep Security Agent 8.0以前でのみ使用可能です。

FTPオプション

[FTPオプション] タブで次のオプションを有効化できます。

注意: 以下のFTPオプションはDeep Security Agent 8.0以前で使用可能です。

- アクティブFTP
 - 受信を許可する: このコンピュータがサーバとして動作しているときにアクティブFTPを許可します。
 - 送信を許可する: このコンピュータがクライアントとして動作しているときにアクティブFTPを許可します。

- パッシブFTP
 - 受信を許可する: このコンピュータがサーバとして動作しているときにパッシブFTPを許可します。
 - 送信を許可する: このコンピュータがクライアントとして動作しているときにパッシブFTPを許可します。

UDPパケットインスペクション

[UDP] タブで次のオプションを有効化できます。

- UDPステートフルインスペクションを有効にする: UDPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

注意: UDPステートフル機能は、未承諾の受信UDPパケットを破棄します。送信UDPパケットごとに、ルールがそのUDP「ステートフル」テーブルをアップデートし、要求に対して60秒以内にUDP応答が発生した場合のみ、UDP応答を許可します。特定の受信UDPトラフィックを許可する場合は、強制的に許可ルールを作成する必要があります。たとえば、DNSサーバを実行している場合、送信先のポート53に受信UDPパケットを許可するには、強制的に許可ルールを作成する必要があります。

警告: UDPトラフィックのステートフルインスペクションがない場合、攻撃者はDNSサーバになりすまして、未承諾のUDP「応答」を送信元のポート53からファイアウォールの内側にあるコンピュータに送信する可能性があります。

- UDPステートフルログを有効にする: このオプションを選択すると、UDPステートフルインスペクションイベントのログを記録できるようになります。

ICMPパケットインスペクション

[ICMP] タブで次のオプションを有効にできます。

注意: ICMPステートフルインスペクションは、Deep Security Agent 8.0以前で使用できません。

- ICMPステートフルインスペクションを有効にする: ICMPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

注意: ICMP (擬似) ステートフル機能は、未承諾の受信ICMPパケットを破棄します。送信ICMPパケットごとに、ルールがそのICMP「ステートフル」テーブルを作成またはアップデートし、要求に対して60秒以内にICMP応答が発生した場合のみ、ICMP応答を許可します(サポートするICMPペアの種類は、タイプ0と8、13と14、15と16、17と18です)。

警告: たとえば、ステートフルICMPインスペクションを有効にすると、エコー要求が送信された場合にICMPエコー応答を許可できます。要求されていないエコー応答は、Smurf増幅攻撃、マスターとデーモン間のライブフラッドネットワーク通信、Loki2バックドアなど、さまざまな種類の攻撃の予兆である可能性があります。

- ICMPステートフルログを有効にする: このオプションを選択すると、ICMPステートフルインスペクションイベントのログを記録できるようになります。

ステートフル設定をエクスポートする

[エクスポート] をクリックし、リストから該当するエクスポート処理を選択すると、すべてのステートフル設定を.csvまたは.xmlファイルにエクスポートできます。ステートフル設定を選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のステートフル設定をエクスポートすることもできます。

ステートフル設定を削除する

ステートフル設定を削除するには、[ファイアウォールステートフル設定] リスト内の設定を右クリックして、[削除] をクリックした後、[OK] をクリックします。

注意: 1台以上のコンピュータに割り当てられたステートフル設定、またはポリシーの一部であるステートフル設定は削除できません。

ステートフル設定が割り当てられたポリシーとコンピュータを表示する

ステートフルインスペクション設定に割り当てられたポリシーとコンピュータは、[割り当て対象] タブに表示できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

オープンポートの検索

Deep Security Managerは、コンピュータのオープンポートを検索することができます。これは、コンピュータを右クリックして [処理]→[オープンポートの検索] を選択するか、最新の検索結果が表示されている **コンピュータエディタ**¹の [ファイアウォール] 画面で [オープンポートの検索] ボタンをクリックして実行します。

この他、Managerの [コンピュータ] 画面で既存のコンピュータを右クリックして、[オープンポートの検索] を選択する方法もあります。また、[予約タスク] を作成して、コンピュータのリストに対して定期的にポート検索を実行する方法もあります。

初期設定では、検索対象のポート範囲は「ウェルノウンポート」と言われる1~1024の範囲ですが、別のポートセットを検索するよう定義できます。

注意: Managerからの受信ハートビート接続を待機するAgentのポート番号は、ポート範囲の設定に関係なく常に検索されます。このポートは、Managerによって開始された通信が送信されるコンピュータ上のポートです。ただし、コンピュータに対して通信方向を [Agent/Applianceから開始] (**コンピュータエディタまたはポリシーエディタ**²の [設定]→[一般]) に設定すると、このポート番号は閉じられます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] に進み、メニューバーの [新規] をクリックします。[新規ポートリスト] 画面が表示されます。
2. [ポート] で、許容される形式を使用して新しいポートリストの名前と説明を入力してから、ポートを定義します(たとえば、ポート100、105、および110~120を検索するには、1行目に「100」、2行目に「105」、および3行目に「110-120」と入力します)。[OK] をクリックします。
3. **コンピュータエディタまたはポリシーエディタ**³の [設定]→[一般] に進み、[検索するポート] メニューをクリックします。新しく定義したポートリストが1つの選択肢として表示されます。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

³これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

コンテナのファイアウォールルール

オーバーレイネットワークを使用するコンテナの保護にDeep Security Agent 11.2以降を利用している場合、初期設定のファイアウォールルールではSwarmまたはKubernetesサービスのネットワークトラフィックがブロックされるため、それらのトラフィックを許可するファイアウォールルールの追加が必要になる場合があります。

Kubernetesファイアウォールルール

Kubernetesを使用している場合、ファイアウォールでk8s通信トラフィックを通過させてサーバストラフィックを送受信できるようにするには、次のルールを追加します。

名前	処理の種類	優先度	方向	フレームの種類	プロトコル	送信元IP	送信元ポート	送信先IP	送信先ポート
HTTP受信TCP 80送信先ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	該当なし	任意	80
HTTP送信TCP 80送信元ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	80	任意	任意
K8s受信TCP 10054ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	任意	任意	10054
K8s送信TCP 10054ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	10054
K8s送信TCP 443ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	443
K8s送信TCP 6443ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	任意	任意	6443
K8s送信TCP 6443ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	6443
K8s送信TCP 8081ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	任意	任意	8081
K8s送信TCP 8081ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	8081
K8s送信UDP 8472ポート	強制的に許可	0 - 最低	送信	IP	UDP	任意	任意	任意	8472
K8s送信UDP 8285ポート	強制的に許可	0 - 最低	送信	IP	UDP	任意	任意	任意	8285
K8s送信UDP 8285ポート	強制的に許可	0 - 最低	受信	IP	UDP	任意	任意	任意	8285

Swarmファイアウォールルール

Swarmを使用している場合、ファイアウォールでk8s通信トラフィックを通過させてサービストラフィックを送受信できるようにするには、次のルールを追加します。

名前	処理の種類	優先度	方向	フレームの種類	プロトコル	送信元IP	送信元ポート	送信先IP	送信先ポート
HTTP受信TCP 80送信先ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	該当なし	任意	80
HTTP送信TCP 80送信元ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	80	任意	任意
Swarm送信TCP 443ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	443
Swarm受信TCP 2377、4789、7946、60012ポート	強制的に許可	0 - 最低	受信	IP	TCP+UDP	任意	任意	任意	2377、4789、7946、60012
Swarm送信TCP 2377、4789、7946、60012ポート	強制的に許可	0 - 最低	送信	IP	TCP+UDP	任意	2377、4789、7946、60012	任意	任意

変更監視によるシステム変更の監視

変更監視モジュールは、Deep Security Agent上のレジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、およびファイルに対する想定外の変更を検索します。変更監視モジュールは、ベースラインの安全な状態を参考にして上記の検索を実行し、想定外の変更が検出されると、イベント (およびオプションのアラート) をログに記録します。

変更監視を有効にして設定するには、"[変更監視の設定](#)" on the next pageを参照してください。

変更監視ルールの作成の詳細については、"[変更監視ルールの作成](#)" on page 895を参照してください。ルールは、ファイルまたはレジストリ監視テンプレートから作成するか、Deep Security XMLベースの[変更監視ルールの言語](#)を使用して作成できます。

変更監視の設定

変更監視保護モジュールは、不審なアクティビティを示している可能性があるファイルや重要なシステム領域 (Windowsレジストリなど) への変更を検出します。検出では、現在の状況が、以前に記録されたベースラインの読み取り値と比較されます。Deep Securityには、事前定義された変更監視ルールが付属しています。新しい変更監視ルールは、セキュリティアップデートで提供されます。

注意: 変更監視ではシステムに加えられた変更が検出されますが、変更の防止や取り消しは実行されません。

変更監視を有効にする方法

変更監視は、ポリシー内で有効にすることも、コンピュータレベルで有効にすることもできます。変更監視を有効にするには、次の手順を実行する必要があります。

1. ["変更監視をオンにする" below](#)
2. ["推奨設定の検索を実行する" on the next page](#)
3. ["変更監視ルールを適用する" on page 889](#)
4. ["コンピュータのベースラインを構築する" on page 891](#)
5. ["変更を定期的に検索する" on page 891](#)
6. ["変更監視をテストする" on page 891](#)

変更監視を有効にしたら、以下についても設定できます。

- ["変更監視検索を実行するタイミング" on page 892](#)
- ["変更監視検索パフォーマンスの設定" on page 893](#)
- ["変更監視イベントのタグ付け" on page 894](#)

変更監視を有効にするための一般的な手順は次のとおりです。

変更監視をオンにする

変更監視は、コンピュータの設定またはポリシーで有効にできます。ポリシーまたはコンピュータエディタを開いて [変更監視]→[一般] に移動します。[設定] を [オン] または [継承 (オン)] に設定して、[保存] をクリックします。

コンピュータ: laptop_adaggs

ヘルプ

概要

- 不正プログラム対策
- Webレピュテーション
- ファイアウォール
- 侵入防御
- 変更監視**
- セキュリティログ監視
- アプリケーション制御
- インタフェース
- 設定
- アップデート
- オーバーライド

一般 詳細 イベント

変更監視

設定: 継承(オン)

ステータス: ● オン。一致するモジュールプラグインが見つかりません。28 ルール

リアルタイム検索の有効化

リアルタイム

変更の検索

前回の変更のフル検索: なし

変更の検索

ベースライン

作成された最新の整合性ベースライン: なし

ベースラインの再構築 ベースラインの表示

現在割り当てられている変更監視ルール

割り当て/割り当て解除... プロパティ... エクスポート 印刷...

名前	重要度	種類	前回のアップ...
1002767 - Microsoft Windows ...	● 高	定義済み	2009-07-29
1002773 - Microsoft Windows - '...	● 高	定義済み	2010-05-26
1002774 - Microsoft Windows ...	● 中	定義済み	2009-06-24
1002775 - Microsoft Windows ...	● 高	定義済み	2009-07-15

推奨設定

現在のステータス: 28個の変更監視ルールが割り当てられています

前回の推奨設定の検索: なし

i 推奨設定の検索結果なし

変更監視ルールの推奨設定を自動的に適用(可能な場合): 継承(いいえ)

推奨設定の検索 推奨設定の検索のキャンセル 推奨設定をクリア

保存 閉じる

推奨設定の検索を実行する

コンピュータで推奨設定の検索を実行して、どのルールが適切か、推奨設定を取得します。コンピュータエディタを開いて[変更監視]→[一般]に移動します。[推奨設定]セクションで、[推奨設定の検索]をクリックします。必要に応じ、検出されたルールの推奨設定をDeep Securityで適用有効にするように指定することもできます。

推奨される変更監視ルールを適用すると、監視対象のエンティティと属性が多くなりすぎる可能性があります。重要で監視すべき対象を特定し、カスタムルールを作成するかまたは事前定義されたルールを調整することをお勧めします。頻繁に変更されるプロパティ(プロセスIDや送信元ポート番号など)を監視するルールでは、検出数が多くなりがちのため、調整が必要になることがあるので、注意が必要です。

リアルタイムの変更監視の検索を有効にしている、頻繁に変更されるディレクトリを監視しているため一部の推奨ルールで生成されるイベントが多すぎる場合は、そのルールのリアルタイム検索を無効にできます。[ポリシー]→[共通オブジェクト]→[ルール]→[変更監視ルール]に移動して、ルールをダブルクリックします。[オプション]タブで、[リアルタイム監視を許可]チェックボックスをオフにします。

変更監視ルールを適用する

前述したように、推奨設定の検索の実行時に推奨されたルールをDeep Securityで自動的に有効にすることができます。また、手動でルールを割り当てることも可能です。

ポリシーまたはコンピュータエディタで、[変更監視]→[一般]に移動します。[現在割り当てられている変更監視ルール]セクションに、このポリシーまたはコンピュータで有効になっているルールが表示されます。変更監視ルールを追加または削除するには、[割り当て/割り当て解除]をクリックします。使用可能なすべての変更監視ルールを示す画面が表示され、ルールを選択したり、選択を解除したりできます。

名前	アプリケーションの種類	優先度	重要度	モード	種類	カテゴリ	CVE
1000083 - Microsoft Windows W...	Web Client Common	2 - 標準	● 高	防御	攻撃コード	なし	CVE-2005-...
1000084 - BlackMal/KamaSutra...	Web Client Common	3 - 高	● 中	防御	攻撃コード	なし	なし
1000086 - CommuniGate System...	Directory Server LDAP	2 - 標準	● 高	防御	脆弱性	なし	CVE-2006-...
1000087 - Computer Associates...	Web Server CA iTechnology Gat...	2 - 標準	● 重大	防御	脆弱性	なし	CVE-2005-...
1000088 - EXAMINE Command...	Mail Server Miscellaneous	1 - 低	● 低	防御	スマート	なし	なし
1000090 - Generic Command Fo...	Mail Server Miscellaneous	1 - 低	● 低	防御	スマート	なし	なし
1000092 - Interaction SIP Proxy...	VoIP Soft Phones	2 - 標準	● 高	防御	脆弱性	なし	CVE-2005-...
1000094 - MailEnable IMAP "LO...	Mail Server MailEnable	1 - 低	● 重大	防御	脆弱性	なし	CVE-2005-...
1000095 - Lupii/Lupper Worm V...	Web Application Perl Based	2 - 標準	● 中	防御	脆弱性	なし	CVE-2005-...
1000101 - Microsoft IIS Malform...	Web Server IIS	2 - 標準	● 高	防御	脆弱性	なし	CVE-2005-...
1000103 - Microsoft Internet Ex...	Web Client Internet Explorer	2 - 標準	● 重大	防御	脆弱性	なし	CVE-2006-...
1000109 - Mozilla Products Grar...	Web Client Mozilla Firefox	3 - 高	● 低	防御	攻撃コード	なし	なし
1000110 - Restrict IMAP Comm...	Mail Server Common	1 - 低	● 低	防御	スマート	なし	なし
1000114 - MailEnable IMAP "ST...	Mail Server MailEnable	1 - 低	● 高	防御	脆弱性	なし	CVE-2005-...
1000115 - Sony DRM CodeSuppr...	Web Client Internet Explorer	3 - 高	● 重大	防御	攻撃コード	なし	CVE-2005-...
1000117 - Trend Micro ServerPr...	Web Server Trend Micro Crystal...	2 - 標準	● 中	防御	脆弱性	なし	CVE-2005-...
1000120 - Microsoft SQL Server...	Database Microsoft SQL	3 - 高	● 高	防御	攻撃コード	なし	CVE-2002-...
1000121 - MS SQL Hello Overflow	Database Microsoft SQL	3 - 高	● 高	防御	攻撃コード	なし	CVE-2002-...
1000122 - MySQL CREATE FUN...	Database MySQL	3 - 高	● 中	防御	攻撃コード	なし	CVE-2005-...

トレンドマイクロが提供する一部の変更監視ルールは、正常に機能するため、ローカルでの設定を必要とします。このようなルールをコンピュータに割り当てるか、ルールが自動的に割り当てられると、設定が必要であることを通知するアラートが発令されます。

変更監視ルールは、ローカルで編集して編集中のコンピュータまたはポリシーにのみ変更内容を適用することも、グローバルに編集してルールを使用する他のすべてのポリシーまたはコンピュータに変更内容を適用することもできます。ルールをローカルで編集するには、そのルールを右クリックして [プロパティ] をクリックします。ルールをグローバルに編集するには、そのルールを右クリックして [プロパティ (グローバル)] をクリックします。

組織にとって重要な特定の変更 (新しいユーザの追加や新しいソフトウェアのインストールなど) を監視するために、カスタムルールを作成することもできます。カスタムルールの作成方法の詳細については、「[変更監視ルールの言語](#)」を参照してください。

ヒント: パフォーマンスを向上させ、競合や誤検出を避けるためには、できるだけ具体的な変更監視ルールを作成します。たとえば、ハードドライブ全体を監視するルールは作成しないでください。

コンピュータのベースラインを構築する

ベースラインは、変更の検索結果の比較対象となる元の状態です。変更の検索用の新しいベースラインをコンピュータで作成するには、コンピュータエディタを開き、[変更監視]→[一般]に進み、[ベースラインの再構築]をクリックします。

現在のベースラインデータを表示するには、[ベースラインの表示]をクリックします。

ヒント: パッチを適用した後は、新しいベースライン検索を実行することをお勧めします。

変更を定期的に検索する

変更は定期的に検索してください。手動検索を実行するには、コンピュータエディタを開き、[変更監視]→[一般]に進み、[変更の検索]をクリックします。検索を定期的に行う[予約タスク](#)を作成することもできます。

変更監視をテストする

以降の変更監視設定の手順に進む前に、ルールとベースラインが正常に動作しているかどうかをテストします。

1. 変更監視が有効になっていることを確認します。
2. コンピュータエディタまたはポリシーエディタ¹で、[変更監視]→[現在割り当てられている変更監視ルール]に移動します。[割り当て/割り当て解除]をクリックします。
3. Windowsユーザの場合:
 - [1002773 - Microsoft Windows - 'Hosts' file modified]を検索し、このルールを有効にします。このルールは、C:\windows\system32\drivers\etc\hostsに変更が加えられた場合にアラートを発令します。

Linuxユーザの場合:

- [1003513 - Unix - File attributes changes in /etc location]を検索し、このルールを有効にします。このルールは、/etc/hostsファイルに変更が加えられた場合にア

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ラートを発令します。

4. 上記のファイルに変更を加え、変更を保存します。
5. コンピュータエディタ¹で、[変更監視]→[一般]に移動し、[変更の検索]をクリックします。
6. [イベントとレポート]→[変更監視イベント]に移動し、ホストファイルの変更が記録されていることを確認します。検出が記録されていれば、変更監視モジュールは正常に動作しています。

変更監視検索を実行するタイミング

変更監視検索を実行するためのオプションは3つあります。

- 手動検索:手動の変更監視検索は、**コンピュータエディタ**²を開いて [変更監視]→[一般] に移動することにより、必要に応じて実行できます。[変更の検索] セクションで、[変更の検索] をクリックします。
- 予約検索: 変更監視検索は、他のDeep Security処理と同様に予約できます。Deep Securityは、監視対象エンティティを確認し、前回検索を実行したときから変更されたイベントを特定し、記録します。前回の検索後に、監視対象エンティティに対して複数回の変更が行われた場合は、最新の変更のみが検出されます。エンティティの状態に対する複数の変更を検出してレポートするためには、予約検索の頻度を上げることを検討します。たとえば、検索を週1回ではなく毎日実施するようにします。または、頻繁に変更されるエンティティについて、リアルタイムの検索を有効にします。変更監視検索の予約を有効にするには、[管理]→[予約タスク]→[新規]に移動します。新規予約タスクウィザードで、[コンピュータの変更を検索]と予約検索の頻度を選択します。新規予約タスクウィザードで要求される情報を目的に応じて入力します。予約タスクの詳細については、["Deep Security予約タスクの設定" on page 479](#)を参照してください。
- リアルタイム検索: リアルタイム検索を有効にできます。このオプションを選択すると、Deep Securityはエンティティの変更をリアルタイムで監視し、変更を検出すると変更監視イベントを生成します。イベントは、リアルタイムでSyslog経由でSIEMに、または次のDeep Security Managerとのハートビート通信時に転送されます。リアルタイム検索を有効にするには、**コンピュータエディタまたはポリシーエディタ**³で [変更監視]→[一般]

¹コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

³これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

に移動し、[リアルタイム] を選択します。64ビットのLinuxプラットフォームでDeep Security Agent 11.0以降を使用している場合、および64ビットのWindows ServerでDeep Security Agent 11.2以降を使用している場合に、リアルタイム検索の結果で、ファイルを変更したユーザとプロセスが表示されるようになりました。この機能をサポートしているプラットフォームの詳細については、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。

注意: ディスク全体を対象にファイルの変更をリアルタイムで監視するとパフォーマンスに影響し、変更監視イベントが大量に記録されることとなります。これを防ぐために、リアルタイムで監視する対象としてルートドライブ (C:\) を選択すると、Deep Securityは実行可能ファイルとスクリプトのみを監視します。リアルタイムですべてのファイルを監視する必要がある場合は、ルートドライブ以外のフォルダを指定してください。

変更監視検索パフォーマンスの設定

以下の設定を変更すると、変更監視検索のパフォーマンスを改善できることがあります。

CPUの使用率を制限する

変更監視のシステム検索ではローカルのCPUリソースを消費します。これは、最初に初期ベースラインが作成され、その後のシステム検索時にはシステムの状態がベースラインと照合されるためです。変更監視が予想以上にリソースを消費していることが判明した場合、CPUの使用率を次のレベルに制限することができます。

- 高: 一時停止せずに、ファイルを次々に検索する
- 中: ファイル検索の間に一時停止処理を行い、CPUリソースの消費を抑える
- 低: ファイル検索の間に、「中」よりも長い時間一時停止処理を行う

[変更監視のCPU使用率レベル] 設定を変更するには、**コンピュータエディタまたはポリシーエディタ**¹を開いて [変更監視]→[詳細] に進みます。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

コンテンツハッシュアルゴリズムを変更する

変更監視モジュールがベースライン情報を保存する際に使用するハッシュアルゴリズムを選択できます。複数のアルゴリズムを選択できますが、パフォーマンスに影響が出るため、複数選択することは推奨しません。

コンテンツハッシュアルゴリズムを変更できます。

仮想マシンの検索キャッシュ設定を有効にする

変更監視に検索キャッシュを使用すると、大規模なVMware環境で複数の仮想マシンから同じ内容を検索する必要性がなくなるため、検索の効率が向上します。仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ**¹を開き、[変更監視]→[詳細]→[仮想マシンの検索キャッシュ]の順に進みます。

変更監視の検索キャッシュ設定の詳細については、"[Virtual Applianceの検索キャッシュ](#)" on [page 899](#)を参照してください。

変更監視イベントのタグ付け

変更監視モジュールによって生成されたイベントは、Deep Security Managerの [イベントとレポート]→[変更監視イベント] に表示されます。イベントのタグ付けを行うと、イベントをソートしやすくなり、問題のないイベントと詳細な調査が必要なイベントを判別しやすくなります。

タグは、イベントを右クリックして [タグの追加] をクリックすることにより、手動でイベントに適用できます。タグを選択したイベントにのみ適用するか、同様のすべての変更監視イベントに適用するかを選択できます。

また、自動タグ付け機能を使用し、複数のイベントをグループ化してラベルを付けることもできます。Deep Security Managerでこの機能を設定するには、[イベントとレポート]→[変更監視イベント]→[自動タグ付け]→[新しい信頼済みのソース]に進みます。タグ付けの実行に使用できるソースは3つあります。

- 信頼済みのローカルコンピュータ
- トレンドマイクロのソフトウェア安全性評価サービス

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- 信頼済みの共通ベースライン。コンピュータグループから収集された、ファイルのステータスのセットです。

イベントのタグ付けの詳細については、"[イベントを識別およびグループ化するためのタグの適用](#)" on page 1129を参照してください。

変更監視ルールの作成

変更監視ルールを使用すると、Deep Security Agentで検索して、コンピュータのファイル、ディレクトリ、レジストリキーと値に対する変更、およびインストール済みのソフトウェア、プロセス、待機中のポート、実行中のサービスにおける変更を検出できます。変更監視ルールは、コンピュータに直接割り当てられることも、ポリシーの一部にすることもできます。

注意: ここでは、変更監視ルールの作成方法を具体的に説明します。変更監視モジュールの設定方法については、"[変更監視の設定](#)" on page 887を参照してください。

変更監視ルールには、ユーザ自身が作成したルールとトレンドマイクロが発行するルールの2種類があります。トレンドマイクロが発行するルールの設定方法については、"[トレンドマイクロが発行する変更監視ルールを設定する](#)" on page 897セクションを参照してください。

新しい変更監視ルールを作成するには、次の手順を実行する必要があります。

1. "[新しいルールを追加する](#)" below。
2. "[変更監視ルール情報を入力する](#)" on the next page。
3. "[ルールテンプレートを選択し、ルールの属性を定義する](#)" on the next page。

変更監視ルールを作成したら、次の方法も学習できます。

- "[ルールイベントとアラートを設定する](#)" on page 898
- "[ルールが割り当てられているポリシーとコンピュータを確認する](#)" on page 899
- "[ルールをエクスポートする](#)" on page 899
- "[ルールを削除する](#)" on page 899

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[変更監視ルール] ページで、新しい変更監視ルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新しい変更監視ルール]の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート]をクリックします。
- 既存のルールをコピーして変更します。[変更監視ルール]リストで、該当のルールを右クリックし、[複製]をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ]をクリックします。

変更監視ルール情報を入力する

1. ルールの [名前] と [説明] を入力します。

ヒント: すべての変更監視ルールへの変更をルールの [説明] フィールドに記録することを推奨します。メンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールの [重要度] を設定します。

注意: ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、変更監視ルールのリストを表示するとき条件をソートする際に役立ちます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します([管理]→[システム設定]→[ランク付け]を参照してください)。

ルールテンプレートを選択し、ルールの属性を定義する

[コンテンツ] タブに移動し、次の3つのテンプレートのいずれかを選択します。

レジストリ値テンプレート

特にレジストリ値への変更を監視する変更監視ルールを作成します。

注意: レジストリ値テンプレートは、Windowsベースコンピュータでのみ使用できます。

1. 監視する [基本キー]、およびサブキーのコンテンツを監視するかどうかを選択します。
2. 含まれる、または除外される [値の名前] が一覧表示されます。ワイルドカード文字として「?」および「*」を使用できます。

3. 監視する [属性] を入力します。「STANDARD」と入力すると、レジストリサイズ、コンテンツ、種類への変更が監視されます。レジストリ値テンプレートの属性の詳細については、「[RegistryValueSet](#)」ドキュメントを参照してください。

ファイルテンプレート

特にファイルへの変更を監視する変更監視ルールを作成します。

1. ルールの [基本ディレクトリ] を入力します (例: C:\Program Files\MySQL)。基本ディレクトリに関連するすべてのサブディレクトリのコンテンツも含めるには、[サブディレクトリも含む] を選択します。ベースディレクトリではワイルドカードはサポートされていません。
2. 特定のファイルを含める、または除外するには、[ファイル名] フィールドを使用します。ワイルドカード (「 ? 」を任意の1文字として、「 * 」を0個以上の文字として) 使用できます。

注意: [ファイル名] フィールドを空白のままにすると、基本ディレクトリ内のすべてのファイルが監視されます。この場合、基本ディレクトリに多数のファイルが含まれていると、大量のシステムリソースが消費されます。

3. 監視する [属性] を入力します。「STANDARD」と入力すると、ファイル作成日、最終更新日、権限、所有者、サイズ、コンテンツ、フラグ (Windows)、SymLinkPath (Linux) が監視されます。ファイルテンプレートの属性の詳細については、「[FileSet](#)」ドキュメントを参照してください。

カスタム (XML) テンプレート

Deep SecurityXMLベースの[変更監視ルール言語](#)を使用して、[ディレクトリ](#)、[レジストリ値](#)、[レジストリキー](#)、[サービス](#)、[プロセス](#)、[インストールされているソフトウェア](#)、[ポート](#)、[グループ](#)、[ユーザ](#)、[ファイル](#)、[WQL](#)を監視するカスタム変更監視ルールテンプレートを作成します。

ヒント: 希望するテキストエディタを使用してルールを作成し、完成したルールを [コンテンツ] フィールドに貼り付けることができます。

トレンドマイクロが発行する変更監視ルールを設定する

トレンドマイクロが発行する変更監視ルールは、作成したカスタムルールと同じ方法では編集できません。トレンドマイクロのルールには、まったく変更できないものと、限定的な設定オ

アクションが提供されているものがあります。いずれのルールも「種類」列に「定義済み」として表示されますが、設定可能なルールは変更監視アイコンに歯車 (🔧) が表示されます。

現在割り当てられている変更監視ルール

割り当て/割り当て解除... プロパティ... エクスポート... 列...				
名前 ^	重要度	種類	前回のアップ...	
 1002766 - Unix - Directory attrib...	● 高	定義済み	2009-07-29	
 1009628 - Applnit DLLs (ATT&C...	● 高	定義済み	2019-04-17	
 1009629 - AppCert DLLs (ATT&...	● 中	定義済み	2019-06-12	
 New Integrity Monitoring Rule	● 中	カスタム	なし	

ルールの設定オプションにアクセスするには、ルールのプロパティを開き、[設定] タブをクリックします。

トレンドマイクロが発行するルールには、[一般] タブの下に補足情報も表示されます。

- ルールがはじめて発行された日付と、最後に更新された日付、およびルールの一意のID。
- ルールを機能させるために最低限必要なAgentとDeep Security Managerのバージョン。

トレンドマイクロが発行するルールは編集できませんが、複製した後にそのコピーを編集することはできます。

ルールイベントとアラートを設定する

変更監視ルールによって検出されたすべての変更は、イベントとしてDeep Security Managerのログに記録されます。

リアルタイムのイベント監視

初期設定では、イベントは発生時にログに記録されます。変更の検索を手動で実行している場合にのみイベントをログに記録するには、[リアルタイム監視を許可] の選択を解除します。

アラート

イベントのログを記録したときに、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション]をクリックしてから、[このルールによってイベントが記録された場合にアラート]を選択します。

ルールが割り当てられているポリシーとコンピュータを確認する

変更監視ルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべての変更監視ルールを、.csvまたは.xmlファイルにエクスポートするには、[エクスポート]をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート]をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[変更監視ルール] リストで該当のルールを右クリックしてから、[削除]→[OK]の順にクリックします。

注意: 1台以上のコンピュータに現在割り当てられている変更監視ルール、またはポリシーの一部である変更監視ルールは削除できません。

Virtual Applianceの検索キャッシュ

検索キャッシュは、仮想マシンの不正プログラム対策および変更監視の検索を最大限に効率化する目的で、Virtual Applianceによって使用されます。検索キャッシュによって、大規模なVMware環境で、複数の仮想マシンから同じ内容を検索する必要性がなくなるため、検索の効率が向上します。検索キャッシュには、Deep Security保護モジュールによって検索されたファイルとその他の検索対象のリストが格納されます。仮想マシン上の検索対象と過去の検索対象が同じであることが確認された場合、その対象はVirtual Applianceによって再度検索されません。エンティティが同じであるかどうかを確認するために使用される属性は、作成時刻、変更

時刻、ファイルサイズ、およびファイル名です。リアルタイム検索キャッシュの場合、Deep Securityはファイルの内容の一部を読み取り、2つのファイルが同じであるかどうかを確認します。ファイルの更新シーケンス番号 (USN、Windowsのみ) を使用するオプション設定もありますが、その設定はクローン作成された仮想マシン以外には使用しないでください。

検索キャッシュによって、クローン作成された仮想マシン間または類似した仮想マシン間で検索結果が共有されるため、変更監視が効率化されます。

後続の検索の速度が向上するため、クローン作成された仮想マシンまたは類似した仮想マシンでの不正プログラムの検索が効率化されます。

また、クローン作成された仮想マシンまたは類似した仮想マシンの起動プロセス検索とアプリケーションアクセス検索の速度が向上するため、不正プログラムのリアルタイム検索が強化されます。

検索キャッシュ設定

検索キャッシュ設定は、有効期限、更新シーケンス番号 (USN)、除外するファイル、含めるファイルなどを指定する設定の集まりです。

注意: 同じ検索キャッシュ設定を使用する仮想マシン間では、同じ検索キャッシュが共有されます。

既存の検索キャッシュ設定のリストを表示するには、[管理]→[システム設定]→[詳細]→[検索キャッシュ設定]の順に進み、[検索キャッシュ設定の表示]をクリックします。Deep Securityには、事前に設定された検索キャッシュの初期設定がいくつか用意されています。これらの設定は、保護する仮想マシンのプロパティと実行する検索の種類に応じて、Virtual Applianceによって自動的に実装されます。

[期限]では、個々のエントリを検索キャッシュに保存する期間を指定します。推奨される初期設定は、手動/予約による不正プログラム検索で1日、不正プログラムのリアルタイム検索で15分、変更監視の検索で1日です。

[USNの使用 (Windowsのみ)]では、Windows NTFSの更新シーケンス番号を使用するかどうかを指定します。更新シーケンス番号は、個々のファイルへの変更を記録するための番号です。このオプションは、クローン作成された仮想マシンにのみ設定してください。

[含めるファイル]と[除外するファイル]では、検索キャッシュに含める、または検索キャッシュから除外するファイルの正規表現パターンとリストを指定します。検索対象のファイルは、まず含めるリストに対して照合されます。

個々のファイルとフォルダは名前で識別できます。また、ワイルドカード (「*」 および 「?」) を使用して、1つの正規表現で複数のファイルや場所を参照することもできます(ゼロ個以上の任意の文字を表すには「*」を、任意の1文字を表すには「?」を使用します)。

注意: 含めるリストと除外リストによって、ファイルの検索に検索キャッシュを使用するかどうかが決まります。ただし、これらのリストを使用することによって、ファイルを従来の方法で検索できなくなるわけではありません。

不正プログラム検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ¹**を開き、[不正プログラム対策]→[詳細]→[仮想マシンの検索キャッシュ]の順に進みます。ここで、不正プログラムのリアルタイム検索に使用する検索キャッシュ設定と、手動/予約検索に使用する検索キャッシュ設定を選択できます。

変更監視の検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ²**を開き、[変更監視]→[詳細]→[仮想マシンの検索キャッシュ]の順に進みます。

検索キャッシュの管理設定

検索キャッシュの管理設定では、検索キャッシュの実行に関する設定ではなく、Virtual Applianceによる検索キャッシュの管理方法を指定します。そのため、検索キャッシュの管理設定は、検索キャッシュ設定と別になっています。検索キャッシュの管理設定は、ポリシーレベルで制御されます。検索キャッシュの管理設定を表示するには、**ポリシーエディタ³**を開き、[設定]→[一般]→[Virtual Appliance]の順に進みます。

同時検索の最大数: Virtual Applianceによって同時に実行される検索の数を指定します。推奨される数は5です。この数が10を超えると、検索のパフォーマンスが低下する可能性があります

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

³ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

す。検索要求はVirtual Applianceで処理待ちの状態となり、到着順に実行されます。この設定は、手動/予約検索にのみ適用されます。

不正プログラムの手動検索キャッシュの最大エントリ数: 不正プログラムの手動検索または予約検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100 MBです。

不正プログラムのリアルタイム検索キャッシュの最大エントリ数: 不正プログラムのリアルタイム検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100MBです。

変更監視の検索キャッシュの最大エントリ数: 変更監視のベースラインデータに含めるエンティティの最大数を指定します。エンティティが20万個の場合、使用されるメモリは約100MBです。

初期設定を変更する場合の考慮事項

検索キャッシュは、同じファイルを再度検索しないことを目的としています。Deep Securityでは、同じファイルであるかどうかを確認するために、すべてのファイルの内容全体を調べることはありません。設定によっては、Deep SecurityでファイルのUSN値をチェックすることもできますが、リアルタイム検索中は、ファイルの内容の一部を読み取り、通常はそのファイル属性を調べることによって、同じファイルであるかどうかを確認します。不正プログラムがファイルに変更を加えた後、それらのファイル属性を変更前の状態に復元することは困難ですが、不可能ではありません。

Deep Securityでは、初期設定でキャッシュの有効期限を短くすることによって、この潜在的な脆弱性を軽減しています。セキュリティを強化するために、キャッシュの有効期限をさらに短くしたり、USNを使用することもできますが、これによってパフォーマンスの向上率が低下したり、より大きなキャッシュの設定が必要になることがあります。特定の仮想マシンに最高レベルのセキュリティを提供し、他から切り離して検索結果を共有しないようにするには、該当する仮想マシン専用のポリシーを作成して、それらが別のゾーンで管理されるようにします。この方法は、異なる部門または組織間で同じインフラストラクチャを共有する場合に適しています(マルチテナントのDeep Security Managerを使用している場合は、この設定が自動的に各テナントに適用されます)。

VDI環境など、ESXiホストあたりのゲスト仮想マシン数が非常に多い場合は、検索中のディスクI/OとCPU使用率を監視してください。検索に時間がかかりすぎる場合は、キャッシュのサイズを増やすか、パフォーマンスが改善されるまで検索キャッシュの管理設定を調整します。キャッシュのサイズを増やす場合は、Deep Security Virtual Applianceシステムメモリの調整も必要になることがあります。

セキュリティログ監視によるログの分析

注意: セキュリティログ監視がサポートされるOSのリストについては、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。

セキュリティログ監視保護モジュールは、OSおよびアプリケーションのログに含まれている可能性のある重要なセキュリティイベントの特定に役立ちます。これらのイベントをセキュリティ情報/イベント管理 (SIEM) システムまたは中央のログサーバに送信して、関連付け、レポート、およびアーカイブに使用できます。また、すべてのイベントはDeep Security Managerで安全に収集されます。イベントのログ記録および転送の詳細については、"[セキュリティログ監視イベントの転送と保存を設定する](#)" on page 907を参照してください。

セキュリティログ監視モジュールで実施できる作業は次のとおりです。

- PCI DSSログ監視の要件を満たす。
- 不審な動作を検出する。
- さまざまなOSとアプリケーションを含む異種環境でイベントを収集する。
- エラーなどのイベントや情報イベント (ディスクがいっぱいである、サービスの開始、サービスの停止など) を表示する。
- 管理者のアクティビティ (管理者のログインまたはログアウト、アカウントのロックアウト、ポリシーの変更など) の監査証跡を作成して維持する。

セキュリティログ監視を有効にして設定するには、"[セキュリティログ監視の設定](#)" belowを参照してください。

Deep Securityのセキュリティログ監視機能を使用すると、サードパーティのログファイルのリアルタイム分析ができます。セキュリティログ監視ルールとデコーダは、多種多様なシステムに対して、イベントの解析、分析、ランク付けおよび関連付けを実行するためのフレームワークを提供します。侵入防御および変更監視と同様、セキュリティログ監視の内容は、セキュリティアップデートに含まれているルールのフォームで配信されます。これらのルールによって、分析するアプリケーションとログの選択を高いレベルで選択することができます。セキュリティログ監視ルールを設定して確認するには、"[ポリシーで使用するセキュリティログ監視ルールを定義する](#)" on page 907を参照してください。

セキュリティログ監視の設定

セキュリティログ監視を使用するには、次の基本手順を実行します。

1. ["セキュリティログ監視モジュールをオンにする" below](#)
2. ["推奨設定の検索を実行する" below](#)
3. ["推奨されるセキュリティログ監視ルールを適用する" on the next page](#)
4. ["セキュリティログ監視をテストする" on page 906](#)
5. ["セキュリティログ監視イベントの転送と保存を設定する" on page 907](#)

セキュリティログ監視モジュールの概要については、["セキュリティログ監視によるログの分析" on the previous page](#)を参照してください。

セキュリティログ監視モジュールをオンにする

1. [ポリシー]に移動します。
2. セキュリティログ監視を有効にするポリシーをダブルクリックします。
3. [セキュリティログ監視]→[一般]の順にクリックします。
4. [セキュリティログ監視のステータス]で[オン]を選択します。
5. [保存]をクリックします。

推奨設定の検索を実行する

ルールは、要件に関連するセキュリティイベントを収集するように設定する必要があります。設定が適切でないと、大量のログエントリがトリガおよび保存され、Deep Securityデータベースの容量を圧迫する場合があります。コンピュータで推奨設定の検索を実行して、どのルールを適用するのが適切か、推奨設定を取得します。

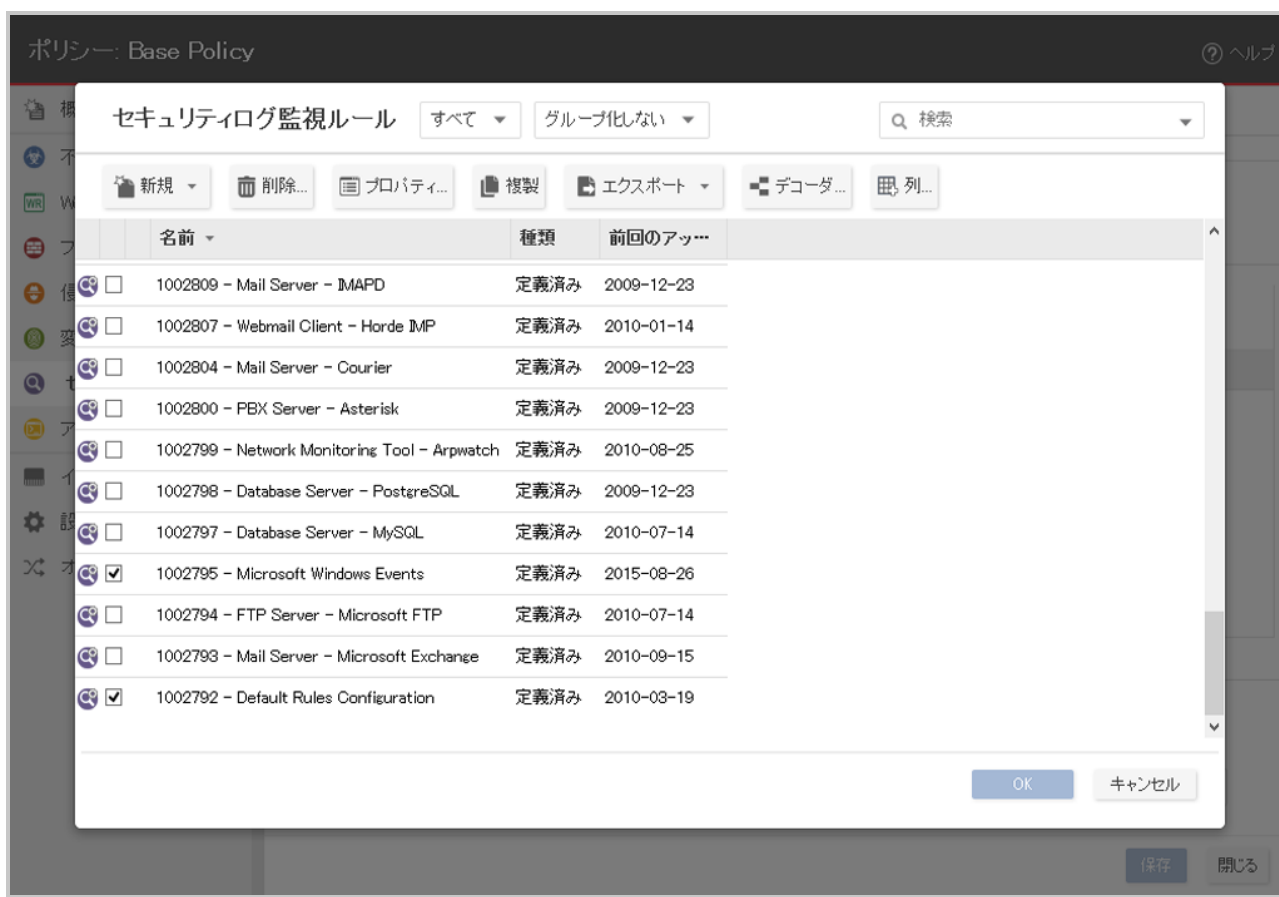
1. [コンピュータ]に移動し、該当するコンピュータをダブルクリックします。
2. [セキュリティログ監視]→[一般]の順にクリックします。
3. [セキュリティログ監視ルールの推奨設定を自動的に適用 (可能な場合)]の設定では、検出されたルールをDeep Securityで実装するかどうかを[はい]または[いいえ]を選択することで決定できます。
4. [推奨設定]セクションで、[推奨設定の検索]をクリックします。トレンドマイクロが提供する一部のセキュリティログ監視ルールは、正常に機能するため、ローカルでの設定を必要とします。このようなルールをコンピュータに割り当てるか、ルールが自動的に割り当てられると、設定が必要であることを通知するアラートが発令されます。

推奨設定の検索の詳細については、["推奨設定の検索の管理と実行" on page 592](#)を参照してください。

推奨されるセキュリティログ監視ルールを適用する

Deep Securityには、さまざまなOSとアプリケーションに対応した、定義済みの多数のルールが用意されています。推奨設定の検索を実行するときは、Deep Securityで[推奨設定のルールを自動的に適用する](#)ことも、次の手順に従ってルールを手動で選択して割り当てることもできます。

1. [ポリシー]に移動します。
2. 設定するポリシーをダブルクリックします。
3. [セキュリティログ監視]→[一般]の順にクリックします。
4. [現在割り当てられているセキュリティログ監視ルール]セクションには、ポリシーで有効になっているルールが表示されます。セキュリティログ監視ルールを追加または削除するには、[割り当て/割り当て解除]をクリックします。



5. 割り当てる、または割り当て解除するルールのチェックボックスをオンまたはオフにします。セキュリティログ監視ルールを編集するには、ルールを右クリックして[プロパティ]を選択してルールをローカルで編集する方法と、[プロパティ (グローバル)]を選択してルールを使用しているその他すべてのポリシーに対して変更内容を適用する方法があ

ります。詳細については、"[セキュリティログ監視ルールの確認](#)" on page 930を参照してください。

6. [OK] をクリックします。

Deep Securityには多数の一般的なOSおよびアプリケーション用のセキュリティログ監視ルールが用意されていますが、独自のカスタムルールを作成することもできます。カスタムルールを作成する場合は、「基本ルール」テンプレートを使用するか、または新しいルールをXMLで記述できます。カスタムルールの作成方法については、"[ポリシーで使用するセキュリティログ監視ルールを定義する](#)" on the next pageを参照してください。

セキュリティログ監視をテストする

以降のセキュリティログ監視設定の手順に進む前に、ルールが正常に動作しているかどうかをテストします。

1. セキュリティログ監視が有効になっていることを確認します。
2. コンピュータエディタまたはポリシーエディタで、>[セキュリティログ監視]→[詳細] に移動します。[Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDSMに送信] を [低 (3)] に変更し、[保存] をクリックします。
3. [一般] タブで、[割り当て/割り当て解除] をクリックします。次の項目を検索して有効にします。
 - [1002792 - Default Rules Configuration] – これは他のすべてのセキュリティログ監視ルールを機能させるために必要なルールです。

Windowsユーザの場合は次の項目を有効にします。

- [1002795 - Microsoft Windows Events] – Windowsの監査機能がイベントを登録するたびに、イベントがログに記録されます。

Linuxユーザの場合は次の項目を有効にします。

- [1002831 - Unix - Syslog] – syslogに記録されたイベントが検査されます。
4. [OK] をクリックし、[保存] をクリックして、ポリシーにルールを適用します。
 5. 存在しないアカウントでサーバーへのログインを試みます。
 6. [イベントとレポート]→[セキュリティログ監視イベント] に移動し、ログイン失敗が記録されていることを確認します。検出が記録されていれば、セキュリティログ監視モジュールは正常に動作しています。

セキュリティログ監視イベントの転送と保存を設定する

セキュリティログ監視ルールがトリガされると、イベントがログに記録されます。これらのイベントを表示するには、[イベントとレポート]→[セキュリティログ監視イベント]に移動するか、ポリシーエディタで[セキュリティログ監視]→[セキュリティログ監視イベント]に移動します。セキュリティログ監視イベントの使用に関する詳細については、"[セキュリティログ監視イベント](#)" on page 1340を参照してください。

イベントの重要度に応じて、Syslogサーバにイベントを送信したり (この機能を有効にする方法の詳細については"[Deep SecurityイベントをSyslogまたはSIEMサーバに転送する](#)" on page 1141を参照)、重要度のクリッピング機能を使用してイベントをデータベースに保存したりすることもできます。

「重要度のクリッピング」では次の2つを設定できます。

- Agent/Applianceイベントが次の重要度以上の場合に、イベントをSyslogに送信: この設定は、Syslogが有効な場合に、ルールによってトリガされたイベントのうちどのイベントがSyslogサーバに送信されるかを決定します
- Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDeep Security Managerに送信: この設定は、どのセキュリティログ監視イベントがデータベースに保存され、[セキュリティログ監視イベント]画面に表示されるかを決定します。

重要度のクリッピングを設定するには、次の手順に従います。

1. [ポリシー]に移動します。
2. 設定するポリシーをダブルクリックします。
3. [セキュリティログ監視]→[詳細]の順にクリックします。
4. [Agent/Applianceイベントが次の重要度以上の場合に、イベントをSyslogに送信]で重要度を [低 (0)] から [重大 (15)] の範囲で選択します。
5. [Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDSMに送信]で重要度を [低 (0)] から [重大 (15)] の範囲で選択します。
6. [保存]をクリックします。

ポリシーで使用する セキュリティログ監視 ルールを定義する

OSSEC セキュリティログ監視 エンジン は Deep Security Agent に統合されており、Deep Security は、コンピュータ上で実行されているオペレーティングシステムおよびアプリケーションによって生成されたログおよびイベントを検査できます。Deep Security Manager に

は、コンピュータまたはポリシーに割り当てることができる、標準のOSSECのセキュリティログ監視ルールセットが付属しています。要件に合う既存ルールが存在しない場合は、カスタムルールを作成することもできます。

トレンドマイクロが発行するセキュリティログ監視ルールは編集できませんが、コピーしたものを編集することはできます。

注意: 1台以上のコンピュータに割り当てられたセキュリティログ監視ルール、またはポリシーの一部であるセキュリティログ監視ルールは削除できません。

セキュリティログ監視ルールを作成するには、次の基本手順を実行します。

- 新しいセキュリティログ監視ルールを作成する
 - ["デコーダ" on page 910](#)
 - ["サブルール" on page 911](#)
 - ["実際の使用例" on page 920](#)
- セキュリティログ監視ルールの重要度レベルと推奨される使用法
- ["strftime\(\) 変換指定子" on page 929](#)
- セキュリティログ監視ルールの確認

セキュリティログ監視 モジュールの概要については、["セキュリティログ監視によるログの分析" on page 903](#)を参照してください。

新しいセキュリティログ監視ルールを作成する

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[ルール]→[セキュリティログ監視ルール]に進みます。
2. [新規]→[新しいセキュリティログ監視ルール]をクリックします。
3. [一般] タブで、ルールの名前と説明を入力します (説明は省略できます)。
4. [コンテンツ] タブで、ルールを定義します。ルールを定義する一番簡単な方法は、[基本ルール]を選択し、表示されるオプションを使用してルールを定義する方法です。さらにカスタマイズが必要な場合は、[カスタム (XML)]を選択し、定義しているルールをXMLビューに切り替えることができます。

注意: [基本ルール] ビューに戻すと、[カスタム (XML)] ビューで加えた変更はすべて失われます。

XMLベースの言語を使用して独自のセキュリティログ監視ルールを作成する場合は、[OSSEC](#)のドキュメントを参照するか、サポートプロバイダにお問い合わせください。

基本ルールテンプレートでは以下のオプションを使用できます。

- **ルールID:** ルールIDは、ルールの一意的識別子です。OSSECでは、ユーザ指定のルール用に100000~109999を定義しますこのフィールドには、新しい一意のルールIDがDeep Security Managerによって事前に入力されています。
- **レベル:** ルールにレベルを割り当てます。ゼロ (0) は、ルールによってイベントが記録されないことを示しますが、このルールを監視する他のルールが発生する可能性があります
- **グループ:** 1つ以上のカンマ区切りのグループにルールを割り当てます。これが便利なのは、ある1つのルールの発生時に発生する複数のルール、または特定のグループに属するルールを作成した後に依存関係が使用されることです。
- **ルールの説明:** ルールの説明。
- **パターン照合:** これは、ルールがログ内を検索するパターンです。一致するものが検出されるとルールがトリガされます。パターン照合では、正規表現またはより簡単な文字列パターンをサポートします。「文字列パターン」というパターンの種類は正規表現よりも処理が高速ですが、サポートされるのは次に示す3つの特殊な処理のみです。
 - **^ (カレット):** テキストの先頭を指定します。
 - **\$ (ドル記号):** テキストの末尾を指定します。
 - **| (パイプ):** 複数のパターン間に「OR」を作成します。

セキュリティログ監視モジュールで使用される正規表現の構文については、<https://www.ossec.net/docs/syntax/regex.html>を参照してください。

- **依存関係:** 別のルールへの依存関係を設定すると、現在のルールでは、このエリアに指定したルールがトリガされた場合にもイベントが記録されます。
- **[頻度]** は、ルールがトリガされるまでの特定の期間内にルールを照合する必要のある回数です。
- **[期間]** は、イベントを記録するためにルールを特定の回数 (上記の頻度) トリガするまでの期間 (秒数) です。

注意: [コンテンツ]タブは、自分で作成したセキュリティログ監視ルールに対してのみ表示されます。トレンドマイクロが発行するセキュリティログ監視ルールの場合は、代わりに [設定] タブが表示されます。このタブには、セキュリティログ監視ルールの設定オプションが表示されます。

1. [ファイル] タブで、ルールによって監視するファイルのフルパスを入力し、そのファイルの種類を指定します。
2. [オプション] タブの [アラート] セクションで、このルールでアラートをトリガするかどうかを選択します。

最小のアラート重要度は、基本ルールまたはカスタム (XML) テンプレートを使用してルールに対してアラートをトリガする最小の重大度レベルを設定します。

注意: 基本ルールテンプレートは、一度に1つのルールを作成します。1つのテンプレートに複数のルールを書き込むには、カスタム (XML) テンプレートを使用できます。カスタム (XML) テンプレート内でレベルが異なる複数のルールを作成する場合は、[最小のアラート重要度]設定を使用して、そのテンプレート内のすべてのルールに対するアラートをトリガする最小の重要度を選択できます。

3. [割り当て対象に割り当てられました]タブには、このセキュリティログ監視ルールを使用しているポリシーとコンピュータが表示されます。新しいルールは作成中であるため、まだ割り当てられていません。
4. [OK] をクリックします。このルールをポリシーとコンピュータに割り当てる準備ができました。

デコーダ

セキュリティログ監視ルールは、変更を監視するファイルのリストと、ルールがトリガするために満たす条件のセットで構成されます。セキュリティログ監視エンジンが監視対象のログファイルで変更を検出すると、その変更はデコーダによって解析されます。デコーダは、raw ログエントリを解析して次のフィールドを生成します。

- log: イベントのメッセージセクション
- full_log: イベント全体
- location: ログの生成元
- hostname: イベント発生元のホスト名
- program_name: イベントのSyslogヘッダで使用されるプログラム名
- srcip: イベント内の送信元のIPアドレス
- dstip: イベント内の送信先のIPアドレス
- srcport: イベント内の送信元のポート番号
- dstport: イベント内の送信先のポート番号
- protocol: イベント内のプロトコル

- action: イベント内で実行された処理
- srcuser: イベント内の送信元のユーザ
- dstuser: イベント内の送信先のユーザ
- id: イベントからのIDとしてデコードされたID
- status: イベント内のデコードされたステータス
- command: イベント内で呼び出されるコマンド
- url: イベント内のURL
- data: イベントから抽出される追加データ
- systemname: イベント内のシステム名

ルールは、このデコードされたデータを確認して、ルールで定義された条件に一致する情報を検索します。

一致する項目の重要度レベルが十分に高い場合は、次のいずれかの処理を実行できます。

- アラートの発令(セキュリティログ監視ルールの [プロパティ] 画面の [オプション] タブで設定できます)
- イベントのSyslogへの書き込み([管理]→[システム設定]→[イベントの転送] タブの [SIEM] エリアで設定できます)
- イベントのDeep Security Managerへの送信(ポリシーエディタまたはコンピュータエディタの [設定]→[イベントの転送] タブの [セキュリティログ監視のSyslog設定] で設定できます)。

サブルール

1つのセキュリティログ監視ルールに複数のサブルールを含めることができます。これらのサブルールには、アトミックとコンポジットという2つの種類があります。アトミックルールは1つのイベントを評価し、コンポジットルールは複数のイベントを確認して、頻度、繰り返し、およびイベント間の相関関係を評価できます。

グループ

各ルールまたはルールのグループは、<group></group> エlement内に定義する必要があります。属性名には、このグループに追加するルールを含めてください。次の例では、Syslogとsshdのルールをグループに含めています。

```
<group name="syslog,sshd,">
</group>
```

注意: グループ名の末尾にカンマが付いていることに注意してください。末尾のカンマは、`<if_group></if_group>` タグを使用して、このルールに別のサブルールを条件付きで追加する場合に必要です。

注意: セキュリティログ監視 ルールのセットがエージェントに送信されると、エージェントのセキュリティログ監視 エンジンが、割り当てられた各ルールからXMLデータを取得し、基本的に単一の長いセキュリティログ監視 ルールになるように組み込みます。グループ定義の中には、トレンドマイクロが作成したすべてのセキュリティログ監視 ルールに共通のものがあります。そのため、トレンドマイクロには「Default Rules Configuration」と呼ばれるルールがあります。このルールはこれらのグループを定義し、常に他のトレンドマイクロのルールとともに割り当てられます(割り当てるルールに「Default Rules Configuration」ルールを選択しない場合は、「Default Rules Configuration」ルールが自動的に割り当てられることを知らせる通知が表示されます)。独自のセキュリティログ監視 ルールを作成し、トレンドマイクロ作成ルールを割り当てずにコンピュータに割り当てる場合は、[初期設定ルール設定]ルールの内容を新しいルールにコピーするか、「初期設定ルールの設定」の「コンピュータへの割り当て」のルールを参照してください。

ルール、ID、およびレベル

グループには必要な数のルールを含めることができます。ルールは、`<rule></rule>` エレメントを使用して定義されます。ルールには少なくとも2つの属性(idおよびlevel)が必要です。idは、署名の一意の識別子です。levelは、アラートの重要度です。次の例では、ルールIDとレベルの異なる、2つのルールが作成されます。

```
<group name="syslog,sshd,">
  <rule id="100120" level="5">
  </rule>
  <rule id="100121" level="6">
  </rule>
</group>
```

注意: カスタムルールには、100,000以上のID値を指定する必要があります。

`<group></group>` タグを使用すると、親グループ内に追加のサブグループを定義できます。このサブグループは、次の表に示す任意のグループを参照できます。

グループの種類	グループ名	説明
攻撃の予兆	connection_attempt web_scan	接続の試行 Web検索

グループの種類	グループ名	説明
	recon	一般的な検索
認証制御	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser account_changed	成功 失敗 無効 ログイン拒否 複数の失敗 ユーザアカウントの追加 ユーザアカウントの変更または削除
攻撃/悪用	automatic_attack exploit_attempt invalid_access spam multiple_spam sql_injection attack virus	ワーム (対象を指定しない攻撃) 攻撃コードのパターン 無効なアクセス スパム 複数のスパムメッセージ SQLインジェクション 一般的な攻撃 ウイルスの検出
アクセス管理	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	アクセス拒否 アクセス許可 存在しないリソースへのアクセス ファイアウォールによるドロップ 複数のファイアウォールによるドロップ クライアントの誤った設定 クライアントエラー
ネットワーク制御	new_host ip_spoof	新しいコンピュータの検出 ARPスプーフィングの疑い
システム監視	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed low_diskspace time_changed	サービスの開始 システムエラー シャットダウン ログのクリア 無効な要求 インタフェースのプロミスキャスモードへの切り替え ポリシーの変更 設定の変更 ディスク容量が少ない 時刻の変更

注意: イベントの自動タグ付けが有効な場合は、イベントにグループ名のラベルが付けられません。セキュリティログ監視 ルールでは、グループをユーザフレンドリなバージョンに変更する変換テーブルを使用します。そのため、たとえば、「login_denied」は「ログイン拒否」と表示されます。カスタムルールのリストには、ルール内に表示されるグループ名が表示されません。

説明

<description></description> タグを含めます。ルールがトリガされると、説明のテキストがイベントに表示されます。

```
<group name="syslog,sshd,">
  <rule id="100120" level="5">
    <group>authentication_success</group>
    <description>SSHD testing authentication success</description>
  </rule>
  <rule id="100121" level="6">
    <description>SSHD rule testing 2</description>
  </rule>
</group>
```

デコード形式

<decoded_as></decoded_as> タグでは、指定されたデコーダがログをデコードした場合にのみルールを適用するようにセキュリティログ監視エンジンを設定します。

```
<rule id="100123" level="5">
  <decoded_as>sshd</decoded_as>
  <description>Logging every decoded sshd message</description>
</rule>
```

注意: 使用可能なデコーダを表示するには、[セキュリティログ監視ルール] 画面で [デコーダ] をクリックします。[1002791-Default Log Decoders] を右クリックして、[プロパティ] を選択します。[設定] タブに進み、[デコーダの表示] をクリックします。

一致項目

特定の文字列をログで検索するには、<match></match> を使用します。Linuxのsshdのパスワードエラーログを次に示します。

```
Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid
user jsmith from 192.168.1.123 port 1799 ssh2
```

「Failed password」という文字列を検索するには、<match></match> タグを使用します。

```
<rule id="100124" level="5">
  <decoded_as>sshd</decoded_as>
  <match>^Failed password</match>
```

```
<description>Failed SSHD password attempt</description>
</rule>
```

注意: 文字列の先頭を示す正規表現のカレット (^) に注意してください。「Failed password」がログの先頭でない場合でも、セキュリティログ監視デコーダはログを複数のセクションに分割します詳細については、「[デコーダ](#) on page 910を参照してください。これらのセクションの1つは、ログ全体を示す「full_log」ではなく、ログのメッセージ部分を示す「log」です。

次の表は、サポートされている正規表現の構文一覧です。

正規表現の構文	説明
\w	A～Z、a～z、0～9の英数字1文字
\d	0～9の数字1文字
\s	単一のスペース (空白文字)
\t	単一のタブ
\p	()*+,-.::;<=>?[]
\W	\w以外
\D	\d以外
\S	\s以外
\.	任意の文字
+	上記のいずれかの1つ以上に一致 (たとえば、\w+、\d+)
*	上記のいずれかの0個以上に一致 (たとえば、\w*、\d*)
^	文字列の先頭 (^<任意の文字列>)
\$	文字列の末尾 (<任意の文字列>\$)
	複数の文字列間の「OR」

条件文

ルールの評価では、trueと評価される他のルールを条件とすることができます。<if_sid></if_sid> タグでは、タグで識別されたルールがtrueと評価された場合にのみこのサブルールを評価するようにセキュリティログ監視エンジンを設定します。次の例では、100123、100124、および100125の3つのルールを示します。<if_sid></if_sid> タグを使用して、ルール100124と100125がルール100123の子になるように変更されています。

```
<group name="syslog,sshd,">
  <rule id="100123" level="2">
    <decoded_as>sshd</decoded_as>
    <description>Logging every decoded sshd message</description>
  </rule>
  <rule id="100124" level="7">
    <if_sid>100123</if_sid>
```

```

    <match>^Failed password</match>
    <group>authentication_failure</group>
    <description>Failed SSHD password attempt</description>
  </rule>
  <rule id="100125" level="3">
    <if_sid>100123</if_sid>
    <match>^Accepted password</match>
    <group>authentication_success</group>
    <description>Successful SSHD password attempt</description>
  </rule>
</group>

```

評価の階層

<if_sid></if_sid> タグでは、基本的に階層型のルールセットを作成します。つまり、<if_sid></if_sid> タグをルールに含めることにより、そのルールは <if_sid></if_sid> タグで参照されるルールの子になります。ルールをログに適用する前に、セキュリティログ監視エンジンは、<if_sid></if_sid> タグを評価し、上位および下位のルールの階層を作成します。

注意: 階層型の親子構造を使用すると、ルールの効率を向上させることができます。親ルールがtrueと評価されない場合、セキュリティログ監視エンジンはその親の子を無視します。

注意: <if_sid></if_sid> タグを使用して、まったく異なるセキュリティログ監視ルール内のサブルールを参照できますが、後でルールを確認することが非常に困難になるため、この処理は避けてください。

次の表は、使用可能なアトミックルールの条件指定のオプションを一覧表示しています。

タグ	説明	備考
match	パターン	イベント (ログ) に対して照合される任意の文字列。
regex	正規表現	イベント (ログ) に対して照合される任意の正規表現。
decoded_as	文字列	事前一致する任意の文字列。
srcip	送信元のIPアドレス	送信元のIPアドレスとしてデコードされる任意のIPアドレス。IPアドレスの前に「!」を使用すると、指定した以外のIPアドレスを意味します。
dstip	送信先のIPアドレス	送信先のIPアドレスとしてデコードされる任意のIPアドレス。IPアドレスの前に「!」を使用すると、指定した以外のIPアドレスを意味します。
srcport	送信元のポート番号	任意の送信元のポート (形式の一致)。
dstport	送信先のポート	任意の送信先のポート (形式の一致)。

タグ	説明	備考
	ト番号	
user	ユーザ名	ユーザ名としてデコードされる任意のユーザ名。
program_name	プログラム名	Syslogプロセス名からデコードされる任意のプログラム名。
hostname	システムのホスト名	Syslogのホスト名としてデコードされる任意のホスト名。
time	次の形式の時刻の範囲 hh:mm - hh:mmまたは hh:mm am - hh:mm pm	トリガするルールに対してイベントが発生する必要のある時刻の範囲。
weekday	曜日 (日曜、月曜、火曜など)	トリガするルールに対してイベントが発生する必要のある曜日。
id	ID	イベントからデコードされる任意のID。
url	URL	イベントからデコードされる任意のURL。

このルールを100125ルールに依存させるには、`<if_sid>100125</if_sid>` タグを使用します。このルールでは、成功したログインルールにすでに一致するsshdメッセージの確認のみが行われます。

```
<rule id="100127" level="10">
  <if_sid>100125</if_sid>
  <time>6 pm - 8:30 am</time>
  <description>Login outside business hours.</description>
  <group>policy_violation</group>
</rule>
```

ログエントリのサイズに関する制限

次の例では、`maxsize`属性を前の例に追加しています。この属性では、`maxsize`よりも文字数が少ないルールの評価のみを行うようにセキュリティログ監視エンジンを設定します。

```
<rule id="100127" level="10" maxsize="2000">
  <if_sid>100125</if_sid>
  <time>6 pm - 8:30 am</time>
  <description>Login outside business hours.</description>
  <group>policy_violation</group>
</rule>
```

次の表は、使用可能なアトミックルールのツリーベースのオプションを一覧表示しています。

タグ	説明	備考
if_sid	ルールID	指定された署名IDに一致するルールの子ルールとしてこのルールを追加します。
if_group	グループID	指定されたグループに一致するルールの子ルールとしてこのルールを追加します。
if_level	ルールレベル	指定された重要度レベルに一致するルールの子ルールとしてこのルールを追加します。
description	文字列	ルールの説明。
info	文字列	ルールの追加情報。
cve	CVE番号	ルールに関連付ける任意のCommon Vulnerabilities and Exposures (CVE)番号。
options	alert_by_email no_email_alert no_log	アラートの処理としてメール生成 (alert_by_email)、メール生成なし (no_email_alert)、またはログへの記録なし (no_log) のいずれかを指定する追加のルールオプション。

コンポジットルール

アトミックルールは、1つのログエントリを確認します。複数のエントリに関連付けるには、コンポジットルールを使用する必要があります。コンポジットルールは、現在のログを受信済みのログと照合します。複合ルールにはさらに2つのオプションが必要です。頻度 オプションは、イベントまたはパターンがアラートを生成するまでに何回発生する必要があるかを指定します。また、 の時間枠の オプションは、セキュリティログ監視 エンジンにどれくらいの時間（秒）遅れて通知します。以前のログを検索する必要があります。すべてのコンポジットルールの構造は次のようになります。

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

たとえば、10分以内にパスワードを5回間違えたら重要度の高いアラートを作成するコンポジットルールを作成できます。<if_matched_sid></if_matched_sid> タグを使用すると、アラートを作成する新しいルールに対して、目的の頻度および期間内にトリガする必要があるルールを指定できます。次の例では、イベントの5つのインスタンスが発生したらトリガするようにfrequency属性が設定されています。また、timeframe属性で、期間が600秒に指定されています。

コンポジットルールが監視するその他のルールを定義する場合は、<if_matched_sid></if_matched_sid> タグが使用されます。

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_sid>100124</if_matched_sid>
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

より詳細なコンポジットルールを作成するのに使用できるタグが他にもいくつかあります。このようなルールを使用すると、次の表に示すように、イベントの特定の部分が同じになるように指定できます。これにより、コンポジットルールを調整して誤判定を減らすことができます。

タグ	説明
same_source_ip	送信元のIPアドレスが同じになるように指定します。
same_dest_ip	送信先のIPアドレスが同じになるように指定します。
same_dst_port	送信先のポートが同じになるように指定します。
same_location	場所 (ホスト名またはAgent名) が同じになるように指定します。
same_user	デコードされるユーザ名が同じになるように指定します。
same_id	デコードされるIDが同じになるように指定します。

認証が失敗するたびにアラートを生成するようにコンポジットルールで指定するには、特定のルールIDを使用する代わりに、<if_matched_sid></if_matched_sid> タグを <if_matched_group></if_matched_group> タグに置き換えます。これにより、authentication_failureなどのカテゴリを指定して、インフラストラクチャ全体での認証の失敗を検索できます。

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_group>authentication_failure</if_matched_group>
  <same_source_ip />
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

<if_matched_sid></if_matched_sid> タグと <if_matched_group></if_matched_group> タグの他にも、<if_matched_regex></if_matched_regex> タグを使用して、受信したログを検索する正規表現を指定することができます。

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_regex>^Failed password</if_matched_regex>
  <same_source_ip />
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

実際の使用例

Deep Securityには、数十種類の一般的なアプリケーションに対応した、多数の初期設定のセキュリティログ監視ルールが含まれています。新しいルールは、セキュリティアップデートを使用して定期的に追加できます。セキュリティログ監視ルールでサポートされるアプリケーションが増えても、サポート対象外のアプリケーションやカスタムアプリケーション用のカスタムルールを作成することが必要な場合があります。

ここでは、Microsoft SQL Serverデータベースをデータリポジトリとして使用するMicrosoft Windows Server IISおよび.Netプラットフォームでホストされる、カスタムCMS (コンテンツ管理システム) の作成について説明します。

最初に、次に示すアプリケーションログの属性を特定します。

1. アプリケーションログを記録する場所
2. ログファイルのデコードに使用できるセキュリティログ監視デコーダ
3. ログファイルメッセージの一般的な形式

ここで示すカスタムCMSの例では、次のようになります。

1. Windowsイベントビューア
2. Windowsイベントログ (eventlog)
3. Windowsイベントログ形式 (次のコア属性を使用)
 - ソース: CMS
 - カテゴリ: なし
 - イベント: アプリケーションイベントID>

次に、アプリケーションの機能別にログイベントのカテゴリを特定し、そのカテゴリを監視用のカスケードグループの階層に分類します。監視対象のすべてのグループでイベントを発生させる必要はなく、一致する項目を条件文として使用できます。各グループについて、ルールで照合条件として使用できるログ形式の属性を特定します。これは、すべてのアプリケーションログの、ログイベントのパターンおよび論理分類を調べて実行することもできます。

たとえば、CMSアプリケーションでは、次の機能をサポートしています。セキュリティログ監視のルールは次のとおりです。

- CMSアプリケーションログ (ソース: CMS)
 - 認証 (イベント: 100~119)
 - ユーザログインの成功 (イベント: 100)
 - ユーザログインの失敗 (イベント: 101)

- 管理者ログインの成功 (イベント: 105)
- 管理者ログインの失敗 (イベント: 106)

- 一般エラー (種類: エラー)
 - データベースエラー (イベント: 200~205)
 - ランタイムエラー (イベント: 206~249)

- アプリケーション監査 (種類: 情報)
 - コンテンツ
 - 新しいコンテンツの追加 (イベント: 450~459)
 - 既存のコンテンツの変更 (イベント: 460~469)
 - 既存のコンテンツの削除 (イベント: 470~479)

 - 管理
 - User
 - 新しいユーザの作成 (イベント: 445~446)
 - 既存のユーザの削除 (イベント: 447~449)

これは、ルール作成に役立つ基本的な構造です。次に、Deep Security Managerで新しいセキュリティログ監視ルールを作成します。

新しいCMSセキュリティログ監視ルールを作成するには

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[ルール]→[セキュリティログ監視ルール]に進み、[新規]をクリックし、[新しいセキュリティログ監視ルールのプロパティ]画面を表示します。
2. 新しいルールの名前と説明を指定し、[コンテンツ]タブをクリックします。
3. 新しいカスタムルールを作成する最も簡単な方法は、基本ルールテンプレートを使用することです。[基本ルール]オプションを選択します。
4. [ルールID]フィールドには、未使用のID番号(100,000以上)が自動的に入力されます。これは、カスタムルール用に予約されたIDです。
5. [レベル]を[低(0)]に設定します。
6. ルールに適切なグループ名を指定します。ここでは「cms」とします。

7. ルールの簡単な説明を入力します。

一般	コンテンツ	ファイル	オプション	割り当て対象
テンプレート				
<input checked="" type="radio"/> 基本ルール <input type="radio"/> カスタム (XML)				
一般情報				
ルールID:	<input type="text" value="100000"/>			
レベル:	<input type="text" value="低 (0)"/>			
グループ (カンマ区切り):	<input type="text" value="cms"/>			
ルールの説明:	<input type="text" value="windows events for 'cms' group"/>			
パターン照合				
照合するパターン:	<input type="text"/>			
パターンの種類:	<input type="text" value="文字列パターン"/>			
依存関係				
<input checked="" type="radio"/> なし <input type="radio"/> 別のルールのトリガ時にイベントをトリガ: <input type="radio"/> 特定のグループに属するルールのトリガ時にイベントをトリガ:				
コンポジット (オプション)				
このルールが、指定された期間 (秒単位) 内に指定の頻度で依存ルールと一致した場合のみ、トリガされます。				
頻度 (1~128):	<input type="text"/>			
期間 (1~86400):	<input type="text"/>			
				<input type="button" value="OK"/> <input type="button" value="キャンセル"/>

8. 次に、[カスタム (XML)] オプションを選択します。「基本」ルール用に選択したオプションがXMLに変換されます。

一般 コンテンツ **ファイル** オプション 割り当て対象

テンプレート

基本ルール
 カスタム (XML)

コンテンツ:

```
<group name="cms">
  <rule id="100000" level="0">
    <description>windows events for 'cms' group</description>
  </rule>
</group>
```

OK キャンセル

9. [ファイル] タブをクリックし、[ファイルの追加] ボタンをクリックして、ルールを適用するアプリケーションログファイルおよびログの種類を追加します。ここでは、「Application」、およびファイルの種類として「eventlog」を選択します。

一般 コンテンツ **ファイル** オプション 割り当て対象

ファイル:

Application eventlog ▼ 削除

ファイルの追加

OK キャンセル

注意: eventlogは、Deep Security固有のファイルの種類です。この場合、ログファイルの場所と名前を指定する必要はありません。その代わりに、Windowsイベントビューアに表示されるログの名前を入力してください。ファイルの種類がeventlogの場合の他

のログの名前は、「Security」、「System」、「Internet Explorer」、またはWindowsイベントビューアに表示されるその他のセクションになる可能性があります。その他のファイルの種類の場合は、ログファイルの場所と名前が必要です(ファイル名の照合にはC/C++ strftime() 変換指定子を使用できます。その他の役立つ変換指定子については、以降の表を参照してください)。

10. [OK] をクリックして基本ルールを保存します。
11. 作成された基本ルールのカスタム (XML) を使用すると、以前に特定されたログのグループに基づいて、グループへの新しいルールの追加を開始することができます。基本ルールの条件は初期ルールに設定します。次の例では、ソース属性が「CMS」のWindowsイベントログが、CMS基本ルールによって特定されています。

```
<group name="cms">
  <rule id="100000" level="0">
    <category>windows</category>
    <extra_data>^CMS</extra_data>
    <description>Windows events from source 'CMS' group
messages.</description>
  </rule>
```

12. 次に、特定されたロググループから後続のルールを作成します。次の例では、認証とログインの成功および失敗を特定し、イベントIDごとにログを記録します。

```
<rule id="100001" level="0">
  <if_sid>100000</if_sid>
  <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
  <group>authentication</group>
  <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
  <if_group>authentication</if_group>
  <id>100</id>
  <description>CMS User Login success event.</description>
</rule>

<rule id="100003" level="4">
  <if_group>authentication</if_group>
  <id>101</id>
  <group>authentication_failure</group>
  <description>CMS User Login failure event.</description>
```

```

</rule>
<rule id="100004" level="0">
  <if_group>authentication</if_group>
  <id>105</id>
  <description>CMS Administrator Login success event.</description>
</rule>
<rule id="100005" level="4">
  <if_group>authentication</if_group>
  <id>106</id>
  <group>authentication_failure</group>
  <description>CMS Administrator Login failure event.</description>
</rule>

```

13. 次に、設定済みのルールを使用して、任意のコンポジットルールまたは相関ルールを追加します。次の例は、重要度の高いコンポジットルールを示しています。このルールは、ログインの失敗が10秒間に5回繰り返されたインスタンスに適用されます。

```

<rule id="100006" level="10" frequency="5" timeframe="10">
  <if_matched_group>authentication_failure</if_matched_group>
  <description>CMS Repeated Authentication Login failure
event.</description>
</rule>

```

14. すべてのルールの重要度レベルが適切かどうかを確認します。たとえば、エラーログの重要度はレベル5以上でなければなりません。情報ルールの重要度は低くなります。
15. 最後に、新しく作成されたルールを開き、[設定] タブをクリックして、カスタムルールのXMLをルールフィールドにコピーします。[適用] または [OK] をクリックして変更内容を保存します。

ルールがポリシーまたはコンピュータに割り当てられると、セキュリティログ監視 エンジン は、指定されたログファイルの検査をただちに開始します。

完成したカスタムCMSセキュリティログ監視ルール:

```

<group name="cms">
  <rule id="100000" level="0">
    <category>windows</category>
    <extra_data>^CMS</extra_data>
    <description>Windows events from source 'CMS' group
messages.</description>
  </rule>
  <rule id="100001" level="0">
    <if_sid>100000</if_sid>

```

```
<id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
<group>authentication</group>
<description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
  <if_group>authentication</if_group>
  <id>100</id>
  <description>CMS User Login success event.</description>
</rule>

<rule id="100003" level="4">
  <if_group>authentication</if_group>
  <id>101</id>
  <group>authentication_failure</group>
  <description>CMS User Login failure event.</description>
</rule>

<rule id="100004" level="0">
  <if_group>authentication</if_group>
  <id>105</id>
  <description>CMS Administrator Login success event.</description>
</rule>

<rule id="100005" level="4">
  <if_group>authentication</if_group>
  <id>106</id>
  <group>authentication_failure</group>
  <description>CMS Administrator Login failure event.</description>
</rule>

<rule id="100006" level="10" frequency="5" timeframe="10">
  <if_matched_group>authentication_failure</if_matched_group>
  <description>CMS Repeated Authentication Login failure
event.</description>
</rule>

<rule id="100007" level="5">
  <if_sid>100000</if_sid>
  <status>^ERROR</status>
```

```

        <description>CMS General error event.</description>
        <group>cms_error</group>
</rule>

<rule id="100008" level="10">
    <if_group>cms_error</if_group>
    <id>^200|^201|^202|^203|^204|^205</id>
    <description>CMS Database error event.</description>
</rule>

<rule id="100009" level="10">
    <if_group>cms_error</if_group>
    <id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|^239|^240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
    <description>CMS Runtime error event.</description>
</rule>

<rule id="100010" level="0">
    <if_sid>100000</if_sid>
    <status>^INFORMATION</status>
    <description>CMS General informational event.</description>
    <group>cms_information</group>
</rule>

<rule id="100011" level="5">
    <if_group>cms_information</if_group>
    <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
    <description>CMS New Content added event.</description>
</rule>

<rule id="100012" level="5">
    <if_group>cms_information</if_group>
    <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
    <description>CMS Existing Content modified event.</description>
</rule>

<rule id="100013" level="5">
    <if_group>cms_information</if_group>
    <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
    <description>CMS Existing Content deleted event.</description>

```

```

</rule>

<rule id="100014" level="5">
  <if_group>cms_information</if_group>
  <id>^445|^446</id>
  <description>CMS User created event.</description>
</rule>

<rule id="100015" level="5">
  <if_group>cms_information</if_group>
  <id>^447|^449</id>
  <description>CMS User deleted event.</description>
</rule>

</group>

```

セキュリティログ監視ルール的重要度レベルと推奨される使用法

レベル	説明	備考
レベル0	無視され、処理は行われない	主に誤判定を回避するために使用されます。これらのルールは、他のすべてのルールより先に検索され、セキュリティとは無関係のイベントが含まれません。
レベル1	事前定義された使用法はなし	
レベル2	システムの優先度の低い通知	セキュリティとは無関係のシステム通知またはステータスメッセージ。
レベル3	成功した/承認されたイベント	成功したログイン試行、ファイアウォールで許可されたイベントなど。
レベル4	システムの優先度の低いエラー	不正な設定または未使用のデバイス/アプリケーションに関連するエラー。セキュリティとは無関係であり、通常は初期設定のインストールまたはソフトウェアのテストが原因で発生します。
レベル5	ユーザによって生成されたエラー	パスワードの誤り、処理の拒否など。通常、これらのメッセージはセキュリティとは関係ありません。
レベル6	関連性の低い攻撃	システムに脅威を及ぼさないワームまたはウイルスを示します (Linuxサーバを攻撃するWindowsワームなど)。また、頻繁にトリガされるIDSイベントおよび一般的なエラーイベントも含まれます。

レベル	説明	備考
レベル7	事前定義された使用法はなし	
レベル8	事前定義された使用法はなし	
レベル9	無効なソースからのエラー	不明なユーザとしてのログインの試行または無効なソースからのログインの試行が含まれます。特にこのメッセージが繰り返される場合は、セキュリティとの関連性がある可能性があります。また、adminまたはrootアカウントに関するエラーも含まれます。
レベル10	ユーザによって生成された複数のエラー	複数回の不正なパスワードの指定、複数回のログインの失敗などが含まれます。攻撃を示す場合や、単にユーザが資格情報を忘れた可能性もあります。
レベル11	事前定義された使用法はなし	
レベル12	重要度の高いイベント	システムやカーネルなどからのエラーまたは警告のメッセージが含まれます。特定のアプリケーションに対する攻撃を示す場合もあります。
レベル13	通常と異なるエラー (重要度: 高)	バッファオーバーフローの試行などの一般的な攻撃パターン、通常のSyslogメッセージ長の超過、または通常のURL文字列長の超過。
レベル14	重要度の高いセキュリティイベント	通常、複数の攻撃ルールと攻撃の兆候が組み合わさったもの。
レベル15	攻撃の成功	誤判定の可能性はほとんどありません。すぐに対処が必要です。

strftime() 変換指定子

指定子	説明
%a	曜日の省略名 (例: Thu)
%A	曜日の正式名 (例: Thursday)
%b	月の省略名 (例: Aug)
%B	月の正式名 (例: August)

指定子	説明
%c	日時形式 (例: Thu Sep 22 12:23:45 2007)
%d	月初から数えた日 (01~31) (例: 20)
%H	24時間形式の時刻 (00~23) (例: 13)
%l	12時間形式の時刻 (01~12) (例: 02)
%j	年初から数えた日 (001~366) (例: 235)
%m	10進表記の月 (01~12) (例: 02)
%M	分 (00~59) (例: 12)
%p	AMまたはPMの指定 (例: AM)
%S	秒 (00~61) (例: 55)
%U	1週目の最初の日を最初の日曜とした場合の週番号 (00~53) (例: 52)
%w	日曜を0とした場合の10進表記の曜日 (0~6) (例: 2)
%W	1週目の最初の日を最初の月曜とした場合の週番号 (00~53) (例: 21)
%x	日付形式 (例: 02/24/79)
%X	時刻形式 (例: 04:12:51)
%y	年の末尾2桁 (00~99) (例: 76)
%Y	年 (例: 2008)
%Z	タイムゾーン名または省略形 (例: EST)
%%	%記号 (例: %)

詳細については、次のWebサイトを参照してください。

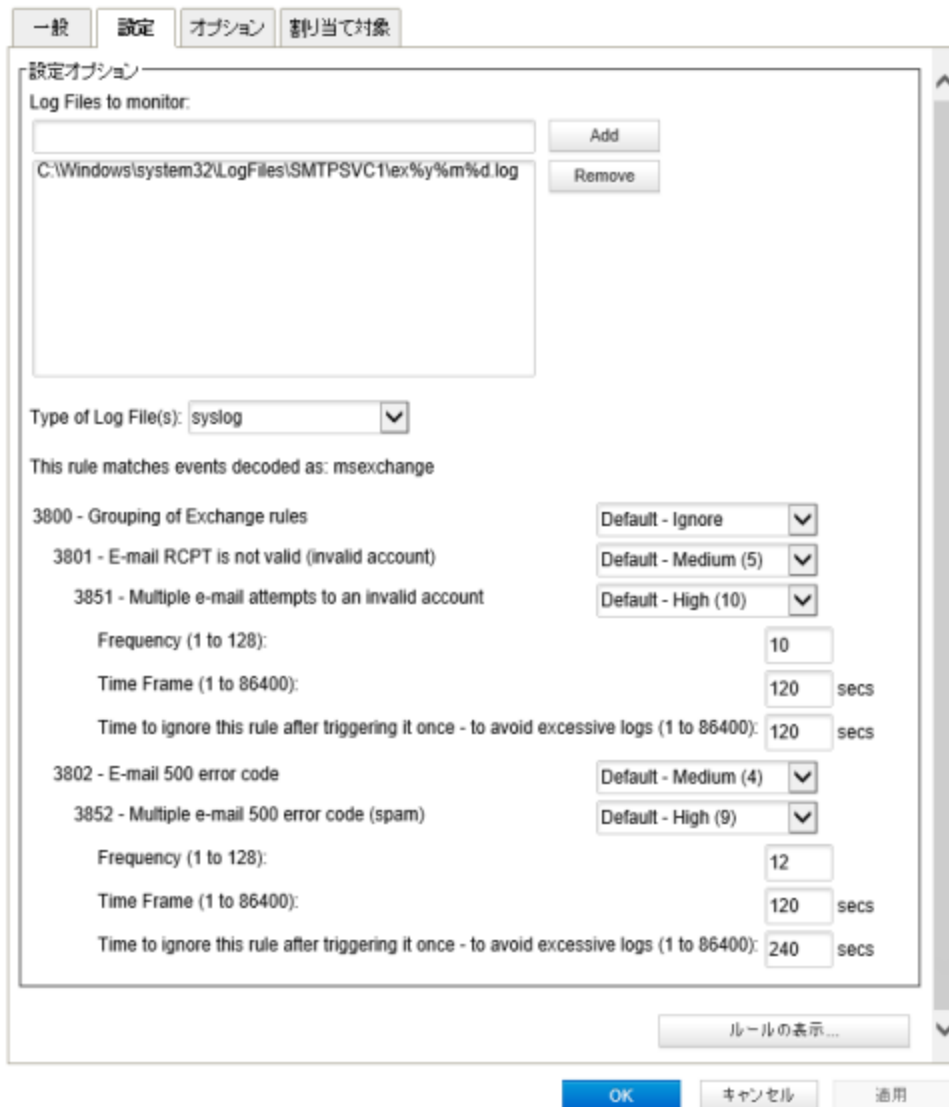
<https://www.php.net/manual/en/function.strftime.php>
www.cplusplus.com/reference/clibrary/ctime/strftime.html

セキュリティログ監視ルールの確認

セキュリティログ監視 ルールは、Deep Security Managerの Policies> Common Objects> Rules> セキュリティログ監視ルールにあります。

セキュリティログ監視 のルール構造とイベント照合プロセス

この画面ショットは、「Microsoft Exchange」セキュリティログ監視 ルールの[プロパティ]画面の[設定][設定]タブの内容を表示します。



次に、ルールの構造を示します。

- 3800 - Grouping of Exchange Rules - Default - ignore
 - 3801 - Email rcpt is not valid (invalid account) - Default - Medium (5)
 - 3851 - Multiple email attempts to an invalid account - Default - High (10)
 - Frequency (1 to 128) - 10
 - Time Frame (1 to 86400) - 120
 - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 120
- 3802 - E-mail 500 error code
 - 3852 - Multiple e-mail 500 error code (spam) - Default - High (9)
 - Frequency (1 to 128) - 12
 - Time Frame (1 to 86400) - 120 secs
 - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 240 secs

- 3802 - Email 500 error code - Default - Medium (4)
 - 3852 - Email 500 error code (spam) - Default - High (9)
 - Frequency (1 to 128) - 12
 - Time Frame (1 to 86400) - 120
 - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 240

セキュリティログ監視 エンジン は、ログイベントをこの構造に適用し、一致が発生したかどうかを確認します。たとえば、Exchange イベントが発生し、そのイベントが無効なアカウントに対するメールの受信である場合、このイベントは3800の行と一致します (3800の行がExchange イベントであるため)。また、同じイベントが、3800の行のサブルールである3801の行と3802の行にも適用されます。

これ以上の一致がない場合、この一致の「連鎖」は3800の行で停止します。3800の重大度は「Ignore」、」なので、セキュリティログ監視 イベントは記録されません。

ただし、無効なアカウントに対するメールの受信は、3800の行のサブルールの1つ、サブルール3801に一致しています。サブルール3801の重要度は「Medium (4)」です。ここで一致が停止した場合、重大度レベルが[中 (4)] のセキュリティログ監視 イベントが記録されます。

しかし、このイベントに該当するルールは他にもあります。サブルール3851です。同じイベントが過去120秒以内に10回発生した場合、サブルール3851とその3つの属性が一致するでしょう。その場合は、重大度が「高 (9)」 のセキュリティログ監視 イベントが記録されます。(「無視」属性は、サブルール3851に、サブルール3801と一致する個々のイベントを今後120秒間無視するように指示しています。これは、「ノイズ」の低減に役立ちます)。

サブルール3851のパラメータが一致したと仮定すると、重大度が「高 (9)」 のセキュリティログ監視 イベントが記録されます。

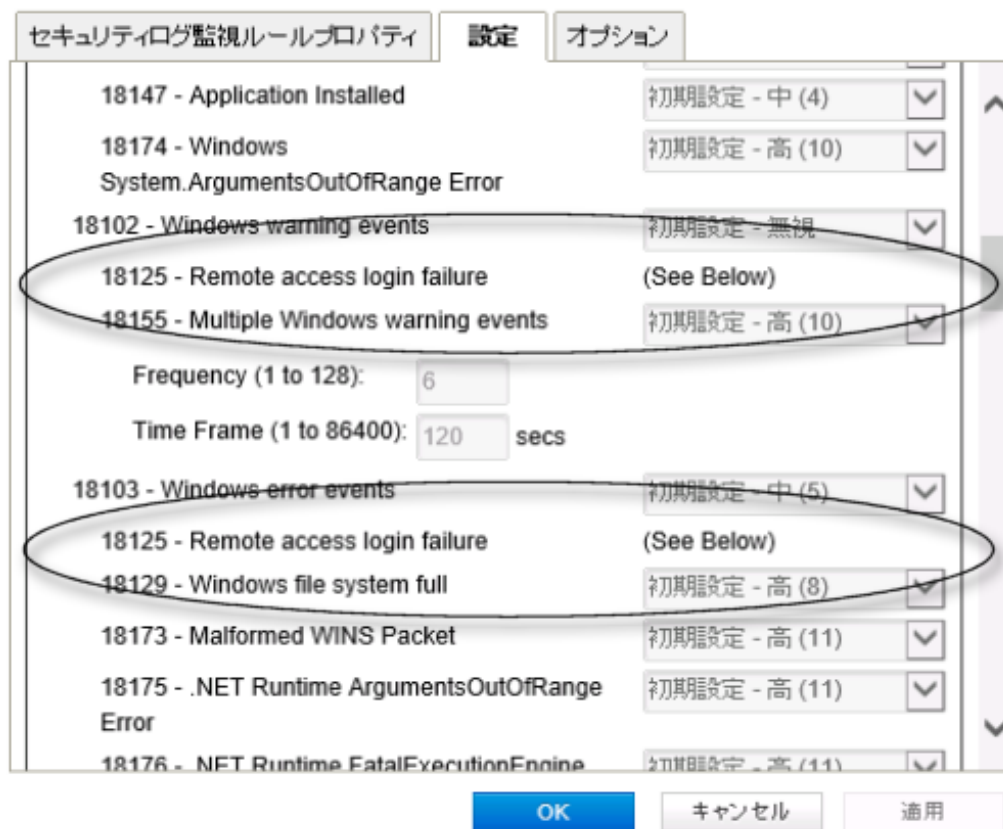
Mail Server - Microsoft Exchange ルールの [オプション] タブを調べてみると、重要度が「中 (4)」 のサブルールが一致していれば、Deep Security Managerによってアラートが発令されることがわかります。この例はこれに該当するため、アラートが発令されます ([このルールによってイベントが記録された場合にアラート] が選択されている場合)。

重複しているサブルール

一部のセキュリティログ監視 ルールに重複するサブルールがあります。例を見るには、[Microsoft Windows Events] ルールを開き、[設定] タブをクリックします。サブルール18125 (Remote access login failure) が、サブルール18102と18103の下に表示されています。また、

どちらの場合も、サブルール18125には重要度の値が示されておらず、単に [See Below] と表示されています。

重複して表示されるのではなく、ルール18125は、[設定] 画面の下部に1回だけ表示されています。



Webレピュテーションによる不正なURLへのアクセスのブロック

注意: Webレピュテーションがサポートされているオペレーティングシステムのリストについては、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。

Webレピュテーションモジュールは、不正なURLへのアクセスをブロックすることによって、Webの脅威から保護します。Deep Securityは、[Trend Micro Smart Protection Network](#)のWebセキュリティデータベースを使用して、ユーザがアクセスしようとしているWebサイトの

レピュテーションを確認します。Webサイトのレピュテーションは、コンピュータに適用されている特定のWebレピュテーションポリシーと比較されます。適用されている[セキュリティレベル](#)に応じて、Deep SecurityがURLへのアクセスをブロックまたは許可します。

注意: Webレピュテーションモジュールでは、HTTPSトラフィックはブロックされません。

Webレピュテーションを有効にして設定するには、次の基本手順を実行します。

1. ["Webレピュテーションモジュールをオンにする"](#) below
2. ["インラインモードとタップモードを切り替える"](#) below
3. ["セキュリティレベルを適用する"](#) on the next page
4. ["例外設定を作成する"](#) on page 936
5. ["Smart Protection Serverを設定する"](#) on page 937
6. ["詳細設定を編集する"](#) on page 938
7. ["Webレピュテーションをテストする"](#) on page 939

Agentコンピュータのユーザに表示されるメッセージを抑制するには、["コンピュータで通知を設定する"](#) on page 749を参照してください。

Webレピュテーションモジュールをオンにする

1. [ポリシー] に移動します。
2. Webレピュテーションを有効にするポリシーをダブルクリックします。
3. [Webレピュテーション]→[一般] をクリックします。
4. [Webレピュテーションのステータス] を [オン] にします。
5. [保存] をクリックします。

インラインモードとタップモードを切り替える

Webレピュテーションは、Deep Securityのネットワークエンジンを使用します。このエンジンは、次のいずれかのモードで動作します。

- **インライン:** パケットストリームがDeep Securityネットワークエンジンを直接流れます。すべてのルールは、プロトコルスタックの上位に伝わる前にネットワークトラフィックに適用されます。
- **タップモード:** パケットストリームは変更されません。トラフィックはWebレピュテーションによって処理されます（有効な場合）。ただし、問題が検出されてもパケットや接続が拒否されることはありません。タップモードでは、Deep Securityはイベントのレコードを提供する以外の保護は提供しません。

タップモードでは、実際のストリームは変更されません。すべての処理は複製されたストリーム上で行われます。タップモードでは、Deep Securityはイベントのレコードを提供する以外の保護は提供しません。

インラインモードとタップモードを切り替えるには、**コンピュータエディタまたはポリシーエディタ**¹を開き、[設定]→[詳細]→[ネットワークエンジンモード]の順に選択します。

ネットワークエンジンの詳細については、"[ファイアウォールルールを配信前にテストする](#)" on [page 836](#)を参照してください。

セキュリティレベルを適用する

既知の不正なWebアドレスまたはその疑いがあるWebアドレスには、次のリスクレベルが割り当てられます。

- 危険: 不正、または脅威の既知の発信源であると確認されたWebアドレス
- 非常に不審: 不正または脅威の発信源である可能性が疑われたWebアドレス
- 不審: スпамメールに関連付けられている、または感染している可能性のあるWebアドレス

セキュリティレベルは、関連付けられたリスクレベルに基づいて、Deep SecurityがURLへのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを [低] に設定すると、Deep SecurityはWebの脅威であることが判明済みのURLのみをブロックします。セキュリティレベルを上げるほど、Webの脅威の検出率が向上しますが、誤判定の可能性も増加します。

セキュリティレベルを設定するには、次の手順に従います。

1. [ポリシー] に移動します。
2. 編集するポリシーをダブルクリックします。
3. [Webレピュテーション]→[一般] をクリックします。
4. 次のセキュリティレベルのいずれかを選択します。
 - 高: ブロック対象のページ:
 - 危険
 - 非常に不審

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- 不審
- 中: ブロック対象のページ:
 - 危険
 - 非常に不審
- 低: ブロック対象のページ:
 - 危険

5. [保存] をクリックします。

例外設定を作成する

独自のブロックまたは許可するURLのリストで、Trend Micro Smart Protection Networkの評価に基づくブロック/許可の動作をオーバーライドできます。

注意: [許可] リストは [ブロック] リストよりも優先されます。[許可] リスト内のエン트리と一致するURLは、[ブロック] リストと照合されません。

URL例外設定を作成するには、次の手順に従います。

1. [ポリシー] に移動します。
2. 編集するポリシーをダブルクリックします。
3. [Webレピュテーション] → [例外] をクリックします。
4. URLを許可するには、次の手順に従います。
 - a. [許可] セクションに移動します。
 - b. [許可リストに追加するURL (1行に1つずつ)] の下の空白に必要なURLを入力します。一度に複数のURLを追加できますが、その場合は改行で区切る必要があります。
 - c. 次のいずれかを選択します。
 - ドメイン内すべてのURLを許可する: ドメイン内のすべてのページを許可します。サブドメインがサポートされています。エントリ内のドメインのみが含まれます (サブドメインはオプション)。たとえば、「example.com」および「another.example.com」は有効なエントリです。
 - URLを許可する: 入力したURLが許可されます。ワイルドカードがサポートされています。たとえば、「example.com/shopping/coats.html」および「example.com/shopping/*」は有効なエントリです。
 - d. [追加] をクリックします。

URLをブロックするには、次の手順に従います。

- a. [ブロック] セクションに移動します。
 - b. [ブロックリストに追加するURL (1行に1つずつ)] の下の空白に必要なURLを入力します。一度に複数のURLまたはキーワードを追加できますが、その場合は改行で区切る必要があります。
 - c. 次のいずれかを選択します。
 - ドメイン内すべてのURLをブロックする: ドメイン内のすべてのページをブロックします。サブドメインがサポートされています。エントリ内のドメインのみが含まれます (サブドメインはオプション)。たとえば、「example.com」および「another.example.com」は有効なエントリです。
 - URLをブロックする: 入力したURLがブロックされます。ワイルドカードがサポートされています。たとえば、「example.com/shopping/coats.html」および「example.com/shopping/*」は有効なエントリです。
 - このキーワードを含むURLをブロックする: キーワードを含むすべてのURLがブロックされます。
 - d. [追加] をクリックします。
5. [保存] をクリックします。

Smart Protection Serverを設定する

Webレピュテーション用のSmart Protectionサービスは、Webレピュテーションモジュールに必要なWeb情報を提供します。詳細については、[「Smart Protection Network - Global Threat Intelligence」](#)を参照してください。

Smart Protection Serverを設定するには、次の手順に従います。

1. [ポリシー] に移動します。
2. 編集するポリシーをダブルクリックします。
3. [Webレピュテーション]→[Smart Protection] の順にクリックします。
4. 次のように、トレンドマイクロのSmart Protectionサービスに直接接続するかどうかを選択します。
 - a. [Global Smart Protectionサービスへの直接接続] を選択します。
 - b. 必要な場合は [Global Smart Protectionサービスへのアクセス時にプロキシを使用する] を選択します。ドロップダウンメニューから [新規] を選択し、使用するプロキシを入力します。

1台または複数のローカルにインストールされたSmart Protection Serverに接続するには、次の手順に従います。

- a. [ローカルにインストールされたSmart Protection Serverの使用] (「http://[server]:5274」など) を選択します。

- b. Smart Protection Server URLをフィールドに入力し、[追加] をクリックします。Smart Protection Server URLを見つけるには、次のいずれかを実行します。
 - Smart Protection Serverにログインし、メイン画面の [Smart Protection Serverのステータス] を参照します。Smart Protection ServerのHTTPまたはHTTPSのURLは [Webレピュテーション] 行に表示されています。HTTPSのURLはバージョン11.0以降のDeep Security Agentでのみサポートされます。10.3以前のAgentをお使いの場合は、HTTP URLを使用してください。

または

- [Smart Protection ServerをAWSに配置した](#)場合は、AWSのCloudFormationサービスに移動し、Smart Protection Serverスタックの横にあるチェックボックスをオンにして、画面の一番下にある [Outputs] タブをクリックします。Smart Protection ServerのHTTPまたはHTTPSのURLは [WRSurl] フィールドと [WRSHTTPSurl] フィールドに表示されます。WRSHTTPSurlはバージョン11.0以降のDeep Security Agentでのみサポートされます。10.3以前のAgentをお使いの場合は、WRSurl URLを使用してください。
- c. 必要に応じて [ドメインに参加していない場合はGlobal Smart Protectionサービスに接続](Windowsのみ) を選択します。

5. [保存] をクリックします。

Smart Protection Serverへの接続の警告

このオプションは、コンピュータのSmart Protection Serverへの接続が切断されたときに、エラーイベントを生成してアラートを発令するかどうかを指定します。[はい] または [いいえ] を選択して [保存] をクリックします。

注意: Smart Protection Serverをローカルにインストールしている場合、Smart Protection Server自体に問題が発生した場合に通知が表示されるよう、少なくとも1台のコンピュータでこのオプションを [はい] に設定する必要があります。

詳細設定を編集する

ブロックページ

ユーザがブロック対象のURLにアクセスしようとする時、ブロックページに転送されます。[リンク] の空欄に、ブロックされたURLへのアクセスを要求するためにユーザが使用できるリンクを指定します。

アラート

[はい] または [いいえ] を選択して、Webレピュテーションイベントがログに記録された場合にアラートを出すかどうかを決定します。

ポート

[有害な可能性のあるWebページを監視するポート] の横にあるドロップダウンリストから、有害な可能性のあるWebページで監視する特定のポートを選択します。

Webレピュテーションをテストする

続行する前に、Webレピュテーションが正常に動作しているかどうかをテストします。

1. Webレピュテーションが有効になっていることを確認します。
2. コンピュータエディタまたはポリシーエディタで、[Webレピュテーション]→[除外] の順に選択します。
3. [ブロック] の下に「<http://www.speedtest.net>」と入力し、[追加] をクリックします。
[保存] をクリックします。
4. ブラウザを開いてこのWebサイトへのアクセスを試みます。アクセスを拒否するメッセージが表示されます。
5. [イベントとレポート]→[Webレピュテーション] の順に選択し、Webアクセスが拒否されたことが記録されているかどうかを確認します。検出が記録されていれば、Webレピュテーションモジュールは正常に動作しています。

SAP NetWeaverとの統合

Deep Security Scannerは、SAP NetWeaverプラットフォームに統合できます。

注意: Deep Security Scannerは、Deep Security AgentがRelayとして有効になっているコンピュータではサポートされません。

注意: FIPSモードが有効な場合、Deep Security Scannerはサポートされません。"[FIPS 140-2のサポート](#)" on page 1457を参照してください。

Deep Security Scanner機能を有効にする

1. Deep Security Managerで、[管理]→[ライセンス]に進みます。
2. [新しいアクティベーションコードの入力]をクリックします。
3. [Deep Security Scanner] エリア ([追加機能] の下) で、Deep Security Scannerアクティベーションコードを入力し、[次へ]をクリックして、画面の指示に従います。

コンピュータエディタまたはポリシーエディタ¹で [設定]→[Scanner] タブに進み、個々のポリシーやコンピュータに対してSAP機能を有効にできます。

注意: Deep SecurityのScanner機能を使用するには、不正プログラム対策モジュールも有効にして、Deep Security Agentでのみ使用可能にする必要があります。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

SAPサーバを追加する

Deep Security Managerで、[コンピュータ]画面に進み、[新規]をクリックします。SAPサーバをコンピュータのリストに追加する方法は複数あります。詳細については、"[Deep Security Managerにコンピュータおよびその他のリソースの追加](#)" on [page 506](#)を参照してください。

コンピュータまたはポリシーでSAP統合機能を有効にする

コンピュータエディタまたはポリシーエディタ¹の [設定]→[Scanner]画面を使用して、個々のコンピュータやポリシーに対してSAP統合モジュールを有効にできます。これらの機能を有効にするには、[設定]を [オン] または [継承 (オン)] に設定します。

SAP統合を設定する

Windows Server 2008 R2 64ビット、Windows Server 2012 R2 64ビット、SUSE Linux Enterprise Server 11/12 (SLES) 64ビット、またはRed Hat Enterprise Linux 6/7 (RHEL) 64ビットOSに自動的にインストールされるライブラリから、Trend Micro Deep Security Agentを呼び出すことができます。

統合は次の手順で実施します。

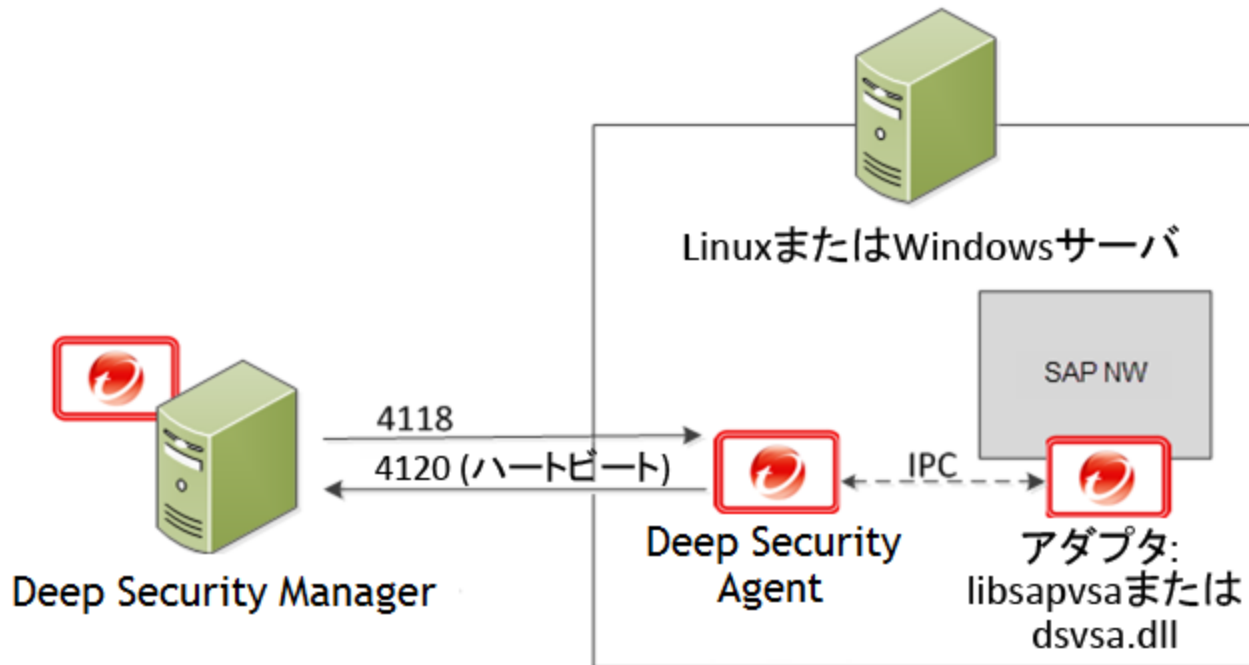
1. Windows Server 2008 R2 64ビット、Windows Server 2012 R2 64ビット、SLES 11/12、またはRHEL 6/7ベースのSAPアプリケーションサーバにDeep Security Agentをインストールします。"[Agentをインストールする](#)" on [page 944](#)を参照してください。
2. SAPサーバをDeep Security Managerに追加し、SAPサーバ上のAgentを有効化します。"[SAPサーバをManagerに追加する](#)" on [page 945](#)を参照してください。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

3. Agentに最新のパターンファイルと検索エンジンを割り当てるために、不正プログラム対策が有効なセキュリティプロファイルを適用します。"[セキュリティプロファイルを割り当てる](#)" on page 948を参照してください。
4. 以下のトランザクションを呼び出して、SAP Virus Scan Interface (VSI) を設定します。"[Agentを使用するようにSAPを設定する](#)" on page 954を参照してください。
 - VSCANGROUP
 - VSCAN
 - VSCANPROFILE
 - VSCANTEST

注意: 使用するOSや環境によっては、ここに記載する出力と若干異なる場合があります。

Deep SecurityとSAPのコンポーネント



Deep Security Managerが、SAP NetWeaverサーバ上のDeep Security Agentに接続します。Agentがlibsapvsaまたはdsvsa.dll (トレンドマイクロが提供する検索用のウイルスアダプタ) に接続します。

このソリューションを構成するコンポーネントは以下のとおりです。

- Deep Security Manager: 管理者がセキュリティポリシーを設定してDeep Security Agentによる保護を実施するのに使用する、Webベースの集中管理コンソール。
- Deep Security Agent: コンピュータに直接インストールされるセキュリティエージェント。保護の内容は、各Deep Security AgentがDeep Security Managerから受け取るルールとセキュリティ設定によって異なります。

- SAP NetWeaver: SAP統合テクノロジーのコンピューティングプラットフォーム。SAP NetWeaver Virus Scan Interface (NW-VSI) は、実際の検索を実行するサードパーティ製品にウイルス検索機能を提供します。NW-VSIインタフェースを有効化する必要があります。
- SAP NetWeaver ABAP WinGUI: SAP NetWeaverに使用されるWindows管理コンソール。このトピックでは、Deep Security AgentとSAP NetWeaver Virus Scan Interfaceの設定に使用します。

Agentをインストールする

Deep Security Agentをインストールすると、最初はコア機能のみがインストールされます。SUSE Linux Enterprise ServerまたはRed Hat Enterprise LinuxにAgentをインストールした後、Agentで各保護モジュールを有効にします。このときに、保護モジュールに必要なプラグインがダウンロードされ、インストールされます。

1. トレンドマイクロのダウンロードセンター (<https://help.deepsecurity.trendmicro.com/ja-jp/software.html>) にアクセスし、使用するOSに対応したDeep Security Agentパッケージをダウンロードします。
2. Agentをターゲットシステムにインストールします。OSに応じて、rpmまたはzypperを使用できます。この例ではrpmを使用し、次のように入力します。
`rpm -ihv Agent-Core-SuSE_<version>.x86_64.rpm`
3. Agentのインストールが完了したことを通知する次のような出力が表示されます。

```
ec2-52-28-57-164.eu-central-1.compute.amazonaws.com - PuTTY
ip-172-21-0-50:/home/ec2-user # rpm -ihv Agent-Core-SuSE_11-9.5.3-2774.x86_64.rpm
Preparing...                               ##### [100%]
 1:ds_agent                                ##### [100%]
Starting ds_agent:                           done
ip-172-21-0-50:/home/ec2-user # █
```

注意: Deep Security Managerで生成されたインストールスクリプトを使用してAgentをインストールすることもできます。

SAPサーバをManagerに追加する

AgentのSAPサーバへのインストールは完了しましたが、保護モジュールはまだ有効になっていません。保護を有効にするには、Deep Security ManagerコンソールにSAPサーバを追加する必要があります。

ManagerでSAPを有効化する

1. Deep Security Managerで、[管理]→[ライセンス]に進みます。
2. [新しいアクティベーションコードの入力]をクリックします。
3. [Deep Security Scanner] エリア ([追加機能] の下) で、SAPアクティベーションコードを入力し、[次へ]をクリックして、画面の指示に従います。

注意: SAP統合機能を使用するには、不正プログラム対策モジュールとWebレピュテーションモジュールも有効にする必要があります。

SAPサーバを追加する

SAPサーバを追加するには、Deep Security Managerコンソールを開き、[コンピュータ] タブで [新規] をクリックします。サーバを追加するには、Microsoft Active Directory、VMware vCenter、Amazon Web Services、またはMicrosoft Azureとの同期を含めて、複数の方法があります。FQDNまたはIPアドレスを使用してコンピュータを追加することもできます。手順の詳細については、"[Deep Security Managerにコンピュータおよびその他のリソースの追加](#)" on page 506を参照してください。

Agentの有効化

インスタンスのステータスは、[非管理対象 (有効化が必要)] または [非管理対象 (不明)] になっています。次に、Agentを有効化して、コンピュータを保護するためのルールとポリシーをManagerから割り当てられるようにする必要があります。有効化プロセスでは、AgentとManager間で一意のフィンガープリントが交換されます。これにより、1つのDeep Security ManagerのみがそのAgentと通信できるようになります。Agentを有効化する方法には、Agentからのリモート有効化とManagerからの有効化の2つがあります。

Managerからの有効化: Managerから有効化する方法では、Deep Security Managerが[ハートビート用の待機ポート番号](#)経由でAgentのFQDNまたはIPに接続できることが必要です。ただし、NATポート転送、ファイアウォール、またはAWSセキュリティグループが原因で難しい場合があります。Managerからの有効化を実行するには、Deep Security Managerコンソールの [コンピュータ] タブに移動し、Agentがインストールされているインスタンスを右クリックし、[処理]→[有効化] の順にクリックします。Managerからの有効化を使用する場合は、承認されていないDeep Security Managerから "[Deep Security Agentの保護](#)" on [page 1055](#)を行うことを強くお勧めします。

Agentからのリモート有効化: Agentからリモートで有効化する方法では、設定されているDeep Security Managerのアドレスに、Deep Security AgentがManagerのハートビート用待機ポート番号経由で接続できることが必要です。

Deep Security Managerのアドレス (FQDNまたはIP) は、Deep Security Managerコンソールの [管理]→[Managerのノード] で確認できます。

また、Deep Security Managerコンソールで [管理]→[システム設定]→[Agent] の順にクリックし、[Agentからのリモート有効化を許可] を選択して、Agentからのリモート有効化を有効にする必要があります。

次に、Deep Security Agentでローカルのコマンドラインツールを使用して、有効化プロセスを開始します。有効化の命令には、少なくとも有効化コマンドとManagerのURL (ポート番号を含む) を含めます。

```
dsa_control -a dsm://[managerurl]:[port]/
```

指定する項目は次のとおりです。

- `-a`はAgentを有効化するコマンドです。
- `dsm://managerurl:4120/`は、Agentに接続先のDeep Security Managerを指示するパラメータです(「managerurl」はDeep Security ManagerのURL、「4120」はAgentからManagerへの通信ポートです)。

ManagerのURLは、有効化コマンドの唯一の必須パラメータです。追加のパラメータを指定することもできます(指定可能なパラメータのリストについては、"[コマンドラインの基本](#)" on [page 447](#)を参照してください)。

以下の例では、Agentからのリモート有効化を使用するために次のように入力します。

```
/opt/ds_agent/dsa_control -a dsm://cetl-dsm.ceur-testlab.trendmicro.de:4120/
```

```
ec2-52-28-57-164.eu-central-1.compute.amazonaws.com - PuTTY
ip-172-21-0-50:/home/ec2-user # rpm -ihv Agent-Core-SuSE_11-9.5.3-2774.x86_64.rpm
Preparing... ##### [100%]
 1:ds_agent ##### [100%]
Starting ds_agent: done
ip-172-21-0-50:/home/ec2-user # /opt/ds_agent/dsa_control -a dsm://cetl-dsm.ceur-testlab.trendmicro.de:4120/
Starting thread 'CScriptThread' with stack size of 1048576
HTTP Status: 200 - OK
Response:
Attempting to connect to https://cetl-dsm.ceur-testlab.trendmicro.de:4120/
SSL handshake completed successfully - initiating command session.
Connected with AES256-SHA to peer at cetl-dsm.ceur-testlab.trendmicro.de
Received a 'GetHostInfo' command from the manager.
Received a 'GetHostInfo' command from the manager.
Received a 'SetDSMCert' command from the manager.
Received a 'SetAgentCredentials' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetInterfaces' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'SetSecurityConfiguration' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Command session completed.
ip-172-21-0-50:/home/ec2-user #
```

上記の出力は、Agentの有効化が完了したことを示しています。

有効化を確認する手順は次のとおりです。

1. Deep Security Managerコンソールで、[コンピュータ] タブに移動します。
2. コンピュータ名をクリックし、[詳細] をクリックして、コンピュータのステータスが「管理対象」であることを確認します。

セキュリティプロファイルを割り当てる

この時点でのAgentのステータスは [管理対象 (オンライン)] ですが、保護モジュールはインストールされていません。つまり、AgentとManagerは通信していますが、Agentが設定を使用していない状態です。

保護を適用するには、いくつかの方法があります。この例では、SAPインスタンス上で直接、不正プログラム対策とSAPを有効化し、初期設定の検索設定を割り当てます。

1. **コンピュータエディタ**¹で、[不正プログラム対策]→[一般]の順に選択します。

¹コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

2. [不正プログラム対策] セクションで、[設定] を [オン] (または [継承 (オン)]) に設定し、[保存] をクリックします。

コンピュータ

概要

不正プログラム対策

Webレピューテーション

ファイアウォール

侵入防御

変更監視

セキュリティログ監視

アプリケーションコントロール

インタフェース

設定

アップデート

オーバーライド

一般

Smart Protection

Connected Threat Defense

詳細

検出

不正プログラム対策

設定:

継承 (オン)

ステータス:

継承 (オン)

オン

オフ

が見つかりません,リアルタ

リアルタイム検索

継承

不正プログラム検索設定:

Default Real-Time Scan Configuration

スケジュール:

Every Day All Day

手動検索

継承

不正プログラム検索設定:

Default Manual Scan Configuration

予約検索

継承

不正プログラム検索設定:

Default Scheduled Scan Configuration

3. [リアルタイム検索]、[手動検索]、または [予約検索] のセクションで、[不正プログラム検索設定] および [スケジュール] を設定するか、それらの設定を親ポリシーから継承するように設定します。
4. [保存] をクリックします。不正プログラム対策モジュールのステータスが、[オフ、インストール保留中] に変わります。このステータスは、AgentがDeep SecurityManagerから必要なモジュールを取得中であることを意味します。モジュールの取得には、クライアントが[Relayの待機ポート番号](#)でDeep Security Relayにアクセスできることが必要です。少し経ってから、Agentがセキュリティアップデート (不正プログラム対策のパターンファイルや検索エンジンなど) のダウンロードを開始します。
5. コンピュータエディタで、[設定]→[Scanner] に進みます。
6. [SAP] セクションで、[設定] を [オン] (または [継承 (オン)]) に設定し、[保存] をクリックします。

Agentのステータスが再び [管理対象 (オンライン)] に変わり、不正プログラム対策モジュールとScanner (SAP) モジュールのステータスが [オン] に変わったら、SAPの設定に進むことができます。

コンピュータ: [REDACTED]



概要

一般

処理

システムイベント



不正プログラム対策



Webレピュテーション



ファイアウォール



侵入防御



変更監視



セキュリティログ監視



アプリケーションコント



インタフェース

ホスト名:

表示名:

説明:

プラットフォーム:

グループ:

ポリシー:

資産の重要度:

セキュリティアップデートのダウ

Red Hat E

Agentを使用するようにSAPを設定する

これでDeep SecurityAgentが稼働状態になり、OSのファイルシステムを検索できるようになりました。次に、AgentにSAPアプリケーションサーバを認識させる必要があります。そのためには、アプリケーションサーバ内にウイルススキャンアダプタを作成します。ウイルススキャンアダプタは、グループに属している必要があります。ウイルススキャンアダプタとウイルススキャングループを作成したら、ウイルススキャンプロファイルを使用して検索の対象と動作を設定します。

必要な手順は以下のとおりです。

1. ["トレンドマイクロのスキナグループを設定する" on the next page](#)
2. ["トレンドマイクロのウイルススキャンプロバイダを設定する" on page 961](#)
3. ["トレンドマイクロのウイルススキャンプロファイルを設定する" on page 967](#)
4. ["ウイルススキャンインタフェースをテストする" on page 977](#)

注意: ウイルススキャングループとウイルススキャンアダプタは、どちらもグローバル設定です (クライアント00)。ウイルススキャンプロファイルは、各テナントで設定する必要があります (クライアント01、02など)。

トレンドマイクロのスキナグループを設定する

Trend Micro Deep Security On-Premise 12.0

1. SAP WinGUIで、VSCANGROUPトランザクションを実行します。編集モードで、[New Entries]を選択します。

Table View Edit Goto Selection Utilities(M) System Help

vsclangroup

Change View "Scanner Groups": Overview


New Entries

Dialog Structure

- Scanner Groups
 - Configuration Param

Scanner Group	Business Add-In	Group Text

Position... Entry 0 of 0



2. 新しいスキャナグループを作成して、[Scanner Group] 領域でグループ名を指定し、[Group Text] 領域でスキャナグループの説明を指定します。

Table View Edit Goto Selection Utilities(M) System Help

✓ [Dropdown]

New Entries: Overview of Added Entries

[Icons]

Dialog Structure

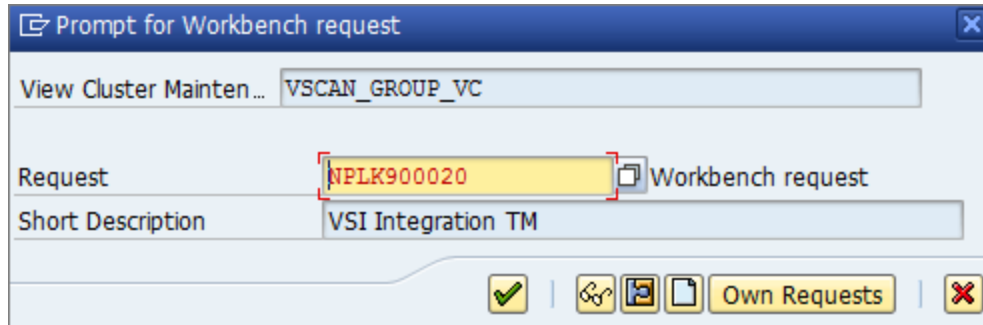
- Scanner Groups
 - Configuration Param...

Scanner Group	Group Text
Z_IMGROUP	VSCANGROUP for Trend Micro Deep Security

Position... Entry 0 of 0

SAP

3. [保存]アイコンをクリックするか、編集モードを終了します。
[ワークベンチの要求を要求]という名前のダイアログボックスが表示されます。次の例では、VSI関連のすべての変更を追跡するための新しいワークベンチ要求が作成されます。



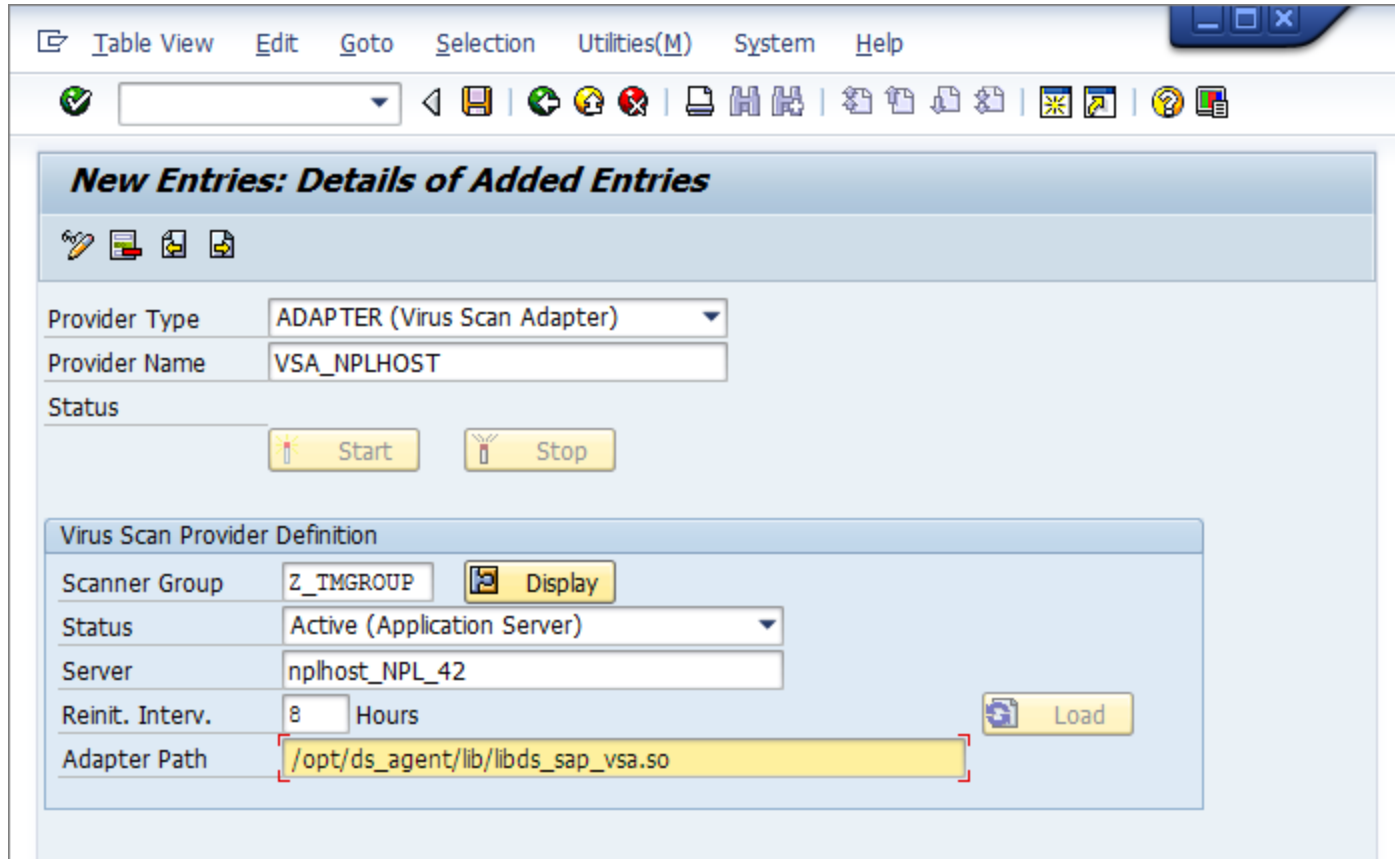
次の手順で、VSI統合を実際に設定します。これはウイルススキャンアダプタと呼ばれます。

トレンドマイクロのウイルススキャンプロバイダを設定する

Trend Micro Deep Security On-Premise 12.0

1. SAP WinGUIで、VSCANトランザクションを実行します。編集モードにして、[New Entries]をクリックします。

2. VSI認定ソリューションの新しい設定を入力します。
以下の例では、次の構成パラメータが設定されています。



設定	値	説明
Provider Type	ADAPTER (Virus Scan Adapter)	自動的に設定されます (初期設定)。
Provider Name	VSA_<ホスト名>	自動的に設定され、エイリアスとして機能します。

設定	値	説明
Scanner Group	前の手順で設定したグループを選択します。	入力ヘルプを使用して、以前に作成されたすべてのスキャナグループを表示できます。
Status	Active (Application Server)	自動的に設定されます (初期設定)。
Server	nplhost_NPL_42	自動的に設定されるホスト名です。
Reinit.Interv.	8 Hours	ウイルススキャンアダプタが再初期化されて新しいウイルス定義がロードされるまでの時間を指定します。
Adapter Path (Linux)	/lib64/libsapvsa.so	初期設定のパスです。
Adapter Path (Windows)	C:\Program Files\Trend Micro\Deep Security Agent\lib\dsvsa.dll	初期設定のパスです。

3. [保存]アイコンをクリックするか、編集モードを終了します。
これをワークベンチ要求にパックするよう求めるプロンプトが表示されます。
4. 要求を確認し、[Start]ボタンをクリックします。
ステータスライトが緑色に変わります。これは、アダプタがロードされてアクティブであることを意味します。

Table View Edit Goto Selection Utilities(M) System Help

New Entries: Details of Added Entries

Provider Type

Provider Name

Status ■

Start Stop

Virus Scan Provider Definition

Scanner Group Display

Status

Server

Trace Level

Reinit. Interv. Hours Last Initialization: 13.04.2015 17:09:48 Load

Adapter Path

Configuration

Engine Data

Version	9.8
Version Text	VSAPI-9.8.1009
Date	Mon Apr 13 15:09:47 2015
Known Viruses	

Loaded Drivers

Version	Driver Name	Date	Known Viruses
11.601	Smart Scan Agent Pattern	Mon Apr 13 14:23:22 2015	
1.175	IntelliTrap Exception Pattern	Mon Apr 13 14:23:22 2015	

Data was saved

ここまでで、VSIの設定はほぼ完了です。アプリケーションサーバは、Deep Securityが提供するウイルススキャンを使用してファイルトランザクションを処理できる状態になりました。

トレンドマイクロのウイルススキャンプロファイルを設定する

1. SAP WinGUIで、VSCANPROFILEトランザクションを実行し、ウイルススキャンが必要なSAPの操作を選択します。
たとえば、/SCET/GUI_UPLOADまたは/SCET/GUI_DOWNLOADのチェックボックスをオンにして、[Save]を選択します。

Table View Edit Goto Selection Utilities(M) System Help

vscanprofile

Change View "Virus Scan Profile": Overview

New Entries

Dialog Structure

- Virus Scan Profile
 - Steps
 - Step Configurat
 - Profile Configuration
 - MIME Types

Virus Scan Profile	Active	Default Pr...	Profile Text
/IC_CCS_MCM/ICI_MAIL	<input type="checkbox"/>	<input type="checkbox"/>	Virus Scan for E-Mails Rece
/SARC/ARCHIVING_ADK	<input type="checkbox"/>	<input type="checkbox"/>	Virus Protection Using the
/SCET/DP_VS_ENABLED	<input type="checkbox"/>	<input type="checkbox"/>	
/SCET/GUI_DOWNLOAD	<input type="checkbox"/>	<input type="checkbox"/>	File Download Using CL_G
/SCET/GUI_UPLOAD	<input type="checkbox"/>	<input type="checkbox"/>	File Upload Using CL_GUI_
/SCMS/KPRO_CREATE	<input type="checkbox"/>	<input type="checkbox"/>	
/SIHTTP/HTTP_DOWNLO...	<input type="checkbox"/>	<input type="checkbox"/>	File Download Using Meth
/SIHTTP/HTTP_UPLOAD	<input type="checkbox"/>	<input type="checkbox"/>	File Upload Using the Metl
/SIWB/KW_UPLOAD_CRE...	<input type="checkbox"/>	<input type="checkbox"/>	Create Versions/Objects ir
/SMIM_API/PUT	<input type="checkbox"/>	<input type="checkbox"/>	Mime Repository
/SRM/RCM_CREATE	<input type="checkbox"/>	<input type="checkbox"/>	

Position... Entry 1 of 11

Change -> Display (Ctrl+F4)

SAP

2. 編集モードにして、[New Entries] をクリックします。

ウイルススキャンプロファイルでは、ウイルススキャンインターフェースに対応して特定のトランザクション (ファイルアップロード、ファイルダウンロードなど) をどのように処理するかが定義されます。アプリケーションサーバで以前に設定したウイルス検索アダプタを使用するには、新しいウイルス検索プロファイルを作成する必要があります。

Trend Micro Deep Security On-Premise 12.0

3. [Scan Profile] ボックスに「Z_TMProfile」と入力し、[Active]、[Default Profile]、[Evaluate Profile Configuration Param] の各チェックボックスをオンにします。

The screenshot displays the configuration interface for Trend Micro Deep Security On-Premise 12.0. At the top, there is a menu bar with options: Table View, Edit, Goto, Selection, Utilities(M), System, and Help. Below the menu is a toolbar with various icons for navigation and actions. The main window title is "New Entries: Details of Added Entries".

On the left side, there is a "Dialog Structure" tree view showing a hierarchy: Virus Scan Profile > Steps > Step Configurat. Below this, there are links for Profile Configuration and MIME Types.

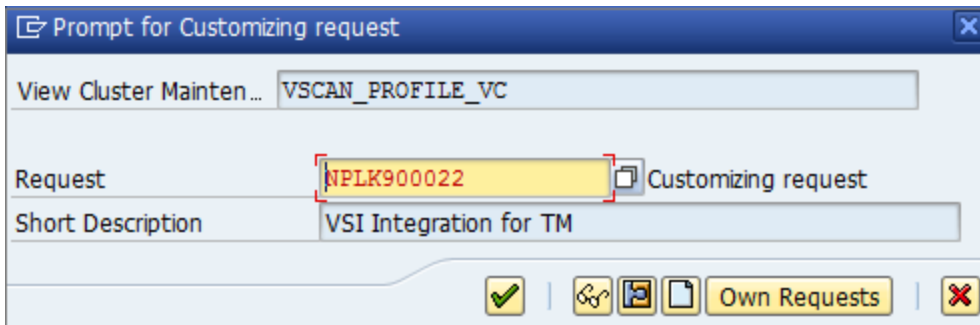
The main configuration area is titled "Virus Scan Profile" and contains the following fields and options:

- Scan Profile: Z_TMProfile
- Profile Text: VSCANPROFILE for Trend Micro Deep Security
- Active:
- Evaluate Profile Configuration Param.:
- Default Profile: (highlighted with a red box)
- Use Reference:
- Link: All steps successful

The SAP logo is visible in the bottom right corner of the interface.

4. 編集モードで、[Steps] フォルダをダブルクリックして、手順を設定します。

5. [New Entries] をクリックします。
ステップは、プロファイルがトランザクションから呼び出されたときの動作を定義します。
6. [Position] を「0」に、[Type] を「Group」に、[Scanner Group] を前の手順で設定したグループの名前に、それぞれ設定します。
7. 既存のプロファイルはアクティブではなく、使用されていないため、通知は無視してください。
この通知を確認すると、設定内容を「カスタマイズリクエスト」にまとめるように求められます。新しいリクエストを作成すると、変更内容を追跡しやすくなります。



8. ステップの設定パラメータを作成するには、[Profile Configuration Parameters] フォルダをダブルクリックし、[New Entries] をクリックしてパラメータを設定します。

パラメータ	種類	説明
CUST_ACTIVE_CONTENT	BOOL	ファイルにスクリプト (Java/PHP/ASPスクリプト) とブロックが含まれているかどうかを確認します
CUST_CHECK_MIME_TYPE	BOOL	<p>ファイルの拡張子がファイルのMIMEタイプと一致するかどうかを確認します。一致しない場合はファイルがブロックされます。すべてのMIMEタイプと拡張子名を正確に照合できます。次に例を示します。</p> <ul style="list-style-type: none"> • Wordファイルは.docまたは.dotでなければならない • JPEGファイルは.jpgでなければならない • テキストファイルとバイナリファイルはどの拡張子でもかまわない (ブロックしない)

パラメータ	種類	説明
		"サポートされているMIMEタイプ" on page 983を参照してください。

9. [Step Configuration Parameters] フォルダをダブルクリックします。[New Entries] をクリックし、パラメータを設定します。

パラメータ	種類	説明
SCANBESTEFFORT	BOOL	スキャンを「ベストエフォート」ベースで実行します。つまり、VSAにオブジェクトの検索を許可するセキュリティ上重要なフラグ (SCANALLFILESやSCANEXTRACTなど) をすべて有効化するだけでなく、内部フラグも有効にします。該当するフラグに関する詳細は証明書に保存することができます。
SCANALLFILES	BOOL	ファイル拡張子に関係なくすべてのファイルをスキャンします。
SCANEXTENSIONS	CHAR	VSAでスキャンする必要があるファイル拡張子のリストです。指定した拡張子のファイルのみがチェックされます。その他の拡張子はブロックされます。ワイルドカードを使用してパターンを検索することも可能です。*は1文字以上の任意の文字、?は任意の1文字を表します。構文は「exe;com;do?;ht* =>」です。「*」は全ファイルをスキャンすることを意味します。
SCANLIMIT	INT	この設定は圧縮ファイルに適用され、解凍されてスキャンされるファイルの最大数を指定します。
SCANEXTRACT	BOOL	アーカイブまたは圧縮オブジェクトを解凍します。
SCANEXTRACT_SIZE	SIZE_T	最大解凍サイズです。
SCANEXTRACT_DEPTH	INT	オブジェクトが解凍される最大の深さ (階層) です。
SCANMIMETYPES	CHAR	スキャン対象となるMIMEタイプのリストです。設定されたMIMEタイプのファイルのみがチェックされます。それ以外のMIMEタイプはブロックされます。このパラメータは、CUST_CHECK_MIME_TYPEが有効になっている場合にのみ機能します。
BLOCKMIMETYPES	CHAR	ブロックするMIMEタイプのリスト。このパラメータは、CUST_CHECK_MIME_TYPE

パラメータ	種類	説明
		が有効になっている場合にのみ機能します。
BLOCKEXTENSIONS	CHAR	ブロックするファイル拡張子のリスト

この設定はクライアント単位であり、SAPアプリケーションサーバの各テナントで設定する必要があります。

ウイルススキャンインターフェースをテストする

Trend Micro Deep Security On-Premise 12.0

1. SAP WinGUIで、VSCANTESTトランザクションを実行します。

Program Edit Goto System Help

vscantest

Test for Virus Scan Interface

Object to Be Checked

- Test Data
 - EICAR Anti-Virus Test File
- Local File
- File on the Application Server

Scanner Selection

- Virus Scan Profile
 - (Defaultprofil)
- Scanner Group
- Virus Scan Provider

General Settings

- Display Scan Details
- Action: Check Only

SAP

VSI対応の各SAPアプリケーションサーバには、設定ステップが正しく実行されたかどうかをチェックするテストも組み込まれています。そのため、特定のスキャンツールを呼び出すことのできるトランザクションにEICARテストウイルス (www.eicar.org) が追加されます。

2. 何も入力しないと、最後の手順で設定した初期設定のプロファイルが呼び出されるため、何も入力しないでください。
3. [実行]をクリックします。
EICARテストウイルスの概要を示す通知が表示されます。

4. 通知を確認します。

トランザクションがインターセプトされました：

Goto System Help

SAP

Result

✘ Return Value: 2- (At least one virus found)

Infections

ID	Virus Name	Object
	Eicar_test_1	/tmp/zUeEbZZ_TMPROFILE

Content Information

File Name	Extension	MIME Type	Object
		text/plain	/tmp/zUeEbZZ_TMPROFILE

.....

T...	Message Text	LText
	Start the processing of virus scan profile Z_TMPROFILE	
	Virus scan profile Z_TMPROFILE, step 00: scanner group Z_TMGROUP	
	Virus scan adapter VSA_NPLHOST was selected from scanner group Z_TMGROUP	
	Virus scan profile Z_TMPROFILE, step 00: scan instance returns 2- (At least one virus fo...	
	Virus "Eicar_test_1" found in object "/tmp/zUeEbZZ_TMPROFILE"	
	Profile Z_TMPROFILE failed, since step 00 failed (AND linkage)	

SAP

[Infections] には、検出された不正プログラムに関する情報が表示されます。

[Content Information] には、ファイルの正しいMIMEタイプが表示されます。

ファイルには、ランダムに生成された7文字のアルファベットにウイルススキャンプロファイル名を付加した名前が付けられません。

この後に、トランザクションの各ステップに関する出力が表示されます。

1. トランザクションが初期設定のウイルススキャンプロファイル (Z_TMPROFILE) を呼び出します。
2. ウイルススキャンプロファイルZ_TMPROFILEは、ウイルススキャングループZ_TMGROUPからアダプタを呼び出すように設定されています。
3. ウイルススキャングループZ_TMGROUPには複数のアダプタが設定されており、そのうちの1つが呼び出されます (この例ではVSA_NPLHOST)。
4. ウイルススキャンアダプタから、ウイルスが見つかったことを示す値「2-」が返されます。
5. 検出された不正プログラムに関する情報として、Eicar_test_1およびファイルオブジェクト/tmp/ zUeEbZZ_TMPROFILEが表示されます。
6. ステップ00 (ウイルススキャングループ) が失敗してファイルトランザクションの処理が停止されたため、呼び出された初期設定のウイルススキャンプロファイルZ_TMPROFILEが失敗します。

クロスチェックのために、この「不正プログラム」イベントの情報がDeep Security Managerコンソールにも表示されます。このイベントを表示するには、**コンピュータエディタ**¹を開き、[不正プログラム対策]→[イベント]の順にクリックします。

サポートされているMIMEタイプ

Deep Security ScannerでサポートされるMIMEタイプは、使用しているDeep Security Agentのバージョンによって異なります。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Trend Micro Deep Security On-Premise 12.0

- Deep Security Agent 9.6ではVSAPI 9.85を使用
- Deep Security Agent 10.0ではATSE 9.861を使用
- Deep Security Agent 10.1ではATSE 9.862を使用
- Deep Security Agent 10.2、10.3、11.0、11.1、および11.2ではATSE 10.000を使用
- Deep Security Agent 11.3以降ではATSE 11.0.000を使用

MIMEタイプ	説明	拡張子	9.6 Agentでサポート	10.0 Agentでサポート	10.1以降の Agentでサポート
application/octet-stream		*	○	○	○
application/com	COMファイル	com	○	○	○
application/ecmascript	EMCScriptファイル	es	○	○	○
application/hta	HTAファイル	hta	○	○	○
application/java-archive	Java Archive (JAR) ファイル	jar	○	○	○
application/javascript	JavaScriptファイル	js、jsxinc、jsx	○	○	○
application/msword	Word for Windows	doc、dot	○	○	○
application/vnd.ms-access	MS Access	mdb	×	×	×
application/vnd.ms-project	MS Project	mpp	×	×	×
application/msword	MS Word	doc、dot	○	○	○
application/octet-stream	COMファイル	com	○	○	○
application/octet-stream	EXEファイル	exe	○	○	○
application/pdf	Adobe Portable Document Format ファイル	pdf	○	○	○
application/postscript	Postscript	ai	○	○	○
application/postscript	Postscript	ps	○	○	○
application/postscript	Postscript	ps	○	○	○
application/rar	RARファイル	rar	○	○	○

Trend Micro Deep Security On-Premise 12.0

MIMEタイプ	説明	拡張子	9.6 Agentでサポート	10.0 Agentでサポート	10.1以降の Agentでサポート
application/rtf	Microsoft RTF	rtf	○	○	○
application/sar	Sarファイル	sar	○	○	○
application/vnd.ms-excel	Excel for Windows	xls、xlt、xla	○	○	○
application/vnd.ms-outlook	Outlook for Windows	msg	×	○	○
application/vnd.ms-powerpoint	Windows PowerPoint	ppt、pot、pps、ppa	○	○	○
application/vnd.ms-publisher	MS Publisher	pub	×	×	○
application/vnd.oasis.opendocument	Open Document	odf	○	○	○
application/vnd.openxmlformats-officedocument.presentationml.presentation	MS Officeファイル	pptx、potx、ppsx、ppam、pptm、potm、ppsm	○	○	○
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	MS Officeファイル	xlsx、xltx、xlsm、xltm、xlam、xlsb	○	○	○
application/vnd.openxmlformats-officedocument.wordprocessingml.document	MS Officeファイル	docx、dotx、docm、dotm	○	○	○
application/vnd.rn-realmedia	Real Media	rm	○	○	○
application/wordperfect	WORDPerfect	wp、wp5、wp6、wpd、w60、w61	○	○	○
application/x-alf		alf	○	○	○
application/x-arc-compressed	ARCファイル	arc	○	○	○
application/x-bzip2	bZIPファイル	*	○	○	○
application/x-cpio	CPIOファイル	*	○	○	○
application/x-director	Macromedia Director Shockwave Movie	dcr	○	○	○
application/x-gzip	Gzip	*	○	○	○
application/xhtml+xml	XHTML	dhtm、dhtml、htm、html、htx、sht、shtm、shtml、stml、xht、xhtm、xhtml、xml、txt	○	○	○
application/x-java-class	JAVAアプレット	class	○	○	○
application/x-kep		kep	○	○	○

Trend Micro Deep Security On-Premise 12.0

MIMEタイプ	説明	拡張子	9.6 Agentでサポート	10.0 Agentでサポート	10.1以降の Agentでサポート
application/x-otf		otf	○	○	○
application/x-sapshortcut		sap、 sapc	○	○	○
application/x-shockwave-flash	Macromedia Flash	swf	○	○	○
application/x-silverlight-app	PKZIP	xap	○	○	○
application/x-sim		sim	○	○	○
application/x-tar	TARファイル	tar	○	○	○
application/x-vbs		*	○	○	○
application/zip	ZIPファイル	zip、 zipx	○	○	○
audio/basic	Audio	snd、 au	○	○	○
audio/midi	MIDI	mid、 midi、 rmi、 mdi、 kar	○	○	○
audio/x-aiff	Apple/SGIのAudio InterChangeファイル形式	aiff、 aif、 aifc	○	○	○
audio/x-mpeg-3	MP3	mp3	○	○	○
audio/x-realaudio	Real Audio	ra	○	○	○
audio/x-voc	Creative Voice Format(VOC)	voc	○	○	○
image/bmp	Windows BMP	bmp	○	○	○
image/gif	GIF	gif	○	○	○
image/ico	Windowsアイコン	ico	○	○	○
image/jpeg	JPEG	jpg、 jpeg、 jpe、 jif、 jfif、 jfi	○	○	○
image/msp	Microsoft Paint	msp	○	○	○
image/png	Portable Network Graphics	png	○	○	○
image/ppm	PPM画像	ppm	○	○	○
image/svg+xml		svg	○	○	○
image/tiff	TIFF	tif、 tiff	○	○	○
image/vnd.ms-modi	Microsoft Document Imaging	mdi	○	○	○
image/x-cpt	Corel PhotoPaint	cpt	○	○	○

Trend Micro Deep Security On-Premise 12.0

MIMEタイプ	説明	拡張子	9.6 Agentでサポート	10.0 Agentでサポート	10.1以降の Agentでサポート
image/x-pcx	PCX	pcx	○	○	○
image/x-pict	Macintosh Bitmap	pct	○	○	○
image/x-ras	Sun Raster(RAS)	ras	○	○	○
image/x-wmf	Windowsメタファイル	wmf	○	○	○
text/csv	CSV	csv、txt	○	○	○
text/html	HTML	dhtm、dhtml、htm、html、htx、sht、shtm、shtml、stml、xht、xhtm、xhtml、xml、txt	○	○	○
text/plain		*	○	○	○
text/plain	テキストファイル	txt	○	○	○
text/xml	XML	dhtm、dhtml、htm、html、htx、sht、shtm、shtml、stml、xht、xhtm、xhtml、xml、txt	○	○	○
text/xsl	XSL	xsl	○	○	○
unknown/unknown		*	○	○	○
video/mpeg		*	○	○	○
video/quicktime	Quick Time Media	qt	○	○	○
video/x-fli	AutoDesk Animator	fli	○	○	○
video/x-flv	Macromedia Flash FLV Video	flv	○	○	○
video/x-ms-asf	Advanced Streaming Format	asf	○	○	○
video/x-scm	Lotus ScreenCam Movie	scm	○	○	○

Deep Securityのベストプラクティスガイド

Deep Security 12 Best Practice Guideは現在、[PDF形式でご利用](#)いただけます。主な内容は以下のとおりです。

- 導入に際しての注意事項と推奨事項
- アップグレードのガイドラインとシナリオ
- サイジングの注意事項と推奨事項
- システムのパフォーマンスを最大化し、管理の手間を削減するための推奨設定
- VDI、プライベート、およびパブリッククラウド環境でのベストプラクティスのヒント

管理

ライセンス情報の確認

注意: 親テナントからライセンスを継承しているマルチテナント設定には該当しません。

Trend Micro Deep Securityのライセンスの詳細が表示されます。Deep Securityは、6個のモジュールパッケージで構成されています。

- 不正プログラム対策とWebレピュテーション
- ファイアウォールと侵入防御
- 変更監視とアプリケーションコントロール
- セキュリティログ監視

Trend Micro Deep Security On-Premise 12.0

- マルチテナント
- Deep Security Scanner

モジュールパッケージごとに製品版または体験版のライセンスが必要です。個別パッケージのライセンスのステータスは、[詳細の表示] をクリックすると確認できます。トレンドマイクロから新しいアクティベーションコードを受け取ったら、[新しいアクティベーションコードの入力] をクリックしてライセンスの情報を入力します。ライセンスで許可された新しい機能がすぐに使用できるようになります。

ライセンスが期限切れになると、既存の機能は維持されますが、アップデートは配信されません。

期限切れが近い、または期限切れになったモジュールがある場合は、ユーザに通知されます。

注意: Trend Micro Deep Securityライセンス種類および価格については、次のサイトをご覧ください。

https://www.trendmicro.com/ja_jp/business/products/hybrid-cloud/deep-security-data-center.html?modal=pdf02-c2aa2b

データベースのバックアップと復元

データベースをバックアップしておく、大規模な障害が発生した場合、またはDeep Security Managerを別のコンピュータに移行する場合にDeep Securityを復元できます。

データベースをバックアップする

データベースのバックアップ方法については、データベースベンダのドキュメントを参照してください。

ヒント: RDSについては、AWSによって提供されている、データベースをS3バケットにバックアップする手順を参照してください。たとえば、[「Amazon RDS for SQL Server - Support for Native Backup/Restore to Amazon S3」](#)を参照してください。

データベースのみを復元する

1. Deep Security Managerのサービスを停止します。
2. データベースを復元します。
同じビルド番号のDeep Security Managerのデータベースである必要があります。
3. Deep Security Managerのサービスを開始します。
4. データベースが復元されたことを確認します。
5. 適切な設定が行われるように、すべてのコンピュータをアップデートします。

Deep Security Managerとデータベースの両方を復元する

1. 紛失または破損したDeepSecurityManagerの残りをすべて削除します。Deep Security Managerをアンインストールするときは、構成ファイルを保持することを選択しないでください。
2. データベースを復元します。
3. データベースコンテンツをサポートするDeepSecurity Managerインストーラーのバージョンを見つけて、インストールします。インストール中に、[データベースオプション]で[新しいマネージャーノードの追加]オプションを選択します。
4. Deep Security Managerを正常にインストールした後、Deep Security Managerコンソールを開き、[管理]> [マネージャーノード]に移動し、古いオフラインマネージャーノードを廃止します。

オブジェクトをXML形式またはCSV形式でエクスポートする

- イベント: いずれかの [イベント] 画面に進み、[詳細検索] オプションを使用してイベントデータをフィルタします。たとえば、「理由」列に「spoofed」という語が含まれる、過去1時間以内にログに記録された、「コンピュータ > Laptops」コ

コンピュータグループ内のコンピュータのすべてのファイアウォールイベントを検索できます。

ファイアウォールイベント すべて グループ化しない 検索

期間: 過去1時間

コンピュータ: グループ: ADMIN-PC

検索: 理由 次の文字列を含む spoofed +

右矢印の付いた送信ボタンをクリックして「クエリ」を実行します。次に、[エクスポート]をクリックして、フィルタしたデータをCSV形式でエクスポートします。表示されているすべてのエントリをエクスポートすることも、選択したデータだけをエクスポートすることもできます。この形式でのログのエクスポートは、主にサードパーティのレポートツールとの統合のために行います。

- コンピュータリスト: コンピュータリストは、[コンピュータ]画面からXML形式またはCSV形式でエクスポートできます。この処理は、1つのDeep Security Managerで管理しているコンピュータの台数が多すぎるために、もう1つDeep Security Managerをセットアップすることを計画している場合に行うことができます。選択したコンピュータのリストをエクスポートすると、すべてのコンピュータを再検出してグループ分けする手間が省けます。

注意: ポリシー、ファイアウォールルール、侵入防御ルールの設定は含まれません。ファイアウォールルール、侵入防御ルール、ファイアウォールステートフル設定、およびポリシーをエクスポートしてから、コンピュータに再適用する必要があります。

- ポリシー: XML形式でエクスポートするには、[ポリシー] を選択します。

注意: 選択したポリシーをXMLにエクスポートすると、子ポリシー (存在する場合) もエクスポートパッケージに追加されます。エクスポートパッケージには、ポリシーに関連する実際のオブジェクトがすべて格納されます。ただし、侵入防御ルール、セキュリティログ監視ルール、変更監視ルール、およびアプリケーションの種類は含まれません。

- ファイアウォールルール: ファイアウォールルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- ファイアウォールステートフル設定: ファイアウォールステートフル設定は、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- 侵入防御ルール: 侵入防御ルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- 変更監視ルール: 変更監視ルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- セキュリティログ監視ルール: セキュリティログ監視ルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- その他の共通オブジェクト: 再利用可能なすべてのコンポーネントの共通オブジェクトは、同じ方法でXMLファイルまたはCSVファイルにエクスポートできます。

CSVにエクスポートする場合、表示されている列のデータのみが含まれます。表示するデータを変更するには、[列] ツールを使用します。グループは無視されるので、データの順序が画面と異なる場合があります。

オブジェクトをインポートする

各オブジェクトをDeep Securityに個別にインポートするには、オブジェクト画面のツールバーにある [新規] の横で、[ファイルからインポート] を選択します。

Deep Security Managerの再起動

Linux

Deep Security Managerを再起動するには、CLIを開き、次のコマンドを実行します。

```
sudo systemctl restart dsm_s
```

Windows

Deep Security Managerを再起動するには、最初に、Deep Security Managerを実行しているWindowsインスタンスにログインし、"[Windowsデスクトップ](#)" [below](#)、"[コマンドプロンプト](#)" [below](#)、または"[PowerShell](#)" [on the next page](#)で、次の手順を実行します。

Windowsデスクトップ

1. Windowsタスクマネージャーを開きます。
2. [サービス] タブをクリックします。
3. [Trend Micro Deep Security Manager] サービスを右クリックし、[再起動] をクリックします。

コマンドプロンプト

コマンドプロンプト (cmd.exe) を開いて、次のコマンドを実行します。

1. `net stop "Trend Micro Deep Security Manager"`
2. `net start "Trend Micro Deep Security Manager"`

PowerShell

PowerShellを開き、次のコマンドを実行します。

1. `Stop-Service 'Trend Micro Deep Security Manager'`
2. `Start-Service 'Trend Micro Deep Security Manager'`

Deep Securityのアップグレード

アップグレードについて

最大限の保護を実現するには、アップデートが利用可能になったら、ソフトウェアアップデート、セキュリティアップデート、および不正プログラムパターンファイルのアップデートをする必要があります。アップデートには次の種類があります。

- ソフトウェアのアップグレード: Deep Security Manager、Virtual Appliance、Agent、Relayなどの新しいソフトウェアのパッケージ。"[Deep Securityのインストールまたはアップグレード](#)" on page 223、"[Deep Security Virtual Applianceのアップグレード](#)" on page 1006、"[Deep Security Agentのアップグレード](#)" on page 998、"[Deep Security Relayのアップグレード](#)" on page 997を参照してください。
- セキュリティアップデート: 潜在的な脅威を特定するためにDeep Securityが使用するセキュリティルールと不正プログラムパターンファイルに対するアップデート。"[セキュリティアップデートの取得と配布](#)" on page 1039を参照してください。

Relayは、ソフトウェアアップデートとセキュリティアップデートの両方をAgentおよびVirtual Applianceに配布します。ソフトウェアアップデートは、[ローカルミラーWebサーバで配布](#)することもできます (セキュリティアップデートは不可)。

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。最初にRelayをアップグレードしないと、セキュリティコンポーネントのアップグレードとソフトウェアのアップグレードが失敗することがあります。詳細については、"[Deep Security Relayのアップグレード](#)" on page 997を参照してください。

このトピックの内容:

- "Agentによるアップデートの整合性の検証方法" below
- "Deep Security Managerによるソフトウェアアップグレードの確認方法" on the next page

Agentによるアップデートの整合性の検証方法

すべてのセキュリティアップデートは、電子署名やチェックサム (ハッシュ)、およびその他の開示されていない方法を使用して、Deep Securityによってその整合性が検証されます。ソフトウェアアップデートはデジタル署名されています。

Agent

ソフトウェア	リリースの種類	ビルド	リリース日	サイズ	ダウンロード
1  Deep Security Agent 11.0.0-211 for amzn1-x86_64	GM: 11.0_GM	11.0.0-211	2018-05-22	69 MB	
2 SHA256: dfe5a4a5a6c0bc04d20593980396ef12f9d08a4745b1003c965397f63e3ec4b4 MD5: f0bf66269c28aa0d2486461f95a8f58c Readme					

署名や[ダウンロードセンター](#)で提供されているチェックサムを手動で検証する場合は、次のようなツールを使用することもできます。

- sha256sum (Linux)
- Checksum Calculator (Windows)
- jarsigner (Java Development Kit (JDK))

たとえば、次のコマンドを入力して、ダウンロードしたファイルの署名を検証することができます。

```
jarsigner -verify <filename>.zip
```

Deep Security Managerによるソフトウェアアップグレードの確認方法

Deep Security Managerは、Trend Microのアップデートサーバに定期的に接続し、[Deep Security Managerのデータベースにインポートした](#)次のソフトウェアに対するアップデートを確認します。

- Deep Security Agent
- Deep Security Virtual Appliance
- Deep Security Manager

最新かどうかの確認は、ダウンロードセンターにあるアップデートとの比較ではなく、ローカルインベントリ内のアップデートと比較して行われます。(ダウンロードセンターに新しいソフトウェアが見つかった場合は、別途アラートが表示されます)。

注意: Deep Securityによって表示されるのは、ソフトウェアの(メジャーバージョンではなく)マイナーバージョンに対するアップデートのみです。

たとえば、バージョン9.6.100のAgentを使用している場合にTrend Microからバージョン9.6.200のAgentがリリースされると、ソフトウェアアップデートが利用可能なことを通知するアラートが表示されます。ただし、その後、Trend Microからメジャーバージョンであるバージョン10.0.xxxのAgentがリリースされた場合、10.0 Agentがデータベース内に存在しなければ、10.0が9.6.100より新しいバージョンであるにもかかわらず、アラートは表示されません。

Managerのアラートでは、ソフトウェアアップデートが利用可能であることが通知されます。[管理]→[アップデート]→[ソフトウェア]の[トレンドマイクロダウンロードセンター]セクションでも、利用可能なアップデートの有無が表示されます。ソフトウェアをDeep Security Managerデータベースにインポート(ダウンロード)したら、使用環境でソフトウェアをアップグレードすることができます。["Deep Security Agentのアップグレード" on the next page](#)および「Deep Security Virtual Applianceのアップグレード」を参照してください。

ヒント: ダウンロードできるすべてのソフトウェアパッケージを確認するには、[管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]に移動します。ソフトウェアパッケージをまだインポートしていない場合もここで確認します。

最後の確認がいつ実行され、成功したかどうかを確認したり、アップデートの確認を手動で開始したりするには、[管理]→[アップデート]→[ソフトウェア]に移動し、[Deep Security]セクションを確認します。アップデートの確認を実行する予約タスクを設定している場合は、次回の予約確認の日時もここに示されますタスクを実行するには、["Deep Security予約タスクの設定" on page 479](#)

インポートされたソフトウェアは、Deep Security Managerデータベースに格納されます。そして、定期的にRelay有効化済みAgentに複製されます。

Deep Security Relayのアップグレード

Deep Security Relayのアップグレードは、2つのソフトウェアが共通しているので、[Deep Security Agentのアップグレード](#)と同じです。

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。最初にRelayをアップグレードしないと、セキュリティコンポーネントのアップグレードとソフトウェアのアップグレードが失敗することがあります。

次の手順に従ってRelayをアップグレードします。

1. Deep Security Managerにログインします。
2. 次のいずれかの方法にてRelayを識別します。
 - [コンピュータ]に移動します。メイン画面で、Relayアイコン () の付いたコンピュータを探します。それが使用しているRelayです。Relayアイコンが Deep Security Manager コンピュータの横に表示されている場合は、RelayがDeep Security Managerにインストールされています。このRelayはアップデートすることができます。または
 - [管理] を選択します。左側で、[アップデート]→[Relayの管理] をクリックします。メイン画面で、[Relayグループ] を展開します。使用しているRelayがRelayアイコン () 付きで表示されます。
3. Relayをダブルクリックします。Relayコンピュータの詳細が表示されているダイアログボックスが開きます。
4. [処理] タブをクリックします。
5. [Agentのアップグレード] をクリックします。ウィザードが表示されます。ウィザードの進め方の詳細については、「["Agentのアップグレードを開始する" on page 1000](#)」のウィザードのページに関する説明を参照してください。これでRelayがアップグレードされました。
6. すべてのRelayをアップグレードしてから、Agentのアップグレードを開始します。

Deep Security Agentのアップグレード

ソフトウェアのアップグレードは、Deep Security Managerを使用して手動で開始することも、サードパーティの配信システムを使用して開始することもできます。

ヒント: Deep Security AgentがインストールされたLinuxコンピュータが環境に含まれている場合は、Agentが有効化または再有効化されたときに、ご利用のDeep Security Managerと互換性のある最新バージョンのソフトウェアにそれらのAgentを自動的にアップグレードすることもできます。詳細については、「[Agentを有効化するとき自動的にアップグレードする](#)」 on [page 397](#)を参照してください。

警告: Deep Security Agentをアップグレードする前に、すべてのDeep Security Relayをアップグレードする必要があります。最初にRelayをアップグレードしないと、セキュリティコンポーネントのアップグレードとソフトウェアのアップグレードが失敗することがあります。詳細については、"[Deep Security Relayのアップグレード](#)" on page 997を参照してください。


警告: LinuxプラットフォームでDeep Security Agentをアップグレードする前に、OS カーネルがエージェントの最新バージョンでサポートされていることを確認してください。詳細については、"[Deep Security AgentのLinuxカーネルサポート](#)" on page 183

このトピックの内容:

- "[アラートからAgentをアップグレードする](#)" below
- "[Agentのアップグレードを開始する](#)" on the next page
- "[新しく有効化されたVirtual ApplianceのAgentを選択する](#)" on page 1001
- "[Agentを手動でアップグレードする](#)" on page 1001

アラートからAgentをアップグレードする

新しいAgentソフトウェアバージョンが利用可能になると、[アラート] にメッセージが表示されます。

 **Agent/Applianceソフトウェアのアップグレードを推奨するコンピュータがあります。** 1 分前

Deep Security Managerは、Managerにインポートされた最新バージョンより古いバージョンのAgent/Applianceがインストールされたコンピュータを検出しました。Agent/Applianceソフトウェアのアップグレードをお勧めします。

[▲ 詳細非表示](#)

時刻: 2019-07-25 23:20

前回のアップデート: 2019-07-25 23:20

重要度: 警告

[旧版のコンピュータをすべて表示](#)

1. アラートで [詳細の表示] をクリックし、[旧版のコンピュータをすべて表示] をクリックします。
[コンピュータ] が開き、[ソフトウェアアップデートステータス] が [旧版] であるすべてのコンピュータが表示されます。

2. "Agentのアップグレードを開始する" belowまたは"Agentを手動でアップグレードする" on the next pageに進みます。

Agentのアップグレードを開始する


ヒント: アップグレードはサーバの負荷が低いときに実行してください。

警告: Solaris 11コンピュータで、trendmicro publisherに以前のアップグレード結果が設定されたままになっている可能性があります。アップグレードの失敗を回避するには、Solaris 11で次のコマンドを実行してから、Agentをアップグレードします。

```
pkg unset-publisher trendmicro  
rm -rf /var/opt/ds_agent/ips_repo
```

[管理]→[アップデート]→[ソフトウェア]の[コンピュータ]セクションには、コンピュータまたはVirtual Applianceがアップグレードを利用できるAgentを実行しているかどうかを示されます。確認は、ダウンロードセンターにあるソフトウェアではなく、Deep Securityにインポート済みのソフトウェアと比較して行われます。最新でないコンピュータがある場合、次のいずれかを実行します。

- 最新でないコンピュータをすべてアップグレードするには、[Agent/Applianceソフトウェアのアップグレード]をクリックします。
- 特定のAgentコンピュータまたはApplianceイメージアップグレードするには、次の手順を実行します。
 - a. [コンピュータ]に移動し、アップグレードするコンピュータを選択して、[処理]→[Agentソフトウェアのアップグレード]の順をクリックします。

警告: 失敗を防ぐには、Agentの前にRelayをアップグレードする必要があります。[詳細を表示](#)。Relayを識別するには、Relayアイコン ()を確認します。

- b. 表示されたダイアログボックスで、[Agentバージョン]を選択します。初期設定の[プラットフォーム用の最新バージョンを使用 (X.Y.Z.NNNN)]を選択することをお勧めします。[次へ]をクリックします。

注意: コンピュータでVirtual Applianceを有効化すると、Red Hat Agentが [Virtual Appliance配信] オプションで指定されたバージョンにアップグレードされます ("新しく有効化されたVirtual ApplianceのAgentを選択する" [below](#)を参照)。最新のRed Hat Agentを削除するためには、最初にすべてのVirtual Applianceソフトウェアパッケージを削除する必要があります。古いバージョンのRed Hat Agentは、使用されていないなければ削除できます。

注意: Solarisでのアップグレードには、完了までに5分以上かかることがあります。

新しく有効化されたVirtual ApplianceのAgentを選択する

注意: Deep Security Virtual Applianceのアップグレードの詳細については、"[Deep Security Virtual Applianceのアップグレード](#)" [on page 1006](#)を参照してください。

Deep Security Virtual Applianceは、64ビット版Red Hat Enterprise LinuxのAgentから保護モジュールプラグインのソフトウェアパッケージを使用します。[Virtual Appliance配信] オプションを使用すると、新しく有効化されたVirtual Applianceに配信されるRed Hat Enterprise Linux Agentソフトウェアのバージョンを選択できます。


初期設定項目の [利用可能な最新バージョン (推奨)] が選択されている場合、使用されるソフトウェアは、インポートされたApplianceソフトウェアの最新バージョンと互換性がある最新バージョンのインポート済みAgentソフトウェアとなります。

インポート済みのApplianceより前のバージョンのAgentソフトウェアはリストに表示されません。

Agentを手動でアップグレードする

場合によっては、接続の制限があるためにDeep Security ManagerからAgentソフトウェアをアップグレードできなかつたり、サードパーティのシステムを使用してアップグレードを配信したりすることがあります。そのような場合は、コンピュータにコピーしたインストーラを使用してAgentソフトウェアをアップグレードできます。

[ダウンロードセンター](#)から新しいAgentソフトウェアをダウンロードするか、Deep Security ManagerからAgentソフトウェアをエクスポートします ("[Deep Security Agentソフトウェアの入手](#)" on page 372を参照)。インストーラを実行します。方法はOSによって異なります。

警告: 失敗を防ぐには、Agentの前にRelayをアップグレードする必要があります。 [詳細を表示](#)。Relayを識別するには、Relayアイコン ()を確認します。

Windows上でAgentを手動でアップグレードする

1. Agentセルフプロテクションを無効にします。この操作を行うには、Deep Security Managerで、**コンピュータエディタ**¹の [設定]→[一般] に移動します。[Agentセルフプロテクション] で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
2. Agentのインストーラをコンピュータにコピーします。
3. Agentのインストーラを実行します。以前のAgentが検出され、アップグレードが実行されます。

Linux上でAgentを手動でアップグレードする

1. Agentのインストーラをコンピュータにコピーします。
2. 次のコマンドを実行します。

```
rpm -U <新しいAgentのインストーラのrpm>
```

(「-U」引数は、インストーラでアップグレードを実行するように設定します。)

Solaris上でAgentを手動でアップグレードする

警告: Solaris 11でDeep Security Agent 9.0からアップグレードする場合は、Deep Security Agent 9.0.0-5616または9.0以降のAgentにアップグレードしてからDeep Security Agent 11.0にアップグレードする必要があります。それ以前のビルドから直接

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

アップグレードすると、Agentを起動できなくなる可能性があります。この問題が発生した場合は、"[Solaris 11でのアップグレードの問題を解決する](#)" on page 1546を参照してください。

多くのSolarisサーバで実行されるワークロードの重大な性質のため、アップグレードの際に次のベストプラクティスに従うことをお勧めします。

- 実稼働サーバをアップグレードする前に、準備環境でアップグレード手順をテストします。
- 実稼働サーバをアップグレードする場合、最初の数台については、1台ずつアップグレードします。各サーバのアップグレードは、それぞれ十分な間隔を空けてから行います。
- 特定のSolarisバージョンおよびアプリケーションの役割（たとえば、リバースプロキシ、Webサーバ、ミドルウェアなど）に対して数多くの本番サーバを個別にバージョンアップした後、)はそのバージョンの残りのサーバとアプリケーションの役割をグループでアップグレードします。

Solaris上のAgentを手動でアップグレードするには

- Solaris 11、1つのゾーン (グローバルゾーンで実行):

```
X86: pkg update -g file:///mnt/Agent-Solaris_5.11-9.x.x-xxxx.x86_64/Agent-Core-Solaris_5.11-9.x.x-xxxx.x86_64.p5p pkg:/security/ds-agent
```

```
SPARC: pkg update -g file:///mnt/Agent-Solaris_5.11-9.x.x-xxxx.x86_64/Agent-Solaris_5.11-9.x.x-xxxx.sparc.p5p pkg:/security/ds-agent
```

- Solaris 11、複数のゾーン (グローバルゾーンで実行):

```
pkg unset-publisher trendmicro
```

```
rm -rf <path>
```

```
mkdir <path>
```

Trend Micro Deep Security On-Premise 12.0

```
pkgrepo create <path>
```

```
pkgrecv -s file:///<dsa core p5p file location> -d <path> '*'
```

```
pkg set-publisher -g <path> trendmicro
```

```
pkg update pkg://trendmicro/security/ds-agent
```

```
pkg unset-publisher trendmicro
```

```
rm -rf <path>
```

- Solaris 10:ds_adm.fileという名前のインストール設定ファイルを次の内容で作成し、ルートディレクトリに保存します。次に、以下のコマンドを実行してパッケージをインストールします。

```
pkgadd -G -v -a /root/ds_adm.file -d Agent-Core-Solaris_5.10_U7-10.0.0-1783.x86_64.pkg
```

ds_adm.fileの内容

```
mail=
```

```
instance=overwrite
```

```
partial=nocheck
```

```
runlevel=quit
```

```
idepend=nocheck
```

```
rdepend=quit
```

```
space=quit
```

```
setuid=nocheck
```

```
conflict=quit
```

```
action=nocheck
```

```
proxy=
```

```
basedir=default
```

AIX上のエージェントを手動でアップグレードする

多くのAIXサーバで実行されるワークロードの重大な性質のため、アップグレード時に次のベストプラクティスに従うことをお勧めします。

- 実稼働サーバをアップグレードする前に、準備環境でアップグレード手順をテストします。
- 実稼働サーバをアップグレードする場合、最初の数台については、1台ずつアップグレードします。各サーバのアップグレードは、それぞれ十分な間隔を空けてから行います。
- 特定のAIXバージョンおよびアプリケーションの役割（たとえば、リバースプロキシ、Webサーバ、ミドルウェアなど）に対して数多くの本番サーバを個別にバージョンアップした後、)は、そのバージョンの残りのサーバおよびアプリケーションの役割をグループ単位でアップグレードします。

AIX上のエージェントを手動でアップグレードするには

1. 最新のAIXエージェントインストーラファイル（BFFファイル）を、AIXコンピュータ上の `/tmp` などの一時フォルダにコピーします。詳細な手順については、"[AIXにAgentをインストールする](#)" on page 381のインストールを参照してください。
2. エージェントをアップグレードしてください。次のコマンドを使用します。

```
/tmp> rm -f ./.*
```

```
/tmp> installp -a -d /tmp/<agent_BFF_file_name> ds_agent
```

ここで、`<agent_BFF_file_name>` は、抽出したBFFインストーラファイルの名前に置き換えられます。

Deep Security Virtual Applianceのアップグレード

トレンドマイクロでは、最新のセキュリティパッチ、アップデート、および継続的なサポートを利用できるように、Deep Security Virtual Applianceを最新バージョンにアップグレードすることを推奨しています。

Applianceを構成する次の2つの要素は、個別にアップグレードできます。

- ApplianceのService Virtual Machine (SVM)
- Appliance SVMに組み込まれたDeep Security Agent

注意: 「Appliance SVM」という用語は、VMwareインフラストラクチャにインストールされているDeep Security Virtual Appliance仮想マシンを指します。

トピック:

- ["Applianceのサポート期間とアップグレードに関する推奨事項" below](#)
- ["Appliance SVM、組み込みのAgent、およびDeep Security Managerのバージョンは一致している必要がありますか" on the next page](#)
- ["アップグレードする必要があるかどうかを確認する" on the next page](#)
- ["Applianceをアップグレードする" on page 1009](#)

Applianceのサポート期間とアップグレードに関する推奨事項

Appliance SVMとApplianceに組み込まれたAgentのリリースサイクルは異なるため、これらのアップグレードはそれぞれ異なるスケジュールで行う必要があります。詳細については、下の表を参照してください。

コンポーネント	リリーススケジュール	アップグレードのベストプラクティス	サポート
Appliance SVM	Deep Securityの 長期間サポート (LTS) リリース のたびにリリースされます。Appliance SVMの Feature Releases (FR) はありません。	年に1回アップグレードする。	3年間の標準サポート 4年間の延長サポート
組み込みのAgent	LTSリリース のたびにAppliance SVMとともにリリースされ、 FR のたびに別途ダウンロードファイルが提供されます。	少なくとも年に1回アップグレードし、互換性のある新しいAgentがリリースされたときには毎回アップグレードする。	Appliance SVMのサポートと一致

Appliance SVM、組み込みのAgent、およびDeep Security Managerのバージョンは一致している必要がありますか

いいえ。ただし、Managerのバージョンは、Appliance SVMおよび組み込みのAgentと同等か、それ以上である必要があります。

アップグレードする必要があるかどうかを確認する

現在実行しているAppliance SVMと組み込みのAgentのバージョンが不明な場合、または新しいバージョンがあるかどうか分からない場合は、このセクションを参照してください。これらに該当しない場合は、このセクションをスキップして、"[Applianceをアップグレードする](#)" on page 1009に直接進んでください。

アップグレードが必要かどうかを判断するには、以下のセクションを参照してください。

- ["現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する"](#) below
- ["新しいAppliance SVMがあるかどうかを確認する"](#) below
- ["新しいAgentがあるかどうかを確認する"](#) on the next page

現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 画面の右上部にある検索ボックスに、「Deep Security Virtual Appliance」と入力してAppliance仮想マシンを検索します。
3. Appliance仮想マシンを右クリックして、次の順にメニュー項目をクリックします: [詳細]→[一般]。
 - [Virtual Applianceのバージョン] プロパティに、組み込みのDeep Security Agentのバージョンが表示されます。このAgentはAppliance SVM上にインストールされています。この値を書き留めます。
 - [Appliance (SVM) のバージョン] プロパティ: この仮想マシンをインストールするために使用されるDeep Security Virtual Applianceパッケージのバージョンを示します。この値を書き留めます。

新しいAppliance SVMがあるかどうかを確認する

1. Deep Security Managerで、[管理] をクリックします。
2. 左側で、[アップデート]→[ソフトウェア]→[ダウンロードセンター] の順に展開します。
3. メイン画面で、上部右の検索バーに「Appliance-ESX」と入力し、<Enter>キーを押します。すべてのAppliance SVMソフトウェアが表示されます。
4. メイン画面で、現在使用しているDeep Security Managerのリリースと一致するLTSリリースを展開します。
5. [バージョン] フィールドに表示されているバージョンが現在インストールされているバージョンよりも新しいかどうかを確認します。
6. アップグレードが必要な場合は、次の["Applianceをアップグレードする"](#) on the next pageセクションに進みます。

新しいAgentがあるかどうかを確認する

1. Deep Security Managerで、[管理] をクリックします。
2. 左側で、[アップデート]→[ソフトウェア]→[ダウンロードセンター] の順に展開します。
3. メイン画面で、上部右の検索バーに、現在インストールされているAppliance SVMと互換性のあるAgentの名前を入力します。詳細については、[互換性の表](#)を参照してください。たとえば、検索ボックスに「Agent-RedHat_EL7」と入力します。互換性のあるAgentのリストが表示されます。
4. メイン画面で最新のリリースを展開し、最新のAgentを表示します。
5. [バージョン] フィールドに表示されているバージョンが現在インストールされているバージョンよりも新しいかどうかを確認します。
6. アップグレードが必要な場合は、次の"[Applianceをアップグレードする](#)" belowセクションに進みます。

Applianceをアップグレードする

Applianceのアップグレードが必要があることがわかった場合は、NSX Data Center for vSphere (NSX-V) とNSX-Tのどちらを使用しているかに応じて、いくつかのアップグレードオプションを選択できます。

NSX-Vを使用している場合は、次の3つのアップグレードオプションを選択できます。

- 方法1: "[既存のAppliance SVMを自動的にアップグレードする](#)" on the next page。次の場合はこのオプションを選択します。
 - 新しいバージョンのAppliance SVMがトレンドマイクロから提供されている。
 - アップグレード中にゲスト仮想マシンの保護が中断されても問題がない。保護が中断されると問題がある場合は、オプション2を選択します。
 - NSX Data Center for vSphere (NSX-V) を使用している。
- 方法2: "[既存のAppliance SVMを手動でアップグレードする](#)" on page 1015。次の場合はこのオプションを選択します。
 - トレンドマイクロから新しいバージョンのAppliance SVMが提供されている。
 - アップグレード中にゲスト仮想マシンの保護が中断されると問題がある。

- 方法3: "[Appliance SVMに組み込まれているAgentをアップグレードし、OSパッチを適用する](#)" on page 1028。次の場合はこのオプションを選択します。
 - Applianceと互換性のある新しいバージョンのAgentがトレンドマイクロから提供されている。
 - Appliance SVMの完全アップグレードを行わずに最新のAgentソフトウェアに備わる最新の保護機能を利用したい。

NSX-Tを使用している場合は、オプション2または3を選択できます。

"[NSXライセンスをアップグレードして、利用できるDeep Securityの機能を増やす](#)" on page 1031も参照してください。

既存のAppliance SVMを自動的にアップグレードする

このアップグレード方法では、アップグレードプロセス中にゲスト仮想マシンの保護が失われます。アップグレードプロセスには、VMwareコンポーネントのリソースとネットワークの安定性に応じて5~15分かかります。ゲスト仮想マシンの保護を維持する場合は、代わりに"[既存のAppliance SVMを手動でアップグレードする](#)" on page 1015を参照してください。

注意: CPUまたはメモリの拡張、パスワードの変更など、現在のAppliance SVMに対して行ったリソース調整やカスタム設定は、アップグレード後の新しいAppliance SVMに引き継がれません。これらの設定は、アップグレードの完了時に手動で再度適用する必要があります。

開始前の準備

1. NSX Data Center for vSphere (NSX-V) を使用していることを確認します。NSX-Tでは、自動アップグレードはサポートされていません。
2. Deep Security Managerで指定したvCenterアカウントに次の権限があることを確認します。
 - `VirtualMachine.Interaction.Power Off`、
 - `VirtualMachine.Inventory.Remove`、
 - `ESX Agent Manager.Modify`

3. Deep Security Managerに登録したNSX Managerアカウントが次のいずれかのNSX Managerロールに属していることを確認します。
 - Security Engineer、
 - Security Administrator、
 - Enterprise Administrator

手順1: 新しいVirtual ApplianceパッケージをManagerにインポートする

1. Deep Security Managerコンピュータで、<https://help.deepsecurity.trendmicro.com/ja-jp/software.html>のソフトウェアページに移動します。
2. 最新のDeep Security Virtual Applianceパッケージをコンピュータにダウンロードします。
3. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に進みます。
4. [インポート]をクリックして、パッケージをDeep Security Managerにアップロードします。

Applianceのパッケージをインポートすると、Applianceの仮想マシンのOSと互換性のあるDeep Security Agentソフトウェアを、Deep Security Managerが自動的にダウンロードします。このAgentソフトウェアは、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に表示されます。Applianceをインストールすると、組み込みのAgentソフトウェアは、初期設定で[ローカルソフトウェア]内の最新の互換バージョンに自動的にアップグレードされます。[管理]→[システム設定]→[アップデート]タブ→[Virtual Applianceの配置]をクリックすると、自動アップグレードのバージョンを変更できます。

注意: Deep Security Virtual Applianceのパッケージのバージョンを [ローカルソフトウェア] に複数表示することも可能です。新しいDeep Security Virtual Applianceをインストールした場合は、常に最新バージョンが選択されます。

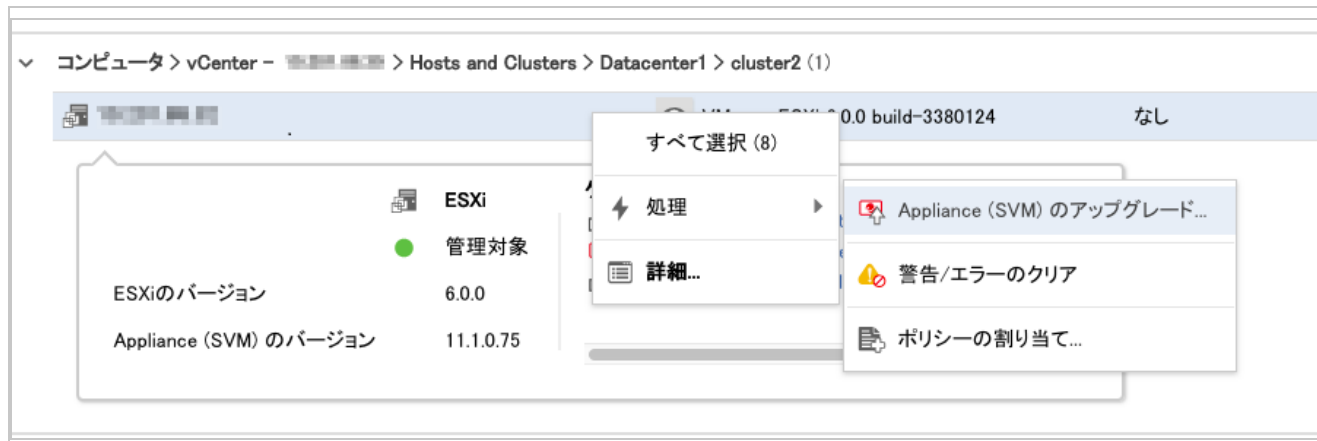
5. オプションで、Microsoft Windowsを実行するゲスト仮想マシンの場合は、Deep Security Notifierをダウンロードすることもできます。Notifierは、Deep Securityシステムイベントのメッセージをシステムトレイに表示するコンポーネントです。詳細については、"[Deep Security Notifierのインストール](#)" on page 437を参照してください。

手順2: ManagerでAppliance SVMをアップグレードする

1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. 既存のAppliance SVMがインストールされているESXiホストを探します。このESXiホストの [プラットフォーム] 列は [VMware ESXi <version_build>] に設定されています (下図を参照)(このホストは、[プラットフォーム] にDeep Security Virtual Applianceと表示されているコンピュータではありません)。
3. ESXiホストを右クリックして、[処理]→[Appliance (SVM) のアップグレード] を選択します。

ヒント: 一度に複数のESXiホストをアップグレードする場合は、<Shift> キーを押しながら複数のESXiホストをクリックして選択できます。

注意: [Appliance (SVM) のアップグレード] オプションは、ローカルソフトウェアの最新のVirtual Applianceパッケージが現在使用中のものよりも新しい場合にのみ使用できます。このオプションを使用するには、[最新のApplianceパッケージをインポート](#)してください。この操作を行ってもうまくいかない場合は、すでに最新バージョンのAppliance SVMを使用している可能性があります。これを確認するには、Applianceの仮想マシンのコンピュータの詳細ページで [Appliance (SVM) のバージョン] プロパティを調べます。



チェックボックス、警告、およびメモを含む [Appliance (SVM) のアップグレード] ページが表示されます。



注意: 使用しているvCenterおよびESXのリソースによっては、アップグレード中にAppliance (SVM) が3～10分間シャットダウンされます。

4. (オプション)アップグレードを開始する前にManagerがNSX Managerからのサービスステータスを確認するよう設定するには、[アップグレードの開始前にNSXアラームを確認し、アラームがある場合は処理をキャンセルしてください]を選択します。この確認をスキップして、アラームが発生した場合もアップグレードを続行するには、チェックボックスをオフにします。
5. ページ上の警告と注意をよく読みます。
6. [OK] をクリックします。

アップグレード前のサービスステータスの確認 (有効にした場合) を含め、アップグレードプロセスが開始されます。

7. (オプション)引き続きManager内で、[コンピュータ] ページに戻ってESXiホストを見つけ、その [タスク] 列でアップグレードのステータスを確認します。

注意: 前の手順で <Shift> キーを押しながら複数のESXiホストをクリックして選択した場合、ESXiホストは1つずつ順番に処理されます。[タスク] 列を見ると、どのサーバが現在処理されているかを確認できます。

[タスク] 列には次のいずれかが表示されます。

- Appliance (SVM) のアップグレード中 (保留中): アップグレード要求がManagerによって受け取られましたが、まだキューに登録されていません。
 - Appliance (SVM) のアップグレード中 (処理待ち): プロセスがManagerによってキューに登録され、まもなくアップグレードが開始されます。
 - Appliance (SVM) のアップグレード中 (実行中): Managerによってアップグレード処理が実行されています。
8. (オプション)引き続きManager内で、いずれかのESXiホストの [コンピュータの詳細] ページに移動し、[システムイベント] タブをクリックして、アップグレードが正常に実行されていることを確認します。

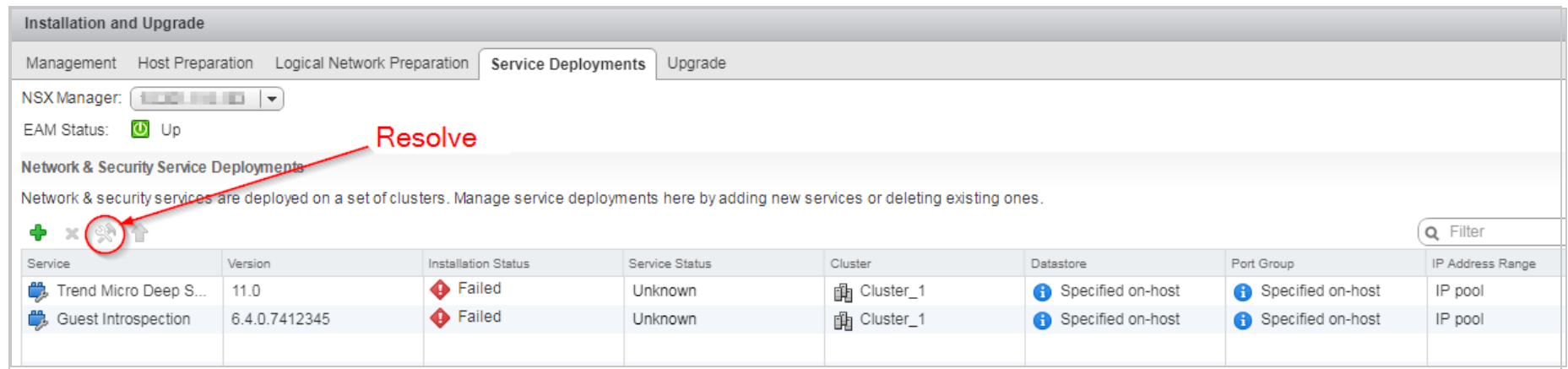
アップグレードが成功したときに表示されるシステムイベントの例を次に示します。その他のイベントについては、[この Appliance SVMのアップグレードイベントの完全なリスト](#)を参照してください。

2018-11-23 17:45:47	情報	2963	Appliance (SVM) のアップグレード完了
2018-11-23 17:42:11	情報	2961	Appliance (SVM) のアップグレード開始
2018-11-23 17:42:11	情報	2960	Appliance (SVM) のアップグレード要求

注意: 「Appliance (SVM) のアップグレード失敗」システムイベントが表示された場合は、"[「Appliance \(SVM\) のアップグレード失敗」システムイベントのトラブルシューティング](#)" on the next pageを参照してください。

「Appliance (SVM) のアップグレード失敗」 システムイベントのトラブルシューティング

「Appliance (SVM) のアップグレード失敗」 システムイベントが表示された場合は、その詳細な説明を読んで、理由と考えられる修正方法を確認します。ワーストケースのシナリオでは、NSX Managerコンソールに移動し、[Resolve] アイコンをクリックします (下の図を参照)。このボタンをクリックすると、手動でアラームを解決し、Applianceを再インストールできます。ゲスト仮想マシンは、古いDeep Security Virtual Applianceをインストールしたときの有効化の設定に従って有効化されます。有効化の設定の詳細については、「[Applianceのインストール \(NSX-V\)](#)」の有効化に関するセクションを参照してください。



The screenshot shows the 'Installation and Upgrade' section of the NSX Manager console. The 'Service Deployments' tab is active. Below the navigation tabs, there is a dropdown for 'NSX Manager' and an 'EAM Status' indicator showing 'Up'. The main section is titled 'Network & Security Service Deployments' and contains a table of service deployments. A red arrow points to a 'Resolve' icon (a circle with a lightning bolt) in the table's header row.

Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Trend Micro Deep S...	11.0	Failed	Unknown	Cluster_1	Specified on-host	Specified on-host	IP pool
Guest Introspection	6.4.0.7412345	Failed	Unknown	Cluster_1	Specified on-host	Specified on-host	IP pool

手順4: 最後の手順

Appliance SVMが正常にアップグレードされます。Managerの [コンピュータ] ページに移動し、Appliance SVMとすべてのゲスト仮想マシンが保護ステータス (緑色のドット) に戻っていることを再確認します。

既存のAppliance SVMを手動でアップグレードする

このアップグレードオプションはNSX-T環境でもNSX-V環境でも使用できます。

手動アップグレードの場合は、vMotionメカニズムを使用してアップグレード中のゲスト仮想マシンの保護を維持します。

Appliance SVMをアップグレードするには、次の手順に従います。

- "手順1: 新しいVirtual ApplianceパッケージをManagerにインポートする" below
- "手順2: 検出ファイルを確認または復元する" on the next page
- "手順3: ゲスト仮想マシンを別のESXiホストに移行する" on the next page
- "手順4: 古いAppliance SVMをアップグレードする" on page 1019
- "手順5: メンテナンスモードがオフになっていることを確認する" on page 1025
- "手順6: 新しいAppliance SVMが有効化されていることを確認する" on page 1025
- "手順7: 最後の手順" on page 1027

手順1: 新しいVirtual ApplianceパッケージをManagerにインポートする

1. Deep Security Managerコンピュータで、<https://help.deepsecurity.trendmicro.com/ja-jp/software.html>のソフトウェアページに移動します。
2. 最新のDeep Security Virtual Applianceパッケージをコンピュータにダウンロードします。
3. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に進みます。
4. [インポート]をクリックして、パッケージをDeep Security Managerにアップロードします。

Applianceのパッケージをインポートすると、Applianceの仮想マシンのOSと互換性のあるDeep Security Agentソフトウェアを、Deep Security Managerが自動的にダウンロードします。このAgentソフトウェアは、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に表示されます。Applianceをインストールすると、組み込みのAgentソフトウェアは、初期設定で [ローカルソフトウェア] 内の最新の互換バージョンに自動的にアップグレードされます。[管理]→[システム設定]→[アップデート]タブ→[Virtual Applianceの配置]をクリックすると、自動アップグレードのバージョンを変更できます。

注意: Deep Security Virtual Applianceのパッケージのバージョンを [ローカルソフトウェア] に複数表示することも可能です。新しいDeep Security Virtual Applianceをインストールした場合は、常に最新バージョンが選択されます。

5. オプションで、Microsoft Windowsを実行するゲスト仮想マシンの場合は、Deep Security Notifierをダウンロードすることもできます。Notifierは、Deep Securityシステムイベントのメッセージをシステムトレイに表示するコンポーネントです。詳細については、"[Deep Security Notifierのインストール](#)" on page 437を参照してください。

手順2: 検出ファイルを確認または復元する

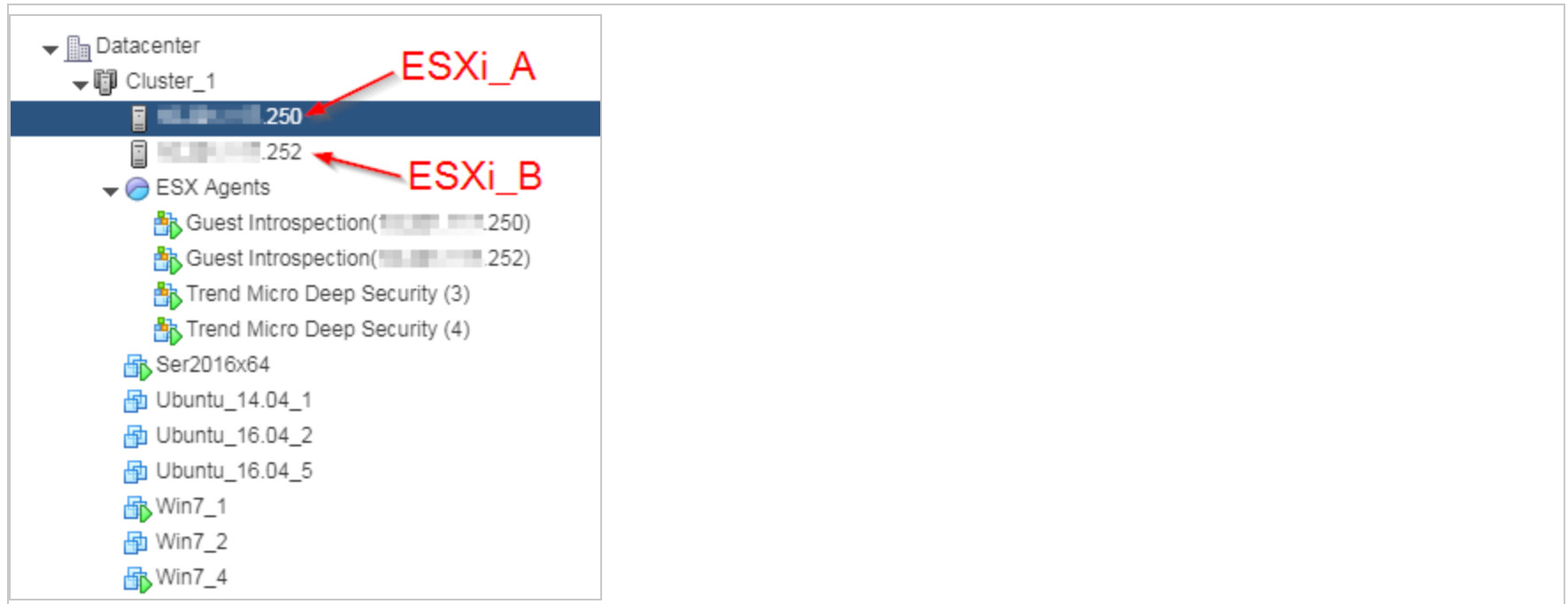
1. 仮想マシンを移動したり、Deep Security Virtual Applianceを削除したりすると検出ファイルが失われるため、必要に応じて、[検出ファイルを確認または復元](#)します。
2. Appliance SVMを置き換える間にゲスト仮想マシンをシャットダウンする必要はありません。

手順3: ゲスト仮想マシンを別のESXiホストに移行する

説明を簡潔にするために、この手順では次の用語を使用します。

- `ESXi_A`は、アップグレードするVirtual Applianceを含むESXiサーバです。
- `ESXi_B`は、Appliance SVMのアップグレードの実行中にゲスト仮想マシンの移行先となるESXiサーバです。このサーバ

は、ESXi_Aと同じクラスタにあるものとします。



1. クラスタのDRSを有効にして、DRSの自動化レベルが [Fully Automated] であることを確認します。詳細については、[こちらのVMwareの記事](#)を参照してください。
2. ESXi_Aを探して、[このESXiサーバをメンテナンスモードに切り替え](#)ます。

メンテナンスモードに移行すると、次のようになります。

- ESXi_Aのゲスト仮想マシンが自動的に ([vMotion](#)を使用して) クラスタ内のESXi_Bに移行されます。
- ESXi_Aを保護しているDeep Security Virtual Applianceが自動的にシャットダウンされます。
- ESXi_Aのメンテナンスモードが終了するまで、ゲスト仮想マシンの電源をオンにできなくなります。

手順4: 古いAppliance SVMをアップグレードする

1. VMware vSphere Web Clientの [Hosts and Clusters] に移動します。
2. 電源がオフになっているTrend Micro Deep Security Appliance SVMを見つけます。緑色の矢印が付いていないものです (次の画像を参照)。Appliance SVMは、対応するESXiサーバをメンテナンスモードにしたときに自動的にオフにされています。

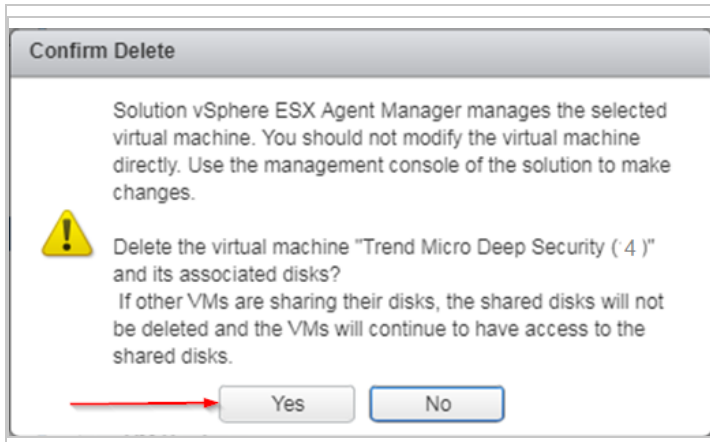
3. オフになっている状態のTrend Micro Deep Security Appliance SVMを右クリックし、[Delete from Disk] を選択します。

Trend Micro Deep Security On-Premise 12.0

The screenshot displays the Trend Micro Deep Security On-Premise 12.0 interface. On the left, a tree view shows the hierarchy: Datacenter > Cluster_1 > ESX Agents > Trend Micro Deep Security (4). The selected item, 'Trend Micro Deep Security (4)', is highlighted in blue. A context menu is open over this item, listing various actions. The 'Delete from Disk' option at the bottom of the menu is circled in red. Other visible options include Power, Guest OS, Snapshots, Open Console, Migrate..., Clone, Template, Fault Tolerance, VM Policies, Compatibility, Export System Logs..., Edit Resource Settings..., Edit Settings..., Move To..., Rename..., Edit Notes..., Tags & Custom Attributes, Add Permission..., Alarms, and Remove from Inventory. A table on the right side of the interface shows a single entry with the name 'datast'.

Name
datast

4. [Confirm Delete] メッセージが表示されたら、[Yes] をクリックします。



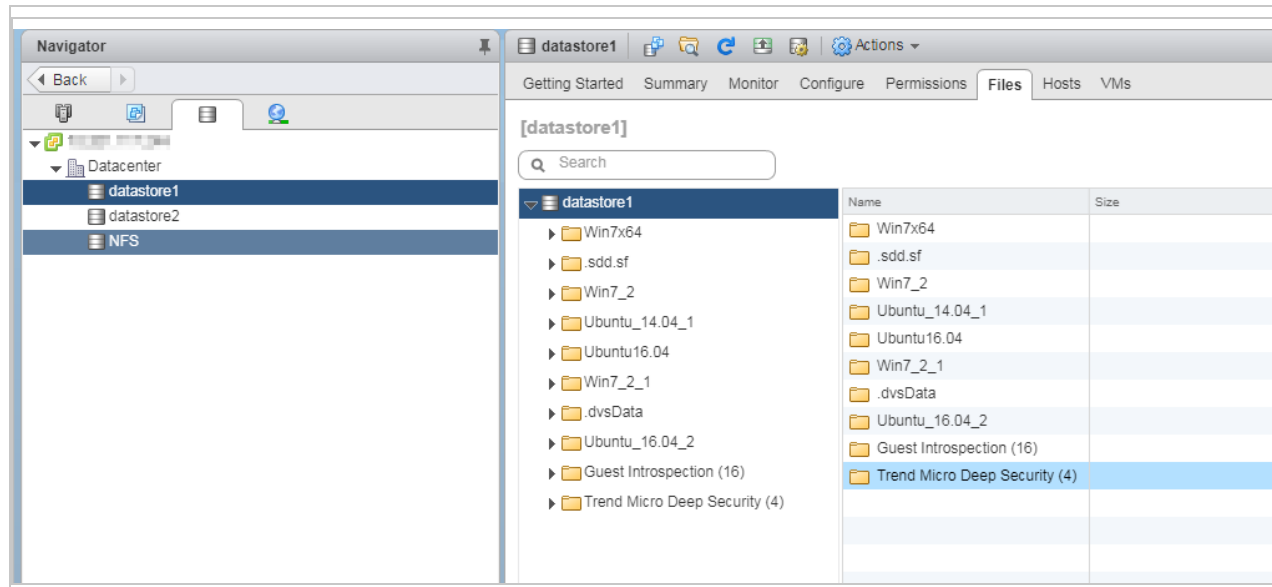
5. 削除に失敗すると、次のメッセージが表示されます。

This operation not allowed in the current state

この場合は、次の手順を実行してください。

- a. もう一度Trend Micro Deep Security Appliance SVMを右クリックします。今回は [Remove from Inventory] を選択します。これは [Delete from Disk] のすぐ上に表示されます。Appliance SVMは、vCenterからは削除されますが、データストアでは保持されます。
- b. ナビゲーション画面でデータストアのタブを選択し、古いVirtual Applianceがあるデータストアを選択します。
- c. メイン画面で [Files] タブをクリックします。

- d. 古いAppliance SVMフォルダを右クリックし、[Delete File] を選択します。



- e. NSX-Vを使用している場合は、次のセクションに進んでください: ["NSX-Vの手順" below](#)
- f. NSX-Tを使用している場合は、次のセクションに進んでください: ["NSX-Tの手順" on page 1025](#)

NSX-Vの手順

- g. VMware vSphere Web Clientを開いて、[Home]→[Networking and Security]→[Installation]→[Service Deployments] の順に選択します。

以下が表示されます。

Trend Micro Deep Security On-Premise 12.0

- 削除したTrend Micro Deep Security Appliance SVMの [Installation Status] 列に [Failed] と表示されます。
- メンテナンスモードの場合は、Guest Introspectionサービスも [Failed] として表示されます。

Installation and Upgrade

Management Host Preparation Logical Network Preparation **Service Deployments** Upgrade

NSX Manager: [dropdown]

EAM Status: ⬆ Up

Network & Security Service Deployments

Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

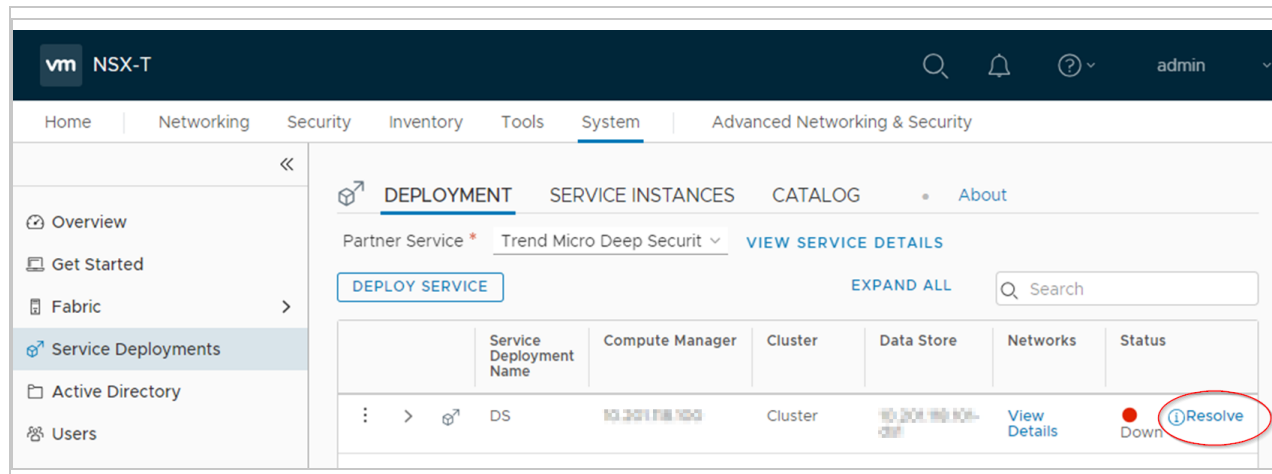
Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Trend Micro Deep S...	11.0	Failed	Unknown	Cluster_1	Specified on-host	Specified on-host	IP pool
Guest Introspection	6.4.0.7412345	Failed	Unknown	Cluster_1	Specified on-host	Specified on-host	IP pool

- h. Guest Introspectionサービスの [Installation Status] が [Failed] になっている場合、そのサービスの [Resolve] ボタンをクリックします。[Failed] ステータスが [Enabling]、[Succeeded] の順に変わります。Guest Introspectionサービスがオンになり、メンテナンスモードが終了します。
- i. [Failed] ステータスのTrend Micro Deep Securityサービスの [Resolve] ボタンをクリックします。[Failed] ステータスが [Enabling]、[Succeeded] の順に変わります。この間には、次の処理が行われます。
 - Deep Security Managerにロードした最新のソフトウェアとともにTrend Micro Deep Security Appliance SVMが再インストールされます。
 - Appliance SVMが有効化されます。
 - Appliance SVMの組み込みのAgentが初期設定で [ローカルソフトウェア] 内の最新の互換バージョンに自動的にアップグレードされます。

NSX-Vを使用している場合の手順はこれで完了です。"手順5: メンテナンスモードがオフになっていることを確認する" on [the next page](#)に進んでください。

NSX-Tの手順

- j. NSX-T Managerを開き、[System]→[Service Deployments]→[DEPLOYMENT] の順に移動します。
- k. 以下が表示されます。



- l. [Resolve]→[RESOLVE ALL]→[OK] の順にクリックします。[Down] ステータスが、[In Progress]、[Up] の順に変わります。

NSX-Tを使用している場合の手順はこれで完了です。"手順5: メンテナンスモードがオフになっていることを確認する" [below](#)に進んでください。

手順5: メンテナンスモードがオフになっていることを確認する

- 以前にメンテナンスモードをオンにした場合は、[オフになっていることを確認](#)します。まだオンの場合は、すぐにオフにします。

手順6: 新しいAppliance SVMが有効化されていることを確認する

1. Deep Security Managerで、画面上部の [コンピュータ] をクリックします。

Trend Micro Deep Security On-Premise 12.0

2. リスト内でTrend Micro Deep Securityを見つけてダブルクリックします。これがApplianceです。
3. 以下を確認します。
 - a. ステータスが [管理対象 (オンライン)] に設定されていることを確認します。これは、Agentが正常に有効化されたことを示します。
 - b. [Virtual Applianceのバージョン] が組み込みのDeep Security Agentのバージョンに設定されていることを確認します。このバージョンは、[管理]→[アップデート]→[ソフトウェア]→[ローカル] で確認できる最新のAgentソフトウェアのバージョン、または [管理]→[システム設定]→[アップデート]→[Virtual Applianceの配置] で設定した特定のバージョンと一致する必要があります。
 - c. [Appliance (SVM) のバージョン] が [管理]→[アップデート]→[ソフトウェア]→[ローカル] で確認できる最新のDeep

Security Virtual Applianceパッケージのバージョンに設定されていることを確認します。

これで、Appliance SVMがアップグレードされました。

手順7: 最後の手順

1. 置き換える必要がある各Appliance SVMに対して、"[手順2: 検出ファイルを確認または復元する](#)" on page 1017から"[手順6: 新しいAppliance SVMが有効化されていることを確認する](#)" on page 1025まで、このセクションのすべての手順を繰り返します。

ゲスト仮想マシンは、古いDeep Security Virtual Applianceをインストールしたときの有効化の設定に従って有効化されます。有効化の設定の詳細については、[「Applianceのインストール \(NSX-V\)」](#) または ["Applianceのインストール \(NSX-T\)" on page 320](#)の有効化に関するセクションを参照してください。

Appliance SVMに組み込まれているAgentをアップグレードし、OSパッチを適用する

Appliance SVMを再インストールせずにAppliance SVMに組み込まれているDeep Security Agentのみをアップグレードして、同時にOSパッチを適用することもできます。

注意: 組み込みエージェントだけをアップグレードすると、アプライアンスSVMの元のサポート終了日が有効なままになります。詳細については、["Applianceのサポート期間とアップグレードに関する推奨事項" on page 1006](#)

Appliance SVMに組み込まれているAgentをアップグレードするには、次の手順に従います。

1. ["現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する" on page 1008](#)。この処理の残りの手順を完了するには、次の情報が必要です。
2. Applianceパッチがある場合はインポートします (失敗すると、パッチがインポートされていないことを示すシステムイベント740が生成されます)。
 - a. Deep Security Managerにログインします。
 - b. 左側で、[アップデート]→[ソフトウェア]→[ダウンロードセンター]の順に展開します。
 - c. メイン画面で、上部右の検索バーに「Agent-DSVA」と入力し、<Enter>キーを押します。
名前がAgent-DSVA-CentOS<version>-<patch-version>-<date>.x86_64.zipの1つ以上のパッチが表示されます。
 - d. Appliance SVMと互換性のあるパッチを選択します。解説については、この後に表示される[互換性の表](#)を参照してください。互換性のあるパッチが表示されない場合は、現在実行しているAppliance SVMのバージョンに対応するパッチが存在しないか、存在していてもインストールする必要がないことを意味しています。
 - e. [今すぐインポート]列のボタンをクリックし、パッチをDeep Security Managerにインポートします。
 - f. 左側で、[ローカルソフトウェア]をクリックし、パッチが正しくインポートされていることを確認します。
 - g. パッチの追加を繰り返します。

3. 互換性のあるAgentをインポートします。
 - a. Deep Security Managerの左側で、[アップデート]→[ソフトウェア]→[ダウンロードセンター]の順に展開します。
 - b. Appliance SVMと互換性のあるAgentソフトウェアを選択します。解説については、この後に表示される[互換性の表](#)を参照してください。
 - c. [今すぐインポート]列のボタンをクリックし、AgentをDeep Security Managerにインポートします。
 - d. 左側で、[ローカルソフトウェア]をクリックし、Agentが正しくインポートされていることを確認します。

Appliance SVMのバージョンと互換性のあるパッチとDeep Security Agentがインポートされました。Appliance SVMのAgentをアップグレードし、パッチを適用する準備ができました。

4. Appliance SVMのAgentをアップグレードし、パッチを適用します。
 - a. [コンピュータ]をクリックし、Applianceコンピュータをダブルクリックします。
 - b. [処理]→[Applianceのアップグレード]の順にクリックします。
 - c. ApplianceにインストールするAgentバージョンを選択します。これは先ほどインポートしたAgentです。
 - d. [OK]をクリックします。
5. [イベントとレポート]をクリックして710を検索し、アップデートファイルのインストールに関するレポートを確認します。

Appliance SVMのAgentがアップグレードされ、1つ以上のOSパッチ (存在する場合) がインストールされました。

Appliance SVMのOSパッチをインポートする前にDeep Security Agentをアップグレードした場合は、システムイベント740が表示されます。この問題を修正するには、次の手順を実行します。

1. アップデートするAppliance SVMのバージョンに対応するApplianceパッチをインポートします。手順については、上記の手順を参照してください。ApplianceパッチはDeep Security Managerの [ローカルソフトウェア] 画面に表示されます。
2. [コンピュータ]画面に移動します。
3. Applianceをアップグレードする仮想マシンを右クリックし、[ポリシーの送信]をクリックします。Applianceがパッチをダウンロードしてインストールします。

ヒント: Applianceがパッチをダウンロードできない場合、Relayがまだパッチファイルを受信していない可能性があります。Relayがファイルを受信するまで待ってから、[ポリシーの送信] をクリックしてください。Relayの詳細については、"[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照してください。

互換性の表: Appliance、Agent、パッチ

Appliance SVMのバージョン	イメージのOS	互換性のあるAgentソフトウェア	互換性のあるApplianceパッチ (存在する場合)
Appliance-ESX-10.0以降	CentOS 7	Agent-RedHat_EL7-<version>.x86_64.zip <version> の部分はAgentソフトウェアのバージョンです。最新バージョンを選択します。このバージョンのAgentが組み込みのAgentとして使用されます。	Agent-DSVA_CENTOS7.0-<patch-version>-<date-stamp>.x86_64.zip

エラー: データベースサーバへの安全な接続を確立できませんでした

Deep Security Managerのインストールまたはアップグレード時に、Microsoft SQL ServerをDeep Securityのデータベースとして使用している場合は次のエラーメッセージが表示されることがあります。

データベースサーバへの安全な接続を確立できませんでした。データベースサーバをアップグレードするか設定して、TLS 1.2の暗号化がサポートされるようにしてください。

このエラーメッセージは、Deep Security Managerのjava.securityファイルでjdk.tls.disabledAlgorithms=設定にTLSv1とTLSv1.1が含まれている場合に表示されます。この場合、初期のTLSが無効になり、TLS 1.2のみが許可されます (java.securityファイルは、TLS 1.2のみが許可されるDeep Security Manager 11.1以降の新規インストールを実行する場合、または[TLS 1.2を強制](#)した後でアップグレードを実行する場合にこのように設定されます)。アップグレード中またはインストー

Trend Micro Deep Security On-Premise 12.0

ル中に、Managerのデータベースドライバは、TLS 1.2を使用してSQL Serverとの通信を試みますが、SQL ServerのバージョンがTLS 1.2をサポートしていない場合は、このエラーが表示されます。

この問題を解決するには、SQL Serverデータベースを、TLS 1.2をサポートするバージョンにアップグレードしてから、Deep Security Managerのインストールまたはアップグレードを再試行する必要があります。TLS 1.2をサポートするSQL Serverバージョンのリストについては、[こちらのMicrosoftの記事](#)を参照してください。

NSXライセンスをアップグレードして、利用できるDeep Securityの機能を増やす

注意: このトピックは、NSX Data Center for vSphere (NSX-V) のみに該当します。NSX-Tライセンスをアップグレードしても、利用できるDeep Securityの機能は変わらないため、このトピックはNSX-Tには該当しません。

Deep Security Virtual ApplianceをNSX for vShield Endpoint (無料)、NSX Standard、NSX Data Center Standard、またはNSX Data Center Professionalにインストールしている場合は、Deep Securityの次の機能を利用できません。

- Deep Securityファイアウォール
- Deep Security侵入防御
- Deep Security Webレピュテーション

詳細については、[こちらの表](#)を参照してください。

これらの機能が必要な場合は、NSX Advanced、NSX Enterprise、NSX Data Center Advanced、NSX Data Center Enterprise Plus、またはNSX Data Center for Remote Office Branch Officeにアップグレードして、Deep Security Virtual Applianceを再インストールする必要があります。次の手順に従います。

- "手順1: NSXライセンスをアップグレードする" on the next page
- "手順2: Deep SecurityをNSXからすべて削除する" on page 1038
- "手順3: Deep Security Virtual Applianceを再インストールする" on page 1038

注意: NSXライセンスをアップグレードする代わりに、Deep Security Agentをゲスト仮想マシンにインストールして上記の機能を利用することもできます。詳細については、[こちらの表](#)のほか、"Agentレスによる保護またはコンバインモードの保護の選択" on page 315を参照してください。

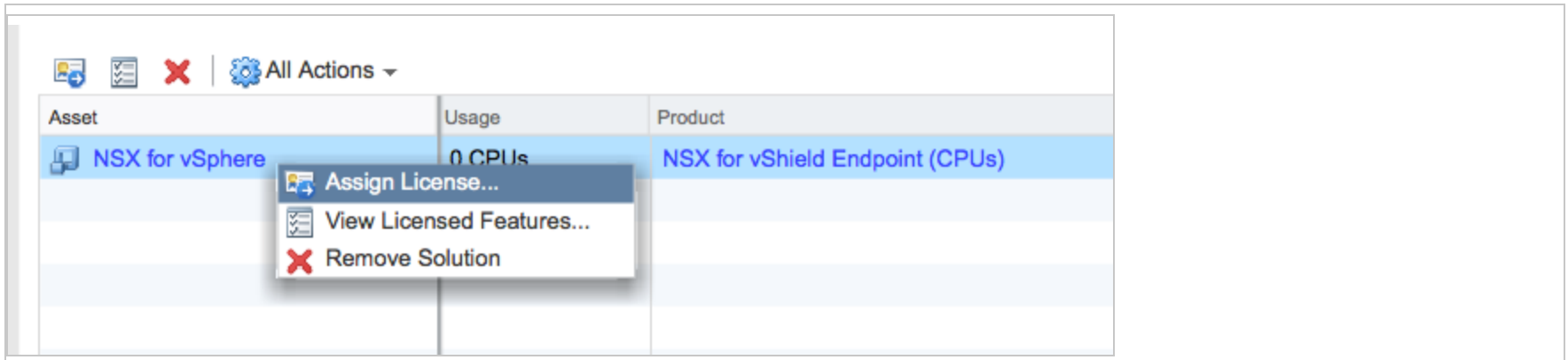
手順1: NSXライセンスをアップグレードする

1. vSphere Web Clientで、[Home]→[Administration]→[Licenses] の順に選択します。
2. メイン画面で、[Assets] をクリックして [Solutions] ボタンをクリックします。

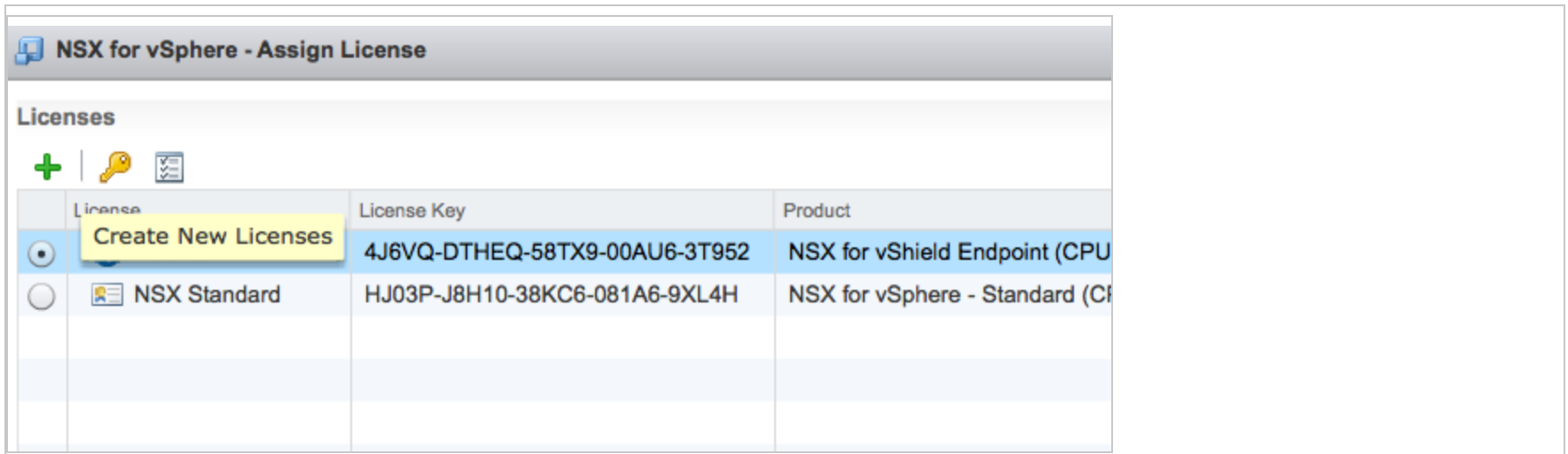
The screenshot shows the VMware vSphere Web Client interface. The left sidebar contains a Navigator menu with 'Licenses' selected under the 'Administration' section. The main content area is titled 'Licenses' and shows the 'Assets' tab selected. The 'License provider' is set to 'All 6.0 vCenter Server instances'. Below the tabs, there is a table with the following data:

Asset	Usage	Product	License
NSX for vSphere	0 CPUs	NSX for vShield Endpoint (CPUs)	License 1

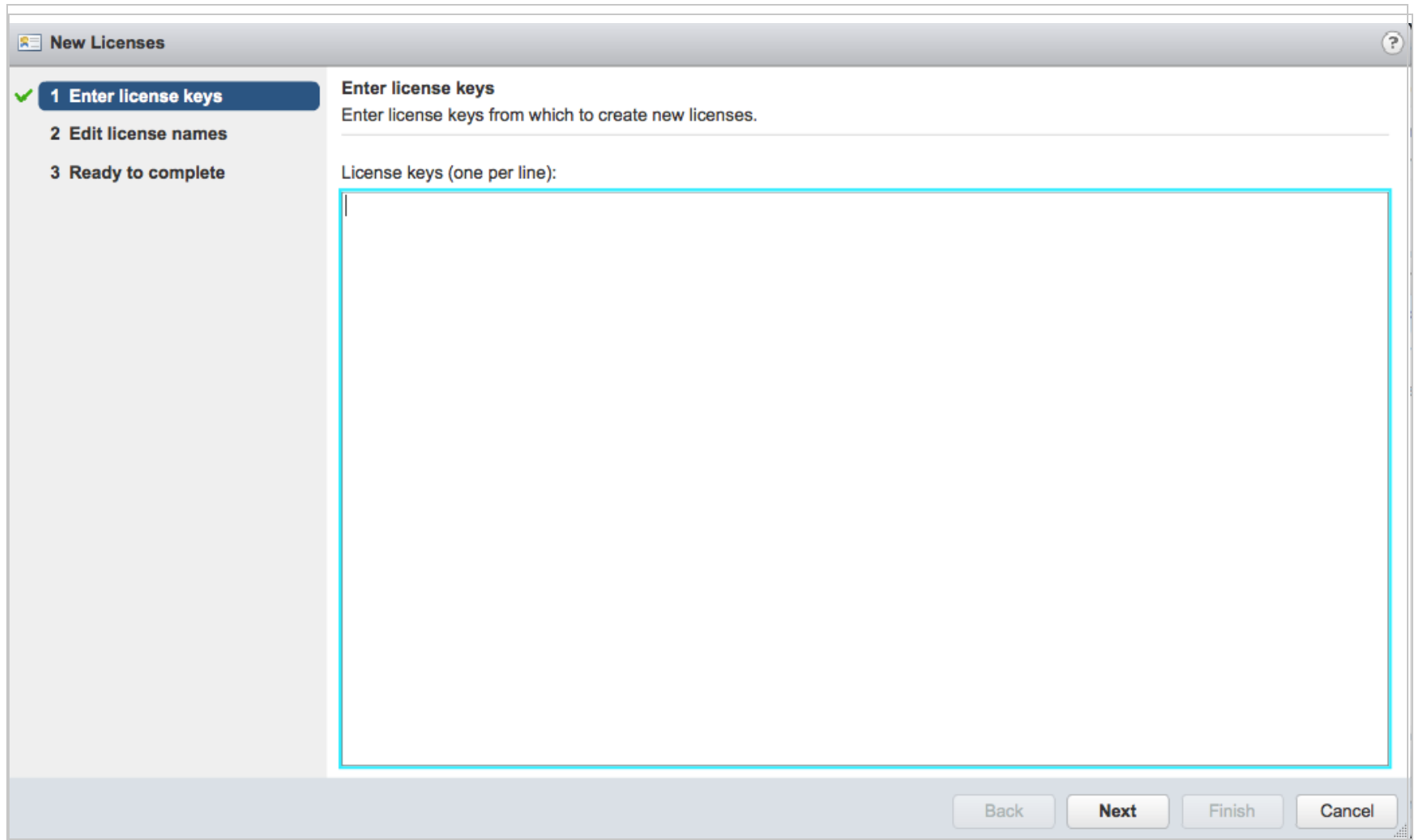
3. [NSX for vSphere] を右クリックし、[Assign License] を選択します。



4. 左側の緑の「+」をクリックし、新しいライセンスを作成します。



ウィザードが表示され、ライセンスキー追加の手順が示されます。



5. ウィザードで、NSX Advanced、NSX Enterprise、NSX Data Center Professional、NSX Data Center Advanced、NSX Data Center Enterprise Plus、またはNSX Data Center for Remote Branch Officeのライセンスキーとライセンス名を入力します。ウィザードの最後で [Finished] をクリックします。




Trend Micro Deep Security On-Premise 12.0




新しいライセンスが [Assign License] 画面のリストに表示されます。

6. 新しいライセンスを選択し、[OK] をクリックします。

NSX for vSphere - Assign License


Licenses

 |  |  Filter

	License	License Key	Product	Usage	Count
<input checked="" type="radio"/>	 (New) NSX Advanced	H1436-J7L00-Q8LCG-03A24-20C4H	NSX for vSphere - Advanced (CPUs)	0 CPUs	3
<input type="radio"/>	 License 1	4J6VQ-DTHEQ-58TX9-00AU6-3T952	NSX for vShield Endpoint (CPUs)	0 CPUs	U
<input type="radio"/>	 NSX Standard	HJ03P-J8H10-38KC6-081A6-9XL4H	NSX for vSphere - Standard (CPUs)	0 CPUs	3

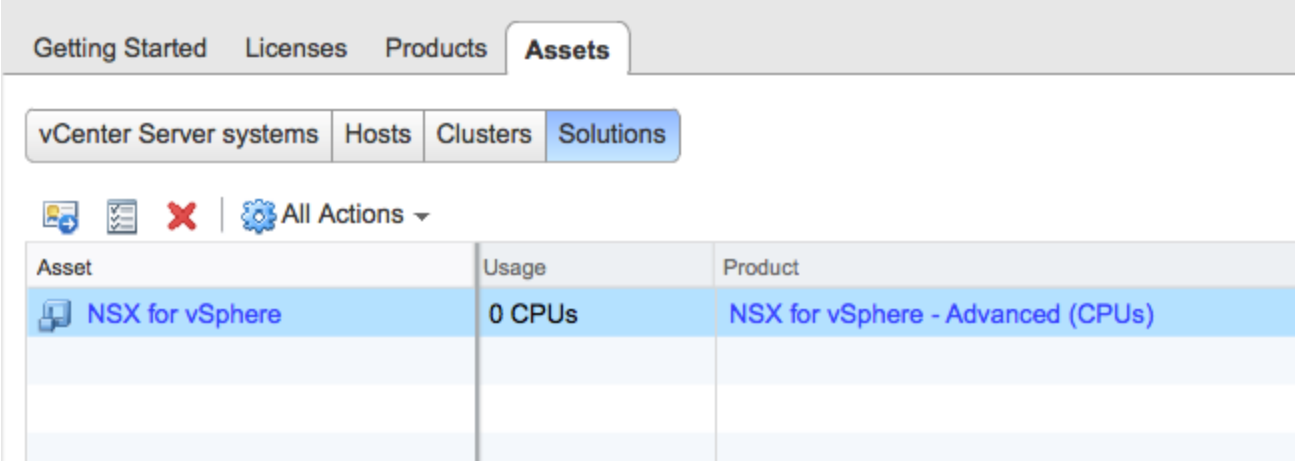
3 items


Assignment Validation for NSX Advanced

 The license assignment is valid.

OK **Cancel**

新しいNSXライセンスが使用中の状態になります。



Asset	Usage	Product
 NSX for vSphere	0 CPUs	NSX for vSphere - Advanced (CPUs)

手順2: Deep SecurityをNSXからすべて削除する

新しいライセンスを有効にするには、Deep SecurityをNSXからすべて削除する必要があります。Deep SecurityをNSXから削除するには、"[NSX環境からのDeep Securityのアンインストール](#)" on page 1507を参照してください。

手順3: Deep Security Virtual Applianceを再インストールする

Deep SecurityをNSXからすべて削除したら、Deep Security Virtual Applianceを再インストールする必要があります。再インストールするには、「[Applianceのインストール \(NSX-V\)](#)」のすべての手順を実行します。

これで、ファイアウォール、侵入防御、Webレピュテーション機能を使用し、以前から利用可能な不正プログラム対策および変更監視機能も引き続き使用できます。

セキュリティアップデートの取得と配布

Deep Security環境は、潜在的な脅威を特定するために使用されるセキュリティアップデートによって常に最新状態を維持する必要があります。Deep Security Agent 12.0以降のセキュリティアップデートでは、デジタル署名により、提供元がトレンドマイクロであることと、Agentに送信される間に改ざんされていないことが証明されます。

セキュリティアップデートには次の2種類があります。

- パターンファイルアップデートは不正プログラム対策モジュールで使用されます。
- ルールアップデートは次のモジュールによって使用されます。
 - ファイアウォール
 - 侵入防御
 - 変更監視
 - セキュリティログ監視

注意: セキュリティアップデートを設定する前に、Agent、Appliance、およびRelayをインストールして、有効化する必要があります。"[Deep Security Agentの手動インストール](#)" on page 376を参照してください。

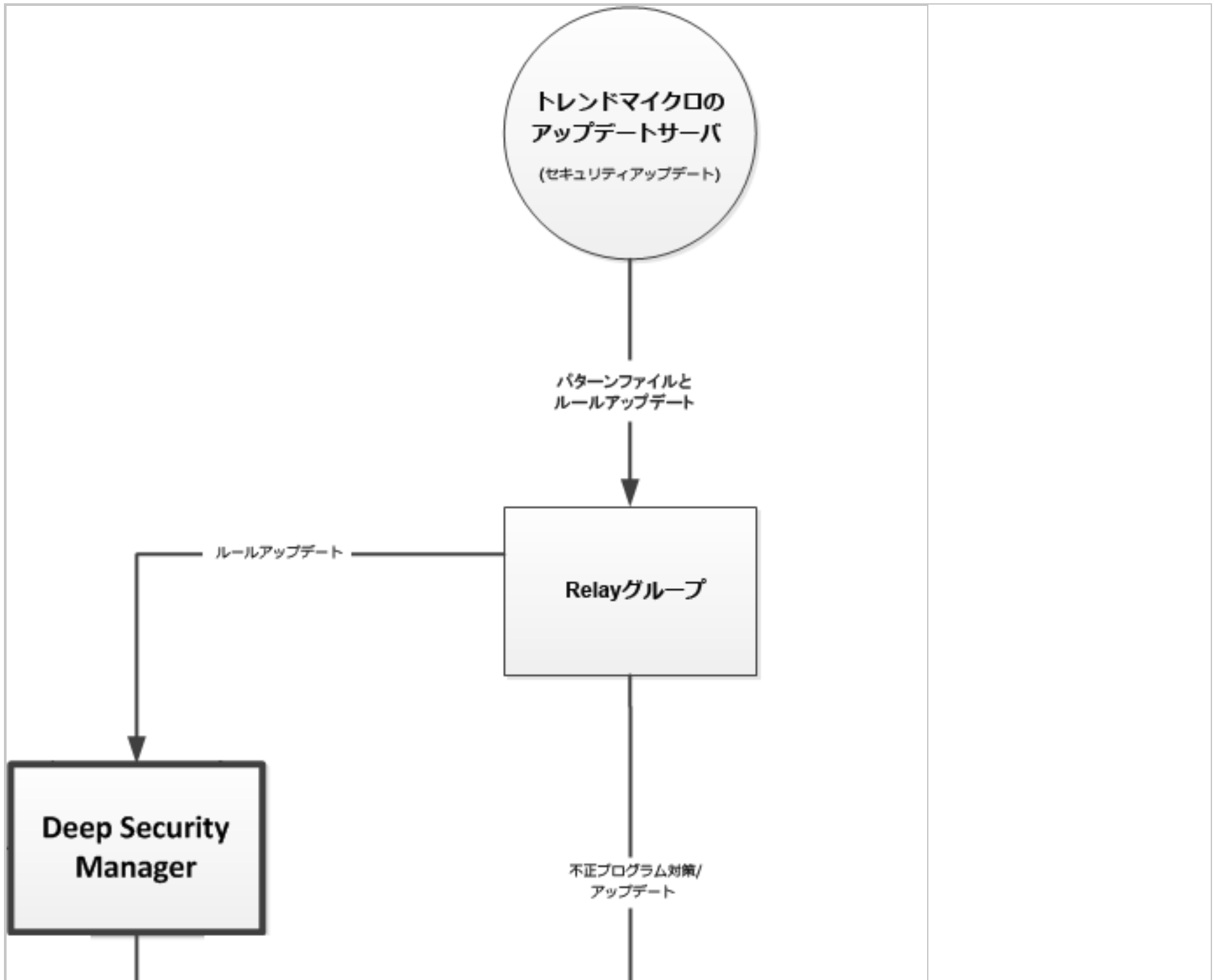
Trend Microは新しいルールアップデートを毎週火曜日にリリースし、新しい脅威が検出されたときは追加のアップデートをリリースします。最新のアップデートに関する詳細については、トレンドマイクロの[セキュリティ情報](#)を参照してください。

セキュリティアップデートを設定するには、次の手順を実行する必要があります。

1. "[セキュリティアップデート元および設定を指定する](#)" on page 1042
2. "[不正プログラム対策エンジンのアップデートを設定する](#)" on page 1043
3. Relay有効化済みAgentをRelayグループにグループ化し、AgentおよびApplianceにRelayグループを割り当て、セキュリティアップデートおよびソフトウェアアップデートのRelay設定を指定する ("[Relayによるセキュリティとソフトウェアのアップデートの配布](#)" on page 438を参照)

4. ["セキュリティアップデートを実行する" on page 1044](#)
5. ["Special case: エアギャップ環境におけるRelay有効化済みAgentでのアップデートを設定する" on page 1044](#)

いつでも、["セキュリティアップデートのステータスを確認する" on page 1045](#)ことができます。



注意: ルールアップデートがトレンドマイクロからダウンロードされてから30分以上経過してもコンピュータが更新されていない場合は、アラートが発令されます。

注意: パターンファイルアップデートがトレンドマイクロのアップデートサーバなどアップデート元からダウンロードされてから1時間以上経過してもAgent/Applianceが更新されていない場合は、アラートが発令されます。

セキュリティアップデート元および設定を指定する

1. [管理]→[システム設定]→[アップデート] の順に選択します。
2. [セキュリティアップデート元] を設定します。初期設定では、アップデート元はインターネット経由でアクセスするトレンドマイクロのアップデートサーバに設定されています。トレンドマイクロサポートセンターから別途指示があった場合を除き、初期設定をそのまま使用してください。その他のアップデート元がある場合は、そのURLを [その他のアップデート元] ボックスに「http://」または「https://」から入力します。
3. [セカンダリのアップデート元] でパターンファイルアップデートを設定します。通常、AgentはRelay有効化済みAgentに接続してセキュリティアップデートを取得します。しかし、Deep Security ManagerまたはRelayとの通信が常時確保されていないローミングするコンピュータにAgentがインストールされている場合は、[Relayに接続できない場合、セキュリティアップデート元からの直接ダウンロードをAgent/Applianceに許可] を選択すると、Relayグループを使用できない場合に、上記の手順で指定したアップデート元を使用するようにAgentを設定できます。
4. 通常は、Deep Security ManagerがAgentまたはApplianceにパターンファイルアップデートのダウンロードを指示します。[Deep Security Managerにアクセスできない場合、セキュリティアップデートの自動ダウンロードをAgent/Applianceに許可] を選択すると、AgentがDeep Security Managerと通信できない場合にも、設定済みのアップデート元からアップデートをダウンロードします。

ヒント: コンピュータがManagerにアクセスできず、近くに利用できるサポートサービスがない場合に、問題を含んでいる可能性のあるセキュリティアップデートを導入するというリスクを冒したくないときは、コンピュータでこのオプションの選択を解除することができます。

5. トレンドマイクロでは、定期的にDeep Securityルールの上アップデートを配信しています。[新しいルールアップデートを自動的にポリシーに適用]の設定では、ルールアップデートをDeep Securityのポリシーに自動的に適用するかどうかを決定します。このオプションを選択しない場合は、[管理]→[アップデート]→[セキュリティ]画面で [ルールをポリシーに適用] ボタンをクリックし、ダウンロードしたルールアップデートをポリシーに手動で適用する必要があります。

ヒント: この設定をオフにしている場合は、新しいセキュリティアップデートはダウンロードされるのみで、Managerには適用されません。適用するには、[管理]→[アップデート]→[セキュリティアップデート]で、[すべてのルールアップデートを表示]を開いて手動で適用を実行します。

注意: 初期設定では、ポリシーに対する変更は自動的に適用されます。この動作を変更するには、**コンピュータエディタ**または**ポリシーエディタ**¹で [設定]→[一般]画面を開き、[ポリシーの変更をすぐに送信]エリアの [ポリシーの変更をコンピュータに自動的に送信]設定を変更します。

6. セキュリティアップデートの実行命令が送信された後、その命令が実行されない場合にアラートが発令されるまでの期間を設定できます。[管理]→[システム設定]→[アラート]をクリックし、[次の期間を超えてアップデートが行われなかった場合にアラートを発令]の値を変更します。

不正プログラム対策エンジンのアップデートを設定する

セキュリティ保護を強化するために、不正プログラム対策エンジンのアップデートを自動化することもできます。デフォルトでは、この設定は無効になっていて、[コンピュータの詳細]→[アップデート]→[高度な脅威検索エンジン]の [最新版]セクションで「なし」と表示されます。

不正プログラム対策エンジンのアップデートを有効にするには

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

1. [コンピュータ] または [ポリシー] に移動し、アップデートするコンピュータまたはポリシーをダブルクリックします。
2. [設定]→[検索エンジンアップデート] の順に選択します。不正プログラム対策エンジンを自動的にアップデートする の横にあるドロップダウンメニューから はい を選択します。

注意: Relay自体の保護と、同じRelayグループの検索エンジンアップデート元を最新の状態に保つために、Relayは常に最新の不正プログラム対策エンジンアップデートを受信します。そのため、Relay上でエンジンのアップデートを直接有効または無効にすることはできません。

セキュリティアップデートを実行する

セキュリティアップデートをチェックするには、定期的にチェックを実行する「セキュリティアップデートの確認」予約タスクを設定することをお勧めします。詳細については、"[Deep Security予約タスクの設定](#)" on page 479を参照してください。

手動でセキュリティアップデートを開始することもできます。

- システム全体をアップデートする場合は、[管理]→[アップデート]→[セキュリティ] の順に選択して、[アップデートを確認してダウンロード] ボタンをクリックします。
- 特定のAgentおよびApplianceでセキュリティアップデートを実行するには、[コンピュータ] に移動して、AgentまたはApplianceを選択し、右クリックして[処理]→[セキュリティアップデートのダウンロード] を選択します。

Special case: エアギャップ環境におけるRelay有効化済みAgentでのアップデートを設定する

一般的な環境では、少なくとも1つのRelay有効化済みAgentを設定し、トレンドマイクロのアップデートサーバからアップデートをダウンロードするように設定できます。残りのAgentやApplianceは、このRelay有効化済みAgentに接続してアップデートをダウンロードします。ただし、Relay有効化済みAgentがインターネット経由でアップデートサーバに接続できない場合は、非武装地帯 (DMZ) でセキュリティアップデートを取得してからエアギャップのRelayにコピーできるようにRelayを設定する必要があります。詳細については、"[インターネットにアクセスできない エージェントを設定する](#)" on page 413を参照してください。

セキュリティアップデートのステータスを確認する

[セキュリティアップデートの概要] 画面 ([管理]→[アップデート]→[セキュリティ]) には、セキュリティアップデートの状態が表示されます。

- **トレンドマイクロのアップデートサーバ:** Relayがトレンドマイクロのアップデートサーバに接続して、最新のセキュリティアップデートの有無を確認できるかどうかが表示されます。
- **Deep Security:** 最後に成功した確認とダウンロードがいつ行われたかと、次回に予定されている確認がいつ行われるかが表示されます。

ヒント: [すべてのRelayは同じコンポーネントを保持しています] では、すべてのRelayが前回正常にダウンロードされたパターンファイルアップデートを配布していることが示されます。最新でない場合、通常はトレンドマイクロのアップデートサーバと通信できないことが原因です。これは、Relayが意図的に「エアギャップ環境」にあり、手動でアップデートする必要があるか、またはネットワーク接続に問題があることを示しています。同期されていないRelayがある場合は、そのRelayへのリンクが表示されます。

- **コンピュータ:** Relayに格納されているパターンファイルアップデートと比較して、すべてのコンピュータが最新であるかどうかを示します。[パターンファイルをコンピュータに送信] をクリックすると、すべてのコンピュータが割り当てられたRelayから最新のパターンファイルアップデートを取得します。

パターンファイルアップデートの詳細を確認する

[管理]→[アップデート]→[セキュリティ]→[パターンファイル] 画面には、パターンファイルアップデートを構成するコンポーネントのリストが表示されます。このページは、Deep Securityに有効なRelayがある場合のみ表示されます。

- **コンポーネント:** アップデートコンポーネントの種類。
- **対象:** このコンポーネントの対象となるDeep Security製品。
- **プラットフォーム:** アップデート対象のOS。


- 現在のバージョン: 現在トレンドマイクロからDeep Securityにダウンロード済みであり、RelayおよびDeep Security Managerによって配布されるアップデート内のコンポーネントのバージョン。
- 前回のアップデート: 現在ダウンロードされているセキュリティアップデートをトレンドマイクロから取得した日付。

ヒント: 特定のコンピュータで有効なセキュリティアップデートコンポーネントのバージョン番号は、コンピュータエディタの [アップデート] で確認できます。

ルールアップデートの詳細を確認する

[管理]→[アップデート]→[セキュリティ]→[ルール] 画面では、Deep Security Managerのデータベースにダウンロードされた、侵入防御、変更監視、およびセキュリティログ監視の最新ルールのリストを表示します。

この画面からは次の処理を実行できます。

- ルールアップデートの詳細を表示する: ルールアップデートを選択して [表示] をクリックすると、アップデートに含まれる特定のルールのリストなどの詳細が表示されます。
- ルールアップデートをロールバックする: お使いの環境で最新のルールアップデートに問題が発生した場合、以前のルールアップデートにロールバックできます。以前のアップデートにロールバックすると、ロールバックの影響を受けるすべてのポリシーが、そのポリシーを使用しているすべてのコンピュータ上でアップデートされます。ロールバックするルールアップデートを選択し、[ロールバック] をクリックします。Deep Security Managerによって生じる変更の概要が生成されるため、ロールバックを確定する前に変更内容を確認できます。
- 現在のルールセットを再適用する:  ルールアップデートが適用されていることを示します。Deep Securityによって保護されているコンピュータにルールアップデートを再適用するには、ルールアップデートを右クリックして [再適用] をクリックします。
- ルールアップデートをインポートする: ルールアップデートは、「セキュリティアップデートの確認」予約タスクの実行時、または [管理]→[アップデート]→[セキュリティ] 画面で [アップデートを確認してダウンロード] をクリックしたときに、Deep Securityに自動的にインポートされます。ルールアップデートを手動でインポートする必要があるのは、インス

ツール時にトレンドマイクロのアップデートサーバに接続できなかったか、サポートプロバイダから指示された場合のみです。

- ルールアップデートをエクスポートする: サポート担当者から別途指示があった場合を除き、通常の状態下では、ルールアップデートをエクスポートする必要はありません。
- ルールアップデートを削除する: [削除] をクリックすると、選択したルールアップデートがDeep Security Managerデータベースから削除されます。

ヒント: Deep Security Managerのデータベースに保持するルールアップデートの個数は、[管理]→[システム設定]→[ストレージ] タブで設定できます。

ヒント: コンピュータでRelay機能が有効になっている場合、コンピュータエディタの [セキュリティのアップデート] 画面には、AgentおよびApplianceにRelayが現在配布中のコンポーネントが表示されます。コンピュータで不正プログラム対策モジュールが有効になっている場合は、コンピュータでローカルで有効なパターンファイルも表示されます。また、この画面からセキュリティアップデートをダウンロードしたりロールバックしたりすることもできます。

ソフトウェアアップデートを配布するWebサーバの使用

Deep Securityのソフトウェアアップデートは、通常はRelayによってホストされ、配信されます。ただし、すでにWebサーバがある場合は、RelayではなくWebサーバ経由でソフトウェアアップデートを提供できます。そのためには、RelayのソフトウェアリポジトリのミラーをWebサーバに作成する必要があります。

注意: ソフトウェアアップデートはDeep Security AgentがWebサーバからダウンロードできますが、セキュリティパッケージのアップデート (不正プログラム対策やIPSの署名など) を配信するためにはRelayが少なくとも1つ必要です ("[セキュリティアップデートの取得と配布](#)" on page 1039を参照)。

注意: ソフトウェアの配布に独自のWebサーバを使用している場合でも、[管理]→[アップデート]→[ソフトウェア] に移動し、Deep Security Manageのデータベースにソフトウェアをインポートする必要があります。インポートが終了したら、Deep

Security Managerにインポートしたソフトウェアと同じソフトウェアが、ソフトウェアWebサーバに格納されていることを確認する必要があります。同じものが格納されていないと、利用可能なアップデートに関する通知を表示するアラートなどのインジケータが正常に機能しません。

Webサーバのシステム要件

ディスク容量: 20 GB

ポート: [Webサーバのポート](#)と[Relayのポート](#)

フォルダ構造をコピーする

Relay有効化済みAgentのソフトウェアリポジトリフォルダのフォルダ構造のミラーを作成します。方法はプラットフォームおよびネットワークによって異なります。たとえば、LinuxコンピュータおよびSSHを許可するネットワークを使用している場合は、SSH経由のrsyncを使用できます。

Windowsの場合、Relay有効化済みAgentのソフトウェアリポジトリフォルダの初期設定の場所は次のとおりです。

```
C:\ProgramData\Trend Micro\Deep Security Agent\relay\www\dsa\
```

Linuxの場合、Relayのソフトウェアリポジトリフォルダの初期設定の場所は次のとおりです。

```
/var/opt/ds_agent/relay/www/dsa/
```

フォルダは次のような構造になっています。

```
|-- dsa
|   |-- <Platform>.<Architecture>
|       |-- <Filename>
|           |-- <Filename>
```


Trend Micro Deep Security On-Premise 12.0

```
|          |-- ...  
|  
|      |--<Platform>.<Architecture>  
|          |-- <Filename>  
|          |-- <Filename>  
|          |-- ...
```

次に例を示します。

```
|-- dsa  
|      |-- CentOS_<version>.x86_64  
|          |-- Feature-AM-CentOS_<version>.x86_64.dsp  
|          |-- Feature-DPI-CentOS_<version>.x86_64.dsp  
|          |-- Feature-FW-CentOS_<version>.x86_64.dsp  
|          |-- Feature-IM-CentOS_<version>.x86_64.dsp  
|          |-- ...  
|  
|      |-- RedHat_EL6.x86_64  
|          |-- Agent-Core-RedHat_<version>.x86_64.rpm  
|          |-- Feature-AM-RedHat_<version>.x86_64.dsp  
|          |-- Feature-DPI-RedHat_<version>.x86_64.dsp  
|          |-- Feature-FW-RedHat_<version>.x86_64.dsp  
|          |-- ...  
|          |-- Plugin-Filter_2_6_32_131_0_15_el6_x86_64-RedHat_<version>.x86_64.dsp  
|          |-- Plugin-Filter_2_6_32_131_12_1_el6_x86_64-RedHat_<version>.x86_64.dsp  
|          |-- ...
```

Trend Micro Deep Security On-Premise 12.0

```
|
|   |-- Windows.x86_64
|       |-- Agent-Core-Windows-<version>.x86_64.msi
|       |-- Agent-Core-Windows-<version>.x86_64.msi
|       |-- Feature-AM-Windows-<version>.x86_64.dsp
|       |-- Feature-AM-Windows-<version>.x86_64.dsp
|       |-- Feature-DPI-Windows-<version>.x86_64.dsp
|       |-- Feature-DPI-Windows-<version>.x86_64.dsp
|       |-- ...
|       |-- Plugin-Filter-Windows-<version>.x86_64.dsp
|       |-- Plugin-Filter-Windows-<version>.x86_64.dsp
|       |-- ...
```

上記の例では少数のファイルとフォルダしか示されていませんが、完全なdsaフォルダ内には、もっと多くのファイルとフォルダが存在します。ディスク容量や帯域幅を節約する必要がある場合は、そのすべてのミラーを作成する必要はなく、使用しているコンピュータのプラットフォームに適用されるファイルのミラーだけで十分です。

新しいソフトウェアリポジトリを使用するようにAgentを設定する

Webサーバにミラーを作成したら、Webサーバからソフトウェアアップデートを取得するようにDeep Security Agentを設定します。

1. Deep Security Managerで、[管理]→[システム設定]→[アップデート]の順に選択します。
2. [ソフトウェアアップデート]セクションで、WebサーバのミラーフォルダのURLを入力します。
3. [保存]をクリックします。

注意: AgentとWebサーバの間の通信が安定していることを確認します。接続がブロックされた場合、Agentは代わりにRelayを使用します。

新しいパターンファイルアップデートアラートのメールの無効化

Deep Security Managerがセキュリティアップデートをダウンロードしてから1時間以内にAgentに適用しないと、[新しいパターンファイルアップデートがダウンロード済みで利用可能] アラートが発令されます。1時間という期間は変更できません。アラートがデフォルトで発令される場合、このアラートはメールで送信されます。

アップデートの解決に1時間では足りないため、このようなメールアラートを数多く受信する場合は、このアラートのメール通知を無効にできます。その代わりに、アラートが発令される時間を設定できるように、「コンピュータがアップデートを受信していない」アラートに関するメールメッセージを受信できます。

1. Deep Security Managerがセキュリティアップデートを自動的にダウンロードするように設定するには、Deep Security Managerで、[管理]→[予約タスク]の順にクリックします。
2. 種類が [セキュリティアップデートの確認] の予約タスクがない場合は、そのタスクを作成します ("[Deep Security予約タスクの設定](#)" on page 479を参照してください)。
3. [管理]→[システム設定]→[アップデート]の順にクリックします。[セキュリティアップデート]の [ルール] セクションで、[新しいルールアップデートを自動的にポリシーに適用] が選択されています。
4. [アラート]→[アラートの設定]の順にクリックします。
5. [アラートの設定] 画面で、[新しいパターンファイルアップデートがダウンロード済みで利用可能] アラートをクリックし、[プロパティ] をクリックします。
6. [アラート情報] 画面で、[このアラートの発令時、通知のメールを送信する] を選択解除し、[OK] をクリックします。
7. [コンピュータがアップデートを受信していない] アラートをクリックして、[プロパティ] をクリックします。
8. [このアラートの発令時、通知のメールを送信する] が選択されていることを確認し、[OK] をクリックします。アラートはアップデートを7日間保留すると発令されます。
9. アップデートを保留してから任意の時間の経過後にアラートを発令するには、[管理]→[システム設定]→[アラート] をクリックします。
10. [アラート] エリアで、ドロップダウンを使用して時間を選択し、[保存] をクリックします。

エージェントパッケージの整合性チェック

Deep Securityは、ソフトウェア・ファイルが署名時以降に変更されていないことを確実にするためのDeep Security Agentであなたの署名を検証します。整合性チェックは次の場合に実行されます。

1. Deep Security Agentをアップグレードしています。
2. カーネルサポートがアップデートされるように、新しいセキュリティモジュールを有効にしています。

検証が失敗した場合は、プラグインのインストールとエージェントのアップグレードがブロックされています。

トラブルシューティング

ID	イベント	Reason	ソリューション
5302	Agent/Plugin パッケージの 署名のダウン ロードに失敗 しました。	エージェントの整合性チェックに使用されるシグネチャファイルは、アップデート元から入手できません。Deep Security Relayが必要なバージョンにアップグレードされないことがあります。	<ol style="list-style-type: none"> 1. [Alerts]画面で、[Relay Upgrade Required For Agent Integrity Check]アラートがないかどうかを確認します。アラートが存在する場合は、"サポートされるDeep Security Relayのバージョン on the next pageと"Deep Security Relayのアップグレード on page 997のアップグレードを参照してください。署名ファイルがアップデート元に同期されていることを確認します。 2. 署名ファイルがアップデート元に同期されていることを確認してください。 3. エージェントをアップグレードするか、アップデートしたポリシーを再度送信してください。 4. 問題が解決しない場合は、"診断パッケージとログの作成 on page 1573をログに記録してトレンドマイクロのサポートチームに送信してください。
5300	Agent/Plugin パッケージ署名の検証に失敗しました。	エージェントパッケージが改ざんされているか、パッケージに問題がある可能性があります。	<ol style="list-style-type: none"> 1. アップデート元から改ざんされている可能性のあるファイルをバックアップして削除します。 2. Deep Security Managerから対応するエージェントパッケージを

ID	イベント	Reason	ソリューション
5301	Agent/Plugin パッケージの検証に失敗しました。		削除します。 3. ダウンロードセンター からエージェントパッケージを再ダウンロードし、Deep Security Managerにインポートしてください。 4. パッケージがアップデート元に同期されていることを確認します。
5303	Agent/Plugin パッケージのシグネチャがポリシー内のシグネチャと一致しません。		5. エージェントをアップグレードするか、アップデートしたポリシーを再度送信してください。 6. 問題が解決しない場合は、" 診断パッケージとログの作成 " on page 1573 をログに記録してトレンドマイクロのサポートチームに送信してください。

サポートされるDeep Security Relayのバージョン

次のDeep Security Relayのバージョンがサポートされています。

- Deep Security 12.0 update 8 (12.0.0.967)
- Deep Security 11.0 update 23 (11.0.1617)

Deep Securityの強化

ご使用のDeep Security環境のセキュリティを強化するには、各種の方法があります。

- "[Agentを使用したDeep Security Managerの保護](#)" on the next page
- "[Deep Security Manager TLS証明書の置き換え](#)" on page 1057
- "[Deep Security Managerとデータベース間の通信の暗号化](#)" on page 1063

- "Deep Security Managerのデータベースのパスワードの変更" on page 1072
- "HTTPセキュリティヘッダの設定" on page 1075
- "ユーザパスワードルールの適用" on page 1081

Agentを使用したDeep Security Managerの保護

Deep Security Managerを保護するには、ManagerのホストコンピュータにAgentをインストールし、Deep Security Managerポリシーを適用します。

1. Managerと同じコンピュータにAgentをインストールします。
2. [コンピュータ] に移動します。
3. Managerのコンピュータを追加します。ポリシーは、まだ適用しないでください。
4. 新しいコンピュータをダブルクリックして [詳細] 画面を表示し、[侵入防御]→[詳細]→[SSL設定] の順に選択します。
5. [新規] をクリックしてウィザードを開始し、新規SSL設定を作成します。
6. Managerで使用するインタフェースを指定します。[次へ] をクリックします。
7. [ポート] 画面で、Deep Security ManagerのGUIのポート番号を保護するかどうかを選択します ([「ポート番号」](#)を参照)。
[次へ] をクリックします。
8. SSLの侵入防御分析をこのコンピュータのすべてのIPアドレスで実行するのか、それとも1つのIPアドレスでのみ実行するのかを指定します(この機能は、1つのコンピュータに複数の仮想マシンを設定する場合に使用できます)。
9. [Deep Security Manager内蔵のSSL資格情報を使用します] を選択します (このオプションは、ManagerのコンピュータのSSL設定を作成する場合にのみ表示されます)。[次へ] をクリックします。
10. ウィザードを終了して、[SSL設定] 画面を閉じます。
11. コンピュータの [詳細] 画面に戻ります。Deep Security Managerポリシーを適用します。このポリシーには、Deep Security ManagerのGUIのポート番号を保護するために必要なファイアウォールルールと侵入防御ルールが含まれています。

これでManagerのコンピュータは保護され、ManagerへのSSLを含むトラフィックはフィルタされます。

注意: SSLトラフィックをフィルタするようにAgentを設定すると、Deep Security Agentからいくつかの更新エラーイベントが返されることがあります。これらは、Managerコンピュータで発行された新しいSSL証明書が原因の証明書の更新エラーです。このエラーを解決するには、Webページを更新し、Deep Security ManagerのGUIに再接続します。

[Deep Security Manager] ポリシーには、Managerをリモートで利用できるように基本のファイアウォールルールが割り当てられています。Managerのコンピュータを別の目的で使用する場合は、追加でファイアウォールルールを割り当てる必要があります。また、このポリシーには、アプリケーションの種類 [Web Server Common] の侵入防御ルールが含まれます。必要に応じて、侵入防御ルールを追加で割り当てることもできます。

アプリケーションの種類 [Webサーバ共通] では通常 [HTTP] ポートリストのポートがフィルタされ、Deep Security ManagerのGUIのポート番号は含まれません。このため、ポリシーの [詳細] 画面の [侵入防御ルール] 画面にあるポート設定にDeep Security ManagerのGUIのポート番号が追加されています ("[ポート番号、URL、およびIPアドレス](#)" on page 190を参照)。

SSLデータの検査の詳細については、"[SSLまたはTLSトラフィックの検査](#)" on page 823を参照してください。

Deep Security Agentの保護

Managerからの通信を有効にし (詳細については"[AgentとManagerの通信](#)" on page 400を参照)、拡張機能によりManagerからの有効化を有効にした場合は、有効化中にAgentを特定のManagerにバインドすることを強く推奨します。詳細については以下のセクションを参照してください。

特定のDeep Security ManagerへのDeep Security Agentのバインド

Deep Security AgentとDeep Security Managerの間でManagerからの有効化が可能になっている場合は、有効化の実行中に特定のManagerからの接続のみを許可してAgentを保護することを推奨しています。悪意のあるDeep Security Managerが含まれている可能性がある環境の場合は、この設定を使用する必要があります。

AgentをManagerにバインドするには、AgentとManagerの通信を保護するために使用されるSSL証明書をエクスポートし、Agentコンピュータに追加する必要があります。次の手順に従います。

1. Deep Security Managerで、次のコマンドを実行してDeep Security Manager SSL証明書をエクスポートします。

```
dsm_c -action exportdsmcert -output ds_agent_dsm.crt [-tenantname TENANTNAME | -tenantid TENANTID]
```

指定する項目は次のとおりです。

- `ds_agent_dsm.crt`は、表示されているとおりに指定する必要があります (別の名前は使用できません)。これは、AgentとManagerの間の通信を保護するために使用されるDeep Security Manager SSL証明書の名前です。
- `-tenantname TENANTNAME` は、マルチテナント環境がある場合にのみ必要です。テナント名 `TENANTNAME` は、Agentがインストールされているテナントの名前に置き換えます。
- `-tenantid TENANTID` は、`-tenantname TENANTNAME` の代替の選択肢です。テナントID `TENANTID` は、AgentがインストールされているテナントのIDに置き換えます。
- 複数のテナントを指定するには、この手順の最後のステップを参照してください。
- マルチテナントの詳細については、"[マルチテナント環境の設定](#)" on page 279を参照してください。

2. 有効化するAgentがインストールされているコンピュータ上で、次のいずれかの場所に`ds_agent_dsm.crt`ファイルを置きます。

- Windows: `%ProgramData%\Trend Micro\Deep Security Agent\dsa_core`
- Linux: `/var/opt/ds_agent/dsa_core`

3. 複数のテナントがある場合は、各テナントに対して上記のコマンドを実行し、各テナントのAgentに証明書をコピーします。

例:

2つのテナントがある場合は、次のコマンドを実行します。

```
dsm_c -action exportdsmcert -output ds_agent_dsm.crt -tenantname TENANT1
```

```
dsm_c -action exportdsmcert -output ds_agent_dsm.crt -tenantname TENANT2
```

...その後、

最初の`ds_agent_dsm.crt`を、TENANT1によって制御されるAgentへコピーします。

2番目の`ds_agent_dsm.crt`を、TENANT2によって制御されるAgentへコピーします。

これで、Deep Security Manager証明書がAgentに追加されました。Agentは証明書を所有するDeep Security Managerからの有効化のみを受け入れるようになりました。テナントがある場合、Agentはエクスポートコマンドで指定されたテナントでのみ有効化できます。

注意: この手順を完了すると、Agentは「事前に有効化された」状態になります。この状態では、他のDeep Security ManagerまたはAgentのローカルdsa_controlユーティリティによって開始された操作は、意図的に正常に機能しません。Agentが有効化されると、すべての通常の操作が再開されます。

注意: Agentをリセットまたは無効化すると、Deep Security Manager証明書がクリアされるため、上記の手順を再度適用する必要があります。

Deep Security Manager TLS証明書の置き換え

Deep Security Managerは、インストール時にWebコンソールへのアクセス用の自己署名TLS証明書を自動生成します。インストールの完了後、この初期設定の証明書を信頼された認証機関（CA）からの証明書に置き換えることができます。

ヒント: 証明書は、Deep Security Managerのアップグレード時に保持されます。

警告: 初期設定の証明書を無効な証明書または不完全な証明書チェーンに置き換えると、Deep Security Managerが到達不能になる可能性があります。証明書を交換する前に、この項の手順をよくお読みください。

オプションAまたはオプションBのいずれかの手順に従って、Deep Security Manager TLS証明書を置き換えます。

オプションA - Deep Security Managerドメイン名の新しい証明書を要求する

これは証明書を置き換える最も信頼性の高い方法です。

1. FIPSモードを有効にしている場合は ("[FIPS 140-2のサポート](#)" on page 1457), で証明書を置き換える前にFIPSモードを無効にしてから、FIPSモードを再度有効にしてください。

2. "秘密鍵とキーストアを生成する" belowします。
3. "CSRを生成して証明書を要求する" on page 1060する
4. "署名された証明書をキーストアにインポートする" on page 1060します。
5. "署名付き証明書ストアを使用するようにDeep Securityを設定する" on page 1062

オプションB - 既存のJava Key Storeファイルを使用する

このシナリオでは、ファイルが以前のインストールからバックアップされたか、ワイルドカード証明書などの共通ドメイン用に作成された状況について説明します。

1. 完全な証明書チェーンがあることを確認してください。必要に応じて、証明書を発行したCAにお問い合わせください。
2. FIPSモードを有効にしている場合は ("FIPS 140-2のサポート" on page 1457), で証明書を置き換える前にFIPSモードを無効にしてから、FIPSモードを再度有効にしてください。
3. "署名付き証明書ストアを使用するようにDeep Securityを設定する" on page 1062

Java Keystoresについて

Javaキーストアは、Javaベースのアプリケーションで使用される証明書を格納するために使用されます。Java KeystoresとKeytoolに詳しくない場合、DigitalOceanには、[Java Keytool Essentials : Javaキーストアの使用](#)の記事の概念が説明されています。

秘密鍵とキーストアを生成する

1. Deep Security Managerが実行されているコンピュータで、管理者としてコマンドプロンプトを開きます。
2. ディレクトリを次のように変更します。
 - Windows:C:\Program Files\Trend Micro\Deep Security Manager\jre\bin
 - Linux:/opt/dsm/jre/bin

Trend Micro Deep Security On-Premise 12.0

3. 次のコマンドを実行して、秘密鍵と新しいキーストアを生成します。

- Windows:keytool -genkey -keyalg RSA -alias tomcat -keystore C:\Users\Administrator\.keystore -validity 365 -keysize 2048
- Linux:keytool -genkey -keyalg RSA -alias tomcat -keystore ~/.keystore -validity 365 -keysize 2048

```
Enter keystore password:
```

```
What is your first and last name?
```

```
[Unknown]: <HOSTNAME>
```

```
What is the name of your organizational unit?
```

```
[Unknown]: <COMPANY_OU>
```

```
What is the name of your organization?
```

```
[Unknown]: <COMPANY_NAME>
```

```
What is the name of your City or Locality?
```

```
[Unknown]: <CITY>
```

```
What is the name of your State or Province?
```

```
[Unknown]: <STATE_IF_APPLIES>
```

```
What is the two-letter country code for this unit?
```

```
[Unknown]: <COUNTRY_CODE>
```

```
Is CN=<HOSTNAME>... correct?
```

```
[no]: yes
```

```
Enter key password for <tomcat>
```

```
(RETURN if same as keystore password):
```

```
Re-enter new password:
```

4. 警告が表示されます。次のコマンドを実行して、キーストアをPKCS #12形式にエクスポートします。

注意: このコマンドは、残りの例で使用する、PKCS #12形式の2番目のキーストア (.keystore2) を作成します。

- Windows: `keytool -importkeystore -srckeystore C:\Users\Administrator\.keystore -destkeystore C:\Users\Administrator\.keystore2 -deststoretype pkcs12`
- Linux: `keytool -importkeystore -srckeystore ~/.keystore -destkeystore ~/.keystore2 -deststoretype pkcs12`

CSRを生成して証明書を要求する

次のコマンドを使用して証明書の署名要求 (CSR,) を生成します。このファイルは、CAに送信して署名付き証明書を要求できます。この例では、ファイルの名前は<HOSTNAME>.csrです。

- Windows:
`keytool -keystore C:\Users\Administrator\.keystore2 -certreq -alias tomcat -keyalg rsa -file <HOSTNAME>.csr`
- Linux :
`keytool -keystore ~/.keystore2 -certreq -alias tomcat -keyalg rsa -file <HOSTNAME>.csr`

次に、CSRファイルを使用して、任意のCAから署名された証明書を要求します。CAから署名された証明書を受け取ったら、引き続き"[署名された証明書をキーストアにインポートする](#)" [below](#) できます。

署名された証明書をキーストアにインポートする

CAから署名された証明書を取得したら、証明書の応答をkeystoreにインポートします。

警告: 証明書は、実際に署名された証明書に到達する前に、ルートCAから1つ以上の中間CAから1つの信頼チェーン内で発行されます。すべてのCA証明書を正しい順序でインポートする必要があります。インポートする内容が不明な場合は、署名された証明書を発行したCAを確認してください。

次の例では、証明書が.crt形式であることを前提としています。

1. ルートCAをキーストアにインポートするには、次のコマンドを使用します。(署名済み証明書がすでにキーストア.)に配置されているルートCAで署名されている場合は、この手順を省略します。
 - Windows:keytool -import -keystore c:\Users\Administrator\.keystore2 -storepass <YOUR_PASSWORD> -alias rootCA -file c:\Users\Administrator\ - Linux:keytool -import -keystore ~/.keystore2 -storepass <YOUR_PASSWORD> -alias rootCA -file ~/<RootCA>.crt
2. 署名された証明書は、1つ以上の中間CAによって署名されている可能性があります。すべての中間CAがキーストア内にある場合は、この手順をスキップできます。それ以外の場合は、次のコマンドを使用して、欠落している中間CAをキーストアにインポートします。
 - Windows:keytool -import -keystore c:\Users\Administrator\.keystore2 -storepass <YOUR_PASSWORD> -trustcacerts -alias intermediateCA -file c:\Users\Administrator\ - Linux:keytool -import -keystore ~/.keystore2 -storepass <YOUR_PASSWORD> -trustcacerts -alias intermediateCA -file ~/<IntermediateCA>.crt
3. 最後に、次のコマンドを使用して、署名された証明書をキーストアにインポートします。
 - Windows: keytool -import -keystore c:\Users\Administrator\.keystore2 -storepass <YOUR_PASSWORD> -trustcacerts -alias tomcat -file c:\Users\Administrator\ - Linux:keytool -import -keystore ~/.keystore2 -storepass <YOUR_PASSWORD> -trustcacerts -alias tomcat -file ~/<HOSTNAME>.crt

インポートに成功した場合は、次のメッセージが表示されます。

```
Certificate reply was installed in keystore
```

署名付き証明書ストアを使用するようにDeep Securityを設定する

次の例では、新しいkeystoreの名前が`.keystore2`であることを前提としています。

1. (Windows) `C:\プログラムFiles \ Trend Micro \ Deep Security Manager \ configuration.properties` または (Linux) `/opt/dsm/configuration.properties` ファイルをバックアップします。
2. 古いkeystoreファイルをバックアップします。
 - Windows:`copy "C:\Program Files\Trend Micro\Deep Security Manager\.keystore" "C:\Program Files\Trend Micro\Deep Security Manager\.keystore.bak"`
 - Linux:`cp /opt/dsm/.keystore /opt/dsm/.keystore.bak`
3. 古いkeystoreファイルを新しいファイルに置き換えます。
 - Windows:`copy "c:\Users\Administrator\.keystore2" "C:\Program Files\Trend Micro\Deep Security Manager\.keystore"`
 - Linux:`cp ~/.keystore2 /opt/dsm/.keystore`

注意: 初期設定のkeystoreファイルを置き換える必要があります。代わりに設定ファイルのパスを変更することを選択した場合、次回Deep Security Managerをアップグレードしたときに設定ファイルが初期設定の場所にリセットされ、変更が元に戻されます。

4. 次のように、(Windows) `C:\Program Files \ Trend Micro \ Deep Security Manager \ configuration.properties` または (Linux) `/opt/dsm/configuration.properties` のキーストアパスワードをアップデートします。

```
...<OTHER_SETTINGS>
```

```
keystorePass=<YOUR_PASSWORD>
```

5. Deep Security Managerサービスを再起動します。

Deep Security Managerとデータベース間の通信の暗号化

初期設定では、Deep Security Managerとデータベース間の通信は暗号化されません。これは、パフォーマンス上の理由と、Managerとデータベースが同じコンピュータ上で実行されているか、または両者がクロスケーブルやプライベートネットワークセグメント、IPSec経由のトンネリングのいずれかで接続されているかにかかわらず、両者間のチャンネルがすでに保護されているということを前提にしているからです。

したがって、Deep Security Managerとデータベース間の通信チャンネルが保護されていない場合は、その間の通信を暗号化する必要があります。これを実行するには、 `\[Deep Security Manager install directory]\webclient\webapps\ROOT\WEB-INF\` 内の `dsm.properties` ファイルを編集します。

この手順は、使用するデータベースによって異なります。

- ["Microsoft SQL Serverデータベース \(Linux\)" on the next page](#)
- ["Microsoft SQL Server \(Windows\)" on page 1066](#)
- ["Oracle Database" on page 1068](#)
- ["PostgreSQL" on page 1069](#)

注意: 複数ノードモードでDeep Security Managerを実行している場合は、以下の変更をノードごとに適用する必要があります。

このセクションでは、["データベースサーバでAgentを実行する" on page 1070](#)に関する情報と、["Managerとデータベース間の暗号化を無効にする" on page 1070](#)方法も示します。

Managerとデータベースの間の通信を暗号化する

Microsoft SQL Serverデータベース (Linux)

前提条件:これらの手順を進める前に、信頼できる認証局 (CA) の証明書がすでにMicrosoft SQL Serverに割り当てられていることを確認します。詳細については、Microsoft MSDNサイトの「[データベース エンジンへの暗号化接続の有効化](#)」を参照してください。

1. Deep Security Managerのサービスを停止します。

```
# service dsm_s stop
```

2. `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties`を編集して次の行を追加します。

```
database.SqlServer.encrypt=true
```

```
database.SqlServer.trustServerCertificate=true
```

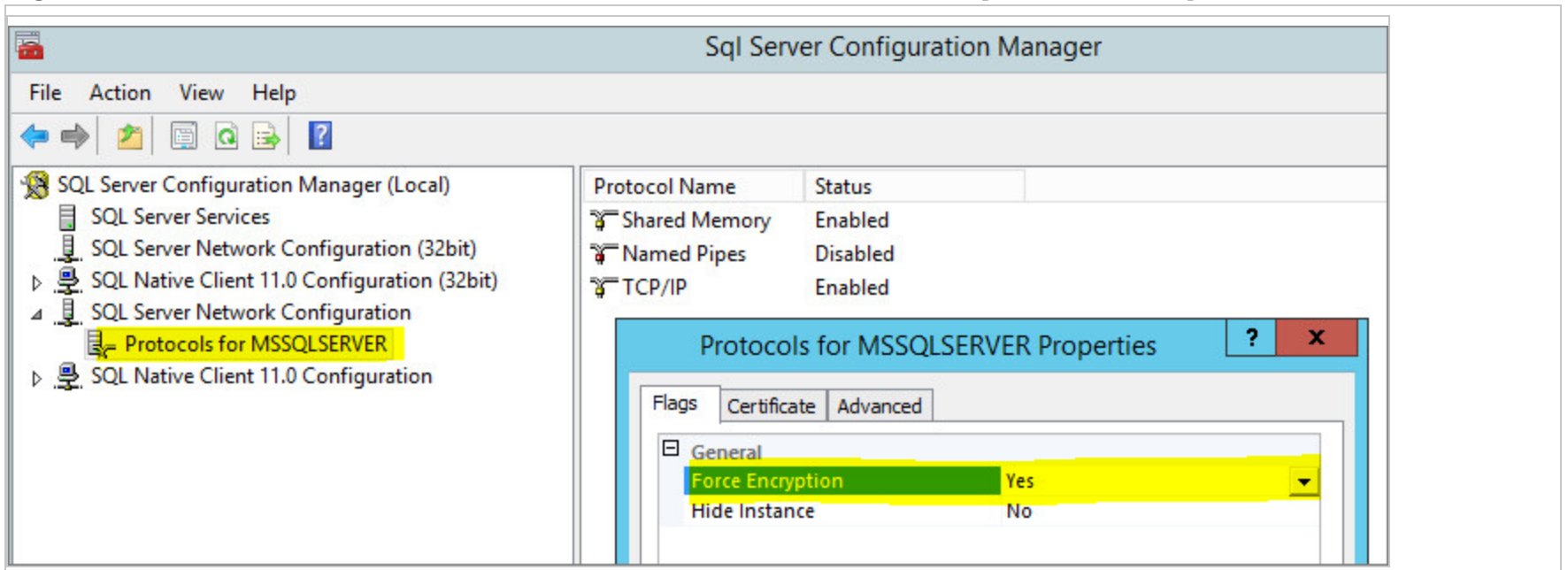
注意: Deep Security 10.1以前のバージョンからアップグレードし、データベースへの接続にトランスポートとして名前付きパイプを使用する場合は、代わりに次の行を追加します。

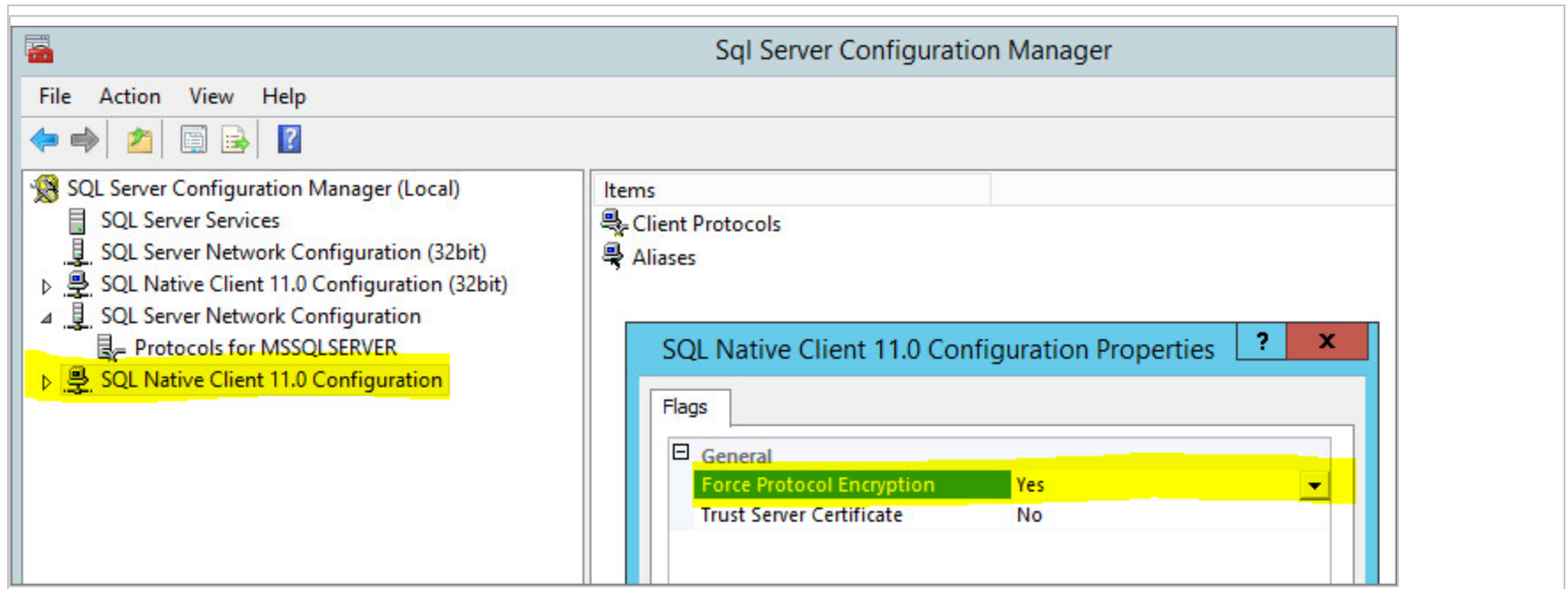
```
database.SqlServer.ssl=require
```

3. Deep Security 10.1以前のバージョンからアップグレードし、データベースへの接続にトランスポートとして名前付きパイプを使用する場合は、`/opt/dsm`に次の行を含む「`dsm_s.vmoptions`」という名前のファイルを作成します。

```
-Djsse.enableCBCProtection=false
```


4. SQL Server構成マネージャを開き、インスタンスのプロトコルプロパティで [強制的に暗号化] を有効にします。





5. Deep Security Managerのサービスを開始します。

```
# service dsm_s start
```

Microsoft SQL Server (Windows)

前提条件:これらの手順を進める前に、信頼できる認証局 (CA) の証明書がすでにMicrosoft SQL Serverに割り当てられていることを確認します。詳細については、Microsoft MSDNサイトの「[データベース エンジンへの暗号化接続の有効化](#)」を参照してください。

1. Deep Security Managerのサービスを停止します。
2. `\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.properties`を編集して次の行を追加します。

```
database.SqlServer.encrypt=true
```

```
database.SqlServer.trustServerCertificate=true
```

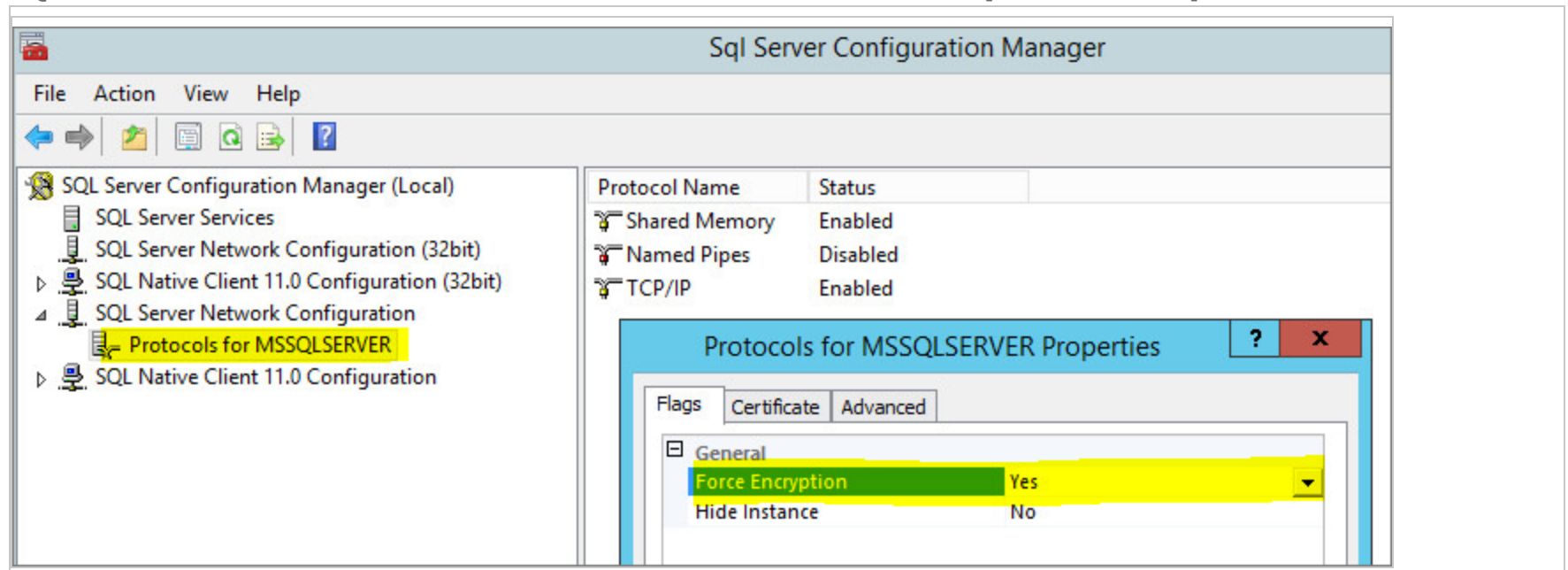
注意: Deep Security 10.1以前のバージョンからアップグレードし、データベースへの接続にトランスポートとして名前付きパイプを使用する場合は、代わりに次の行を追加します。

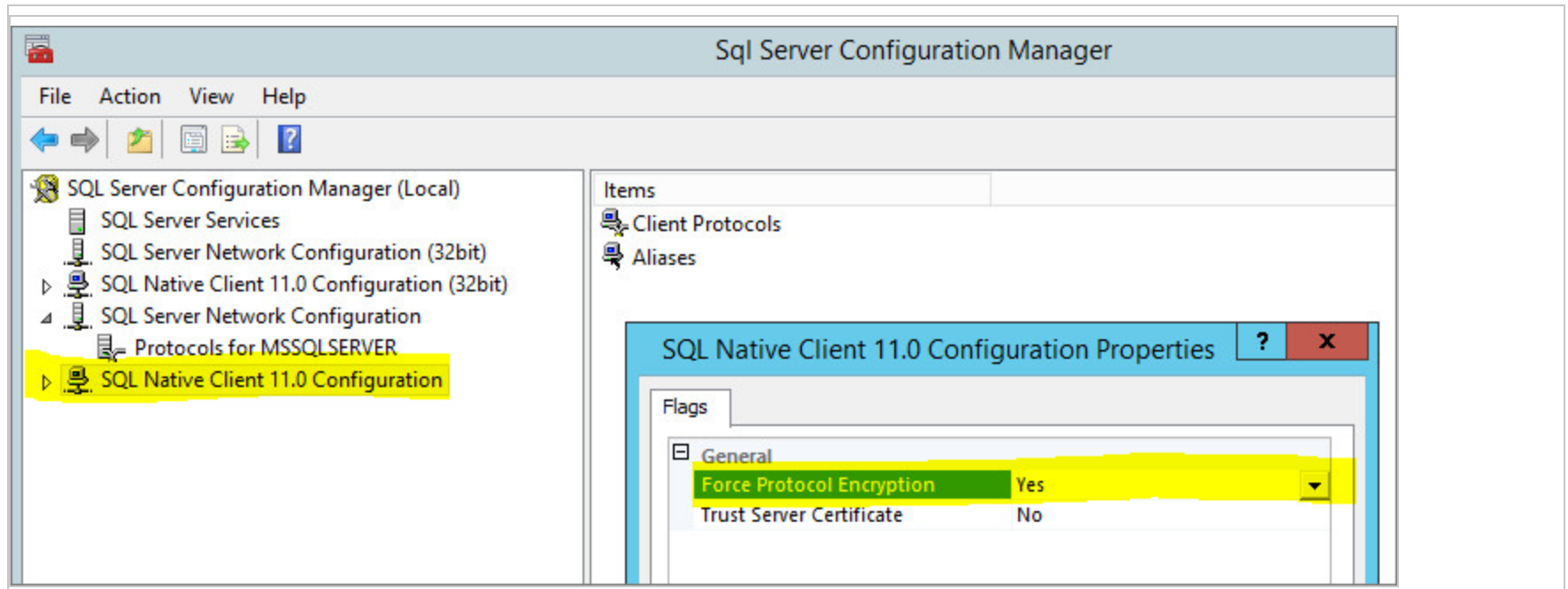
```
database.SqlServer.ssl=require
```

3. Deep Security 10.1以前のバージョンからアップグレードし、データベースへの接続にトランスポートとして名前付きパイプを使用する場合は、`\Program Files\Trend Micro\Deep Security Manager`に次の行を含む「Deep Security Manager.vmoptions」という名前のファイルを作成します。

```
-Djsse.enableCBCProtection=false
```

4. SQL Server構成マネージャを開き、インスタンスのプロトコルプロパティで [強制的に暗号化] を有効にします。





5. Deep Security Managerのサービスを開始します。

Oracle Database

1. 次の行を `dsm.properties` に追加します (例)。

```
database.Oracle.oracle.net.encryption_types_client=(AES256)
```

```
database.Oracle.oracle.net.encryption_client=REQUIRED
```

```
database.Oracle.oracle.net.crypto_checksum_types_client=(SHA1)
```

```
database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
```

2. ファイルを保存して、閉じます。"[Deep Security Managerの再起動](#)" on page 993をします。

先頭に「`database.Oracle.`」が付いているすべてのパラメータがOracleドライバに渡されます。

`encryption_types_client`に指定できる値は次のとおりです。

Trend Micro Deep Security On-Premise 12.0

- AES256
- AES192
- AES128
- 3DES168
- 3DES112
- DES56C
- DES40C
- RC4_256
- RC4_128
- RC4_40
- RC4_56

`crypto_checksum_types_client`に指定できる値は次のとおりです。

- MD5
- SHA1

その他のオプションについては、https://docs.oracle.com/cd/B28359_01/java.111/b31224/clntsec.htmを参照してください。

PostgreSQL

1. PostgreSQLでSSLを有効にします。オンプレミスのPostgreSQLデータベースでのこの方法の詳細については、[「Secure TCP/IP Connections with SSL」](#)を参照してください。Amazon RDS for PostgreSQLの場合は、[「PostgreSQL DB インスタンスで SSL を使用する」](#)を参照してください。
2. Trend Micro Deep Security Managerサービスを停止します。
3. `dsm.properties`ファイルに次の行を追加します。
`database.PostgreSQL.connectionParameters=ssl=true`

4. Trend Micro Deep Security Managerサービスを再起動します。
5. ManagerがTLSを使用して接続していることを確認するには、次のクエリを使用して [SSL] 列を確認します。

```
select a.client_addr, a.application_name, a.username, s.* from pg_stat_ssl s join pg_stat_activity a using (pid) where a.datname='<Deep Securityデータベース名>';
```

注意: 自己署名証明書を使用している場合、または証明書をローテーションする場合は、証明書をcacertsにインポートしてからDeep Security Managerを起動する必要があります。1.信頼するCAをバックアップします。<DSM directory>\jre\lib\security\cacerts。

2. 証明書をcacertsにインポートします ([証明書ファイル]を置換してください)。証明書ファイル名は:
\[Deep Security Manager install directory]\jre\bin\keytool -import -alias rds-root -keystore \[Deep Security Manager install directory]\jre\lib\security\cacerts -file [Certificate File] -storepass changeitです。

データベースサーバでAgentを実行する

Agentを使用してデータベースを保護している場合は、暗号化を有効にする必要があります。セキュリティアップデートを実施すると、Deep Security Managerはデータベースに新規の侵入防御ルールを格納します。データが暗号化されていないと、Agentによるルールの解析の際に、ルール名が原因である誤判定がほぼ間違いなく発生してしまいます。

Managerとデータベース間の暗号化を無効にする

まれに、Deep Security Managerとデータベース間の暗号化を無効にすることが必要になる場合があります。たとえば、古いバージョンのSQL Serverを使用している場合は、接続エラーを回避するために暗号化を無効にしなければならないことがあります。詳細については、"[エラー: データベースサーバへの安全な接続を確立できませんでした](#)" on page 1030を参照してください。

暗号化を無効にするには、データベースの種類に応じた手順に従ってください。

Microsoft SQL Serverデータベース (Linux)

1. Deep Security Managerのサービスを停止します。

```
# service dsm_s stop
```

2. /opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.propertiesを編集して次の行を削除します。

```
database.SqlServer.encrypt=true  
database.SqlServer.trustServerCertificate=true
```

注意: Deep Security 10.1以前のバージョンからアップグレードし、データベースへの接続にトランスポートとして名前付きパイプを使用する場合は、代わりに次の行を削除します。

```
database.SqlServer.ssl=require
```

3. SQL Server構成マネージャを開き、インスタンスのプロトコルプロパティで [強制的に暗号化] を無効にします。
4. Deep Security Managerのサービスを開始します。

```
# service dsm_s start
```

Microsoft SQL Server (Windows)

1. Deep Security Managerのサービスを停止します。
2. \Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.propertiesを編集して次の行を削除します。

```
database.SqlServer.encrypt=true  
database.SqlServer.trustServerCertificate=true
```

注意: Deep Security 10.1以前のバージョンからアップグレードし、データベースへの接続にトランスポートとして名前付きパイプを使用する場合は、代わりに次の行を削除します。

```
database.SqlServer.ssl=require
```

3. SQL Server構成マネージャを開き、インスタンスのプロトコルプロパティで [強制的に暗号化] を無効にします。
4. Deep Security Managerのサービスを開始します。

Oracle Database

1. 次の行を `dsm.properties` から削除します (例)。

```
database.Oracle.oracle.net.encryption_types_client=(AES256)
database.Oracle.oracle.net.encryption_client=REQUIRED
database.Oracle.oracle.net.crypto_checksum_types_client=(SHA1)
database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
```

2. ファイルを保存して、閉じます。"[Deep Security Managerの再起動](#)" on page 993をします。

PostgreSQL

1. Trend Micro Deep Security Managerサービスを停止します。
2. `dsm.properties` ファイルの次の行を削除します。

```
database.PostgreSQL.connectionParameters=ssl=true
```
3. Trend Micro Deep Security Managerサービスを再起動します。

Deep Security Managerのデータベースのパスワードの変更

組織のセキュリティポリシーによっては、Deep Security Managerがデータベースへのアクセスに使用するパスワードを定期的に変更する必要があります。

- "[Microsoft SQL Serverのパスワードを変更する](#)" on the next page
- "[Oracleのパスワードを変更する](#)" on the next page
- "[PostgreSQLのパスワードを変更する](#)" on page 1074

Microsoft SQL Serverのパスワードを変更する

1. Windowsでは、各Deep Security Managerインスタンスで、Trend Micro Deep Security Managerサービスを停止します。

Linuxでは、サービスを停止するコマンドは次のとおりです。

```
# service dsm_s stop
```

2. SQL Server Management Studioを使用してSQLユーザパスワードを変更します。
3. 各Deep Security Managerインスタンスで、`/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties`ファイルを変更して新しいパスワードを指定します。このファイルを開くと、次のような難読化されたパスワード値が記載されています。

```
database.SqlServer.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
```

この値を新しいパスワードで上書きします (新しいパスワードはサービスを再起動したときに難読化されます)。

```
Database.SqlServer.password=NEW PASSWORD GOES HERE
```

4. Windowsでは、各Deep Security ManagerインスタンスでTrend Micro Deep Security Managerサービスを開始します。

Linuxでは、サービスを開始するコマンドは次のとおりです。

```
# service dsm_s start
```

Oracleのパスワードを変更する

1. Windowsでは、各Deep Security Managerインスタンスで、Trend Micro Deep Security Managerサービスを停止します。

Linuxでは、サービスを停止するコマンドは次のとおりです。

```
# service dsm_s stop
```

Trend Micro Deep Security On-Premise 12.0

- Oracleのツールを使用してパスワードを変更します。
- 各Deep Security Managerインスタンスで、`/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties`ファイルを変更して新しいパスワードを指定します。このファイルを開くと、次のような難読化されたパスワード値が記載されています。

```
database.Oracle.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
```

この値を新しいパスワードで上書きします (新しいパスワードはサービスを再起動したときに難読化されます)。

```
Database.Oracle.password=NEW PASSWORD GOES HERE
```

- Windowsでは、各Deep Security ManagerインスタンスでTrend Micro Deep Security Managerサービスを開始します。
Linuxでは、サービスを開始するコマンドは次のとおりです。

```
# service dsm_s start
```

PostgreSQLのパスワードを変更する

- Windowsでは、各Deep Security Managerインスタンスで、Trend Micro Deep Security Managerサービスを停止します。
Linuxでは、サービスを停止するコマンドは次のとおりです。

```
# service dsm_s stop
```

- パスワードを変更するには、PostgreSQLドキュメントの手順に従います。
- 各Deep Security Managerインスタンスで、`/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties`ファイルを変更して新しいパスワードを指定します。このファイルを開くと、次のような難読化されたパスワード値が記載されています。

```
database.PostgreSQL.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
```

この値を新しいパスワードで上書きします (新しいパスワードはサービスを再起動したときに難読化されます)。

```
Database.PostgreSQL.password=NEW PASSWORD GOES HERE
```

4. Windowsでは、各Deep Security ManagerインスタンスでTrend Micro Deep Security Managerサービスを開始します。

Linuxでは、サービスを開始するコマンドは次のとおりです。

```
# service dsm_s start
```

HTTPセキュリティヘッダの設定

セキュリティヘッダとは、Webブラウザでのセキュリティ対策を設定するためにWebアプリケーションで使用されるディレクティブです。ブラウザはこれらのディレクティブに基づき、クロスサイトスクリプティングやクリックジャッキングなど、クライアント側の脆弱性を利用するのを困難にすることができます。また、ヘッダを使用すると、有効なTLS通信のみを許可したり、有効な証明書の使用を強制したり、特定のサーバ証明書の使用を強制したりするようにブラウザを設定することもできます。

以降のセクションでは、各種のセキュリティヘッダと、Deep Securityにおける各種ヘッダのサポート状況について詳しく説明します。

- ["カスタマイズ可能なセキュリティヘッダ" below](#)
- ["強制的に適用されるセキュリティヘッダ" on page 1079](#)
- ["サポートされていないセキュリティヘッダ" on page 1080](#)

カスタマイズ可能なセキュリティヘッダ

環境要件によっては、次のヘッダを有効にして設定することができます。

- ["HTTPの厳密なトランスポートセキュリティ \(HSTS\)" below](#)
- ["Content Security Policy \(CSP\)" below](#)
- ["HTTP公開鍵ピンニング \(HPKP\)" on page 1078](#)

注意: プライマリテナントの場合は、Deep Security Managerで["カスタマイズ可能なセキュリティヘッダを有効化する" on page 1078](#)ことや、["設定をリセットする" on page 1078](#)ことができます。

HTTPの厳密なトランスポートセキュリティ (HSTS)

HTTPの厳密なトランスポートセキュリティは、Webアプリケーションと通信する際、常に有効で安全な接続を使用するようにWebブラウザを設定するヘッダです。サーバのTLS証明書が突然期限切れになったり信頼されなくなったりした場合、ブラウザはWebアプリケーションとの接続を行わなくなります。また、ユーザがhttp://で始まるURLを使用してWebアプリケーションにアクセスしようとした場合は、自動的にhttps://に変更されます。これらのセキュリティ対策は、中間者攻撃に加え、セッションハイジャッキングなどの攻撃を防ぐのに役立ちます。

インストール直後のDeep Security Managerコンソールでは、(信頼されていない) 自己署名証明書とHSTSがオフになっています。これは、各組織で、Managerのホスト名と一致する特定の証明書を使用してDeep Security Webアプリケーションを設定する必要がありますためです。この設定は、AWS ELB/ALBなどのTLS終端機能を持つロードバランサを設定することで完了することもできます。

有効なTLS設定が行われると、の[管理]→[システム設定]→[セキュリティ]からHTTP Strict Transport Securityヘッダを有効にできます。

HTTPの厳密なトランスポートセキュリティ (HSTS) を有効化する方法については、["カスタマイズ可能なセキュリティヘッダを有効化する" on page 1078](#)を参照してください。

Content Security Policy (CSP)

Content Security Policyには、ブラウザへの読み込みやブラウザでの実行を許可するコンテンツの種類を制限することにより、クロスサイトスクリプティングやクリックハイジャッキングなどのクライアント側攻撃を防止するのに役立つ包括的なディレク

タイプが含まれています。

注意: CSPを有効にすると、悪影響が生じる場合があります。たとえば、組み込みスクリプトが機能しなくなったり、jQueryなどのサードパーティコンポーネントで必要とされる特定の種類のイメージが読み込まれなくなったりすることがあります。

CSPを有効にする場合は、最初に [Report-only] をオンにしてCSPを実行し、必要なアプリケーション機能で指定したURL関連する違反がレポートされていないか確認することを推奨しています。

Deep Security CSPは、の[管理]→[システム設定]→[セキュリティ]で設定できます。

Deep Securityで推奨される設定は次のとおりです。

```
default-src 'self'
```

```
script-src 'self' 'unsafe-eval' 'unsafe-inline'
```

```
frame-src 'self'
```

```
frame-ancestors 'self'
```

```
style-src 'self' 'unsafe-inline' blob:
```

```
form-action 'self'
```

```
img-src 'self' data:
```

```
report-uri https://your_report_uri.org/DS_CSP_Violation
```

注意: 初期設定では、[Report-only] チェックボックスがオンになっています。CSPを有効にしても必要なアプリケーション機能に影響しないことを確認できたら、[Report-only] を選択解除してこのポリシーを適用できます。

Content Security Policy (CSP) を有効化する方法については、"[カスタマイズ可能なセキュリティヘッダを有効化する](#)" [on the next page](#)を参照してください。

HTTP公開鍵ピンニング (HPKP)

HPKPヘッダを有効にすると、ブラウザは安全な通信を開始する際に、特定の証明書または特定の認証局のみを信頼するようになります。このヘッダを有効にすると、感染した信頼済み認証局やクライアントに不正にインストールされた信頼済み認証局を利用した攻撃を防止できます。

注意: HPKPを有効にすると、ヘッダが変更されずに証明書のみが変更された場合に、ブラウザがサーバと接続できなくなる可能性があります。

HTTP公開鍵ピンニング (HPKP) を有効化する方法については、"[カスタマイズ可能なセキュリティヘッダを有効化する](#)" [below](#) を参照してください。

カスタマイズ可能なセキュリティヘッダを有効化する

注意: マルチテナントモードの場合、セキュリティヘッダの設定はプライマリテナントでのみ使用可能です。

1. [管理]→[システム設定]→[セキュリティ] の順に選択します。
2. HTTPの厳密なトランスポートセキュリティ (HSTS)、Content Security Policy (CSP)、またはHTTP公開鍵ピンニング (HPKP)のディレクティブを対応するフィールドに入力します。

注意: 設定を有効にする前にポリシーをテストするには、[Report-only] オプションを選択し、ポリシー違反レポートの内容に問題がないことを確認します。

ヒント: 各ポリシーのディレクティブを別々の行に入力できます。

3. 画面下部の [保存] をクリックします。

設定をリセットする

ディレクティブの設定中に問題が発生し、Deep Security Managerで問題を修正できない場合は、ManagerにSSHで接続し、対応するコマンドを実行して設定をリセットします。

HTTPの厳密なトランスポートセキュリティ

```
dsm_c -action changesetting -name settings.configuration.enableHttpStrictTransportSecurity -value ""
```

```
dsm_c -action changesetting -name settings.configuration.enableHttpStrictTransportSecurity -value "false"
```

Content Security Policy (CSP)

```
dsm_c -action changesetting -name settings.configuration.contentSecurityPolicy -value ""
```

```
dsm_c -action changesetting -name settings.configuration.contentSecurityPolicyReportOnly -value "true"
```

Public Key Pinning Policy

```
dsm_c -action changesetting -name settings.configuration.publicKeyPinPolicy -value ""
```

```
dsm_c -action changesetting -name settings.configuration.publicKeyPinPolicyReportOnly -value "true"
```

強制的に適用されるセキュリティヘッダ

次のヘッダは初期設定で強制的に適用され、変更できません。

- ["Cache-ControlおよびPragma" below](#)
- ["X-XSS-Protection" on the next page](#)
- ["X-Frame-Options" on the next page](#)

Cache-ControlおよびPragma

これらのヘッダは、ブラウザでのコンテンツのキャッシュ方法を設定します。認証されたアプリケーションから機密情報を含むコンテンツをキャッシュする場合、複数のユーザが使用するマシンにコンテンツがキャッシュされたり、ユーザがアプリケーションからログアウトした後にロック解除されたマシンへ攻撃者がアクセスできる状態になっていたりすると、セキュリティ上

の脆弱性につながる恐れがあります。そのため、Deep Securityでは、`no-cache`および`no-store`の値を強制的に適用することにより、静的でないすべてのコンテンツのキャッシュが無効化されます。

X-XSS-Protection

XSS-Protectionヘッダは、ブラウザのクロスサイトスクリプティング (XSS) ヒューリスティックを強制的に有効にしてXSS攻撃を検出します。Deep Securityの初期設定では、このヘッダがブロックモードで強制的に適用されます。そのため、XSS攻撃の可能性がブラウザで検出されると、ページ全体の読み込みがブロックされます。この方法は、潜在的な不正要素を置き換えることによってページを無害化しようとする他の方法よりも安全です。

注意: XSS-Protectionは、あらゆる種類の攻撃に対して有効なわけではなく、XSSフィルタを備えていないブラウザもあります。

X-Frame-Options

このヘッダは、クリックハイジャッキング攻撃の防止に役立ちます。Deep Security Managerでは、このヘッダの `SAMEORIGIN` という値を強制的に適用することにより、同じドメインでホストされているWebアプリケーションへの組み込みのみが許可されます。

注意: このヘッダの効果は、CSPの`frame-ancestors`ディレクティブと同じです。`frame-ancestors`ディレクティブはX-Frame-Optionsヘッダの値よりも優先されます。

サポートされていないセキュリティヘッダ

次の種類のヘッダはサポートされていません。

X-Content-Type-Options

`nosniff`という値を含むこのヘッダを使用すると、MIMEタイプスニフingからの保護に役立ちます。MIMEタイプスニフing攻撃は、ブラウザでテキストコンテンツやバイナリコンテンツがHTMLとして解釈される可能性がある特定のシナリオにおいてのみ影響を及ぼします。たとえば、ユーザが`xss.html`というアバタファイルを読み込み、Webアプリケーションが画像を提供する際にContent-typeヘッダを設定していない場合、ブラウザはコンテンツタイプの判定を試み、`xss.html`をHTMLファイルとして扱う可能性があります。その場合、攻撃者はユーザを`xss.html`に誘導してクロスサイトスクリプティング攻撃を実行することが可能になります。

このヘッダを有効にするとリダイレクトの動作に悪影響を及ぼすことがあります。Deep Securityでは現在、このヘッダを有効にすることはできませんが、これに関連する攻撃のシナリオがManager Webアプリケーションとその基本的な機能に影響する可能性は低いと考えられます。

ユーザパスワードルールの適用

Deep Security Managerのパスワードとユーザ認証に関するその他の設定に対してパスワード要件を指定できます。

パスワード要件を指定する

注意: セキュリティを強化するため、パスワード要件を厳しく指定することを推奨します。文字数は8文字以上で、英数字の両方を含める、大文字と小文字の両方を含める、英数字以外の文字を含める、期限を設ける、などを組み合わせます。

[管理]→[システム設定]→[セキュリティ]の順に選択します。[ユーザセキュリティ]セクションでは次の設定を変更できます。

- セッションアイドルタイムアウト: ユーザの再ログオンが必要になるまでの期間を指定します。
- 最大セッション期間: Deep Security Managerにログオンしてから再ログオンが必要になるまでの最長の期間。
- ログオン失敗の許容回数 (ロックアウト前): 特定のユーザ名を持つ各ユーザが、間違ったパスワードを使用してログオンを試行できる回数。この回数を超えるとロックされます。ユーザのロックを解除できるのは、「ユーザのプロパティを編集で

きる」権限を持つユーザのみです ("[ユーザロールの定義](#)" on page 1382を参照)。

注意: ログオンの失敗回数が多すぎるなど、特定の理由でユーザがロックされた場合に、そのアカウントのロックを解除する権限を持つユーザがないときは、「コマンドラインの使用方法」セクションを参照して、Deep Security Managerのコマンドラインを使用してロック解除を行ってください。

- ユーザごとに許可された同時セッション数: ユーザごとに許可されている同時セッションの最大数。

注意: 一度に2人のユーザとしてログオンする場合、Firefoxでは、画面ベースではなくプロセスベースでセッションCookieが設定されます。つまり、何らかの理由で同時に2人のユーザとしてログオンする場合は、2つの異なるブラウザ (一方はFirefox) を使用するか、2台の異なるコンピュータからログオンする必要があります。

- 同時セッション制限を超えた場合の処理: 同時セッション数の上限に達した場合の処理を指定します。
- ユーザパスワードの有効期限: パスワードが有効な日数。無期限に設定することもできます。
- ユーザパスワードの最小文字数: パスワードに必要な最小の文字数。
- ユーザパスワードには文字と数字の両方を含めることを要求する: 英字 (a~z、A~Z) と数字 (0~9) の両方をパスワードに使用する必要があります。
- ユーザパスワードには大文字と小文字の両方を含めることを要求する: 大文字と小文字の両方を使用する必要があります。
- ユーザパスワードには英数字以外の文字を含めることを要求する: 英数字以外の文字をパスワードに使用する必要があります。
- パスワードの有効期限が近いユーザにメールを送信: ユーザのパスワードの有効期限が切れる前にメールメッセージが送信されます。この機能を使用するには、"[メール通知のSMTPの設定](#)" on page 308を行う必要があります。

ログオンに別のIDプロバイダを使用する

SAMLシングルサインオンを使用するようにDeep Securityを設定することもできます。詳細については、"[SAMLシングルサインオンを設定する](#)" on page 1412を参照してください。

Deep Security Manager ログオンページにメッセージを追加する

[管理]→[システム設定]→[セキュリティ] 画面で [ログオンページのメッセージ] を使用し、Deep Security Managerのログオンページに表示するテキストを入力します。

ユーザに使用条件を提示する

Deep Security Managerへのログオン時にユーザに使用条件への同意を求めるように設定することができます。

この機能を有効にするには、[管理]→[システム設定]→[セキュリティ] 画面で [使用条件へのユーザの同意が必要] を選択します。ユーザがログオンページで [条件を表示] リンクをクリックしたときに表示するタイトルと条件のリストを、該当する2つのテキストボックスに入力します。

その他のセキュリティ設定

[管理]→[システム設定]→[セキュリティ] 画面では次の機能も有効にできます。

- ["信頼された証明書の管理" on page 424](#)
- ["HTTPセキュリティヘッダの設定" on page 1075](#)

多要素認証の設定

Deep Security Managerでは、多要素認証 (MFA) を使用することができます。MFAはユーザ名とパスワードの他にも情報を必要とするアクセス管理方式であり、ベストプラクティスとして推奨されています。

このトピックの内容:

- ["多要素認証を有効にする" on the next page](#)
- ["多要素認証を無効にする" on page 1086](#)

- ["サポートされる多要素認証 \(MFA\) アプリケーション" on page 1087](#)
- ["MFAをトラブルシューティングする" on page 1088](#)

多要素認証を有効にする

1. Deep Security Managerで、右上に表示されるユーザ名の下メニューから [ユーザプロパティ] を選択します。
2. [一般] タブで [多要素認証の有効化...] ボタンをクリックします。多要素認証の有効化ウィザードが開くので、ウィザードの指示に従って作業を進めます。
3. ウィザードの最初の画面で、互換性がある仮想MFAアプリケーション (Google Authenticatorなど) をインストールするように求めるメッセージが表示されます。詳細については、この後の["サポートされる多要素認証 \(MFA\) アプリケーション" on page 1087](#)を参照してください。
4. デバイスがQRコードの読み取りに対応している場合は、カメラで読み取ってMFAアプリケーションを設定し、[次へ] をクリックします。

対応していない場合は、[QRコードの読み取りに対応していないため、手動設定用の秘密鍵を表示する]を選択します。

5. 認証コードをスペースなしで入力します。例: 228045。



6. 認証コードが正しければアカウントでMFAが有効になり、ログオン時に毎回新しいMFAコードの入力が要求されるようになります。

The screenshot shows the login interface for Trend Micro Deep Security. At the top, there is a dark header with the Trend Micro logo and the text 'Deep Security'. To the right of the header is a link for 'サポート情報' (Support Information). The main content area is titled 'ログオン' (Login). Below the title, there are four input fields: 1. 'ユーザー名' (Username) with the value 'MasterAdmin'. 2. 'パスワード' (Password) which is masked with black dots. 3. A checkbox labeled '多要素認証を使用する' (Use Multi-Factor Authentication) which is checked. 4. '認証コード' (Authentication Code) with the value '264387'. At the bottom right of the form is a blue button labeled 'ログオン' (Login).

多要素認証を無効にする

1. Deep Security Managerで、右上に表示されるユーザ名の下メニューから [ユーザプロパティ] を選択します。
2. [一般] タブで [MFAを無効にする] ボタンをクリックします。

3. 確認画面で [OK] をクリックしてMFAを無効にします。



4. ユーザプロパティ画面に、MFAが変更されたことを示すメッセージが表示されます。[OK] をクリックして画面を閉じます。

サポートされる多要素認証 (MFA) アプリケーション

MFAには以下のスマートフォンとアプリケーションの使用を推奨しますが、RFC 6238準拠のTime-base One-time Password Algorithmを実装するアプリケーションは機能します。

スマートフォン	MFAアプリ
Android	Google Authenticator 、 Duo
iPhone	Google Authenticator 、 Duo
Blackberry	Google Authenticator

MFAをトラブルシューティングする

MFAデバイスを有効にしても機能しない場合の対処

MFAログインに関する問題のほとんどは、Deep Security Managerの時間がデバイスと同期していないことが原因で発生します。

選択したOSの以下に示す手順に従って、時間が適切に同期しているかを確認してください。

Deep Security ManagerがLinuxの場合:

コマンドラインに「`ntpstat`」と入力して、NTPが正常に動作していることを確認します。現在のシステムの時刻と日付を表示するには、「`date`」と入力します。

Deep Security ManagerがWindowsの場合:

Windowsのタイムサービスが正常に動作していることを確認します。現在のシステムの時刻と日付を表示するには、コマンドラインに「`time`」および「`date`」と入力します。

MFAデバイスが紛失または動作停止した場合の対処

MFAデバイスが紛失、破損、あるいは動作を停止した場合は、アカウントのMFAを無効にしてログオンを可能にする必要があります。

1. ログオン資格情報の担当者に連絡し、"[多要素認証を無効にする](#)" on page 1086に記載されている手順を実行してもらいます (これでユーザ名とパスワードだけでログオンできるようになります)。
2. ログオン後、パスワードを変更します。
3. "[多要素認証を有効にする](#)" on page 1084に記載されている手順を実行します。

AWSリージョンの管理

Amazon Web Servicesのリージョンを追加する

AWSクラウドアカウント追加ウィザードを使用してクラウドアカウントを追加するときにEC2リソースをホストしているAmazon Web Services (AWS) のリージョンが表示されない場合は、このリージョンを手動で追加します。

Deep Security Managerをホストするサーバで、次のコマンドを入力します。

1. `dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT`

パラメータは次のとおりです。

パラメータ	説明	例
REGION	Amazon Web ServicesのリージョンID。	ca-east-1
DISPLAY	AWSクラウドアカウント追加ウィザードで使用するリージョンの表示文字列。	Canada East (Ottawa)
ENDPOINT	リージョンで使用するAmazon Elastic Compute Cloud (EC2) エンドポイントの完全修飾ドメイン名。	ec2.ca-east-1.amazonaws.com

注意: Deep Security ManagerがLinuxサーバ上で実行されている場合は、`sudo`でコマンドを実行するか、`root`などのスーパーユーザアカウントを使用します。

2. 特定のAWSリージョンで信頼された証明書をインポートする必要がある場合は (ほとんどありません)、"[信頼された証明書の管理](#)" on page 424を参照してください。

Amazon Web Servicesのリージョンを表示する

CLIを使用して追加したAWSリージョンを表示できます。

Deep Security Managerをホストするサーバで、次のコマンドを入力します。

```
dsm_c -action listregions
```

注意: Deep Security ManagerがLinuxサーバ上で実行されている場合は、sudoでコマンドを実行するか、rootなどのスーパーユーザアカウントを使用します。

Amazon Web Servicesのリージョンを削除する

CLIを使用して追加したAWSリージョンを削除できます。リージョンの既存のクラウドアカウントは削除されるまで引き続き使用できますが、管理者はそのリージョンに新しいクラウドアカウントを作成できなくなります。

1. Deep Security Managerをホストするサーバで、次のコマンドを入力します。

```
dsm_c -action listregions
```

2. 削除するリージョンのIDを検索します。
3. 次のコマンドを入力します。

```
dsm_c -action removeregion -region リージョン  
REGIONパラメータは必須です。
```

パラメータ	説明	例
REGION	Amazon Web ServicesのリージョンID。	ca-east-1

注意: Deep Security ManagerがLinuxサーバ上で実行されている場合は、sudoでコマンドを実行するか、rootなどのスーパーユーザアカウントを使用します。

アラートの設定

アラートは、管理者が実行したコマンドの失敗、ハードディスクの容量不足など、Deep Securityがユーザに注意を促す必要があるときに生成されます。Deep Securityには、定義済みの一連のアラートがあります (リストについては、"[事前定義アラート](#)" [on page 1249](#)を参照してください)。また、保護モジュールのルールを作成するときに、ルールがトリガされたときにアラートを生成するように設定できます。

どのアラートがトリガされたのかを確認するには、次の方法があります。

- Deep Security Managerの「アラートステータス」ダッシュボードウィジェットに表示します。
- Deep Security Managerの [アラート] 画面に表示します ("[Deep Security Managerにアラートを表示する](#)" [below](#)を参照)。
- アラートのトリガ時にメール通知を受け取ります ("[アラートのメール通知を設定する](#)" [on the next page](#)を参照)。
- アラートレポートを生成します ("[アラートやその他のアクティビティに関するレポートの生成](#)" [on page 1099](#)を参照)。

セキュリティイベントやシステムイベントと違って、アラートは一定期間後もデータベースから削除されません。手動または自動で消去されないかぎり、アラートは保持されます。

Deep Security Managerにアラートを表示する

Deep Security Managerの [アラート] 画面には、生成された未対応のアラートがすべて表示されます。アラートは、同じようなアラートをグループ化した概要ビュー、またはすべてのアラートを個別に一覧表示したリストビューで表示できます。これらの2つのビューを切り替えるには、画面のタイトルの [アラート] の横にあるメニューを使用します。また、時刻または重要度でアラートをソートできます。

概要ビューで、[詳細の表示] をクリックしてアラートパネルを展開すると、その特定のアラートを生成したコンピュータ (またはユーザ) がすべて表示されます。コンピュータをクリックすると、コンピュータの [詳細] 画面が表示されます。アラートが適用されるコンピュータが5台を超える場合、5台目のコンピュータの後ろに省略記号 (「...」) が表示されます。省略記号をクリックすると、リスト全体が表示されます。アラートに対して適切な処理を実行したら、対象のアラートの横にあるチェックボックスをオンにし、[消去] をクリックして、アラートを消去できます (リストビューでは、アラートを右クリックすると、ショートカットメニューにオプションのリストが表示されます)。

「Relayアップデートサービスを利用不可」などの消去できないアラートは、アラートの状態が解消されたときに自動的に消去されます。

注意: 同じコンピュータでアラートが表示されるイベントが複数回発生した場合は、最初に発生したときの時刻がアラートに表示されます。アラートの消去後にまた同じ状態が発生した場合は、消去後に最初に発生したときの時刻が表示されます。

ヒント: [コンピュータ] フィルタバーを使用して、特定のコンピュータグループ内のコンピュータや、特定のポリシーを保持するコンピュータなど、特定のコンピュータに関連するアラートのみを表示できます。

セキュリティイベントやシステムイベントと違って、アラートは一定期間後もデータベースから削除されません。手動または自動で消去されないかぎり、アラートは保持されます。

アラートを設定する

アラートを個別に設定するには、Deep Security Managerの [アラート] 画面に移動して、[アラートの設定] をクリックします。これにより、すべてのアラートのリストが表示されます。アラートの横にある緑色のチェックマークは、有効になっていることを意味します。該当する状況が発生した場合は、アラートがトリガされ、Deep Security Managerに表示されます。

アラートを選択して、[プロパティ] をクリックすると、重要度などのその他のアラート設定やメール通知設定を変更できます。

アラートのメール通知を設定する

Deep Security Managerでは、選択したアラートがトリガされた場合に、特定のユーザにメールを送信できます。

メール通知を有効にするには、次の手順に従います。

1. Deep Security ManagerにSMTPメールサーバへのアクセス権を付与します ("[メール通知のSMTPの設定](#)" on page 308を参照)。
2. どのアラートでメール通知を送信するかを指定します。たとえば、最も重大なアラートの場合のみメールを送信できます。初期設定では、ほとんどのアラートでメール通知が送信されます ("[アラートメールのオンとオフを切り替える](#)" on the next pageを参照します)。
3. メール通知の受信者を指定します。アラートメールを受信するようにユーザアカウントを設定できます ("[アラートメールを受信するユーザを個別に設定する](#)" on page 1099を参照)。また、アラートを設定してユーザのメールアカウントまたは配信リストを指定できます。このオプションを使用すると、ユーザアカウントの設定に関係なく、メールが送信されます ("[すべてのアラートメールの受信者を設定する](#)" on page 1099を参照)。

アラートメールのオンとオフを切り替える

Trend Micro Deep Security On-Premise 12.0

1. [アラート] 画面に移動し、[アラートの設定] をクリックしてアラートのリストを表示します。

アラート設定		グループ化しない ▼
プロパティ...		
アラート ▲	重要度	オン
⚠️ Agent/Applianceのアップグレードが必要	警告	✓
⚠️ Agent/Applianceのアップグレード推奨	警告	✓
⚠️ Agent/Applianceのアップグレード推奨 (新しいバージョンが使用可能)	警告	✓
⚠️ Agent/Applianceのアップグレード推奨 (非互換のセキュリティアップデ...	警告	✓
⚠️ Agent/Applianceのディスク容量の不足	警告	✓
⚠️ Agentのアップグレード推奨 (Applianceと非互換)	警告	✓
⚠️ Agentの設定パッケージが大きすぎる	警告	✓
❌ Agentインストールの失敗	重大	✓
⚠️ Agentソフトウェアのアップグレード失敗	警告	✓
⚠️ Azure ADアプリケーションのパスワードがまもなく期限切れ	警告	✓
❌ Azure ADアプリケーションの更新が必要	重大	✓
⚠️ Azureキーペアがまもなく期限切れ	警告	✓
❌ Azureキーペアの期限切れ	重大	✓
⚠️ CPUの警告しきい値の超過	警告	✓
❌ CPUの重大しきい値の超過	重大	✓
⚠️ Deep Security Managerソフトウェアのアップグレード推奨 (非互換のセ...	警告	✓
❌ Filter Driverとの接続失敗	重大	✓
⚠️ Filter Driverのアップグレード推奨 (新しいバージョンが使用可能)	警告	✓
⚠️ Managerがオフライン	警告	✓
⚠️ Managerのディスク容量不足	警告	✓
❌ Managerの時刻が非同期	重大	✓
❌ Relayアップデートサービスを利用不可	重大	✓

2. アラートの横にある緑色のチェックマークは、有効になっていることを意味します。該当する状況が発生した場合は、アラートがトリガされ、Deep Security Manager GUIに表示されます。アラートメールも受信する場合は、アラートをダブルクリックして [プロパティ] 画面を表示し、[メールの送信] チェックボックスを少なくとも1つオンにします。

一般

アラート情報

アラート: 不正プログラム対策アラート

説明: 1台以上のコンピュータで、アラートを発するように設定された不正プログラム検索設定によってイベントが発生しました。

消去可能: はい

オン
オンのとき、条件を満たす場合、アラートが発令されます。

オプション

 重要度:

(ルール設定に関係なく) すべてのルールでアラート

このアラートの発令時、通知のメールを送信する

このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

このアラートが存在しなくなったとき、通知のメールを送信する

 オフ
オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

OK キャンセル 適用

アラートメールを受信するユーザを個別に設定する

1. [管理]→[ユーザ管理]→[ユーザ] の順に選択し、ユーザアカウントをダブルクリックして [プロパティ] 画面を表示します。
2. [連絡先情報] タブで、メールアドレスを入力し、[アラートメールを受信] を選択します。

すべてのアラートメールの受信者を設定する

注意: 指定したアドレス、またはメール配信リストには、そのユーザアカウントのプロパティでメール通知の受信設定がされていなくても、すべてのアラートメールが送信されます。

1. [管理]→[システム設定]→[アラート] の順に選択します。
2. [アラートメールアドレス - すべてのアラートメールの送信先メールアドレス] で、メールアドレスまたは配信用のメールアドレスリストを指定します。

アラートやその他のアクティビティに関するレポートの生成

Deep Security Managerは、PDFまたはRTFの形式でレポートを生成します。ほとんどのレポートには、日付範囲、コンピュータグループ別のレポートなどの設定可能なパラメータがあります。パラメータのオプションは、それらが適用されないレポートの場合は無効になります。1回限りのレポート ("[単独レポートを設定する](#)" [below](#)を参照) を設定したり、レポートの実行を定期的にスケジュール設定したりできます ("[定期レポートを設定する](#)" [on page 1103](#))。"

単独レポートを設定する

1. Deep Security Managerで、[イベントとレポート] タブに移動し、左側の画面で [レポートの生成]→[単独レポート] の順にクリックします。
2. [レポート] リストで、生成するレポートの種類を選択します。使用している保護モジュールに応じて、次のレポートを利用可能です。

- アラートレポート: 最も一般的なアラートのリスト
- 不正プログラム対策レポート: 上位25台の感染コンピュータのリスト
- 攻撃レポート: 分析アクティビティを含む概要テーブル (モード別)。詳細については、[About attack reports](#)を参照してください。
- AWS従量課金レポート: インスタンスサイズとインストールの種類に応じて、1日あたりのAWS従量課金消費 (時間単位) をまとめた表
- コンピュータレポート: [コンピュータ] タブに表示される各コンピュータの概要
- 侵入防御ルールの推奨状況レポート: 侵入防御ルールの推奨設定。このレポートは、一度に1つのセキュリティポリシーまたはコンピュータでのみ実行できます。
- ファイアウォールレポート: ファイアウォールルールおよびステートフル設定アクティビティの記録
- コンピュータフォレンジックス監査レポート: コンピュータ上のAgentの設定
- 変更監視ベースラインレポート: 特定の時間におけるコンピュータのベースライン (タイプ、キー、フィンガープリントの日付)
- 変更監視の詳細な変更レポート: 検出された変更についての詳細
- 変更監視レポート: 検出された変更の概要
- 侵入防御レポート: 侵入防御ルールアクティビティの記録
- セキュリティログ監視の詳細レポート: 収集されたログデータの詳細
- セキュリティログ監視レポート: 収集されたログデータの概要
- 推奨設定レポート: 推奨設定の検索アクティビティの記録
- セキュリティモジュールの累積使用状況レポート: 保護モジュールの現在のコンピュータ使用状況 (累計と100件ごとの合計)
- セキュリティモジュールの使用状況レポート: 保護モジュールの現在のコンピュータ使用状況
- 概要レポート: Deep Securityアクティビティ全体の概要

- 不審なアプリケーション活動レポート: 不審なアクティビティについての情報
 - システムイベントレポート: システムアクティビティ (セキュリティ以外) の記録
 - システムレポート: コンピュータ、連絡先、ユーザの概要
 - テナントレポート: テナント概要
 - ユーザおよび連絡先レポート: ユーザと連絡先の内容およびアクティビティの詳細
 - Webレピュテーションレポート: Webレピュテーションイベントの多いコンピュータのリスト
3. レポートの [形式] で、PDFまたはRTFのどちらかを選択します。(「セキュリティモジュールの使用状況レポート」と「セキュリティモジュールの累積使用状況レポート」は例外で、常にCSV形式で出力されます)。
 4. PDFまたはRTFのレポートには、オプションで分類を追加することもできます。分類には、「空白」、「TOP SECRET」、「SECRET」、「CONFIDENTIAL」、「FOR OFFICIAL USE ONLY」、「LAW ENFORCEMENT SENSITIVE (LES)」、「LIMITED DISTRIBUTION」、「UNCLASSIFIED」、「INTERNAL USE ONLY」があります。
 5. [タグ] エリアで、イベントタグを使用してレポートをフィルタできます (イベントデータを含むレポートを選択した場合)。[すべて] はすべてのイベントを、[タグなし] はタグ付けされていないイベントのみを、[タグ] を選択して1つ以上のタグを指定すると指定したタグを含むイベントのみを、それぞれレポートに含めることができます。
- 注意:** 複数の矛盾するタグを適用すると、タグが組み合わさるのではなく、相互に影響を及ぼしてしまいます。たとえば、[ユーザのログオン]と[ユーザのログオフ]を選択すると、システムイベントが発生しません。
6. [期間] エリアで、ログの記録期間を任意に設定できます。これは、セキュリティ監査に役立ちます。期間のオプションは次のとおりです。
 - 過去24時間: 過去24時間のイベントが含まれます。正時 (0分0秒) に記録を開始および終了します。たとえば、12月5日の午前10:14にレポートを生成した場合、12月4日の午前10:00から12月5日の午前10:00の間に発生したイベントのレポートが作成されます。
 - 過去7日間: 過去1週間のイベントが含まれます。週の開始および終了は深夜0時です。たとえば、12月5日の午前10:14にレポートを生成する場合、11月28日の午前00:00から12月5日の午前00:00の間に発生したイベントのレポートが作成されます。

- 前月: 前月のイベントが含まれます。深夜0時に記録を開始および終了します。たとえば、11月15日にこのオプションを選択すると、10月1日の0時から11月1日の0時までに発生したイベントのレポートが送信されます。
- カスタム範囲: 任意の日付と時刻の範囲をレポートに指定できます。レポートでは、開始日が3日以上前の場合、開始時間が深夜0時に変更される可能性があります。
- **注意:** レポートには、カウンタに保存されたデータが使用されます。カウンタは、イベントから定期的に集計されたデータです。カウンタのデータは、最新の3日間は時間単位で集計されます。現在の時間のデータはレポートに含まれません。3日より古いデータは日単位で集計されてカウンタに保存されます。そのため、レポートでカバーされる期間は、最新の3日に関しては時間単位で指定できますが、3日より前になると日単位のみ指定可能になります。

7. [コンピュータ] エリアで、データをレポートに含めるコンピュータを選択します。

- すべてのコンピュータ: Deep SecurityManagerのすべてのコンピュータ
- マイコンピュータ: 特定のコンピュータのみの表示権限がある場合は、このオプションを選択すると、表示できるすべてのコンピュータが対象となります。
- グループ: Deep Securityグループのコンピュータ。
- 使用ポリシー: 選択したポリシー (およびオプションでそのサブポリシー) を使用しているコンピュータに、レポートの対象を限定できます。
- コンピュータ: レポートの対象を、選択した1台のコンピュータに限定できます。

注意: 複数のコンピュータグループから特定のコンピュータに関するレポートを生成するには、まず該当するコンピュータのみの閲覧権限があるユーザを作成し、「すべてのコンピュータ」レポートを定期的に生成する予約タスクを作成するか、作成したユーザでログオンして「すべてのコンピュータ」レポートを実行します。レポートには、そのユーザが閲覧できるコンピュータのみが記載されます。

8. [暗号化] エリアで、現在ログインしているユーザのパスワードか、レポートごとに設定された新規パスワードでレポートを保護できます。

- レポートのパスワードの無効化: レポートはパスワードで保護されません。
- 現在のユーザのレポートのパスワードの使用: 現在のユーザのPDFレポートのパスワードを使用します。ユーザのPDFレポートのパスワードを表示または変更するには、[管理]→[ユーザ管理]→[ユーザ]→[プロパティ]→[設定]→[レポート]に進みます。
- カスタムレポートのパスワードの使用: このレポートのワンタイムパスワードを作成します。パスワードに複雑さの要件はありません。

定期レポートを設定する

定期レポートとは、レポートを定期的に生成して、任意の数のユーザまたは連絡先宛てに配布する予約タスクのことです。

定期レポートを設定するには、[イベントとレポート] タブに移動し、左側の画面で [レポートの生成]→[定期レポート] の順にクリックします。[新規] をクリックします。新規予約タスクウィザードが開き、手順に従って設定プロセスを実行できます。ほとんどのオプションは前述の単独レポートと同じですが、[期間] オプションだけは例外です。

- 過去 [N] 時間: [N] に60未満の値を指定した場合、開始時刻と終了時刻は指定した時間の正時となります。[N] に60より大きな値を指定すると、指定した期間の開始時のデータは時間単位で集計されていないため、レポートの開始時刻は開始日の深夜0時 (00:00) に変更されます。
- 過去 [N] 日間: [N] 日前の深夜0時から現在の日付の深夜0時までのデータがレポートされます。
- 過去 [N] 週間: 過去 [N] 週間のイベントがレポートされます。開始および終了時刻は深夜0時 (00:00) です。

- 過去 [N] か月間: 過去 [N] か月間の暦月のイベントがレポートされます。開始および終了時刻は深夜0時 (00:00) です。たとえば、11月15日に「過去1か月間」を選択すると、10月1日の0時から11月1日の0時までに発生したイベントのレポートが送信されます。

注意: レポートには、カウンタに保存されたデータが使用されます。カウンタは、イベントから定期的に集計されたデータです。カウンタのデータは、最新の3日間は時間単位で集計されます。現在の時間のデータはレポートに含まれません。3日より古いデータは日単位で集計されてカウンタに保存されます。そのため、レポートでカバーされる期間は、最新の3日に関しては時間単位で指定できますが、3日より前になると日単位のみ指定可能になります。

予約タスクの詳細については、"[Deep Security予約タスクの設定](#)" on page 479を参照してください。

ダッシュボードのカスタマイズ

ダッシュボードは、Deep Security Managerにログインすると最初に表示される画面です。

ユーザは、ダッシュボードの内容とレイアウトを各自でカスタマイズできます。カスタマイズした設定は自動的に保存され、次回ログインしたときもダッシュボードに反映されます。データの期間およびデータを表示するコンピュータまたはコンピュータグループも設定できます。

アラートステータス

● 重大: 56 ● 警告: 4

最新のアラート:

アラート内容	期間
新しいパターンファイルアップデ...	6分
不正プログラム対策保護がよいか...	25分
不正プログラム対策コンポーネン...	25分
メモリの警告しきい値の超過	25分
空のRelayグループの割り当て - d...	25分

コンピュータのステータス

コンピュータのステータス

● 重大	0
● 警告	1
● 管理対象	49
● ロック	0
● 非管理対象	6

ユーザ情報の概要

MasterAdmin

役割: Full Access

総ログオン回数: 4

最終ログオン: 2016-08-17 12:03

前回のログオン: 2016-08-17 10:43

ランサムウェアのステータス

0 ランサムウェア イベント / 過去24時間

0 合計 ランサムウェア イベント / 過去過去13週間

ランサムウェアイベント履歴

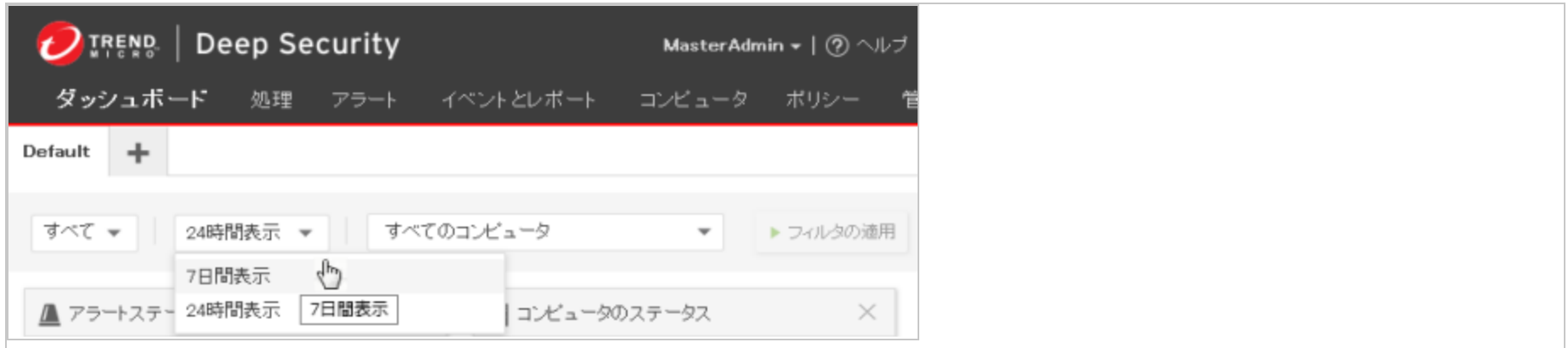
イベントの種類

- 不正プログラム対策
- Webレピュテーション
- 侵入防御
- 変更監視

時間: 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00

日時の範囲

ダッシュボードには、過去24時間または7日間のデータを表示できます。



コンピュータおよびコンピュータグループ

[コンピュータ] メニューを使用して、特定のコンピュータのデータのみが表示されるように表示データをフィルタします。たとえば、「Linux Server」セキュリティポリシーを使用しているコンピュータのみを表示できます。

タグごとのフィルタ

Deep Securityのタグは、イベント自体にもともと含まれていない属性を追加するために、イベントに適用できるメタデータの単位です。タグを使用すると、イベントをフィルタして、イベントの管理および監視タスクを簡素化できます。タグの一般的な目的は、処理が必要なイベントと、調査済みで安全であることがわかっているイベントを区別することです。

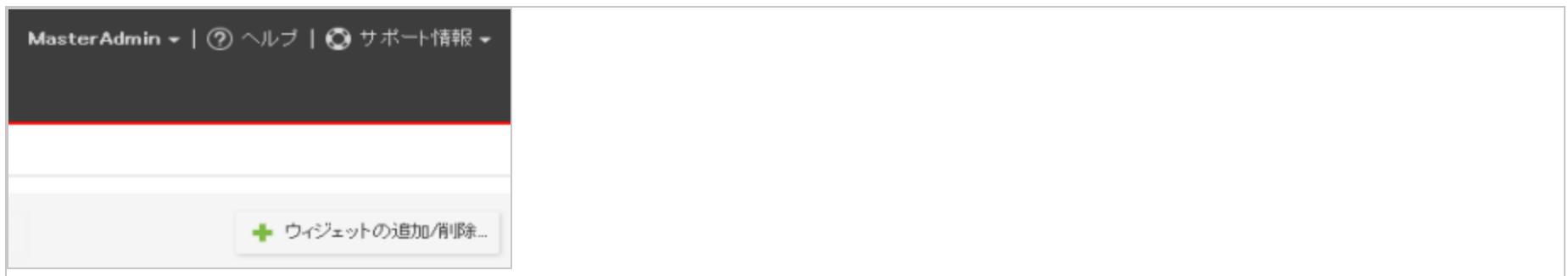
ダッシュボードに表示されるデータは、タグを使ってフィルタできます。



タグ付けの詳細については、"[イベントを識別およびグループ化するためのタグの適用](#)" on page 1129を参照してください。

ダッシュボードのウィジェットを選択する

[ウィジェットの追加/削除] をクリックし、ウィジェットの選択画面を表示して、表示するウィジェットを選択します。



注意: ウィジェットがダッシュボード上で1x1を超えるより大きなスペースを占める場合は、その寸法が名前の横に表示されません。

以下のウィジェットを使用できます。

監視:

- アクティビティ概要: 保護されている時間数やデータベースのサイズなど、アクティビティの概要。
- アラート履歴 [2x1]: 最近のアラート履歴を、アラートの重要度を含めて表示します。
- アラートステータス: 経過時間や重要度など、アラートの概要。
- コンピュータのステータス: コンピュータが管理対象であるか非管理対象であるかや、警告または重大なアラートがあるかどうかなど、コンピュータの概要。
- Managerノードのステータス [3x1]: Managerノード上の名前、CPU使用率、メモリ、ジョブ、およびシステムイベントを表示します。
- セキュリティアップデートのステータス: 最新の状態のコンピュータ、最新でない状態のコンピュータ、および不明なコンピュータの数など、コンピュータのアップデートのステータスを表示します。
- テナントのデータベース使用状況: データベースサイズによってランク付けされたテナントトップ5を表示します。
- テナントのジョブアクティビティ: ジョブの総数によってランク付けされたテナントトップ5を表示します。
- テナントの保護アクティビティ: 保護されている時間数でランク付けされたテナントトップ5を表示します。
- テナントのセキュリティイベントアクティビティ: セキュリティイベントの総数によってランク付けされたテナントトップ5を表示します。
- テナントのログオンアクティビティ: ログオンアクティビティによってランク付けされたテナントトップ5を表示します。
- テナントのシステムイベントアクティビティ: システムイベントの総数によってランク付けされたテナントトップ5を表示します。
- テナント: テナント数や保護されている時間数など、テナント情報を表示します。

システム:

- ログオン履歴: 過去50回のログオン試行と、それが成功したかどうかを表示します。
- ユーザ情報の概要 [2x1]: 名前、ロール、ログオン情報など、ユーザの概要を表示します。
- ソフトウェアアップデート: 最新の状態でないコンピュータを表示します。
- システムイベント履歴 [2x1]: 最近のシステムイベント履歴を、情報、警告、またはエラーとして分類されているイベントの数を含めて表示します。

ランサムウェア:

- ランサムウェアイベント履歴 [3x1]: 最近のランサムウェアのイベント履歴を、イベントの種類を含めて表示します。
- ランサムウェアのステータス: 過去24時間、過去7日間、または過去13週間に発生したランサムウェアイベントの数など、ランサムウェアのステータスを表示します。

不正プログラム対策:

- 不正プログラム対策イベント履歴 [2x1]: 最近の不正プログラム対策イベントの履歴を、イベントに対して実行されたアクションを含めて表示します。
- 不正プログラム対策の保護ステータス: コンピュータが保護されているか、保護されていないか、保護不可能かなど、コンピュータに対する不正プログラム対策の保護ステータスの概要を表示します。
- 不正プログラム対策のステータス (コンピュータ) [2x1]: 感染コンピュータのトップ5を、駆除できなかったファイルの数と影響を受けたファイルの総数を含めて表示します。
- 不正プログラム対策のステータス (不正プログラム) [2x1]: 検出された不正プログラムのトップ5を、不正プログラムの名前、駆除できなかったファイルの数、およびそれがトリガされた回数を含めて表示します。
- 不正プログラム検索のステータス [2x1]: 不正プログラムの予約検索が不完全だったアプライアンスのトップ5を表示します。

Webレピュテーション:

- Webレピュテーションのコンピュータのアクティビティ: Webレピュテーションイベントのあるコンピュータのトップ5を、イベント数を含めて表示します。
- Webレピュテーションイベント履歴 [2x1]: 最近のWebレピュテーションイベント履歴を、イベントの重要度を含めて表示します。
- WebレピュテーションのURLのアクティビティ: WebレピュテーションイベントをトリガしたURLのトップ5を、それらがアクセスされた回数を含めて表示します。

ファイアウォール:

- ファイアウォールのアクティビティ (検出): パケットが検出された理由のトップ5を、回数を含めて表示します。
- ファイアウォールのアクティビティ (防御): パケットが防御された理由のトップ5を、回数を含めて表示します。
- ファイアウォールコンピュータのアクティビティ (検出): 検出されたファイアウォールイベントを生成したコンピュータのトップ5と、イベントの発生回数を表示します。
- ファイアウォールコンピュータのアクティビティ (防御): 防御されたファイアウォールイベントを生成したコンピュータのトップ5と、イベントの発生回数を表示します。
- ファイアウォールイベント履歴 [2x1]: 最近のファイアウォールイベント履歴を、イベントが検出または防御されたかどうかを含めて表示します。
- ファイアウォールIPのアクティビティ (検出): 検出されたファイアウォールイベントを生成した送信元IPのトップ5と、イベントの発生回数を表示します。
- ファイアウォールIPのアクティビティ (防御): 防御されたファイアウォールイベントを生成した送信元IPのトップ5と、イベントの発生回数を表示します。
- ファイアウォールポートのアクティビティ (検出): 検出されたファイアウォールイベントの送信先ポートのトップ5と、イベントの発生回数を表示します。

- ファイアウォールポートのアクティビティ (防御): 防御されたファイアウォールイベントを生成したコンピュータのトップ5と、イベントの発生回数を表示します。
- 攻撃の予兆検索のアクティビティ: 検出された攻撃の予兆検索のトップ5と、検索の発生回数を表示します。
- 攻撃の予兆検索のコンピュータ: 攻撃の予兆検索が発生したコンピュータのトップ5と、検索の発生回数を表示します。
- 攻撃の予兆検索履歴 [2x1]: 最近の攻撃の予兆検索履歴を、発生した検索の種類を含めて表示します。

侵入防御:

- アプリケーションの種類のアクティビティ (検出): 検出されたアプリケーションの種類を、トリガされた回数を含めて表示します。
- アプリケーションの種類のアクティビティ (防御): 防御されたアプリケーションの種類を、トリガされた回数を含めて表示します。
- アプリケーションの種類ツリーマップ (検出) [2x2]: 検出されたアプリケーションの種類を、トリガされた回数、および各重要度の割合が表示されます。
- アプリケーションの種類ツリーマップ (防御) [2x2]: 防御されたアプリケーションの種類を、トリガされた回数、および各重要度の割合が表示されます。
- IPSのアクティビティ (検出): 侵入防御イベントが検出された理由のトップ5を、トリガされた回数を含めて表示します。
- IPSのアクティビティ (防御): 侵入防御イベントが防御された理由のトップ5を、トリガされた回数を含めて表示します。
- IPSコンピュータのアクティビティ (検出): 侵入防御イベントが検出されたコンピュータのトップ5を表示します。
- IPSコンピュータのアクティビティ (防御): 侵入防御イベントが防御されたコンピュータのトップ5を表示します。
- IPSイベント履歴 [2x1]: 最近の侵入防御イベント履歴を、イベントが検出または防御されたかどうかを含めて表示します。
- IPS IPのアクティビティ (検出): 検出された侵入防御イベントを生成した送信元IPのトップ5を表示します。
- IPS IPのアクティビティ (防御): 防御された侵入防御イベントを生成した送信元IPのトップ5を表示します。
- 最新のIPSのアクティビティ (検出): 最新のアップデート以降に侵入防御イベントが検出された理由のトップ5を表示します。

- 最新のIPSのアクティビティ (防御): 最新のアップデート以降に侵入防御イベントが防御された理由のトップ5を表示します。

変更監視:

- 変更監視のアクティビティ: 変更監視イベントが発生した理由のトップ5を、回数を含めて表示します。この場合、理由はトリガされたルールを示しています。
- 変更監視コンピュータのアクティビティ: 変更監視イベントが発生したコンピュータのトップ5を、イベントの数を含めて表示します。
- 変更監視イベント履歴 [2x1]: 最近の変更監視イベント履歴を、イベントの重要度を含めて表示します。
- 変更監視キーのアクティビティ: 変更監視イベントのキーのトップ5を表示します。キーのソースは、エンティティセットによって異なります。ファイルとディレクトリの場合はそのパスであり、ポートの場合は一意のプロトコル、IP、ポート番号、またはタプルです。

セキュリティログ監視:

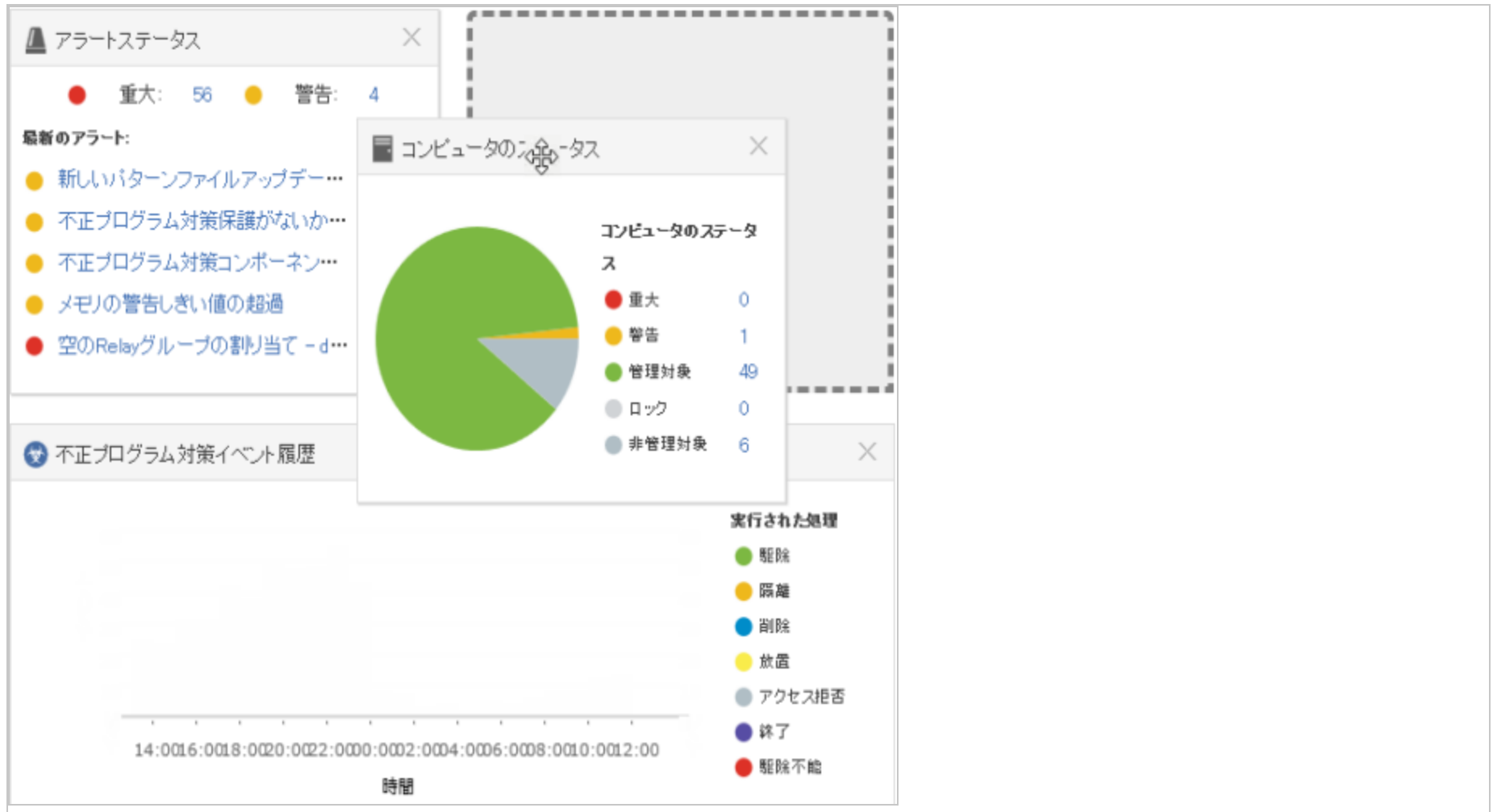
- セキュリティログ監視のアクティビティ: 変更監視イベントが発生した理由のトップ5を、数を含めて表示します。この場合、理由はトリガされたルールを示しています。
- セキュリティログ監視コンピュータのアクティビティ: セキュリティログ監視イベントが発生したコンピュータのトップ5を、イベントの数を含めて表示します。
- セキュリティログ監視の説明のアクティビティ: セキュリティログ監視イベントの説明のトップ5を、イベントの発生回数を含めて表示します。説明は、トリガされたイベントを示します。
- セキュリティログ監視イベント履歴 [2x1]: 最近のセキュリティログ監視イベント履歴を、イベントの重要度を含めて表示します。

アプリケーションコントロール:

- アプリケーションコントロールメンテナンスモードのステータス [2x1]: メンテナンスモードのコンピュータを、モードの開始および終了時刻を含めて表示します。

レイアウトを変更する

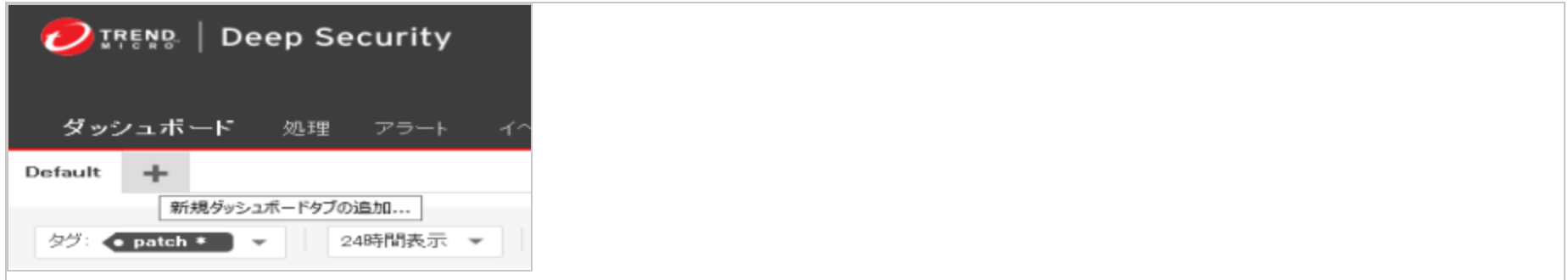
選択したウィジェットは、そのタイトルバーをドラッグすることによってダッシュボード上を移動できます。既存のウィジェットの上に選択したウィジェットを移動すると、それぞれのウィジェットの場所が入れ替わります(表示しようとしているウィジェットは、一時的にグレー表示になります)。



ダッシュボードのレイアウトを保存/管理する

複数のダッシュボードレイアウトを作成し、それぞれ別のタブとして保存できます。ログオフ後、ダッシュボードの設定とレイアウトを他のユーザが確認することはできません。新しいダッシュボードタブを作成するには、ダッシュボードの右端のタブに

ある「+」記号をクリックします。



Deep Securityのイベント

Deep Security Agentでは、保護モジュールのルールまたは条件がトリガされると「セキュリティイベント」が記録されます。また、AgentとDeep Security Managerでは、管理またはシステム関連のイベント (管理者のログインやAgentソフトウェアのアップグレードなど) が発生すると、「システムイベント」が記録されます。イベントのデータを使用して、Deep Security Managerの各種レポートやグラフが作成されます。

イベントを表示するには、Deep Security Managerの [イベントとレポート] に移動します。

Agentでのイベントログの場所

イベントログの場所はOSによって異なります。Windowsの場合は、次の場所に保存されます。

```
C:\Program Data\Trend Micro\Deep Security Agent\Diag
```

Linuxの場合は、次の場所に保存されます。

```
/var/opt/ds_agent/diag
```

注意: これらの場所に保存されるのは標準レベルのログのみで、診断デバッグレベルのログは別の場所に保存されます。パフォーマンス上の理由から、デバッグレベルのログは初期設定では無効になっています。デバッグログは、Trend Microのテクニカルサポートで問題を診断する場合にのみ有効にし、診断が終了したら必ず無効にしてください。

イベントがManagerに送信されるタイミング

コンピュータで発生するほとんどのイベントは、次のハートビート処理時にDeep Security Managerに送信されます。ただし、例外として、通信の設定で、Relay/Agent/Applianceから通信を開始できるようになっている場合、次のイベントはすぐに送信されます。

- スマートスキャンサーバがオフライン
- スマートスキャンサーバがオンライン復帰
- 変更監視検索が完了
- 変更監視のベースライン作成
- 変更監視ルール内に認識できないエレメント
- 変更監視ルールのエレメントがローカルプラットフォームでサポートされていない
- 異常な再起動の検出
- ディスク容量不足の警告
- セキュリティログ監視がオフライン
- セキュリティログ監視がオンライン復帰

- 攻撃の予兆検索の検出 ([コンピュータまたはポリシーエディタ](#)¹の [ファイアウォール]→[攻撃の予兆] で、設定が有効になっている場合)

イベントが保持される期間

イベントは、Deep Security Managerによって収集された後、[管理]→[システム設定]→[ストレージ] 画面で指定された一定の期間保持されます。詳細については、"[ログとイベントの保存に関するベストプラクティス](#)" on page 1122を参照してください。

システムイベント

Deep Securityのシステムイベントは、[管理]→[システム設定]→[システムイベント] タブで確認および設定できます。個々のイベントを記録するかどうか、またSIEMシステムに転送するかどうかを設定できます。システムイベントの詳細については、"[システムイベント](#)" on page 1271を参照してください。

セキュリティイベント

各保護モジュールでは、ルールがトリガされるか、その他の設定の条件が満たされると、イベントが生成されます。セキュリティイベント生成に関する一部の設定は変更が可能です。特定の種類のセキュリティイベントに関する詳細については、次のトピックを参照してください。

- "[不正プログラム対策イベント](#)" on page 1319
- "[検出した不正プログラムの確認と復元](#)" on page 778
- "[アプリケーションコントロールイベント](#)" on page 1317

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- ["ファイアウォールイベント" on page 1322](#)
- ["変更監視イベント" on page 1337](#)
- ["侵入防御イベント" on page 1331](#)
- ["セキュリティログ監視イベント" on page 1340](#)
- ["Webレピュテーションイベント" on page 1342](#)

コンピュータで有効になっているファイアウォールステートフル設定を変更して、TCP、UDP、およびICMPのイベントログを有効または無効にできます。ステートフルファイアウォール設定のプロパティを編集するには、[ポリシー]→[共通オブジェクト]→[その他]→[ファイアウォールステートフル設定]に移動します。ログのオプションは、ファイアウォールステートフル設定の[プロパティ]画面の[TCP]、[UDP]、[ICMP]の各タブにあります。ファイアウォールイベントの詳細については、["ファイアウォールイベント" on page 1322](#)を参照してください。

ポリシーまたはコンピュータに関連付けられたイベントを確認する

ポリシーエディタ¹と**コンピュータエディタ**²は、どちらも保護モジュールに[イベント]タブがあります。ポリシーエディタには、現在のポリシーに関連付けられたイベントが表示されます。コンピュータエディタには、現在のコンピュータに固有のイベントが表示されます。

イベントの詳細を表示する

イベントの詳細を確認するには、ダブルクリックします。

[一般] タブには次の項目が表示されます。

¹ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

²コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- 時刻: Deep Security Managerをホストするコンピュータ上のシステム時計に準じた時刻。
- レベル: 発生したイベントの重要度。イベントレベルには、情報、警告、エラーが含まれます。
- イベントID: イベントの種類に一意的識別子。
- イベント: イベントIDに関連付けられたイベントの名前。
- 対象: イベントに関連付けられたシステムオブジェクトは、ここで識別されます。オブジェクトのIDをクリックすると、オブジェクトのプロパティシートが表示されます。
- イベント送信元: イベントの送信元であるDeep Securityコンポーネント。
- 処理実行者: イベントをユーザが実行した場合は、そのユーザのユーザ名がここに表示されます。ユーザ名をクリックすると、[ユーザプロパティ]画面が表示されます。
- Manager: Deep Security Managerのコンピュータのホスト名。
- 説明: 必要に応じて、どのような処理が実行されてこのイベントがトリガされたのか、処理の詳細がここに表示されます。

[タグ] タブには、このイベントに関連付けられているタグが表示されます。イベントのタグ付けの詳細については、[ポリシー]→[共通オブジェクト]→[その他]→[タグ]、および"[イベントを識別およびグループ化するためのタグの適用](#)" on page 1129を参照してください。

リストをフィルタしてイベントを検索する

[期間] ツールバーでリストをフィルタし、特定の期間内に発生したイベントだけを表示できます。

[コンピュータ] ツールバーで、コンピュータグループ別またはコンピュータポリシー別にイベントログエントリを表示できます。

[検索]→[詳細検索を開く] をクリックすると、詳細検索バーの表示を切り替えることができます。

検索バーの右側にある「検索バーの追加」ボタン (+) をクリックすると、追加の検索バーが表示され、検索に複数のパラメータを適用できます。準備が整ったら、送信ボタン (ツールバーの右側にある上部に右矢印の付いたボタン) をクリックします。

イベントをエクスポートする

表示されたイベントはCSVファイルにエクスポートできます (ページの指定はできません。すべてのページがエクスポートされます)。表示されたリストをエクスポートするか、または選択したアイテムをエクスポートするかを選択できます。

ログのパフォーマンスを向上する

イベント収集のパフォーマンスを最大限にするためのヒントを以下に示します。

- 重要でないコンピュータのログ収集を減らすか、無効にします。
- ファイアウォールステートフル設定の [プロパティ] 画面でログオプションの一部を無効にして、ファイアウォールルール処理のログを削減することを検討します。たとえば、UDPログを無効にすると、「許可されていないUDP応答」のログエントリは除外されます。

ログとイベントの保存に関するベストプラクティス

ログおよびイベントのデータストレージのベストプラクティスは、PCIやHIPAAなど、満たす必要があるデータコンプライアンス規制に基づいています。また、データベースを最適に使用できるように考慮する必要があります。保存するデータが多すぎると、データベースのパフォーマンスやサイズの要件に影響する可能性があります。

データベースに保存するデータが多すぎると、次のような症状が発生することがあります。

- データベースの処理が実行されていない可能性を示すエラーメッセージが表示される
- ソフトウェアアップデートをインポートできない
- Deep Securityの処理が全般的に遅くなる

これらの症状を防ぐには、次の手順に従います。

1. 準拠する標準の要件に合わせて、保存するシステムイベントを設定します。
2. システムおよびセキュリティイベントを外部ストレージに転送します。"[Deep SecurityイベントをSyslogまたはSIEMサーバに転送する](#)" on page 1141を参照してください。これにより、ローカルデータベースでのイベント保持期間を短縮できるようになります。
3. セキュリティログ監視モジュールで、イベントの保存と転送に関するしきい値を設定します。[重要度のクリッピング]を使用すると、セキュリティログ監視ルールの重要度レベルに基づいて、イベントをSyslogサーバ (有効な場合) に送信、またはイベントを保存できます。詳細については、"[セキュリティログ監視イベントの転送と保存を設定する](#)" on page 907を参照してください。

次の表に、ローカルストレージの初期設定を示します。これらの設定を変更するには、[管理]→[システム設定]→[ストレージ]の順に選択します。ソフトウェアバージョンまたは古いルールアップデートを削除するには、[管理]→[アップデート]→[ソフトウェア]→[ローカル] または [管理]→[アップデート]→[セキュリティ]→[ルール] に移動します。

ヒント: データベースのディスク使用量を削減するには、イベントを外部SyslogサーバまたはSIEMに転送し、ローカルのイベント保持期間を短縮します。ローカルではカウンタのみを保持してください。

データタイプの設定	データ削除の初期設定
次の日数を経過した不正プログラム対策イベントを自動的に削除する	7日
次の日数を経過したWebレピュテーションイベントを自動的に削除する:	7日
次の日数を経過したファイアウォールイベントを自動的に削除する:	7日
次の日数を経過した侵入防御イベントを自動的に削除する:	7日
次の日数を経過した変更監視イベントを自動的に削除する:	7日
次の日数を経過したセキュリティログ監視イベントを自動的に削除する:	7日
次の日数を経過したアプリケーションコントロールイベントを自動的に削除する:	7日
次の期間を経過したシステムイベントを自動的に削除する:	53週間
次の期間を超過したサーバログを自動的に削除する:	7日
次の期間を経過したカウンタを自動的に削除する:	13週間
プラットフォームごとに保持しておく古いソフトウェアバージョンの数: *	5
保持しておく古いルールアップデートの数:	10

* マルチテナントが有効になっている場合、この設定は使用できません。

注意: PostgreSQLデータベースを使用している場合、古いイベントはただちに削除されない場合があります。古いイベントのデータベースパーティションはPostgreSQLメンテナンスジョブによって定期的に削除されます。削除は次の予約ジョブの実行中に行われます。

イベントは、個々のイベントのレコードです。イベントは [イベント] ページに表示されます。

カウンタは、個々のイベントが発生した回数です。カウンタはダッシュボードのウィジェット (過去7日間のファイアウォールイベントの数など) およびレポートに表示されます。

サーバログファイルはDeep Security ManagerのWebサーバのデータで、ネットワークのWebサーバにインストールされたAgentのイベントログは含まれません。

トラブルシューティング

トラブルシューティングの際にログレベルを上げてイベントをより詳細に記録すると、問題解決に役立つ場合があります。

ログレベルを上げると、ディスク使用量が大幅に増える可能性があります。トラブルシューティングが完了したら、ログレベルを再度下げてください。

1. **コンピュータまたはポリシーエディタ¹**を開きます。
2. [設定]→[一般]→[ログレベル] の順に選択します。
3. このコンピュータに割り当てられたポリシーからログ記録のオーバーライド設定を継承する場合は 継承、ログ記録の設定をオーバーライドしない場合は オーバーライドしない、トリガされたファイアウォールルールをすべて記録する場合は 完全なファイアウォールイベントのログ記録、トリガされた侵入防御ルールをすべて記録する場合は 完全な侵入防御イベントのログ記録、トリガされたルールをすべて記録する場合は 完全なログ記録 を選択します。
4. [保存] をクリックします。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ログファイルのサイズを制限する

個々のログファイルの最大サイズ、および保持される最新ファイルの数を指定できます。イベントログファイルは、最大許容サイズに達するまで書き込まれ、最大サイズに達すると新しいファイルが作成され、そのファイルが最大サイズに達するまで書き込まれます。最大ファイル数に達すると、最も古いファイルが削除され、その後、新しいファイルが作成されます。通常、イベントログエントリのサイズは平均約200バイトであるため、4MBのログファイルには約20,000ログエントリが保持されます。ログファイルがどのぐらいの期間でいっぱいになるかは、実行されるルールの数によって異なります。

1. 設定するポリシーの**コンピュータエディタ**または**ポリシーエディタ**¹を開きます。
2. [設定]→[詳細]→[イベント]の順に選択します。
3. 次のプロパティを設定します。
 - イベントログファイルの最大サイズ (Agent/Appliance):ログファイルの最大サイズです。このサイズに達すると、新しいファイルが作成されます。
 - 保管するイベントログファイル数 (Agent/Appliance):保持されるログファイルの最大数です。ログファイルの最大数に達すると、最も古いファイルが削除され、その後、新しいファイルが作成されます。
 - 次の送信元IPのイベントは記録しない:このオプションは、Deep Securityで特定の信頼されたコンピュータからのトラフィックのイベントが記録されないようにする場合に役立ちます。

注意: 集約されたイベントは、次の3つの設定で調整します。ディスク容量を節約するため、Deep Security AgentおよびApplianceは複数発生する同一イベントを1つのエントリに集約し、「繰り返し回数」および「初出現」と「最終出現」のタイムスタンプを追加します。イベントエントリを集約するために、Deep Security AgentおよびApplianceでは、エントリをメモリ内にキャッシュしてからディスクに書き込む必要があります。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- キャッシュサイズ: 指定された時間にいくつのイベントの種類を追跡するか決定します。値を10に設定すると、繰り返し回数、初出現、最終出現のタイムスタンプを付けた、10種類のイベントを追跡することになります。新規のイベントの種類が発生すると、最も古い10のイベントは集約され、キャッシュから消去されてディスクに書き込まれます。
- キャッシュの寿命: ディスクへ書き込まれる前に、どれだけの期間キャッシュに保存するかを決定します。値が10分に設定され、記録をフラッシュする状況が発生しなければ、10分を経過した記録はディスクへ書き込まれます。
- キャッシュの有効期間: 最近更新されていない繰り返し回数のレコードをどのくらいの期間保持しておくかを決定します。キャッシュの寿命が10分で有効期間が2分の場合、更新されずに2分経過したイベントのレコードはディスクへ書き込まれ、キャッシュから消去されます。

注意: 上記の設定にかかわらず、イベントがDeep Security Managerへ送信されるたびに、キャッシュは消去されます。

4. [保存] をクリックします。

イベントログのヒント

- 重要度が低いコンピュータのログ収集量を変更します。この設定は、**コンピュータエディタまたはポリシーエディタ**¹の [設定]→[詳細] タブにある、[イベント] エリアおよび [ネットワークエンジンの詳細オプション] エリアで変更できます。
- [ファイアウォールステートフル設定] のログオプションを無効にして、ファイアウォールルール処理のイベントログを削減することを検討します(たとえば、UDPログを無効にすると、未承諾UDPのログエントリが除外されます)。
- 侵入防御ルールの場合、破棄されたパケットのみをログに記録することをお勧めします。パケットの変更をログに記録すると、ログエントリが多くなりすぎることがあります。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- 侵入防御ルールの場合、特定の攻撃の挙動に関する調査が必要なときのみパケットデータを含めます (侵入防御ルールの [プロパティ] 画面のオプション)。すべてのパケットデータを含めることは、ログサイズが大きくなるので推奨されません。

不正プログラム検索の失敗イベント

次のセクションでは、不正プログラム検索の失敗イベントについて説明します。このイベントには、イベント発生時の処理に役立つ推奨される処理も含まれます。

注意: 手動検索、クイック検索、または予約検索で検索失敗イベントが発生することがあります。

イベントの理由	説明	推奨処理
空の設定	不正プログラム検索を開始できませんでした。これは、不正プログラム検索設定が空であるために発生します。	<ol style="list-style-type: none"> 1. コンピュータまたはポリシーエディタで、[不正プログラム対策]→[一般的な]の順に選択します。 2. 不正プログラム検索の設定が[予約検索]に割り当てられていることを確認してください。 3. 検索を再実行してください。
不正プログラム対策モジュールがオフです	不正プログラム検索を開始できませんでした。これは、不正プログラム対策モジュールがオフになっているためです。	<ol style="list-style-type: none"> 1. コンピュータまたはポリシーエディタで、[不正プログラム対策]→[一般的な]の順に選択します。 2. 不正プログラム対策の状態が「オン」または「継承(オン)」であることを確認します。 3. 検索を再実行してください。
不正プログラム対策サービスが停止します	不正プログラム対策サービスを終了中であるため、不正プログラム検索に失敗しました。	<ol style="list-style-type: none"> 1. コンピュータエディタまたはポリシーエディタで、[概要]→[一般的な]の順に選択し、[ステータスの確認]をクリックします。 2. 不正プログラム対策のステータスが「不正プログラム対策エンジンオフライン,」の場合、"エラー:

イベントの理由	説明	推奨処理
		<p>不正プログラム検索エンジンオフライン on page 1351 問題を解決する手順に従ってください。</p> <ol style="list-style-type: none"> 3. 検索を再実行してください。
不正プログラム対策エンジンがオフラインです	不正プログラム対策エンジンがオフラインであるため、不正プログラム検索に失敗しました。	<ol style="list-style-type: none"> 1. 次の手順に従って "エラー：不正プログラム検索エンジンオフライン on page 1351 問題を解決してください。 2. 検索を再実行してください。
設定にアクセスできません	不正プログラム検索にアクセスできませんでした。不正プログラム対策設定にアクセスできませんでした。(これは予期しない内部エラーまたはタイミングの問題が原因の可能性があります。)	<ol style="list-style-type: none"> 1. [コンピュータ] ページで、対象コンピュータを右クリックし、[処理] → [ポリシーの割り当て] に移動します。 2. 検索を再実行してください。
その他の検索タスクが実行中です。	他の検索タスクが実行中であるため、不正プログラムの検索に失敗しました。(これは予期しない内部エラーまたはタイミングの問題が原因の可能性があります。)	<ol style="list-style-type: none"> 1. [コンピュータ] ページで、別の不正プログラム検索が実行中かどうかを対象コンピュータの[タスク]列で確認します。 2. 検出された場合は、現在の検索タスクが完了するまで待機するか、対象コンピュータを右クリックして、[処理] → [不正プログラム検索のキャンセル] に移動します。 3. 検索を再実行してください。
エージェントの不明な理由	不明な理由により、不正プログラム検索に失敗しました。	<ol style="list-style-type: none"> 1. システムイベント情報を収集し、"診断パッケージとログの作成 on page 1573 をログに記録します。 2. サポート担当者 にお問い合わせください。

イベントを識別およびグループ化するためのタグの適用

Deep Securityでは、イベントを特定したりソートしたりするときに使用するタグを作成できます。たとえば、タグを使用して、安全なイベントと調査の必要があるイベントを区別できます。また、ダッシュボードのカスタマイズやレポートの作成にも使用できます。

イベントのタグ付けはさまざまな目的に使用できますが、本来の目的はイベント管理の負担を軽減することです。あるイベントを分析して安全であると判断した場合は、コンピュータ (および構成やタスクが類似しているその他のコンピュータ) のイベントログを調べて、類似イベントを検索し、同じラベルを適用できます。こうすると、各イベントを個別に分析する必要がなくなります。

現在使用中のタグを表示するには、[ポリシー]→[共通オブジェクト]→[その他]→[タグ] の順に選択します。

注意: タグによってイベント自体のデータが変更されることや、ユーザにイベントの削除が許可されることはありません。タグはManagerによって指定される追加属性です。

タグ付けには次の方法があります。

- **"手動によるタグ付け" on the next page:** 必要に応じて特定のイベントをタグ付けできます。
- **"自動タグ付け" on the next page:** 既存イベントをモデルとして使用し、同一または別のコンピュータの類似イベントに自動でタグ付けします。「類似性」のパラメータを定義するには、タグを適用する場合にモデルイベントの属性と一致する必要があるイベント属性を選択します。
- **"信頼済みのソースを使用したタグ付け" on page 1132:** 信頼済みのソースの既知のイベントとの類似性に基づいて、変更監視イベントに自動でタグ付けします。

注意: 標準のタグ付けと信頼済みのソースを使用したタグ付けには重要な違いがあります。[今すぐ既存のイベントに実行] を実行できるのは、標準のタグ付けのみです。

手動によるタグ付け

1. [イベント]→[レポート]→[イベント]の順に選択し、イベントリストを選択します。イベントを右クリック (または複数のイベントを選択して右クリック) し、[タグを追加] をクリックします。
2. タグの名前を入力します。Deep Security Managerによって、入力した名前に一致する既存のタグの候補が表示されます。
3. [選択された [イベントの種類] イベント] を選択します。[次へ] をクリックします。
4. 必要に応じてコメントを記入し、[完了] をクリックします。

イベントリストの [タグ] 列にタグが表示されます。

自動タグ付け

Deep Security Managerでは、類似イベントに同じタグを自動的に適用するルールを定義できます。保存済みの既存の自動タグ付けルールを表示するには、任意の [イベント] 画面で、メニューバーの [自動タグ付け] を選択します。この画面から、保存済みのルールを手動で実行できます。

1. [イベント]→[レポート]→[イベント]の順に選択し、イベントリストを選択します。ベースにするイベントを右クリックし、[タグの追加] を選択します。
2. タグの名前を入力します。Deep Security Managerによって、入力した名前に一致する既存のタグの候補が表示されます。
3. [選択されたものと類似の [イベントの種類] イベントに適用] を選択し、[次へ] をクリックします。
4. イベントの自動タグ付けを行うコンピュータを選択し、[次へ] をクリックします。システムイベントへのタグの適用時には、このページはスキップされます。
5. イベントの類似性を判定する基準となる属性を選択します。属性オプションは [イベント] リスト画面の列に表示される情報とほとんど同じです。イベントの選択処理に含めるための属性を選択したら、[次へ] をクリックします。
6. 次の画面で、イベントにタグを付けるタイミングを指定します。[既存の [イベントの種類] イベント] を選択した場合は、[今すぐ自動タグルールを適用する] を選択して自動タグ付けルールをすぐに適用するか、[バックグラウンドで自動タグルールを適用する] を選択し、優先度を下げてバックグラウンドで実行するかを選択できます。今後発生するイベントに自動タグ付けルールを適用するには、[今後の [イベントの種類] イベント] を選択します。また、[自動タグルールの保存] を選択して必要に応じて名前を入力することで、自動タグ付けルールを保存することもできます。[次へ] をクリックします。
7. 自動タグ付けルールの概要を確認し、[完了] をクリックします。

イベントリストで、ベースにしたイベントおよび同様のすべてのイベントにタグが付けられていることを確認できます。

注意: イベントのタグ付けが実行されるのは、AgentまたはApplianceから取得されたイベントがDeep Security Managerのデータベースに登録された後です。

自動タグ付けルールに優先度を設定する

自動タグ付けルールを作成したら、[優先度] 値を割り当てることができます。将来のイベントに自動タグ付けルールを適用するように設定した場合、設定された自動タグ付けルールを受信イベントに適用する順番は、ルールの優先度によって決まります。たとえば、すべての「ユーザのログオン」イベントに自動タグ付けルール「suspicious」をタグ付けする優先度が「1」のルールと、対象 (ユーザ) が自分自身であるすべての「ユーザのログオン」イベントから「suspicious」タグを削除する優先順位が「2」のルールを設定したとします。この結果、将来発生するすべての「ユーザのログオン」イベントのうち、ユーザが自分以外のものに「suspicious」タグが適用されます。

1. イベントリストで、[自動タグ付け] をクリックして、保存済みの自動タグ付けルールのリストを表示します。
2. 自動タグ付けルールを右クリックし、[詳細] をクリックします。
3. [一般] タブで、ルールの [優先度] を選択します。

セキュリティログ監視イベントを自動でタグ付けする

セキュリティログ監視イベントは、ログファイル構造内でのグループに基づいて自動でタグ付けされます。これにより、Deep Security Manager内のセキュリティログ監視イベントの処理が簡略化および自動化されます。セキュリティログ監視グループのタグを自動的に付加するには、自動タグ付けを使用します。セキュリティログ監視ルールのグループは、ルールに関連付けられています。次に例を示します。

```
<rule id="18126" level="3">
  <if_sid>18101</if_sid>
  <id>^20158</id>
  <description>Remote access login success</description>
  <group>authentication_success,</group>
</rule>
```

```
<rule id="18127" level="8">  
<if_sid>18104</if_sid>  
<id>^646|^647</id>  
<description>Computer account changed/deleted</description>  
<group>account_changed,</group>  
</rule>
```

それぞれのグループ名には、わかりやすい名前の文字列が関連付けられています。上記の例では、「authentication_success」には「Authentication Success」、「account_changed」には「Account Changed」が関連付けられています。このチェックボックスを設定すると、そのイベントのタグとして、このわかりやすい名前が自動的に追加されます。複数のルールがトリガされる場合は、複数のタグがイベントに追加されます。

信頼済みのソースを使用したタグ付け

注意: 信頼済みのソースを使用したイベントのタグ付けは、変更監視保護モジュールによって生成されたイベントにのみ使用できます。

変更監視モジュールを使用すると、コンピュータ上のシステムコンポーネントおよび関連属性に関する変更を監視できます。

「変更」には編集だけでなく、作成と削除も含まれます。変更を監視できるコンポーネントには、ファイル、ディレクトリ、グループ、インストールされたソフトウェア、待機ポート番号、プロセス、レジストリキーなどがあります。

分析の必要があるイベントの数を削減するには、信頼済みのソースを使用したイベントのタグ付けを指定して、許可された変更に関連するイベントが自動識別されるように設定します。

変更監視モジュールでは、類似イベントの自動タグ付けだけでなく、[信頼済みのソース]で検出されたイベントやデータの類似性に基づいてイベントにタグ付けできます。信頼済みのソースには、次のいずれかを使用できます。

1. 信頼済みのローカルコンピュータ
2. トレンドマイクロの[ソフトウェア安全性評価サービス]
3. 信頼済みの共通ベースライン。コンピュータグループから収集された、ファイルのステータスのセットです。

信頼済みのローカルコンピュータ

信頼済みのコンピュータは、安全なイベントまたは無害なイベントのみを生成することが判明している、「モデル」コンピュータとして使用されるコンピュータです。「対象」コンピュータは、不正な、または予想外の変更が発生しないか監視されているコンピュータです。自動タグ付けルールでは、対象コンピュータのイベントが調査され、これらのイベントと信頼済みのコンピュータのイベントが比較されます。一致するイベントがあった場合は、これらのイベントに自動タグ付けルールで定義されたタグが付けられます。

保護されているコンピュータのイベントと信頼済みのコンピュータのイベントを比較する、自動タグ付けルールを設定できます。たとえば、あるパッチの計画済みロールアウトを、信頼済みのコンピュータに適用するとします。パッチの適用に関連するイベントには「Patch X」のタグを付けることができます。その他のシステムで発生した類似イベントには自動でタグ付けをして許容される変更として識別し、フィルタで除外して評価が必要なイベント数を減らすことができます。

対象コンピュータのイベントと信頼済みのソースコンピュータのイベントの一致をDeep Securityで判別する仕組み

変更監視イベントには、状態の変化に関する情報が含まれています。つまり、イベントにはイベント前およびイベント後の情報が含まれています。イベントを比較すると、自動タグ付けエンジンによってイベント前後の状態が比較されます、2つのイベントでイベント前後の状態が同じ場合、これらのイベントは一致すると判定され、2番目のイベントにタグが適用されます。これは作成および削除イベントにも当てはまります。

注意: 信頼済みのソースを使用したイベントのタグ付けに、信頼済みのコンピュータを使用している場合は、変更監視ルールによって生成されたイベントにタグが付けられます。つまり、変更監視ルールを使用して対象コンピュータでイベントを生成している場合は、この変更監視ルールを信頼済みソースのコンピュータでも実行する必要があります。

注意: 信頼済みのソースを使用したイベントのタグ付けを適用する前に、信頼済みのソースのコンピュータで不正プログラムを検索する必要があります。

注意: Linuxのprelinkingのような、システムのファイルの中身を定期的に変更するユーティリティは、信頼済みのソースを使用したイベントのタグ付けと干渉することがあります。

信頼済みのローカルコンピュータに基づいてイベントにタグを付ける

1. 信頼済みのコンピュータで不正プログラム対策のフルスキャンを実行し、不正プログラムがないことを確認します。
2. イベントを自動的にタグ付けするコンピュータで、信頼済みソースのコンピュータと同じ (または部分的に同じ) 変更監視ルールを実行していることを確認します。
3. Deep Security Managerで、[イベントとレポート]→[変更監視イベント]に進み、ツールバーの [自動タグ付け] をクリックします。
4. [自動タグルール (変更監視イベント)] 画面で [新しい信頼済みのソース] をクリックし、タグウィザードを表示します。
5. [信頼済みのローカルコンピュータ] を選択して [次へ] をクリックします。
6. リストから信頼済みソースとして使用するコンピュータを選択し、[次へ] をクリックします。
7. 信頼済みソースコンピュータのイベントに一致した対象コンピュータのイベントに割り当てるタグを、1つ以上指定します。[次へ] をクリックします。

注意: 新しいタグをテキストで入力するか、既存のタグのリストから選択します。

8. 信頼済みソースとイベントを照合する対象コンピュータを指定します。[次へ] をクリックします。
9. オプションで、ルールの名前を指定し、[完了] をクリックします。

トレンドマイクロのソフトウェア安全性評価サービスに基づいてイベントにタグを付ける

ソフトウェア安全性評価サービスは、トレンドマイクロが管理している既知の正常なファイルの署名のリストです。このタイプの信頼済みソースのタグ付けでは、対象コンピュータにファイル関連の変更監視イベントが発生していないかが監視されます。イベントが記録された場合は、変更後のファイルの署名が、信頼できる既知のトレンドマイクロのファイル署名リストと比較されます。一致が見つかったら、イベントにタグが付けられます。

1. Deep Security Managerで、[イベントとレポート]→[変更監視イベント]に進み、ツールバーの [自動タグ付け] をクリックします。
2. [自動タグルール (変更監視イベント)] 画面で [新しい信頼済みのソース] をクリックし、タグウィザードを表示します。

3. ソフトウェア安全性評価サービスを選択して [次へ] をクリックします。
4. ソフトウェア安全性評価サービスに一致した場合に対象コンピュータのイベントに割り当てるタグを、1つ以上指定します。 [次へ] をクリックします。
5. ソフトウェア安全性評価サービスとイベントを照合する対象コンピュータを指定します。 [次へ] をクリックします。
6. オプションで、ルールの名前を指定し、 [完了] をクリックします。

信頼済みの共通ベースラインに基づいてイベントにタグを付ける

信頼済みの共通ベースライン方式では、コンピュータグループ内でイベントを比較します。コンピュータグループが特定されると、グループ内のコンピュータで有効になっている変更監視ルールの監視対象のファイルおよびシステムのステータスに基づいて、共通ベースラインが生成されます。グループ内のあるコンピュータで変更監視イベントが発生した場合、変更後の署名が共通ベースラインと比較されます。ファイルの新しい署名と一致するものが共通ベースライン内にある場合、イベントにタグが付加されます。信頼済みのコンピュータ方式では変更監視イベントの前と後のステータスが比較されますが、信頼済みの共通ベースラインでは、イベント後のステータスだけが比較されます。

注意: この方法では、共通グループ内のすべてのコンピュータが、保護されていて不正プログラムがないことを前提とします。共通ベースラインが生成される前に、グループ内のすべてのコンピュータで不正プログラム対策のフルスキャンを実行してください。

注意: あるコンピュータに対して変更監視のベースラインが生成されると、Deep Securityは、そのコンピュータが信頼済みの共通ベースライングループに含まれているかどうかを最初に確認します。信頼済みの共通ベースライングループに含まれている場合、コンピュータのベースラインデータを、グループの信頼済みの共通ベースラインに追加します。これにより、共通ベースライングループのコンピュータに変更監視ルールが適用される前に、信頼済みの共通ベースラインの自動タグ付けルールが実施されます。

1. 信頼済みの共通ベースラインを構成するコンピュータグループに追加するすべてのコンピュータで、不正プログラム対策のフルスキャンを実行し、不正プログラムがないことを確認します。
2. Deep Security Managerで、 [イベントとレポート] → [変更監視イベント] に進み、ツールバーの [自動タグ付け] をクリックします。

3. [自動タグルール (変更監視イベント)] 画面で [新しい信頼済みのソース] をクリックし、タグウィザードを表示します。
4. [信頼済みの共通ベースライン] を選択して [次へ] をクリックします。
5. 信頼済みの共通ベースラインに一致した場合にイベントに割り当てるタグを1つ以上指定します。[次へ] をクリックします。
6. 信頼済みの共通ベースラインの生成に使用するグループに含めるコンピュータを特定します。[次へ] をクリックします。
7. オプションで、ルールの名前を指定し、[完了] をクリックします。

タグを削除する

1. イベントリストで、削除するタグが付いたイベントを右クリックし、[タグの削除] を選択します。
2. 削除するタグを選択します。[選択された [イベントの種類] イベント] からタグを削除するか、[選択されたものと類似の [イベントの種類] イベントに適用] を選択します。[次へ] をクリックします。
3. 必要に応じてコメントを記入し、[完了] をクリックします。

ログに記録するイベントの数を減らす

ログに記録するイベント数を減らすため、Deep Security Managerでは複数ある詳細なログ記録ポリシーモードのいずれかで動作するように設定することができます。これらのモードは、**コンピュータまたはポリシーエディタ**¹の [設定]→[詳細]→[ネットワークエンジンの詳細設定] エリアで設定できます。

次の表に、詳細なログ記録ポリシーモードのより複雑な4つについて、どのイベントのタイプが無視されるかを示します。

モード	無視するイベント
ステートフルおよび正規化の抑制	セッション情報なし 不正なフラグ 不正なシーケンス

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

モード	無視するイベント
	不正なACK 許可されていないUDP応答 許可されていないICMP応答 ポリシーで未許可 再送の破棄
ステートフル、正規化、およびフラグメントの抑制	セッション情報なし 不正なフラグ 不正なシーケンス 不正なACK 許可されていないUDP応答 許可されていないICMP応答 ポリシーで未許可 CEフラグ 不正なIP 不正なIPデータグラム長 フラグメント化 不正なフラグメントオフセット 最初のフラグメントが最小サイズ未満 範囲外のフラグメント 最小オフセット値以下のフラグメント IPv6パケット 受信接続の上限 送信接続の上限 SYN送信の上限 ライセンスの期限切れ 不明なIPバージョン 不正なパケット情報 ACK再送の上限 切断された接続上のパケット 再送の破棄
ステートフル、フラグメント、および検証機能の抑制	セッション情報なし 不正なフラグ 不正なシーケンス

モード	無視するイベント
	不正なACK 許可されていないUDP応答 許可されていないICMP応答 ポリシーで未許可 CEフラグ 不正なIP 不正なIPデータグラム長 フラグメント化 不正なフラグメントオフセット 最初のフラグメントが最小サイズ未満 範囲外のフラグメント 最小オフセット値以下のフラグメント IPv6パケット 受信接続の上限 送信接続の上限 SYN送信の上限 ライセンスの期限切れ 不明なIPバージョン 不正なパケット情報 不正なデータオフセット IPヘッダなし 読み取り不能なイーサネットヘッダ 未定義 送信元および送信先IPが同一 不正なTCPヘッダ長 読み取り不能なプロトコルヘッダ 読み取り不能なIPv4ヘッダ 不明なIPバージョン ACK再送の上限 切断された接続上のパケット 再送の破棄
タップモード	セッション情報なし 不正なフラグ 不正なシーケンス 不正なACK

モード	無視するイベント
	ACK再送の上限 切断された接続上のパケット 再送の破棄

イベントのランク付けによる重要度の数値化

ランク付けシステムでは、イベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、ルールに重要度またはリスクの値を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度(ランク)が計算されます。これによって、イベントをランクでソートできます。

注意: 他のモジュールと異なり、不正プログラムはイベントの重要度をランク付けするために資産価値を使用しません。

Webレピュテーションイベントのリスク値

Webレピュテーションイベントのリスク値は、Webレピュテーションのページの[General]タブでWebレピュテーションの設定で使用される3つのレベルのリスクにリンクされます。

- 危険: 「不正、または脅威の既知の発信源であると確認されたURL」に相当
- 非常に不審: 「不正または脅威の発信源である可能性が疑われたURL」に相当
- 不審: 「スパムメールに関連付けられている、または感染している可能性のあるURL」に相当
- 管理者によるブロック: Webレピュテーションサービスのブロックリストに含まれているURL
- 未評価: リスクレベルが設定されていないURL

ファイアウォールルールの重大度の値

ファイアウォールルールの重大度の値は、拒否、ログのみ、およびパケット拒否の各処理にリンクされます。（後者は、ファイアウォールのステートフルな設定。）のために拒否されたパケットを参照します。このパネルを使用して、ファイアウォールイベントの順位を決定するコンピュータの資産価値に乘算される重大度値を編集します。（ファイアウォールルールの処理は、ルールの[プロパティ][]ウィンドウで表示および編集できます。.)

侵入防御ルールの重大度の値

侵入防御のルールの重要度の値は、重要度レベル（重大、高、中、低、またはエラー）にリンクされます。このパネルを使用して、侵入防御イベントの順位を決定するためにコンピュータの資産額を乗算する値を編集します。侵入防御ルールの重大度の設定は、ルールの[プロパティ][]画面で確認できます。

整合性監視ルールの重大度値

変更監視ルールの重要度の値は、重要度レベル（重大、高、中、低）にリンクされます。このパネルを使用して値を編集します。この値はコンピュータの資産価値で乗算され、変更監視イベントの順位が決定されます。変更監視ルールの重大度は、ルールの[プロパティ][]画面で確認できます。

検査ルールの重大度の値の記録

[Log inspection]のルールの重大度の値は、重要度レベル（[重大]、[高]、[中]、または[低]）にリンクされています。このパネルを使用して値を編集します。この値はコンピュータの資産価値と乗算され、ログ検査イベントの順位が決定されます。ログ検査ルールの重大度レベルは、ルールの Properties 画面から確認および編集できます。

資産評価

アセット値は、侵入防御ルールやファイアウォールルールなど、他のプロパティと関連付けられていません。資産評価は、それ自体がプロパティです。コンピュータの資産評価は、コンピュータの [詳細] 画面から表示および編集できます。資産評価の割り当て処理を簡略化するために、コンピュータの最初の [詳細] 画面の [資産の重要度] リストに表示される値の一部を事前定義できます。既存の事前定義されたコンピュータの資産評価を表示するには、このパネルの [資産評価の表示] ボタンをクリックします。[資産評価] 画面に、事前定義された設定が表示されます。これらの値は変更可能で、新しい値を作成できます(新しい設定は、すべてのコンピュータのリストに表示されます)。

Deep SecurityイベントをSyslogまたはSIEMサーバに転送する

イベントは、外部のSyslogサーバまたはSecurity Information and Event Management (SIEM) サーバに送信できます。これは、集中管理された監視、カスタムレポート、またはDeep Security Managerのローカルディスクの空き容量の確保に役立ちます。

注意: 外部サーバへのイベント転送を有効にしても、Deep Security Managerはシステムおよびセキュリティイベントをローカルに記録し、レポートやグラフに表示します。したがって、ディスクの空き容量を減らす必要がある場合は、イベント転送では不十分です。[イベントをローカルに保持する期間](#)も設定する必要があります。

ヒント: または、イベントをAmazon SNSに公開する場合は、["Amazon SNSでのイベントへのアクセス" on page 1200](#)でのイベントのアクセスを参照してください。

基本的な手順は次のとおりです。

1. ["イベント転送ネットワークトラフィックを許可する" on the next page](#)
2. ["クライアント証明書を要求する" on the next page](#)
3. ["Syslog設定を定義する" on the next page](#)
4. ["システムイベントを転送する" on page 1146](#) または ["セキュリティイベントを転送する" on page 1146](#)

イベント転送ネットワークトラフィックを許可する

すべてのルータ、ファイアウォール、およびセキュリティグループでは、Deep Security Managerからの受信トラフィック（およびセキュリティイベントの直接転送のために、エージェントからの受信トラフィック）をSyslogサーバに送信する必要があります。["ポート番号、URL、およびIPアドレス" on page 190](#)も参照してください。

クライアント証明書を要求する

イベントを安全に転送するには (TLS), を使用し、Syslogサーバでクライアント認証が必要な場合は クライアントの（サーバではない）証明書の署名要求 (CSR.) を生成する必要があります。Deep Security Managerは、クライアントとしてSyslogサーバに接続する際に、この証明書を使用して自身を識別および認証します。クライアント証明書の要求方法の詳細については、CA (CA.) にお問い合わせください。

注意: 一部のSyslogサーバでは、自己署名サーバ証明書を使用できません (Deep Security Managerの初期設定の).など) CA署名されたクライアント証明書が必要です。

Syslogサーバが信頼するCA、または証明書が信頼されたルートCAによって直接的または間接的に署名された中間CAのいずれかを使用します。（これは「信頼チェーン」または「署名チェーン」.）とも呼ばれます。

CAから署名された証明書を受信すると、CA証明書をDeep Security Managerにアップロードするために、["Syslog設定を定義する" below](#)を続行します。

Syslog設定を定義する

Syslog設定では、システムイベントまたはセキュリティイベントの転送時に使用できる宛先と設定を定義します。

2017年1月26日より前にSIEMまたはSyslogを設定した場合、Syslog設定に変換されています。同じ設定がマージされました。

1. [Policies]→[Common Objects]→[Other]→[Syslog Configurations]→の順に選択します。
2. [新規]→[新規設定] の順にクリックします。

3. [General]タブで、次の項目を設定します。

- 名前： 設定を識別する一意の名前。
- 説明: 設定の説明 (オプション)。
- ログのソースID： Deep Security Managerのホスト名の代わりに使用するオプションの識別子。

Deep Security Managerがマルチノードの場合、各サーバノードのホスト名はそれぞれ異なります。したがって、ログソースIDは異なる場合があります。IDがホスト名に関係なく同じである必要がある場合（たとえば、フィルタ目的の）、では、ここで共有ログソースIDを設定できます。

この設定は、Deep Security Agentによって直接送信されるイベントには適用されません。このイベントは、ログオン元IDとして常にホスト名が使用されます。

- サーバ名： 受信SyslogサーバまたはSIEMサーバのホスト名またはIPアドレス。
- サーバポート： SIEMまたはSyslogサーバ上のポート番号を待機します。UDPの場合、IANA標準のポート番号は514です。通常、UDPにはポート6514、"[ポート番号、URL、およびIPアドレス](#)" on page 190も参照してください。
- トランスポート： トランスポートプロトコルが安全である（TLS）かどうか（UDP.)

UDPの場合、Syslogメッセージは64 KBに制限されます。長いメッセージの場合は、データが切り捨てられることがあります。

TLSの場合、マネージャとSyslogサーバはお互いの証明書を信頼する必要があります。ManagerからSyslogサーバへの接続は、TLS 1.2,1.1、または1.0で暗号化されます。

注意:

TLS では、Deep Security Manager でログを転送するように設定する必要があります (間接の).エージェントはTLSでの転送をサポートしていません。

- イベントの形式： ログメッセージの形式がLEEF、CEF、またはBasic Syslogのいずれであるか。 "[syslogメッセージの形式](#)" on page 1149

注意: LEEF format では、エージェントが Deep Security Manager 経由でログを転送するように設定する必要があります。

注意: 基本Syslog形式は、Deep Securityの不正プログラム対策、Webレピュテーション、変更監視、およびアプリケーション制御ではサポートされません。

- イベントにタイムゾーンを含めます。 イベントに完全な日付（年と時間帯を含む）を追加するかどうかを指定します。

例（選択された）: 2018-09-14T01:02:17.123 +04:00。

例（選択解除された）: Sep 14 01:02:17。

注意: 日付を指定するには、エージェントがログをDeep Security Managerに転送するように設定する必要があります（間接的）。

- ファシリティ： イベントが関連付けられるプロセスのタイプ。 Syslogサーバは、ログメッセージの機能フィールドに基づいて優先順位を付けたり、フィルタを適用したりできます。 関連項目 [Syslogの機能とレベルとは](#)
- エージェントはログを転送する必要があります： イベントを送信するかどうか Syslogサーバ または に直接接続する Deep Security Manager 経由で（間接的に）。

ログをSyslogサーバに直接転送する場合、クライアントはクリアテキストUDPを使用します。ログには、セキュリティシステムに関する機密情報が含まれています。インターネットなどの信頼されていないネットワークを介してログを送信する場合は、VPNトンネルなどを追加して偵察や改ざんを防止することを検討してください。

注意: Managerを介してログを転送する場合、ファイアウォールおよび侵入防御パケットデータは含まれません。ただし、Deep Security Managerを設定しない限り、そのデータは含まれません。手順については、[Deep Security Manager \(DSM\)](#) によるSyslogへのパケットデータの送信を参照してください。

4. TLSクライアントがクライアント認証を行うことをSyslogサーバまたはSIEMサーバで要求する場合（バイラテラルまたは相互認証とも呼ばれます。"[クライアント証明書を要求する](#)" on page 1142), 要求を参照し、[Credentials]タブで次の項目を設定します)。
 - 秘密鍵： Deep Security Managerのクライアント証明書の秘密鍵を貼り付けます。
 - 証明書： Deep Security ManagerがSyslogサーバへのTLS接続で自身を識別するために使用する クライアントの 証明書を貼り付けます。Base64エンコード形式とも呼ばれるPEMを使用します。
 - 証明書チェーン： 中間CAがクライアント証明書に署名したが、SyslogサーバがそのCAを認識して信頼しない場合は、CA証明書を貼り付けて証明書を信頼するルートCAに関連付けます。各CA証明書の間Enterキーを押します。
5. [Apply] をクリックします。
6. TLS転送メカニズムを選択した場合は、Deep Security ManagerとSyslogサーバの両方が互いの証明書に接続して信頼できることを確認します。
 - a. [接続テスト] をクリックします。

Deep Security Managerは、ホスト名の解決と接続を試行します。失敗した場合は、エラーメッセージが表示されません。

Deep Security ManagerによってSyslogまたはSIEMサーバ証明書がまだ信頼されていない場合、接続は失敗し、サーバ証明書を受け入れられますか？ メッセージが表示されます。このメッセージには、Syslogサーバの証明書の内容が表示されます。
 - b. Syslogサーバの証明書が正しいことを確認してから、[OK]をクリックして認証を受け入れられます。

証明書は、の[Administration]→[System Settings]→[Security]で、管理者の信頼された証明書のリストに追加されま
す。Deep Security Managerは自己署名証明書を受け入れることができます。

c. [接続のテスト]をもう一度クリックします。

今すぐTLS接続が成功する必要があります。

7. 続行するには、転送するイベントを選択します。"[システムイベントを転送する](#)" below and/or "[セキュリティイベントを
転送する](#)" belowを参照してください。

システムイベントを転送する

Deep Security Managerは、システムイベント（管理者ログインやエージェントソフトウェア).のアップグレードなど）を生成し
ます。

1. [管理]→[システム設定]→[イベントの転送]に進みます。
2. システムイベントを、設定を使用してリモートコンピュータ（Syslog経由）に転送する場合は、既存の設定を選択する
か、[新規]を選択します。詳細については、"[Syslog設定を定義する](#)" on page 1142の定義を参照してください。
3. [Save]をクリックします。

注意: Deep Security Managerがマルチノードである場合、システムイベントは1つのノードからのみ送信され、重複が回避さ
れます。

セキュリティイベントを転送する

Deep Security Agentの保護機能は、セキュリティイベントを生成します（不正プログラムの検出やIPSルールの起動など）。
次のいずれかのイベントを転送できます。

- 直接
- 間接的に、Deep Security Manager経由で

[一部のイベント転送オプション](#)では、Deep Security Manager経由で間接的にエージェントイベントを転送する必要があります。

他のポリシー設定と同様に、特定のポリシーまたはコンピュータのイベント転送設定を無効にすることもできます。["ポリシー、継承、およびオーバーライド" on page 587](#)を参照してください。

1. [ポリシー] に移動します。
2. コンピュータで使用されているポリシーをダブルクリックします。
3. Settings を選択し、[Event Forwarding] タブを選択します。
4. From Eventの送信間隔、イベントの転送間隔を選択します。
5. の不正プログラム対策のSyslog設定 とその他の保護モジュールのドロップダウンメニューから、使用するSyslog設定を選択するか、の[編集]をクリックして変更するか、なしを選択して無効にするか、[New]をクリックします。詳細については、["Syslog設定を定義する" on page 1142](#)の定義を参照してください。
6. [保存] をクリックします。

イベント転送のトラブルシューティング

「Syslogメッセージの送信に失敗」アラート

Syslog設定に問題がある場合、次のアラートが表示されることがあります。

```
Failed to Send Syslog Message
The Deep Security Manager was unable to forward messages to a Syslog Server.
Unable to forward messages to a Syslog Server
```

このアラートには、該当するSyslog設定へのリンクも記載されています。リンクをクリックして設定を開き、[Test Connection]をクリックして詳細な診断情報を取得します。接続が成功したことを示すか、原因に関する詳細が記載されたエラーメッセージが表示されます。

Syslog設定を編集できません

Syslog設定を表示できても編集することができない場合は、アカウントに関連付けられた役割に適切な権限が割り当てられていないことが考えられます。役割を設定できる管理者は、[管理]→[ユーザ管理]の順に選択して権限を確認できます。ユーザ名を選択して[プロパティ]をクリックします。Syslog設定を編集できるかどうかは、[その他の権限] タブの [Syslog設定] の設定で制御されます。ユーザと役割の詳細については、"[ユーザの作成と管理](#)" on page 1376を参照してください。

証明書が期限切れのためにSyslogが転送されない

有効な証明書は、TLS経由で安全に接続するために必要です。TLSクライアント認証を設定しても証明書の有効期限が切れた場合、メッセージはSyslogサーバに送信されません。この問題を修正するには、新しい証明書を取得し、Syslog設定を新しい証明書の値でアップデートし、接続をテストしてから設定を保存します。

サーバ証明書が期限切れであるか変更されたためにSyslogが配信されない

有効な証明書は、TLS経由で安全に接続するために必要です。Syslogサーバの証明書が期限切れまたは変更されている場合は、Syslog設定を開き、[接続テストのテスト]をクリックします。新しい証明書を受け入れるように求められます。

互換性

Deep Securityは次のエンタープライズ版でテスト済みです。

- Splunk 6.5.1
- IBM QRadar 7.2.8 Patch 3 (TLSプロトコルパッチのPROTOCOL-TLSSyslog-7.2-20170104125004.noarchを適用)
- HP ArcSight 7.2.2 (ArcSight-7.2.2.7742.0-Connectorツールを使用して作成されたTLS Syslog-NGコネクタを使用)

他の標準のSyslogソフトウェアも動作する可能性がありますが、検証されていません。

ヒント: Splunkを使用している場合は、[Deep Security app for Splunk](#)ダッシュボードと保存された検索を取得します。

syslogメッセージの形式

Common Event Format (CEF) と Log Event Extended Format (LEEF) のログメッセージ形式は少し異なります。たとえば、GUI の [送信元ユーザ] 列に対応するフィールドは、CEFでは「suser」で、LEEFでは「userName」です。ログメッセージのフィールドは、イベントが Deep Security エージェントまたは Manager で発生したかどうか、およびログメッセージが作成された機能によって異なります。

注意: Syslogメッセージが切り捨てられている場合は、User Datagram Protocol (UDP) を使用していることが原因である可能性があります。切り捨てを防止するには、代わりに Transport Layer Security (TLS) 経由で Syslogメッセージを転送します。TLSに切り替える手順については、"[Syslog設定を定義する](#)" on page 1142を参照してください。

注意: 基本的な Syslog形式は、不正プログラム対策、Webレピュテーション、整合性監視、およびアプリケーション制御の保護モジュールではサポートされていません。

Syslogメッセージがマネージャから送信される場合、いくつかの違いがあります。元の Deep Security Agent ホスト名 (イベントのソース) を維持するため、新しい拡張 (「dvc」または「dvchost」) が使われます。「dvc」はホスト名が IPv4 アドレスの場合、「dvchost」はホスト名が IPv6 アドレスの場合に使用されます。さらに、イベントにタグが付けられている場合は、「TrendMicroDsTags」という拡張子が使用されます。(これは、今後の run を使用した自動タグ付けにのみ適用されます。イベントは Syslog 経由で転送されるのは、マネージャ。)によって収集されるためです。マネージャから中継されるログの製品は、引き続き「Deep Security エージェント";」と表示されます。ただし、製品バージョンはマネージャのバージョンです。

CEFのsyslogメッセージの形式

イベントの元の Deep Security Agent ソースを特定するために、すべての CEF イベントに「dvc = IPv4 Address」または「dvchost = Hostname」(「または「IPv6 address」が含まれます。この拡張子は、Deep Security Virtual Appliance または Manager から送信されるイベントにとって重要です。この場合、メッセージの Syslog 送信者はイベントの発信者ではないためです。

Trend Micro Deep Security On-Premise 12.0

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

Deep Security ManagerとDeep Security Agentのどちらからのログエントリかを判断するには、「デバイス製品 (Device Product)」フィールドを確認します。

CEFログエントリのサンプル: Jan 18 11:07:53 dsmhost CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|Administrator Signed In|4|suser=Master...

注意: Virtual Applianceで保護されていて、Agentで保護されていない仮想マシンで発生したイベントも、Agentからのイベントとして識別されます。

イベントをトリガしたルールの種類を判断するには、「署名ID (Signature ID)」フィールドと「名前 (Name)」フィールドを確認します。

ログエントリのサンプル: Mar 19 15:19:15 root CEF:0|Trend Micro|Deep Security Agent|<DSA version>|123|Out Of Allowed Policy|5|cn1=1...

次の「署名ID (Signature ID)」の値は、トリガされたイベントの種類を示します。

署名ID	説明
10	カスタムIPS（侵入防御）ルール
20	ログのみのファイアウォールルール
21	ファイアウォールルールの拒否
30	カスタム変更監視ルール
40	カスタムログ検査ルール
100-7499	システムイベント
100-199	ポリシーファイアウォールルールとファイアウォールステートフル設定
200-299	IPSの内部エラー
300-399	SSL/TLSイベント
500-899	IPSの正規化
1,000,000-1,999,999	トレンドマイクロのIPSルール。署名IDは、IPSルールIDと同一です。

Trend Micro Deep Security On-Premise 12.0

署名ID	説明
2,000,000-2,999,999	整合性監視ルール。署名IDは、変更監視ルールID + 1,000,000です。
3,000,000-3,999,999	ログ検査ルール。署名IDは、[Log Inspection]ルールID + 2,000,000です。
4,000,000-4,999,999	不正プログラム対策イベント。現在は、以下の署名IDのみが使用されています。 <ul style="list-style-type: none"> • 4,000,000 - 不正プログラム対策 - リアルタイム検索 • 4,000,001 - 不正プログラム対策 - 手動検索 • 4,000,002 - 不正プログラム対策 - 予約検索 • 4,000,003 - 不正プログラム対策 - クイック検索 • 4,000,010 - スパイウェア対策 - リアルタイム検索 • 4,000,011 - スパイウェア対策 - 手動検索 • 4,000,012 - スパイウェア対策 - 予約検索 • 4,000,013 - スパイウェア対策 - クイック検索 • 4,000,020 - 不審なアクティビティ - リアルタイム検索 • 4,000,030 - 不正変更 - リアルタイム検索
5,000,000-5,999,999	Webレピュテーションイベント。現在は、以下の署名IDのみが使用されています。 <ul style="list-style-type: none"> • 5,000,000 - Webレピュテーション - ブロック • 5,000,001 - Webレピュテーション - 検出のみ
6,000,000-6,999,999	アプリケーション制御イベント。現在は、以下の署名IDのみが使用されています。 <ul style="list-style-type: none"> • 6,001,100 - アプリケーションコントロール - ブロックリスト内の検出のみ • 6,001,200 - アプリケーションコントロール - 検出のみ、未許可のリスト • 6,002,100 - アプリケーションコントロール - ブロックリスト (ブロックリスト内) • 6,002,200 - アプリケーションコントロール - 許可リストに含まれていないブ

署名ID	説明
	ロック

注意: 次のイベントログの形式の表に示すすべてのCEF拡張が必ずしも各ログエントリに含まれているわけではありません。また、CEF拡張の順序が常に同じであるとは限りません。正規表現を使用してエントリを解析する場合は、表にある各キーと値のペアがあることを前提としたり、またはその順序に依存したりしないようにしてください。

注意: Syslogメッセージは、Syslogプロトコル仕様によって最大64KBに制限されています。長いメッセージの場合は、データが切り捨てられることがあります。Basic Syslog形式は、最大1KBに制限されています。

LEEF 2.0のsyslogメッセージの形式

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEF 2.0ログエントリのサンプル (DSMシステムイベントログのサンプル): LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPUWarning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity:Warning TrendMicroDsTenant=Primary

マネージャーから発信されたイベント

システムイベントログの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|User Signed In|3|src=10.52.116.160 suser=admin target=admin msg=User signed in from 2001:db8::5

Trend Micro Deep Security On-Premise 12.0

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEF 2.0ログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning TrendMicroDsTenant=Primary

注意: LEEF形式では、重要度を示す「sev」という予約キーと、名前を示す「name」という予約キーが使用されます。

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
src	src	Source IP Address	Deep Security ManagerのIPアドレス。	src=10.52.116.23
suser	usrName	Source User	Deep Security Managerの管理者のアカウント。	suser=MasterAdmin
target	target	Target Entity	イベントの件名。Deep Security Managerまたはコンピュータにログインした管理者アカウントである可能性があります。	target=MasterAdmin target=server01
targetID	targetID	Target Entity ID	Managerで追加された識別子。	targetID=1
targetType	targetType	Target Entity Type	イベントの対象のエンティティの種類。	targetType=Host
msg	msg	Details	システムイベントの詳細。イベントの詳細な説明が含まれる場合があります。	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...
TrendMicroDsTags	TrendMicroDsTags	Event Tags	イベントに割り当てられたDeep Securityのイベントタグ	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant	Deep Securityのテナント	TrendMicroDsTenant=Primary

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
		Name		
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=3
None	cat	Category	イベントのカテゴリ	cat=System
None	name	Name	イベント名	name=Alert Ended
None	desc	Description	イベントの説明	desc:Alert: CPUの警告しきい値の超過

Agentで発生するイベント

不正プログラム対策イベントの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|4000000|Eicar_test_file|6|cn1=1
cn1Label=Host ID dvchost=hostname cn2=205 cn2Label=Quarantine File Size cs6=ContainerImageName | ContainerName
| ContainerID cs6Label=Container filePath=C:\\Users\\trend\\Desktop\\eicar.exe act=Delete msg=Realtime
TrendMicroDsMalwareTarget=N/A
TrendMicroDsMalwareTargetType=N/TrendMicroDsFileMD5=44D88612FEA8A8F36DE82E1278ABB02F
TrendMicroDsFileSHA1=3395856CE81F2B7382DEE72602F798B642F14140
TrendMicroDsFileSHA256=275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_
CERBER.C;Ransom_CRYPNISCA.SM

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF: 2.0|Trend Micro|Deep Security Agent|<DSA version>|4000030|cat=Anti-Malware
name=HEU_AEGIS_CRYPT desc=HEU_AEGIS_CRYPT sev=6 cn1=241 cn1Label=Host ID dvc=10.0.0.1 TrendMicroDsTags=FS

Trend Micro Deep Security On-Premise 12.0

TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 filePath=C:\\Windows\\System32\\virus.exe act=Terminate
 msg=Realtime TrendMicroDsMalwareTarget=Multiple TrendMicroDsMalwareTargetType=File System
 TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E#011
 TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1#011
 TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E
 TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_
 CERBER.C;Ransom_CRYPNISCA.SM

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agent コンピュータの一意の内部識別子。	cn1=1
cn1Label	cn1Label	Host ID	フィールド cn1 の名前ラベル。	cn1Label=Host ID
cn2	cn2	File Size	検出 ファイルのサイズ。	cn2=100
cn2Label	cn2Label	File Size	フィールド cn2 の名前ラベル。	cn2Label=Quarantine File Size
cs3	cs3	Infected Resource	スパイウェア アイテムのパ	cs3=C:\\test\\atse_samples\\SPYW_Test_Virus.exe

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			ス。このフィールドはスパイウェア検出イベント専用です。	
cs3Label	cs3Label	Infected Resource	フィールドcs3の名前ラベル。このフィールドはスパイウェア検出イベント専用です。	cs3Label=Infected Resource
cs4	cs4	Resource Type	Resource Typeの値: 10=ファイルとディレ	cs4=10

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			クトリ	
			11=システムレジストリ	
			12=インターネットCookie	
			13=インターネットURLショートカット	
			14=メモリ内のプログラム	
			15=プログラム起動領域	

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			16=ブラウザヘルパーオブジェクト	
			17=レイヤーサービスプロバイダ	
			18=hostsファイル	
			19=Windowsポリシー設定	
			20=ブラウザ	
			23=Windowsシェル	

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			設定 24=IEで ダウン ロード したプ ログラ ムファ イル 25=プ ログラ ムの追 加/削除 26= サービ ス その他= その他 たとえ ば、シ ステム の再起 動後も	

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			スパイウェアファイルを継続させるためにレジストリ実行キーを作成する spy.exe という名前のスパイウェアファイルがある場合、スパイウェアのレポートには次	

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			<p>spy.exe のアイ テムは cs4=10 (ファイ ルと ディレ クト リ)、実 行キー のアイ テムは cs4=11 (システ ムレジ ストリ) となり ます。</p> <p>この フィー ルドは スパイ ウェア 検出イ ベント 専用で す。</p>	

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cs4Label	cd4Label	Resource Type	フィールドcs4の名前ラベル。このフィールドはスパイウェア検出イベント専用です。	cs4Label=Resource Type
cs5	cs5	Risk Level	リスクレベルの値: 0=超低 25=低 50=中 75=高 100=超高 このフィールドはスパイ	cs5=25

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			ウェア 検出イ ベント 専用で す。	
cs5Label	cs5Label	Risk Level	フィー ルドcs5 の名前 ラベ ル。こ の フィー ルドは スパイ ウェア 検出イ ベント 専用で す。	cs5Label=Risk Level
cs6	cs6	Conta iner	不正プ ログラ ムが検 出され た Docker コンテ ナの一 メー ジ名、 コンテ ナ名、 コンテ ナID。	cs6=ContainerImageName ContainerName ContainerID

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cs6Label	cs6Label	Container	フィールドcs6の名前ラベル。	cs6Label=Container
filePath	filePath	File Path	不正プログラムファイルの場所。	filePath=C:\\Users\\Mei\\Desktop\\virus.exe
act	act	Action	不正プログラム対策エンジンによって実行された処理。値には、Deny、Access、Quarantine、Delete、Pass、Clean、Terminate、Unspecifiedが	act=Clean act=Pass

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			あります。	
msg	msg	Message	検索の種類。値には、Realtime、Scheduled、Manualがあります。	msg=Realtime msg=Scheduled
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchos	dvc=10.1.144.199

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			tを使用 しま す)。	
dvchost	dvchost	Device host name	cn1の ホスト 名また はIPv6 アドレ ス。 送信元 がIPv4 アドレ スの場 合は表 示され ません (代わり にdvc フィー ルドを 使用し ます)。	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5
TrendMicroDsTags	TrendMicroDsTags	Event s tags	イベン トに割 り当て られた Deep Securit	TrendMicroDsTags=suspicious

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			yのイベントタグ	
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityのテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID	TrendMicroDsTenantId=0
TrendMicroDsMalwareTarget	TrendMicroDsMalwareTarget	Target(s)	不正プログラムが操作を試みた対象のファイル、プロセス、またはレジストリキー(ある場合)。不正プログラムの対象	TrendMicroDsMalwareTarget=N/A TrendMicroDsMalwareTarget=C:\\Windows\\System32\\cmd.exe TrendMicroDsMalwareTarget=HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings TrendMicroDsMalwareTarget=Multiple

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			<p>が複数に及ぶ場合、このフィールドの値は「Multiple」になります。</p> <p>このフィールドの値が報告されるのは、不審なアクティビティと不正な変更を監視している場合だけで</p>	

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
TrendMicroDsMalwareTargetType	TrendMicroDsMalwareTargetType	TargetType	<p>す。</p> <p>この不正プログラムが操作を試みたシステムリソースの種類。</p> <p>ファイルシステム、プロセス、Windowsレジストリなどです。</p> <p>このフィールドの値が報告され</p>	<p>TrendMicroDsMalwareTargetType=N/A</p> <p>TrendMicroDsMalwareTargetType=Exploit</p> <p>TrendMicroDsMalwareTargetType=File System</p> <p>TrendMicroDsMalwareTargetType=Process</p> <p>TrendMicroDsMalwareTargetType=Registry</p>

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			るのは、不審なアクティビティと不正な変更を監視している場合だけです。	
TrendMicroDsFileMD5	TrendMicroDsFileMD5	File MD5	ファイルのMD5ハッシュ。	TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E
TrendMicroDsFileSHA1	TrendMicroDsFileSHA1	File SHA1	ファイルのSHA1ハッシュ。	TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1
TrendMicroDsFileSHA256	TrendMicroDsFileSHA256	File SHA256	ファイルのSHA256ハッシュ。	TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E
TrendMicroDsDetectionConfidence	TrendMicroDsDetectionConfidence	Threat Probability	ファイルが不正プログラム	TrendMicroDsDetectionConfidence=95

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			モデルと一致する割合(%表示)を示します。	
TrendMicroDsRelevantDetectionNames	TrendMicroDsRelevantDetectionNames	ProbableThreatType	機械学習型検索が分析を他の既知の脅威(セミコロン「;」で区切る)と比較した後、ファイルに含まれる脅威の最も可能性の高い種類を示します。	TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM
None	sev	Severity	イベントの重要度。重要度は1が最も低	sev=6

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			く、10が最も高くなります。	
None	cat	Category	Category	cat=Anti-Malware
None	name	Name	イベント名	name=SPYWARE_KEYL_ACTIVE
None	desc	Description	イベントの説明。不正プログラム対策では、イベント名が説明として使用されます。	desc=SPYWARE_KEYL_ACTIVE

アプリケーション制御イベントの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF: 0|Trend Micro|Deep Security Agent|10.2.229|6001200|AppControl detectOnly|6|cn1=202 cn1Label=Host ID dvc=192.168.33.128 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 fileHash=80D4AC182F97D2AB48EE4310AC51DA5974167C596D133D64A83107B9069745E0 suser=root suid=0 act=detectOnly filePath=/home/user1/Desktop/Directory1//heartbeatSync.sh fsize=20 aggregationType=0 repeatCount=1 cs1=notWhitelisted cs1Label=actionReason

Trend Micro Deep Security On-Premise 12.0

```
cs2=0CC9713BA896193A527213D9C94892D41797EB7C cs2Label=sha1 cs3=7EA8EF10BEB2E9876D4D7F7E5A46CF8D
cs3Label=md5
```

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|10.0.2883|60|cat=AppControl
 name=blocked desc=blocked sev=6 cn1=2 cn1Label=Host ID dvc=10.203.156.39 TrendMicroDsTenant=Primary
 TrendMicroDsTenantId=0 fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
 suser=root suid=0 act=blocked filePath=/bin/my.jar fsize=123857 aggregationType=0 repeatCount=1 cs1=notWhitelisted
 cs1Label=actionReason

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=2
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cs1	cs1	Reason	アプリケーションコントロールが指定された処理を実行した理由 (例: notWhitelisted: ソフトウェアに一致するルールがなく、承認さ	cs1=notWhitelisted

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			れていないソフトウェアをブロックするようにアプリケーションコントロールが設定されていた)。	
cs1Label	cs1Label		フィールドcs1の名前ラベル。	cs1Label=actionReason
cs2	cs2		ファイルのSHA-1ハッシュ (計算済みの場合)。	cs2=156F4CB711FDBD668943711F853FB6DA89581AAD
cs2Label	cs2Label		フィールドcs2の名前ラベル。	cs2Label=sha1
cs3	cs3		ファイルのMD5ハッシュ (計算済みの場合)。	cs3=4E8701AC951BC4537F8420FDAC7EFBB5
cs3Label	cs3Label		フィールドcs3の名前ラベル。	cs3Label=md5
act	act	Action	アプリケーション制御エンジンによって実行	act=blocked

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			される処理。値には、Blocked、Allowedがあります。	
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合には表示されません(代わりにdvchostを使用します)。	dvc=10.1.1.10
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合には表示されま	dvchost=www.example.com dvchost=2001:db8::5

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			せん(代わりにdvcフィールドを使用します)。	
suid	suid	User ID	ユーザ名のアカウントID番号。	suid=0
suser	suser	User Name	保護対象コンピュータにソフトウェアをインストールしたユーザアカウントの名前。	suser=root
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityのテナント名。	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID番号。	TrendMicroDsTenantId=0
fileHash	fileHash	File hash	ソフトウェアファイルを識別するSHA 256ハッシュ。	fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
filePath	filePath	File Path	不正プログラムファイルの場所。	filePath=/bin/my.jar

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
filesize	filesize	File Size	ファイルサイズ (バイト)。	filesize=16
aggregationType	aggregationType	Aggregation Type	<p>イベントの集約方法を示す整数:</p> <ul style="list-style-type: none"> • 0: イベントが集約されません。 • 1: イベントが、ファイル名、パス、イベントの種類に 	aggregationType=2

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			<p>応じて集約されます。</p> <ul style="list-style-type: none"> • 2: イベントがイベントの種類に応じて集計されます。 <p>イベント集約については、"アプリケーションコントロールイベントログを表示する"</p>	

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			on page 706の 表示を参照 してください。	
repeatCount	repeatCount	Repeat Count	イベントの 発生回数。 非集約イベ ントの値に は1を指定 します。集 約イベント には2以上 の値を指定 します。	repeatCount=4
None	sev	Severity	イベントの 重要度。重 要度は1が 最も低く、 10が最も高 くなります。	sev=6
None	cat	Category	Category	cat=AppControl
None	name	Name	イベント名	name=blocked
None	desc	Descripti on	イベントの 説明。アプ リケーショ ンコント ロールは、 アクション を説明とし て使用しま	desc=blocked

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			す。	

ファイアウォールイベントログの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF: 0|Trend Micro|Deep Security Agent|<DSA version>|20|Log for TCP Port 80|0|cn1=1
cn1Label=Host ID dvc=hostname act=Log dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP
src=192.168.126.150 dst=72.14.204.147 out=1019 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49617 dpt=80
cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 TrendMicroDsPacketData=AFB...

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|21|cat=Firewall name=Remote
Domain Enforcement (Split Tunnel) desc=Remote Domain Enforcement (Split Tunnel) sev=5 cn1=37 cn1Label=Host ID
dvchost=www.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dstMAC=67:BF:1B:2F:13:EE
srcMAC=78:FD:E7:07:9F:2C TrendMicroDsFrameType=IP src=10.0.110.221 dst=105.152.185.81 out=177 cs3=
cs3Label=Fragmentation Bits proto=UDP srcPort=23 dstPort=445 cnt=1 TrendMicroDsPacketData=AFB...

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
act	act	Action		act=Log act=Deny
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cnt	cnt	Repeat Count	このイベントが連続して繰り返された回数。	cnt=8
cs2	cs2	TCP Flags		cs2=0x10 ACK cs2=0x14 ACK RST

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cs2Label	cs2Label	TCP Flags	フィールドcs2の名前ラベル。	cs2Label=TCP Flags
cs3	cs3	Packet Fragmentation Information		cs3=DF cs3=MF cs3=DF MF
cs3Label	cs3Label	Fragmentation Bits	フィールドcs3の名前ラベル。	cs3Label=Fragmentation Bits
cs4	cs4	ICMP Type and Code	(ICMPプロトコルの場合のみ) ICMPタイプとコード (スペース区切り)。	cs4=11 0 cs4=8 0
cs4Label	cs4Label	ICMP	フィールドcs4の名前ラベル。	cs4Label=ICMP Type and Code
dmac	dstMAC	Destination MAC Address	送信先コンピュータのネットワークインタフェースのMACアドレス。	dmac= 00:0C:29:2F:09:B3
dpt	dstPort	Destination Port	(TCPプロトコルおよびUDPプロトコルの場合のみ) 送信先コンピュータの接続またはセッションのポート番号。	dpt=80 dpt=135
dst	dst	Destination IP Address	送信先コンピュータのIPアドレス。	dst=192.168.1.102 dst=10.30.128.2
in	in	Inbound Bytes Read	(受信接続の場合のみ) 読み取られた受信バイト数。	in=137 in=21
out	out	Outbound Bytes Read	(送信接続の場合のみ) 読み取られた送信バイト数。	out=216 out=13
proto	proto	Transport protocol	使用するトランスポートプロトコルの名前。	proto=tcp proto=udp proto=icmp

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
smac	srcMAC	Source MAC Address	送信元コンピュータのネットワークインタフェースのMACアドレス。	smac= 00:0E:04:2C:02:B3
spt	srcPort	Source Port	(TCPプロトコルおよびUDPプロトコルの場合のみ) 送信元コンピュータの接続またはセッションのポート番号。	spt=1032 spt=443
src	src	Source IP Address	このイベントにおけるパケットの送信元IPアドレス。	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	TrendMicroDsFrameType	Ethernet frame type	接続のイーサネットフレームの種類。	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	TrendMicroDsPacketData	Packet data	Base64で表されるパケットデータ。	TrendMicroDsPacketData = AFB...
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレ	dvchost=exch01.example.com dvchost=2001:db8::5

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			スの場合は表示されません(代わりにdvcフィールドを使用します)。	
TrendMicroDsTags	TrendMicroDsTags	Event Tags	イベントに割り当てられたDeep Securityのイベントタグ	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant Name	Deep Securityのテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=5
None	cat	Category	Category	cat=Firewall
None	name	Name	イベント名	name=Remote Domain Enforcement (Split Tunnel)
None	desc	Description	イベントの説明。ファイアウォールイベントでは、イベント名が説明として使用されます。	desc=Remote Domain Enforcement (Split Tunnel)

整合性監視イベントのログ

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

Trend Micro Deep Security On-Premise 12.0

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|30|New Integrity Monitoring Rule|6|cn1=1 cn1Label=Host ID dvchost=hostname act=updated filePath=c:\\windows\\message.dll suser=admin msg=lastModified,sha1,size

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合には省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|2002779|cat=Integrity Monitor name=Microsoft Windows - System file modified desc=Microsoft Windows - System file modified sev=8 cn1=37 cn1Label=Host ID dvchost=www.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=updated suser=admin

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
act	act	Action	変更監視ルールによって検出される処理。値は、created、updated、deleted、またはrenamedのいずれかです。	act=created act=deleted
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
filePath	filePath	Target Entity	変更監視ルールの対象のエンティティ。監視対象の口	filePath=C:\\WINDOWS\\system32\\drivers\\etc\\hosts

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			グファイルが含まれます。	
suser	suser	Source User	監視対象のファイルを変更したユーザーのアカウント。	suser = WIN-038M7CQDHIN \ Administrator
msg	msg	Attribute changes	(「renamed」処理の場合のみ) 変更された属性名のリスト。 [Manager経由でリレーする]を選択した場合、すべてのイベント処理の種類に完全な説明が含まれます。	msg=lastModified,sha1,size
oldfilePath	oldfilePath	Old target entity	(「renamed」処理の場合のみ) filePath フィールドに記録された新しいエンティティに名前変更された、以前の変更監視ルールの対象のエンティティ。	oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log
dvc	dvc	Device address	cn1のIPv4アドレス。	dvc=10.1.144.199

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	dvchost=www.example.com dvchost=2001:db8::5
TrendMicroDsTags	TrendMicroDsTags	Events tags	イベントに割り当てられたDeep Securityのイベントタグ	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityのテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度	sev=8

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			は1が最も低く、10が最も高くなります。	
None	cat	Category	Category	cat=Integrity Monitor
None	name	Name	イベント名	name=Microsoft Windows - System file modified
None	desc	Description	イベントの説明。変更監視では、イベント名が説明として使用されます。	desc=Microsoft Windows - System file modified

侵入防御イベントログの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|1001111|Test Intrusion Prevention Rule|3|cn1=1 cn1Label=Host ID dvchost=hostname dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.105 out=1093 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49786 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=IDS:Reset cn3=10 cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream Position cs6=8 cs6Label=Intrusion Prevention Flags TrendMicroDsPacketData=R0VUIC9zP3...

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|1000940|cat=Intrusion Prevention name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities sev=10 cn1=6 cn1Label=Host ID dvchost=exch01 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 dstMAC=55:C0:A8:55:FF:41 srcMAC=CA:36:42:B1:78:3D TrendMicroDsFrameType=IP

Trend Micro Deep Security On-Premise 12.0

src=10.0.251.84 dst=56.19.41.128 out=166 cs3= cs3Label=Fragmentation Bits proto=ICMP srcPort=0 dstPort=0 cnt=1
 act=IDS:Reset cn3=0 cn3Label=DPI Packet Position cs5=0 cs5Label=DPI Stream Position cs6=0 cs6Label=DPI Flags
 TrendMicroDsPacketData=R0VUIC9zP3...

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
act	act	Action	(Deep Securityバージョン7.5 SP1以前に作成されたIPSルールでは、Insert、Replace、Deleteも実行することができましたが、現在これらの処理は実行されません。これらの処理の実行を試みる古いIPSルールが実行された場合、ルールが検出のみモードで適用されたことを示すイベントが記録されます)。	act=Block
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cn3	cn3	Intrusion Prevention Packet Position	イベントをトリガしたデータの Paket 内の位置。	cn3=37
cn3Label	cn3Label	Intrusion Prevention Packet Position	フィールドcn3の名前ラベル。	cn3Label=Intrusion Prevention Packet Position
cnt	cnt	Repeat Count	このイベントが連続	cnt=8

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			して繰り返された回数。	
cs1	cs1	Intrusion Prevention Filter Note	(オプション) DPI ルールに関連する短いバイナリまたはテキストによる備考を含めることのできる注記用フィールド。注記用フィールドの値がすべて印刷可能なASCII文字の場合、値はテキストとしてログに記録され、スペース(空白文字)はアンダースコアに変換されます。バイナリデータが含まれる場合は、Base64エンコードを使用してログに記録されます。	cs1=Drop_data
cs1Label	cs1Label	Intrusion Prevention Note	フィールドcs1の名前ラベル。	cs1Label=Intrusion Prevention Note
cs2	cs2	TCP Flags	(TCPプロトコルの場合のみ) TCPフラグバイトの後には、[URG]、[ACK]、[PSH]、[RST]、[SYN]、[FIN]の各フィールドが続きます。このフラグバイトは、TCPヘッダが設定されている場合に存在する可能性が	cs2=0x10 ACK cs2=0x14 ACK RST

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			あります。	
cs2Label	cs2Label	TCP Flags	フィールドcs2の名前ラベル。	cs2Label=TCP Flags
cs3	cs3	Packet Fragmentation Information		cs3=DF cs3=MF cs3=DF MF
cs3Label	cs3Label	Fragmentation Bits	フィールドcs3の名前ラベル。	cs3Label=Fragmentation Bits
cs4	cs4	ICMP Type and Code	(ICMPプロトコルの場合のみ) 単一のスペースで区切って個別の順序で格納されているICMPタイプとコード。	cs4=11 0 cs4=8 0
cs4Label	cs4Label	ICMP	フィールドcs4の名前ラベル。	cs4Label=ICMP Type and Code
cs5	cs5	Intrusion Prevention Stream Position	イベントをトリガしたデータのストリーム内の位置。	cs5=128 cs5=20
cs5Label	cs5Label	Intrusion Prevention Stream Position	フィールドcs5の名前ラベル。	cs5Label=Intrusion Prevention Stream Position
cs6	cs6	Intrusion Prevention Filter Flags	フラグの値の合計値。 1 - Data truncated - データをログに記録できませんでした。 2 - Log Overflow - ログがオーバーフローしました。 4 - Suppressed - □	1 (Data truncated) と8 (Have Data) の組み合わせの例: cs6=9

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			グのしきい値が抑制されました。 8 - Have Data - パケットデータが含まれます。 16 - Reference Data - 以前にログに記録されたデータを参照します。	
cs6Label	cs6Label	Intrusion Prevention Flags	フィールドcs6の名前ラベル。	cs6=Intrusion Prevention Filter Flags
dmac	dstMAC	Destination MAC Address	送信先コンピュータのネットワークインタフェースMACアドレス。	dmac= 00:0C:29:2F:09:B3
dpt	dstPort	Destination Port	(TCPプロトコルおよびUDPプロトコルの場合のみ) 送信先コンピュータの接続ポート。	dpt=80 dpt=135
dst	dst	Destination IP Address	送信先コンピュータのIPアドレス。	dst=192.168.1.102 dst=10.30.128.2
xff	xff	X-Forwarded-For	X-Forwarded-Forヘッダ内の最後のハブのIPアドレス。 通常は、存在する可能性のあるプロキシを越えた送信元のIPアドレスです。srcフィールドも参照してください。 イベントにxffを含めるには、1006540 [X-Forwarded-For	xff=192.168.137.1

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			HTTPヘッダのログを有効にする] 侵入防御ルール を有効にします。	
in	in	Inbound Bytes Read	(受信接続の場合のみ) 読み取られた受信バイト数。	in=137 in=21
out	out	Outbound Bytes Read	(送信接続の場合のみ) 読み取られた送信バイト数。	out=216 out=13
proto	proto	Transport protocol	使用する接続トランスポートプロトコルの名前。	proto=tcp proto=udp proto=icmp
smac	srcMAC	Source MAC Address	送信元コンピュータのネットワークインタフェースMACアドレス。	smac= 00:0E:04:2C:02:B3
spt	srcPort	Source Port	(TCPプロトコルおよびUDPプロトコルの場合のみ) 送信元コンピュータの接続ポート。	spt=1032 spt=443
src	src	Source IP Address	送信元コンピュータのIPアドレス。これは、最後のプロキシサーバ (存在する場合) のIP、またはクライアントIPです。xffフィールドも参照してください。	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	TrendMicroDsFrameType	Ethernet frame type	接続のイーサネットフレームの種類。	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
TrendMicroDsPacketData	TrendMicroDsPacketData	Packet data	Base64で表されるパケットデータ。	TrendMicroDsPacketData = R0VUIC9zP3...
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	dvchost=www.example.com dvchost=2001:db8::5
TrendMicroDsTags	TrendMicroDsTags	Event tags	イベントに割り当てられたDeep Securityのイベントタグ	TrendMicroDsTags=Suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityのテナント名	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=10

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
None	cat	Category	カテゴリ	cat=Intrusion Prevention
None	name	Name	イベント名	name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities
None	desc	Description	イベントの説明。侵入防御イベントは、イベント名を説明として使用します。	desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities

ログ検査イベントの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|3002795|Microsoft Windows Events|8|cn1=1 cn1Label=Host ID dvchost=hostname cs1Label=LI Description cs1=Multiple Windows Logon Failures fname=Security src=127.0.0.1 duser=(no user) shost=WIN-RM6HM42G65V msg=WinEvtLog Security: AUDIT_FAILURE(4625): Microsoft-Windows-Security-Auditing: (no user): no domain: WIN-RM6HM42G65V: An account failed to log on.Subject: ..

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|3003486|cat=Log Inspection name=Mail Server - MDaemon desc=Server Shutdown. sev=3 cn1=37 cn1Label=Host ID dvchost=exch01.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cs1=Server Shutdown. cs1Label=LI Description fname= shost=msg=

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cs1	cs1	Specific Sub-Rule	このイベントをトリガしたセキュリティログ監視のサブルール。	cs1=Multiple Windows audit failure events
cs1Label	cs1Label	LI Description	フィールドcs1の名前ラベル。	cs1Label=LI Description
duser	duser	User Information	(解析可能なユーザ名が存在する場合) ログエントリを記録した対象ユーザの名前。	duser=(no user) duser=NETWORK SERVICE
fname	fname	Target entity	ログ検査ルールの対象エンティティ。監視対象のログファイルが含まれません。	fname=Application fname=C:\Program Files\CMS\logs\server0.log
msg	msg	Details	ログ検査イベントの詳細。検出されたログイベントの詳細な説明が含まれる場合があります。	msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz'
shost	shost	Source Hostname	送信元コンピュータのホスト名。	shost=webserver01.corp.com
src	src	Source IP Address	送信元コンピュータのIPアドレス。	src=192.168.1.105 src=10.10.251.231
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代	dvchost=www.example.com dvchost=2001:db8::5

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			わりにdvcフィールドを使用します)。	
TrendMicroDsTags	TrendMicroDsTags	Events tags	イベントに割り当てられたDeep Securityのイベントタグ	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityのテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=3
None	cat	Category	Category	cat=Log Inspection
None	name	Name	イベント名	name=Mail Server - MDaemon
None	desc	Description	イベントの説明。	desc=Server Shutdown

Webレピュテーションイベントの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|5000000|WebReputation|5|cn1=1
cn1Label=Host ID dvchost=hostname request=example.com msg=Blocked By Admin

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|5000000|cat=Web Reputation
name=WebReputation desc=WebReputation sev=6 cn1=3 cn1Label=Host ID dvchost=exch01.example.com
TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 request=http://yw.olx5x9ny.org.it/HvuauRH/eighgSS.htm
msg=Suspicious

Trend Micro Deep Security On-Premise 12.0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=1
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
request	request	Request	要求のURL。	request=http://www.example.com/index.php
msg	msg	Message	処理の種類。値には、Realtime、Scheduled、Manualがあります。	msg=Realtime msg=Scheduled
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	dvchost=www.example.com dvchost=2001:db8::5
TrendMicroDsTags	TrendMicroDsTags	Events tags	イベントに割り当	TrendMicroDsTags=suspicious

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			てられたDeep Securityのイベントタグ	
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityのテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityのテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=6
None	cat	Category	Category	cat=Web Reputation
None	name	Name	イベント名	name=WebReputation
None	desc	Description	イベントの説明。Webレピュテーションでは、イベント名が説明として使用されます。	desc=WebReputation

Red Hat Enterprise Linuxでイベントログを受信するための設定

Red Hat Enterprise Linux 6または7でSyslogを設定する

次の手順は、Deep Securityからログを受信するための、Red Hat Enterprise Linux 6または7でのrsyslogの設定方法を示しています。

1. rootでログインします。
2. 次のコマンドを実行します。
`vi /etc/rsyslog.conf`
3. `rsyslog.conf`の先頭付近にある次の行をコメント解除します。変更前のコードは、次のとおりです。

```
#ModLoad imudp
```

Trend Micro Deep Security On-Premise 12.0

```
#$UDPServerRun 514  
#$ModLoad imtcp  
#$InputTCPServerRun 514
```

変更後のコードは、次のとおりです。

```
$ModLoad imudp  
$UDPServerRun 514  
$ModLoad imtcp  
$InputTCPServerRun 514
```

4. `rsyslog.conf`の末尾に、次の2行を追加します。
 - `#Save Deep Security Manager logs to DSM.log`
 - `Local4.* /var/log/DSM.log`

注意: Managerの設定内容によっては、`Local4`を別の値に置き換える必要があります。

5. ファイルを保存して、終了します。
6. 「`touch /var/log/DSM.log`」と入力して、`/var/log/DSM.log`ファイルを作成します。
7. Syslogが書き込めるよう、DSMログに権限を設定します。
8. ファイルを保存して、終了します。
9. Syslogを再起動します。
 - Red Hat Enterprise Linux 6で次のコマンドを実行します。 `service rsyslog restart`
 - Red Hat Enterprise Linux 7で次のコマンドを実行します。 `systemctl restart rsyslog`

Syslogが機能すると、`/var/log/DSM.log`に記録されます。

Red Hat Enterprise Linux 5でSyslogを設定する

次の手順は、Deep Securityからログを受信するための、Red Hat Enterprise LinuxでのSyslogの設定方法を示しています。

1. rootでログインします。
2. 次のコマンドを実行します。

```
vi /etc/syslog.conf
```
3. `syslog.conf`の末尾に、次の2行を追加します。
 - `#Save Deep Security Manager logs to DSM.log`
 - `Local4.* /var/log/DSM.log`

注意: Managerの設定内容によっては、Local4を別の値に置き換える必要があります。

4. ファイルを保存して、終了します。
5. 「`touch /var/log/DSM.log`」と入力して、`/var/log/DSM.log`ファイルを作成します。
6. Syslogが書き込めるよう、DSMログに権限を設定します。
7. 次のコマンドを実行します。

```
vi /etc/sysconfig/syslog
```
8. 「`SYSLOGD_OPTIONS`」の行を編集して、オプションに「`-r`」を追加します。
9. ファイルを保存して、終了します。
10. Syslogを再起動します。 `/etc/init.d/syslog restart`

Syslogが機能すると、`/var/log/DSM.log`に記録されます。

Amazon SNSでのイベントへのアクセス

AWSアカウントを保有している場合、Amazon Simple Notification Service (SNS) を利用してDeep Securityイベントに関する通知を公開し、サブスクライバに配信できます。SNSの詳細については、<https://aws.amazon.com/sns/>を参照してください。

Amazon SNSを設定するには下記のタスクを行います。

1. ["AWSユーザを作成する" below](#)
2. ["Amazon SNSトピックを作成する" on the next page](#)
3. ["SNSを有効にする" on the next page](#)
4. ["サブスクリプションを作成する" on page 1203](#)

これらのタスクの実行方法については、以下のセクションを参照してください。

AWSユーザを作成する

Deep SecurityでAmazon SNSを使用するには、SNSに必要な権限を持つAWSユーザを作成する必要があります。尚、この後の手順のSNSを有効化する時にユーザの アクセスキーと秘密鍵が必要になる為、それらをメモしておきます。

作詞するAWSユーザには、Deep Securityを公開するすべてのSNSトピックに対する「sns:Publish」権限が必要です、以下は、この権限が設定されたポリシーの例です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

公開権限を単一のトピックに制限する場合は、`"Resource": "*"を "Resource": "TOPIC ARN"に置き換えます。`

詳細については、Amazon AWSドキュメントの「[Controlling User Access to Your AWS Account](#)」と「[Amazon SNS ポリシーの特別な情報](#)」を参照してください。

Amazon SNSトピックを作成する

AWSで、イベントを公開するSNSトピックを作成します。Amazon SNSの作成手順については、[Amazon SNSドキュメント](#)の「トピックの作成」を参照してください。手順3で必要になるため、SNSトピックのARNを書き留めておきます。

SNSを有効にする

1. Deep Security Managerで、[管理]→[システム設定]→[イベントの転送]に進みます。
2. [Amazon SNS] セクションで [AWS Simple Notification Serviceにイベントを公開] を選択します。
3. 次の情報を入力します。
 - アクセスキー: セクション1で作成したAWSユーザのアクセスキー。
 - 秘密鍵: セクション1で作成したAWSユーザの秘密鍵。
 - SNSトピックARN: イベントの送信先となるSNSトピックのARN。これは、セクション2で書き留めたARNです。
4. SNSに転送するイベントのタイプを選択します。

イベントを選択すると、JSON SNS設定が自動的に生成されます。

5. (オプション) イベントを詳細にフィルタして、フィルタごとに転送指示を設定する場合、[JSON SNS設定の編集] をクリックしてJSON SNS設定を直接編集することもできます。設定言語の詳細については、"[JSON形式でのSNS設定](#)" on the [next page](#)を参照してください。

注意:JSONを編集すると、イベントのチェックボックスは使用できなくなります。イベントのチェックボックスをオンまたはオフにするには、[基本的なSNS設定に戻す] をクリックします。ただし、JSON SNS設定に加えたカスタマイズは破棄されます。

6. [保存] をクリックします。

サブスクリプションを作成する

これでSNSが有効になり、イベントがトピックに公開されるようになりました。次に、Amazon SNSコンソールに移動し、トピックにサブスクライブしてイベントにアクセスします。イベントにサブスクライブするには、[メール](#)、[SMS](#)、[Lambdaエンドポイント](#)など複数の方法があります。

注意: Lambdaは一部のAWSリージョンでは使用できません。

JSON形式でのSNS設定

[Amazon SNSトピックへのイベントの転送を有効にした](#)場合に使用されるJSON設定を編集できます。この設定では、イベントをトピックに公開するために満たさなければならない条件を定義します。設定言語は、[AmazonのSNS向けポリシー言語](#)に倣っています。

各フィールドの詳細を以下に示します。基本的なSNS設定は次のような構文で記述されます。

```
{
  "Version": "2014-09-24",
  "Statement": [statement1, statement2, ...]
}
```

例については、["SNS設定の例" on page 1221](#)を参照してください。

Version

Versionエレメントは、設定言語のバージョンを指定します。

注意: 現在有効な「Version」値は、文字列「2014-09-24」のみです。

```
"Version": "2014-09-24",
```

Statement

Statementエレメントは、複数の文の配列です。それぞれの文は、所定の条件を満たした場合にイベントを送信するSNSトピックを示すJSONオブジェクトを指定します。

```
"Statement": [{...}, {...}, ...]
```

それぞれのステートメントの形式は次のとおりです。

```
{  
  "Topic": "destination topic",  
  "Condition": {conditions event must meet to be published to the destination topic}  
}
```

Topic

Topicエレメントには、発行先のSNSトピックのAmazon Resource Nameを指定する必要があります。

```
"Topic": "arn:aws:sns:us-east-1:012345678901:myTopic"
```

Condition

Conditionエレメントは最も複雑な部分で、イベントをトピックに公開する条件を指定します。

各条件には、トピックに含めるイベントと一致しなければならない (条件の種類によっては一致してはならない) 1つ以上のキーと値のペアを指定できます。キーは任意の有効なイベントプロパティです(イベントプロパティについては、"[JSON形式のイベント](#)" on page 1223を参照してください)。有効な値はキーによって異なります。キーによっては複数の値がサポートされる場合もあります。

```
"Condition":{
  "ConditionName":{
    "key1":[value1, value2],
    "key2":value3
  },
  "ConditionName2":{
    "key3":[value4]
  },
  ...
}
```

有効な条件の名前と構文を以下に示します。

Bool

Bool条件は、ブール値の照合を行います。該当するプロパティがあり、その値が指定したブール値と一致していれば、条件に一致するイベントとみなされます。該当するプロパティがあるものの、その値がブール値でない場合は、次のようにしてプロパティがテストされます。

- 数値0はfalseと評価されます。0以外の数値はtrueと評価されます。
- 空の文字列と文字列「false」および「0」はfalseと評価されます。それ以外の文字列はtrueと評価されます。
- それ以外の値を持つイベントのプロパティについては、値をブール値に変換できず、照合されません。

Trend Micro Deep Security On-Premise 12.0

複数値の使用: ×

次の設定例では、「DetectOnly」プロパティの値がfalseである場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "Bool": {
          "DetectOnly": false
        }
      }
    }
  ]
}
```

Exists

Exists条件は、イベントにプロパティがあるかどうかをテストします。プロパティの値は考慮されません。

複数値の使用: ×

次の設定例では、「Severity」プロパティがあり、かつ「Title」プロパティがない場合にイベントが公開されます。

Trend Micro Deep Security On-Premise 12.0

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "Exists": {
          "Severity": true,
          "Title": false
        }
      }
    }
  ]
}
```

IpAddress

IpAddress条件は、イベントのプロパティの値がCIDR形式で指定したIPアドレス範囲に含まれるかどうか、または単一のIPアドレスに完全に一致するかどうかをテストします。

複数値の使用: ○

次の設定例では、「DestinationIP」プロパティのIPアドレスが10.0.1.0/24の範囲に含まれているか、10.0.0.5と一致する場合にイベントが公開されます。

Trend Micro Deep Security On-Premise 12.0

```
"Version": "2014-09-24",
"Statement": [
  {
    "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
    "Condition": {
      "IpAddress": {
        "DestinationIP": ["64.23.0.0/16", "216.104.20.189"]
      }
    }
  }
]
```

NotIpAddress

NotIpAddress条件は、イベントのプロパティの値が指定したいずれのIPアドレス範囲にも含まれないかどうかをテストします。

複数値の使用: ○

次の設定例では、「DestinationIP」プロパティのIPアドレスが10.0.0.0/8の範囲に含まれていない場合にイベントが公開されます。

```
"Version": "2014-09-24",
"Statement": [
  {
    "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
```



```
"Condition": {
  "NotIpAddress": {
    "DestinationIP": "10.0.0.0/8"
  }
}
]
```

NumericEquals

NumericEquals条件は、イベントのプロパティの数値が指定した1つ以上の値と等しいかどうかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、次のようにしてプロパティがテストされます。

- 文字列は数値に変換されます。数値に変換できない文字列は照合されません。
- それ以外の値を持つイベントのプロパティについては、値を数値に変換できず、照合されません。

複数値の使用: ○

次の設定例では、「Protocol」プロパティの値が6または17である場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
```

```
    "NumericEquals": {
      "Protocol": [6, 17]
    }
  }
}
]
```

NumericNotEquals

NumericNotEquals条件は、イベントのプロパティの数値が指定したいずれの値とも等しくないかどうかをテストします。

複数値の使用: ○

次の設定例では、「Protocol」プロパティの値が6以外で、かつ「Risk」プロパティの値が2または3以外である場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericNotEquals": {
          "Protocol": 6,
          "Risk" : [2, 3]
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

NumericGreaterThan

NumericGreaterThan条件は、イベントのプロパティの数値が指定した値よりも大きいかどうかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

複数値の使用: ×

次の設定例では、「Protocol」プロパティの値が6よりも大きい場合にイベントが公開されます。

```
{  
  "Version": "2014-09-24",  
  "Statement": [  
    {  
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",  
      "Condition": {  
        "NumericGreaterThan": {  
          "Protocol": 6  
        }  
      }  
    }  
  ]  
}
```

```
]
}
```

NumericGreaterThanEquals

NumericGreaterThanEquals条件は、イベントのプロパティの数値が指定した値以上であることをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

複数値の使用: ×

次の設定例では、「Number」プロパティの値が600以上の場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericGreaterThanEquals": {
          "Number": 600
        }
      }
    }
  ]
}
```

NumericLessThan

NumericLessThan条件は、イベントのプロパティの数値が指定した値よりも小さいかどうかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

複数値の使用: ×

次の設定例では、「Number」プロパティの値が1000よりも小さい場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericLessThan": {
          "Number": 1000
        }
      }
    }
  ]
}
```

NumericLessThanEquals

NumericLessThanEquals条件は、イベントのプロパティの数値が指定した値以下であることをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

Trend Micro Deep Security On-Premise 12.0

複数値の使用: ×

次の設定例では、「Number」プロパティの値が500以下の場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericLessThanEquals": {
          "Number": 500
        }
      }
    }
  ]
}
```

StringEquals

StringEquals条件は、イベントのプロパティの文字列値が指定したいいずれかの値と完全に一致するかどうかをテストします。

複数値の使用: ○

次の設定例では、「EventType」プロパティの値が「SystemEvent」と一致し、かつ「TargetType」プロパティの値が「User」または「Role」と一致する場合にイベントが公開されます。

Trend Micro Deep Security On-Premise 12.0

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringEquals": {
          "EventType": ["SystemEvent"],
          "TargetType" : ["User", "Role"]
        }
      }
    }
  ]
}
```

StringNotEquals

StringNotEquals条件は、イベントのプロパティの文字列値が指定したいずれの値にも一致しないかどうかをテストします。

複数値の使用:○

次の設定例では、「EventType」プロパティの値が「PacketLog」と「IntegrityEvent」のいずれにも一致しない場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
```

Trend Micro Deep Security On-Premise 12.0

```
"Statement": [  
  {  
    "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",  
    "Condition": {  
      "StringNotEquals": {  
        "EventType": ["PacketLog", "IntegrityEvent"]  
      }  
    }  
  }  
]
```

StringEqualsIgnoreCase

StringEqualsIgnoreCase条件は、StringEquals条件と同じ文字列の照合を行いますが、大文字と小文字が区別されません。

StringNotEqualsIgnoreCase

StringNotEqualsIgnoreCase条件は、StringNotEquals条件と同じ文字列の照合を行いますが、大文字と小文字が区別されません。

StringLike

StringLike条件は、イベントのプロパティの文字列値が指定したいずれかの値と一致するかどうかをテストします。この条件では、任意の数の文字と一致する「*」、任意の1文字と一致する「?」をワイルドカードとして使用できます。文字列の比較では大文字と小文字が区別されます。

Trend Micro Deep Security On-Premise 12.0

複数値の使用: ○

次の設定例では、「Title」プロパティの値に「User」または「Role」という文字列が含まれる場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringLike": {
          "Title": ["*User*", "*Role*"]
        }
      }
    }
  ]
}
```

StringNotLike

StringNotLike条件は、イベントのプロパティの文字列値が指定したいずれの値にも一致しないかどうかをテストします。この条件では、任意の数の文字と一致する「*」、任意の1文字と一致する「?」をワイルドカードとして使用できます。文字列の比較では大文字と小文字が区別されます。

複数値の使用: ○

次の設定例では、「システム設定の保存」イベントを除くすべてのイベントが公開されます。

Trend Micro Deep Security On-Premise 12.0

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title": "System Settings Saved"
        }
      }
    }
  ]
}
```

次の設定例では、「Title」プロパティの値の先頭が「User」でなく、かつ末尾が「Created」でない場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title": ["User*", "*Created"]
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

複数の文と複数の条件

同じSNSトピックに対して作成した複数の文は、「or」で結合されたものとして評価されます。1つの文に複数の条件が含まれている場合、それらの条件は「and」で結合されたものとして評価されます。

複数の文

間違った設定例を次に示します。最初の文で「System Settings Saved」以外のすべてのイベントを転送するよう指定し、2つ目の文ですべての「System Settings Saved」イベントを転送するよう指定しています。結果は、すべてのイベントが最初の文の条件または2つ目の文の条件に一致するため、すべてのイベントが転送されます。

```
{  
  "Version": "2014-09-24",  
  "Statement": [  
    {  
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",  
      "Condition": {  
        "StringNotLike" : {  
          "Title" : "System Settings Saved"  
        }  
      }  
    }  
  ]  
}
```

```
    },  
    {  
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",  
      "Condition": {  
        "StringLike" : {  
          "Title" : "System Settings Saved"  
        }  
      }  
    }  
  ]  
}
```

複数の条件

間違った設定例をもう1つ示します。最初の条件で「System Settings Saved」以外のすべてのイベントを転送するよう指定し、2つ目の条件ですべての「System Settings Saved」イベントを転送するよう指定しています。結果は、どのイベントも最初の文の条件および2つ目の文の条件の両方には一致しないため、イベントは転送されません。

```
{  
  "Version": "2014-09-24",  
  "Statement": [  
    {  
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",  
      "Condition": {  
        "StringNotLike" : {  
          "Title" : "System Settings Saved"  
        }  
      },  
    },  
  ],  
}
```

Trend Micro Deep Security On-Premise 12.0

```
    "StringLike" : {
      "Title" : "System Settings Saved"
    }
  }
}
]
```

SNS設定の例

以下は、一部の特定シナリオに合ったイベントを送信する設定です。SNSトピックのフィルタとして使用できるイベントプロパティ名および値の詳細については、["JSON形式のイベント" on page 1223](#)を参照してください。

重大なすべての侵入防御イベントをSNSトピックに送信する

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericEquals": {
          "Severity": 4
        },
        "StringEquals" : {
          "EventType" : "PayloadLog"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

イベントごとに異なるSNSトピックに送信する

この例では、すべてのシステムイベントを1つのトピックに送信し、すべての変更監視イベントを別のトピックに送信します。

```
{  
  "Version": "2014-09-24",  
  "Statement": [  
    {  
      "Topic": "arn:aws:sns:us-east-1:012345678901:systemEventsTopic",  
      "Condition": {  
        "StringEquals" : {  
          "EventType" : "SystemEvent"  
        }  
      }  
    },  
    {  
      "Topic": "arn:aws:sns:us-east-1:012345678901:integrityTopic",  
      "Condition": {  
        "StringEquals" : {  
          "EventType" : "IntegrityEvent"  
        }  
      }  
    }  
  ]  
}
```

```

    }
  }
}
]
}

```

JSON形式のイベント

Amazon SNSに公開される際、イベントは文字列にエンコードされるJSONオブジェクトの配列として、SNS Messageで送信されます。配列内の各オブジェクトが1つのイベントです。

有効なプロパティはイベントの種類によって異なります。たとえば、MajorVirusTypeはDeep Security不正プログラム対策イベントのみに有効なプロパティであり、システムイベントなどには適用されません。有効なプロパティ値はプロパティごとに異なります。例については、"[JSON形式のイベントの例](#)" on page 1245を参照してください。

イベントプロパティ値は、SNSトピックに公開されるイベントをフィルタする際に使用できます。詳細については、"[JSON形式でのSNS設定](#)" on page 1203を参照してください。

有効なイベントプロパティ

注意: イベントによっては、その種類のイベントに通常適用されるプロパティの一部を備えていない場合があります。

プロパティ名	データ タイプ	説明	適用されるイベントの種類
Action	文字列 (列挙)	アプリケーションコントロールイベントに対して実行された処理。「ソフトウェアの実行をルールでブロック」、「承認されていないソフトウェアの実行を許可」(検出のみモードのため)、「承認されていないソフトウェアの実行をブロック」など。	アプリケーションコントロールイベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
Action	整数 (列挙)	ファイアウォールイベントに対して実行された処理。 [検出のみ]の値は、ルールが有効になっていた場合に 実行されたであろう処理を示します。0=不明、1=拒 否、6=ログのみ、0x81=検出のみ: 拒否。	ファイアウォールイ ベント
Action	整数 (列挙)	侵入防御イベントに対して実行された処理。0=不明、 1=拒否、2=リセット、3=挿入、4=削除、5=置換、6= ログのみ、0x81=検出のみ: 拒否、0x82=検出のみ: リ セット、0x83=検出のみ: 挿入、0x84=検出のみ: 削 除、0x85=検出のみ: 置換。	侵入防御イベント
ActionBy	文字 列	イベントを実行したDeep Security Managerユーザの 名前。ユーザによって生成されたイベントでない場合 は「システム」になります。	システムイベント
ActionString	文字 列	処理の文字列への変換。	ファイアウォールイ ベント、侵入防御イ ベント
AdministratorID	整数	処理を実行したDeep Securityユーザの一意的識別 子。ユーザではなくシステムによって生成されたイベ ントには、識別子は割り当てられません。	システムイベント
AggregationType	整数 (列挙)	アプリケーションコントロールイベントが繰り返し発 生したかどうか。「AggregationType」が「0」以外 の場合、発生回数が「RepeatCount」に入ります。0= 未集計、1=ファイル名、パス、およびイベントの種類 に基づいた集計、2=イベントの種類に基づいた集計	アプリケーションコ ントロールイベント
ApplicationType	文字 列	侵入防御ルールに関連付けられたネットワークアプリ ケーションの種類の名前 (該当する場合)。	侵入防御イベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
BlockReason	整数 (列挙)	処理に応じた実行理由。0=不明、1=ルールによってブロック、2=承認されていないためブロック	アプリケーションコントロールイベント
Change	整数 (列挙)	変更監視イベントでファイル、プロセス、レジストリキーなどに対して行われた変更の種類。1=作成、2=アップデート、3=削除、4=拡張子変更。	変更監視イベント
ContainerID	文字列	不正プログラムが検出されたDockerコンテナのID。	不正プログラム対策イベント
ContainerImageName	文字列	不正プログラムが検出されたDockerコンテナのイメージ名。	不正プログラム対策イベント
ContainerName	文字列	不正プログラムが検出されたDockerコンテナの名前。	不正プログラム対策イベント
Description	文字列	エンティティに対して行われた変更 (作成、削除、アップデート) の説明と変更された属性に関する詳細。	変更監視イベント
Description	文字列	イベントの内容を示す簡単な説明。	システムイベント
DestinationIP	文字列 (IP)	パケットの送信先のIPアドレス。	ファイアウォールイベント、侵入防御イベント
DestinationMAC	文字列	パケットの送信先のMACアドレス。	ファイアウォールイベント、侵入防御イベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
	(MAC)		
DestinationPort	整数	パケットの送信先のネットワーク ポート番号 。	ファイアウォールイベント、侵入防御イベント
DetectionCategory	整数 (列挙)	Webレピュテーションイベントの検出カテゴリ。12=ユーザ定義、13=カスタム、91=グローバル。	Webレピュテーションイベント
DetectOnly	ブール	イベントが返されたときに [検出のみ] フラグがオンだったかどうか。trueの場合、URLへのアクセスが検出されましたが、ブロックはされていません。	Webレピュテーションイベント
Direction	整数 (列挙)	ネットワークパケットの方向。0=受信、1=送信。	ファイアウォールイベント、侵入防御イベント
DirectionString	文字列	方向の文字列への変換。	ファイアウォールイベント、侵入防御イベント
DriverTime	整数	ドライバで記録されたログ生成時刻。	ファイアウォールイベント、侵入防御イベント
EndLogDate	文字列 (日付)	繰り返し発生したイベントについての最終ログ日付。繰り返し発生したイベント以外に対しては表示されません。	ファイアウォールイベント、侵入防御イベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
EngineType	整数	不正プログラム対策エンジンの種類。	不正プログラム対策イベント
EngineVersion	文字列	不正プログラム対策エンジンのバージョン。	不正プログラム対策イベント
EntityType	文字列 (列挙)	変更監視イベントが該当するエンティティの種類:Directory、File、Group、InstalledSoftware、Port、Process、RegistryKey、RegistryValue、Service、User、またはWql	変更監視イベント
ErrorCode	整数	不正プログラム検索イベントのエラーコード。0以外の場合、検索に失敗したことを示しており、検索処理および検索結果のフィールドに詳細が表示されます。	不正プログラム対策イベント
EventID	整数	イベントの識別子。識別子は同じ種類のイベントでは一意ですが、種類が異なるイベントでは同じになる場合があります。たとえば、EventTypeがファイアウォールとIPSのイベントのEventIDがどちらも1になることがあります。Deep Securityでイベントを完全かつ一意に識別するには、EventID、EventType、およびTenantIDを組み合わせる必要があります。このプロパティはDeep Security Managerのシステムイベントの「イベントID」プロパティには関連付けられていません。	すべての種類のイベント
EventType	文字列 (列挙)	イベントの種類。次のいずれかです: 「SystemEvent」、「PacketLog」、 「PayloadLog」、「AntiMalwareEvent」、 「WebReputationEvent」、「IntegrityEvent」、 「LogInspectionEvent」、「AppControlEvent」。	すべての種類のイベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
FileName	文字列	「script.sh」など、許可またはブロックされたソフトウェアのファイル名 (フルパスは「Path」内に分けられています)。	アプリケーションコントロールイベント
Flags	文字列	ネットワークパケットから記録されたフラグ (スペース区切りの文字列のリスト)。	ファイアウォールイベント、侵入防御イベント
Flow	整数 (列挙)	ネットワーク接続フロー。有効な値: -1=利用不可、0=接続フロー、1=リバースフロー	ファイアウォールイベント、侵入防御イベント
FlowString	文字列	フローの文字列への変換。	ファイアウォールイベント、侵入防御イベント
Frame	整数 (列挙)	フレームの種類。-1=不明、2048=IP、2054=ARP、32821=REVARP、33169=NETBEUI、0x86DD=IPv6	ファイアウォールイベント、侵入防御イベント
FrameString	文字列	Frameの内容を示す文字列。	ファイアウォールイベント、侵入防御イベント
GroupID	文字列	「0」など、ソフトウェアを起動しようとしたユーザーアカウントのグループID (ある場合)。	アプリケーションコントロールイベント
GroupName	文字列	「root」など、ソフトウェアを起動しようとしたユーザーアカウントのグループ名 (ある場合)。	アプリケーションコントロールイベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
HostAgentVersion	文字列	イベントが検出されたコンピュータを保護していた Deep Security Agent のバージョン。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
HostAgentGUID	文字列	Deep Security Manager で有効化された場合の Deep Security Agent のグローバル一意識別子 (GUID)。	アプリケーションコントロールイベント
HostAssetValue	整数	イベントが生成された時点のコンピュータの資産評価。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostGroupID	整数	イベントが検出されたコンピュータが属するコンピュータグループの一意的識別子。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイ

プロパティ名	データ タイプ	説明	適用されるイベントの種類
			ベント、侵入防御イベント
HostGroupName	文字列	イベントが検出されたコンピュータが属するコンピュータグループの名前。コンピュータグループ名は一意とは限らないことに注意してください。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
HostID	整数	イベントが発生したコンピュータの一意的識別子。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostInstanceID	文字列	イベントが検出されたコンピュータのクラウドインスタンスID。このプロパティは、クラウドコネクタと同期されたコンピュータに対してのみ設定されます。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイ

プロパティ名	データ タイプ	説明	適用されるイベントの種類
			イベント、侵入防御イベント
Hostname	文字列	イベントが生成されたコンピュータのホスト名。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostOS	文字列	イベントが検出されたコンピュータのOS。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostOwnerID	文字列	イベントが検出されたコンピュータのクラウドアカウントID。このプロパティは、クラウドコネクタと同期されたコンピュータに対してのみ設定されます。	不正プログラム対策イベント、Webレピューテーションイベント、変更監視イベント、セキュリティ

プロパティ名	データ タイプ	説明	適用されるイベントの種類
			ログ監視イベント、 ファイアウォールイ ベント、侵入防御イ ベント
HostSecurityPolicyID	整数	イベントが検出されたコンピュータに適用されている Deep Securityポリシーの一意の識別子。	不正プログラム対策 イベント、Webレ ピューテーションイ ベント、変更監視イ ベント、セキュリティ ログ監視イベント、 ファイアウォールイ ベント、侵入防御イ ベント、アプリケー ションコントロール イベント
HostSecurityPolicyName	文字 列	イベントが検出されたコンピュータに適用されている Deep Securityポリシーの名前。セキュリティポリ シー名は一意とは限らないことに注意してください。	不正プログラム対策 イベント、Webレ ピューテーションイ ベント、変更監視イ ベント、セキュリティ ログ監視イベント、 ファイアウォールイ ベント、侵入防御イ ベント、アプリケー ションコントロール イベント
HostVCUID	文字 列	イベントが適用されるコンピュータのvCenter UUID (特定された場合)。	不正プログラム対策 イベント、Webレ ピューテーションイ ベ

プロパティ名	データ タイプ	説明	適用されるイベントの種類
			ント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
InfectedFilePath	文字列	不正プログラム検出で見つかった感染ファイルのパス。	不正プログラム対策イベント
InfectionSource	文字列	不正プログラム感染元のコンピュータの名前 (特定された場合)。	不正プログラム対策イベント
Interface	文字列 (MAC)	パケットを送信または受信するネットワークインタフェースのMACアドレス。	ファイアウォールイベント、侵入防御イベント
IPDatagramLength	整数	IPデータグラムの長さ。	侵入防御イベント
IsHash	文字列	ファイルの変更後のSHA-1コンテンツハッシュ (16進エンコード)。	変更監視イベント
Key	文字列	整合性イベントが参照しているファイルまたはレジストリキー。	変更監視イベント
LogDate	文字列 (日付)	イベントが記録された日時。Deep Security Agentで生成されたイベント (ファイアウォールやIPSなど) の場合は、Deep Security Managerでイベントを受信した日時ではなく、Agentでイベントを記録した日時です。	すべての種類のイベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
MajorVirusType	整数 (列挙)	検出された不正プログラムの分類。0=ジョーク、1=トロイの木馬、2=ウイルス、3=テスト、4=スパイウェア、5=パッカー、6=一般的なプログラム、7=その他	不正プログラム対策イベント
MajorVirusTypeString	文字列	MajorVirusTypeの内容を示す文字列。	不正プログラム対策イベント
MalwareName	文字列	検出された不正プログラムの名前。	不正プログラム対策イベント
MalwareType	整数 (列挙)	検出された不正プログラムの種類。1=一般的な不正プログラム、2=スパイウェア。一般的な不正プログラムの場合はInfectedFilePathが表示され、スパイウェアの場合は表示されません。	不正プログラム対策イベント
ManagerNodeID	整数	イベントが生成されたDeep Security Managerノードの一意的識別子。	システムイベント
ManagerNodeName	文字列	イベントが生成されたDeep Security Managerノードの名前。	システムイベント
MD5	文字列	ソフトウェアのMD5チェックサム (ハッシュ) (ある場合)。	アプリケーションコントロールイベント
Number	整数	システムイベントにイベントを識別する追加IDが指定されています。Deep Security Managerで、このプロパティが「イベントID」として表示されます。	システムイベント
Operation	整数 (列挙)	0=不明、1= 検出のみモードのため許可、2=ブロック	アプリケーションコントロール

プロパティ名	データ タイプ	説明	適用されるイベントの種類
Origin	整数 (列挙)	イベントの生成元。-1=不明、0=Deep Security Agent、1=VMのゲストエージェント、2=Deep Security Appliance、3=Deep Security Manager	すべての種類のイベント
OriginString	文字列	Originの内容を示す判読可能な文字列。	すべての種類のイベント
OSSEC_Action	文字列	OSSECの処理	セキュリティログ監視イベント
OSSEC_Command	文字列	OSSECのコマンド	セキュリティログ監視イベント
OSSEC_Data	文字列	OSSECのデータ	セキュリティログ監視イベント
OSSEC_Description	文字列	OSSECの説明	セキュリティログ監視イベント
OSSEC_DestinationIP	文字列	OSSECの送信先IP	セキュリティログ監視イベント
OSSEC_DestinationPort	文字列	OSSECの送信先ポート	セキュリティログ監視イベント
OSSEC_DestinationUser	文字列	OSSECの送信先ユーザ	セキュリティログ監視イベント
OSSEC_FullLog	文字列	OSSECの完全なログ	セキュリティログ監視イベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
OSSEC_Groups	文字列	OSSECのグループの結果 (例: syslog,authentication_failure)	セキュリティログ監視イベント
OSSEC_Hostname	文字列	OSSECのホスト名。これはログエントリから読み取られたホストの名前であり、イベントが生成されたホストの名前と同じとは限りません。	セキュリティログ監視イベント
OSSEC_ID	文字列	OSSECのID	セキュリティログ監視イベント
OSSEC_Level	整数 (列挙)	OSSECのレベル。0～15の整数。0～3=重要度: 低、4～7=重要度: 中、8～11=重要度: 高、12～15=重要度: 重大。	セキュリティログ監視イベント
OSSEC_Location	文字列	OSSECの場所	セキュリティログ監視イベント
OSSEC_Log	文字列	OSSECのログ	セキュリティログ監視イベント
OSSEC_ProgramName	文字列	OSSECのプログラム名	セキュリティログ監視イベント
OSSEC_Protocol	文字列	OSSECのプロトコル	セキュリティログ監視イベント
OSSEC_RuleID	整数	OSSECのルールID	セキュリティログ監視イベント
OSSEC_SourceIP	整数	OSSECの送信元IP	セキュリティログ監視

プロパティ名	データ タイプ	説明	適用されるイベントの種類
			視イベント
OSSEC_SourcePort	整数	OSSECの送信元ポート	セキュリティログ監視イベント
OSSEC_SourceUser	整数	OSSECの送信元ユーザ	セキュリティログ監視イベント
OSSEC_Status	整数	OSSECのステータス	セキュリティログ監視イベント
OSSEC_SystemName	整数	OSSECのシステム名	セキュリティログ監視イベント
OSSEC_URL	整数	OSSECのURL	セキュリティログ監視イベント
PacketData	整数	取り込まれたパケットデータの16進エンコード (パケットデータを取り込むようにルールで設定されている場合)。	侵入防御イベント
PacketSize	整数	ネットワークパケットのサイズ。	ファイアウォールイベント
Path	文字列	「/usr/bin/」など、許可またはブロックされたソフトウェアファイルのディレクトリパス (ファイル名は「FileName」内に分けられています)。	アプリケーションコントロールイベント
PatternVersion	整数 (列挙)	不正プログラム検出パターンファイルのバージョン。	不正プログラム対策イベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
PayloadFlags	整数	侵入防御フィルタフラグ。次のフラグ値を含むビットマスク値: 1 - データ切り捨て - データをログに記録できませんでした。2 - ログオーバーフロー - このログの後にログがオーバーフローしました。4 - 抑制 - このログの後にログ数のしきい値が抑制されました。8 - データあり - パケットデータが格納されています。16 - 参照データ - 以前にログに記録されたデータを参照しています。	侵入防御イベント
PosInBuffer	整数	イベントをトリガしたデータの packets 内の位置。	侵入防御イベント
PosInStream	整数	イベントをトリガしたデータのストリーム内の位置。	侵入防御イベント
Process	文字列	イベントを生成したプロセスの名前 (該当する場合)。	変更監視イベント
ProcessID	整数	イベントを生成したプロセスの識別子 (PID) (該当する場合)。	アプリケーションコントロールイベント
ProcessName	文字列	「/usr/bin/bash」など、イベントを生成したプロセスの名前 (該当する場合)。	アプリケーションコントロールイベント
Protocol	整数 (列挙)	ネットワークプロトコルの ID。-1=不明、1=ICMP、2=IGMP、3=GGP、6=TCP、12=PUP、17=UDP、22=IDP、58=ICMPv6、77=ND、255=RAW	ファイアウォールイベント、侵入防御イベント
ProtocolString	文字列	Protocolの内容を示す文字列。	ファイアウォールイベント、侵入防御イベント

プロパティ名	<u>データ タイプ</u>	説明	適用されるイベントの種類
Rank	整数	イベントのランク。コンピュータに割り当てられている資産評価に、この重要度のイベントに対して設定されている重要度の値を掛けた数値です。	変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
Reason	文字列	イベントのトリガとなったDeep Securityルールまたは設定オブジェクトの名前。ファイアウォールと侵入防御の場合、ルール以外がトリガとなったイベントではステータスにマッピングされた文字列になります。アプリケーションコントロールでは、「Reason」が「なし」になる場合があります。その場合は、代わりに「BlockReason」を参照してください。	ファイアウォール、侵入防御、変更監視、ログ検査、不正プログラム対策、およびアプリケーションコントロールイベント
RepeatCount	整数	このイベントが繰り返し発生した回数。1の場合は、イベントが1回だけ確認され、その後に繰り返されていないことを示しています。	ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
Risk	整数 (列挙)	アクセスしたURLのリスクレベル: 変換後。2=不審、3=非常に不審、4=危険、5=未評価、6=管理者によるブロック	Webレピュテーションイベント
RiskLevel	整数	URLのリスクレベル: 変換前 (0~100)。URLがブロックルールによってブロックされた場合は表示されません。	Webレピュテーションイベント
RiskString	文字列	Riskの内容を示す文字列。	Webレピュテーションイベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
ScanAction1	整数	検索処理1。検索処理1と2、検索結果処理1と2、およびエラーコードの組み合わせによって1つの「summaryScanResult」が生成されます。	不正プログラム対策イベント
ScanAction2	整数	検索処理2。	不正プログラム対策イベント
ScanResultAction1	整数	検索結果処理1。	不正プログラム対策イベント
ScanResultAction2	整数	検索結果処理2。	不正プログラム対策イベント
ScanResultString	文字列	不正プログラム検索の結果を示す文字列。ScanAction 1と2、ScanActionResult 1と2、およびErrorCodeの組み合わせです。	不正プログラム対策イベント
ScanType	整数 (列挙)	イベントを生成した不正プログラム検索の種類。0=リアルタイム、1=手動、2=予約、3=クイック検索	不正プログラム対策イベント
ScanTypeString	文字列	ScanTypeの内容を示す文字列。	不正プログラム対策イベント
Severity	整数	1=情報、2=警告、3=エラー	システムイベント
Severity	整数 (列挙)	1=低、2=中、3=高、4=重大	変更監視イベント、 侵入防御イベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
SeverityString	文字列	Severityの内容を示す判読可能な文字列。	システムイベント、 変更監視イベント、 侵入防御イベント
SeverityString	文字列	OSSEC_Levelの内容を示す判読可能な文字列。	セキュリティログ監視 イベント
SHA1pacteracontextmathced	文字列	ソフトウェアのSHA-1チェックサム (ハッシュ) (ある場合)。	アプリケーションコントロール イベント
SHA256pacteracontextmathced	文字列	ソフトウェアのSHA-256チェックサム (ハッシュ) (ある場合)。	アプリケーションコントロール イベント
SourceIP	文字列 (IP)	パケットの送信元IPアドレス。	ファイアウォールイベント、 侵入防御イベント
SourceMAC	文字列 (MAC)	パケットの送信元MACアドレス。	ファイアウォールイベント、 侵入防御イベント
SourcePort	整数	パケットのネットワーク送信元ポート番号。	ファイアウォールイベント、 侵入防御イベント
Status	整数	このイベントが特定のファイアウォールルールによって生成されたものでない場合は、約50個のハードコードされたルールのうちのいずれかになります。例: 123=ポリシーで未許可	ファイアウォールイベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
Status	整数	このイベントが特定の侵入防御ルールによって生成されたものでない場合は、約50個のハードコードされたルールの中のいずれかになります。例: -504=無効なUTF8の符号化	侵入防御イベント
Tags	文字列	イベントに適用されているタグのカンマ区切りのリスト。このリストには、イベントの生成時に自動的に適用されるタグのみが含まれます。	すべての種類のイベント
TagSetID	整数	イベントに適用されたタグのグループの識別子。	すべての種類のイベント
TargetID	整数	イベントの対象の一意の識別子。この識別子は、テナント内の同じ種類の対象では一意ですが、異なる種類の対象では同じになる場合があります。たとえば、コンピュータとポリシーの対象IDがどちらも10になることがあります。	システムイベント
TargetIP	文字列 (IP)	Webレピュテーションイベントの生成時にアクセスしていたIPアドレス。	Webレピュテーションイベント
TargetName	文字列	イベントの対象の名前。システムイベントの対象は、コンピュータ、ポリシー、ユーザ、ロール、タスクなど、さまざまです。	システムイベント
TargetType	文字列	イベントの対象の種類。	システムイベント
TenantID	整数	イベントに関連付けられたテナントの一意の識別子。	すべての種類のイベント

プロパティ名	データ タイプ	説明	適用されるイベントの種類
TenantName	文字列	イベントに関連付けられたテナントの名前。	すべての種類のイベント
Title	文字列	イベントのタイトル。	システムイベント
URL	文字列 (URL)	イベントの生成時にアクセスしていたURL。	Webレピュテーションイベント
User	文字列	変更監視イベントの対象となったユーザアカウント (特定された場合)。	変更監視イベント
UserID	文字列	「0」など、ソフトウェアを起動しようとしたユーザアカウントのユーザID (UID) (ある場合)。	アプリケーションコントロールイベント
UserName	文字列	「root」など、ソフトウェアを起動しようとしたユーザアカウントのユーザ名 (ある場合)。	アプリケーションコントロールイベント

イベントプロパティのデータタイプ

JSONとして転送されるイベントでは、通常は他のデータタイプのエンコードに文字列が使用されます。

データ タイプ	説明
ブール	JSON <code>true</code> または <code>false</code> 。
整数	JSON <code>int</code> .Deep Securityのイベントでは、浮動小数点数は出力されません。

データ タイプ	説明
	<p>注意: イベント内の整数は32ビットを超えることがあります。イベント処理用のコードでこの整数を処理できることを確認してください。たとえば、JavaScriptのNumberデータタイプは、32ビットを超える整数を安全に処理できません。</p>
整数 (列挙)	JSON <code>int</code> 。一連の列挙値に限定されます。
文字 列	JSON <code>string</code> 。
文字 列 (日 付)	JSON <code>string</code> 。日時として、YYYY-MM-DDThh:mm:ss.sssZのパターン (ISO 8601) で形式設定されています。「Z」はタイムゾーンです。「sss」は1秒未満の秒数を表す3桁です。 W3Cの日付と時刻の形式に関する説明 も参照してください。
文字 列 (IP)	JSON <code>string</code> 。IPv4またはIPv6アドレスとして形式設定されています。
文字 列 (MAC)	JSON <code>string</code> 。ネットワークMACアドレスとして形式設定されています。
文字 列 (URL)	JSON <code>string</code> 。URLとして形式設定されています。

データ タイプ	説明
文字 列 (列 挙)	JSON string。一連の列挙値に限定されます。

JSON形式のイベントの例

システムイベント

```
{
  "Type" : "Notification",
  "MessageId" : "123abc-123-123-123-123abc",
  "TopicArn" : "arn:aws:sns:us-west-2:123456789:DS_Events",
  "Message" : "[
    {
      "ActionBy": "System",
      "Description": "Alert: New Pattern Update is Downloaded and
Available\\nSeverity: Warning\\",
      "EventID": 6813,
      "EventType": "SystemEvent",
      "LogDate": "2018-12-04T15:54:24.086Z",
      "ManagerNodeID": 123,
      "ManagerNodeName": "job7-123",
      "Number": 192,
      "Origin": 3,
      "OriginString": "Manager",
```

Trend Micro Deep Security On-Premise 12.0

```
        "Severity":1,
        "SeverityString":"Info",
        "Tags":"\",
        "TargetID":1,
        "TargetName":"ec2-12-123-123-123.us-west-
2.compute.amazonaws.com",
        "TargetType":"Host",
        "TenantID":123,
        "TenantName":"Umbrella Corp.",
        "Title":"Alert Ended"
    }
]",
"Timestamp" : "2018-12-04T15:54:25.130Z",
"SignatureVersion" : "1",
"Signature" : "500PER10NG5!gnaTURE==",
"SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
abc123.pem",
"UnsubscribeURL" : "https://sns.us-west-
2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:123456:DS_
Events:123abc-123-123-123-123abc"
}
```

不正プログラム対策イベント

各SNS Messageに複数のウイルス検出イベントを含めることができます (簡略化のため、次の例では繰り返されるイベントプロパティを省略し、「...」で示しています)。

```
{ "Type" : "Notification", "MessageId" : "123abc-123-123-123-123abc", "TopicArn" : "arn:aws:sns:us-west-2:123456789:DS_Events", "Message" : "[ { \"AMTargetTypeString\": \"N/A\", \"ATSEDetectionLevel\": 0, \"CreationTime\": \"2018-12-04T15:57:18.000Z\", \"EngineType\": 1207959848, \"EngineVersion\": \"10.0.0.1040\", \"ErrorCode\": 0, \"EventID\": 1, \"EventType\": \"AntiMalwareEvent\", \"HostAgentGUID\": \"4A5BF25A-4446-DD8B-DFB7-564C275F5F6B\", \"HostAgentVersion\": \"11.1.0.163\", \"HostID\": 1, \"HostOS\": \"Amazon Linux (64 bit) (4.14.62-65.117.amzn1.x86_64)\", \"HostSecurityPolicyID\": 3, \"HostSecurityPolicyName\": \"PolicyA\", \"Hostname\": \"ec2-12-123-123-123.us-west-2.compute.amazonaws.com\", \"InfectedFilePath\": \"/tmp/eicar_1543939038890.txt\", \"LogDate\": \"2018-12-04T15:57:19.000Z\", \"MajorVirusType\": 2, \"MajorVirusTypeString\": \"Virus\", \"MalwareName\": \"Eicar_test_file\", \"MalwareType\": 1, \"ModificationTime\": \"2018-12-04T15:57:18.000Z\", \"Origin\": 0, \"OriginString\": \"Agent\", \"PatternVersion\": \"14.665.00\", \"Protocol\": 0, \"Reason\": \"Default Real-Time Scan Configuration\", \"ScanAction1\": 4, \"ScanAction2\": 3, \"ScanResultAction1\": -81, \"ScanResultAction2\": 0, \"ScanResultString\": \"Quarantined\", \"ScanType\": 0, \"ScanTypeString\": \"Real Time\", \"Tags\": \"\", \"TenantID\": 123, \"TenantName\": \"Umbrella Corp.\"}, { \"AMTargetTypeString\": \"N/A\", \"ATSEDetectionLevel\": 0, \"CreationTime\": \"2018-12-04T15:57:21.000Z\", ... }, { \"AMTargetTypeString\": \"N/A\", \"ATSEDetectionLevel\": 0, \"CreationTime\": \"2018-12-04T15:57:29.000Z\", ... } ]\", \"Timestamp\" : \"2018-12-04T15:57:50.833Z\", \"SignatureVersion\" : \"1\", \"Signature\" : \"500PER10NG5!gnaTURE==\", \"SigningCertURL\" : \"https://sns.us-west-2.amazonaws.com/SimpleNotificationService-abc123.pem\", \"UnsubscribeURL\" : \"https://sns.us-west-
```

```
2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:123456:DS_Events:123abc-123-123-123-123abc" }
```

リモートコンピュータにSNMP経由でシステムイベントを転送

Deep Securityでは、Deep Security Managerからコンピュータへのシステムイベントの転送でSNMPがサポートされます。Windowsの場合、MIBファイル (DeepSecurity.mib) の場所は、\Trend Micro\Deep Security Manager\utilです。Linuxの場合、初期設定の場所は/opt/dsm/utilです。

イベントとアラートのリスト

次のセクションでは、発生する可能性があるDeep Securityのアラートとイベントをすべて示します。

- ["事前定義アラート" on the next page](#)
- ["Agentイベント" on page 1265](#)
- ["システムイベント" on page 1271](#)
- ["アプリケーションコントロールイベント" on page 1317](#)
- ["不正プログラム対策イベント" on page 1319](#)
- ["ファイアウォールイベント" on page 1322](#)
- ["侵入防御イベント" on page 1331](#)
- ["変更監視イベント" on page 1337](#)
- ["セキュリティログ監視イベント" on page 1340](#)

事前定義アラート

アラート	初期設定の重要度	消去可能	説明
異常な再起動の検出	警告	○	<p>コンピュータで異常な再起動が検出されました。この状況は、さまざまな原因で発生します。Agent/Applianceが根本原因であると疑われる場合は、診断パッケージ ([コンピュータの詳細] 画面の [サポート] セクション) を起動する必要があります。</p> <p>このアラートは、Deep Security Agentサービスが異常な状態で再起動されたことを示しています。このアラートは消去してもかまいません。アラートが再度発生した場合は、診断パッケージを作成してテクニカルサポートでサポートケースを開いてください。</p>
有効化の失敗	重大	×	<p>Agent/Applianceに問題がある可能性もありますが、Agentセルフプロテクションが有効になっている場合にもこのエラーが発生します。Deep Security Managerで、[コンピュータエディタ]¹→[設定]→[一般] の順に選択します。[Agentセルフプロテクション] で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。</p>
Deep Security Relayのセキュリティコンポーネントをダウンロードできません	重大	×	<p>Deep Security Relayがセキュリティコンポーネントを正しくダウンロードできません。ネットワーク接続の問題、またはDeep Security Managerの [管理]→[システム設定]→[アップデート] の下の誤った設定が原因である可能性があります。ネットワーク設定 (Relayグループのプロキシ設定など) と [システム設定] を確認し、[管理]→[アップデート]→[ソフトウェア] 画面の [セキュリティアップデートのダウンロード] オプションを使用して手動でRelayのアップデートを開始してください。</p>
Agentの設定パッケージが大きすぎる	警告	○	<p>これは通常、割り当てられているファイアウォールルールおよび侵入防御ルールが多すぎるのが原因です。安全に割り当てを解除できるルールがあるかどうかを判断するには、コンピュータで推奨設定の検索を実行してください。</p>

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

アラート	初期設定の重要度	消去可能	説明
Agentインストールの失敗	重大	○	Agentを1台以上のコンピュータに正常にインストールできませんでした。これらのコンピュータは現在保護されていません。コンピュータを再起動し、Agentインストールプログラムを自動的に再起動する必要があります。 ○ Agent/Applianceに問題がある可能性もありますが、Agentセルフプロテクションが有効になっている場合にもこのエラーが発生します。Deep Security Managerで、 [コンピュータエディタ] ¹ →[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザーによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
Agentのアップグレード推奨 (Applianceと非互換)	警告	×	Deep Security Managerは、Applianceと互換性のないバージョンのAgentがインストールされたコンピュータを検出しました。この構成では、Applianceが常にネットワークトラフィックをフィルタリングするため、保護が冗長になります。(9.5で廃止)
Agent/Applianceのアップグレード推奨	警告	×	Deep Security Managerが、コンピュータの機能の一部をサポートしていない古いバージョンのAgent/Applianceを検出しました。Agent/Applianceソフトウェアのアップグレードを推奨します。(9.5で廃止)
Agent/Applianceのアップグレード推奨 (非互換のセキュリティアップデート)	警告	×	Deep Security Managerは、コンピュータに割り当てられた1つ以上のセキュリティアップデートと互換性のないバージョンのAgent/Applianceがインストールされたコンピュータを検出しました。Agent/Applianceソフトウェアのアップグレードを推奨します。
Agent/Applianceのアップグレード	警告	×	Deep Security Managerは、Managerにインポートされた最新バージョンより古いバージョンのAgent/Applianceがインストールされたコンピュータを検出しました。Agent/Applianceソフトウェ

¹コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

アラート	初期設定の重要度	消去可能	説明
ド推奨 (新しいバージョンが使用可能)			アのアップグレードを推奨します。
Agent/Applianceのアップグレードが必要	警告	×	Deep Security Managerは、本バージョンのManagerと互換性のないバージョンのAgent/Applianceがインストールされたコンピュータを検出しました。Agent/Applianceソフトウェアのアップグレードが必要です。
ルールのアップデートが利用可能	警告	×	アップデートされたルールをダウンロード済みですが、ポリシーに適用されていません。ルールを適用するには、[管理]→[アップデート]→[セキュリティ]に移動し、[ルールアップデート]列で[ルールをポリシーに適用]をクリックします。
不正プログラム対策アラート	警告	○	1台以上のコンピュータで、アラートを発するように設定された不正プログラム検索設定によってイベントが発生しました。
不正プログラム対策コンポーネントの障害	重大	○	1台以上のコンピュータで不正プログラム対策コンポーネントの障害が発生しました。詳細については各コンピュータのイベントの説明を参照してください。
不正プログラム対策コンポーネントのアップデート失敗	警告	×	1つ以上のAgentまたはRelayで不正プログラム対策コンポーネントをアップデートできませんでした。詳しくは該当するコンポーネントを参照してください。
不正プログラム対策エンジンがオフライン	重大	×	AgentまたはApplianceが、不正プログラム対策エンジンが応答していないことをレポートしました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
不正プログラム対策保護がないか、期限切れ	警告	×	このコンピュータのAgentは、不正プログラム対策保護の初期設定パッケージを受信していないか、不正プログラム対策保護の期限が切れています。Relayが使用可能であること、およびAgentからRelayへの通信が正しく設定されていることを確認してください。Relayおよびその他のアップデートオプションを設定するには、[管理]→[システム設定]→[アップデート]に移動します。
不正プログラム対策モジュール	警告	○	検出ファイルの保存に使用する最大ディスク容量に達したため、不正プログラム対策モジュールでファイルを分析または隔離できませんでした。検出ファイルの設定で最大ディスク容量の設定を変更

アラート	初期設定の重要度	消去可能	説明
で検出ファイル保存用の最大ディスク容量を超過			するには、コンピュータエディタまたはポリシーエディタを開き、[不正プログラム対策]→[詳細] タブに移動してください。
APIキーのロックアウト	警告	×	APIキーは、手動でロックアウトできます。また、繰り返し認証に失敗した場合にもロックアウトされます。
アプリケーションコントロールエンジンオフライン	重大	×	エージェントは、アプリケーションコントロールエンジンを初期化できませんでした。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
アプリケーションコントロールルールセットとAgentのバージョンとの間に互換性がありません	重大	×	アプリケーションコントロールルールセットを1台以上のコンピュータに割り当てることができませんでした。これは、インストールされているAgentのバージョンでこのルールセットがサポートされていないためです。通常、ハッシュベースのルールセットが古いDeep Security Agentに割り当てられていることが問題です。ハッシュベースのルールセットと互換性があるのは、Deep Security Agent 11.0以降のみです。Deep Security Agent 10.xでは、ファイルベースのルールセットのみをサポートしています(詳細については、" Deep Security Agent 10と11におけるファイルの比較方法の相違点 " on page 695を参照してください)。この問題を解決するには、Deep Security Agentをバージョン11.0以降にアップグレードしてください。ローカルルールセットを使用している場合は、Agentのアプリケーションコントロールをリセットする方法もあります。また、共有ルールセットを使用している場合は、共有ルールセットを使用するすべてのAgentをDeep Security Agent 11.0以降にアップグレードするまで、Deep Security 10.xで作成した共有ルールセットを使用します。
アプリケーションの種類が誤った設定	警告	×	アプリケーションの種類が誤って設定されている場合は、セキュリティが正しく適用されない可能性があります。
アプリケーションの種類推奨設定	警告	○	Deep Security Managerは、コンピュータにアプリケーションの種類を割り当てる必要があることを検出しました。この理由としては、新しいコンピュータにAgentがインストールされ、脆弱性のあるアプリケーションが検出されたか、以前は安全であると考えられていたインストール済みアプリケーションが新しい脅威として検出されたことが考えられます。コンピュータにアプリケーションの種類

アラート	初期設定の重要度	消去可能	説明
			を割り当てるには、[コンピュータの詳細] ダイアログボックスを開き、[侵入防御ルール] をクリックし、アプリケーションの種類を割り当てます。
AWS契約ライセンス数の超過	重大	×	AWS契約ライセンスが期限切れになっているか、AWS契約資格数を超過しています。
Azure ADアプリケーションのニーズの更新	重大	×	Azure ADアプリケーションでクラウドデータを同期できません。アプリケーションのパスワードの有効期限が切れているか、アプリケーションが削除されている可能性があります。[コンピュータ>のプロパティ] (対象グループを右クリック) でアプリケーションを更新してください。>アプリケーションを更新してください。
Azure ADアプリケーションの有効期限がすぐに終了	警告	×	Azure ADアプリケーションのパスワードがまもなく期限切れになります。このアラートは、[コンピュータ>のプロパティ] (対象グループを右クリック) で更新することで削除できます。[>アプリケーションの更新]
Azureキーペアの期限切れ	重大	×	Azureサービスの鍵のペアが期限切れです。このアラートは、Azureサービスのプロパティページでキーペアをアップデートすることで削除できます。
Azureキーペアがまもなく期限切れ	警告	×	Azureサービスのキーペアはまもなく期限切れになります。このアラートは、Azureサービスのプロパティページでキーペアをアップデートすることで削除できます。
Census、Good File Reputation、機械学習型検索サービスへの接続解除	警告	○	Census、Good File Reputation、機械学習型検索サービスへの接続が解除されました。考えられる解決策については、イベントの詳細を参照してください。 トラブルシューティングのヒントについては、" 警告: Census、Good File Reputation、機械学習型検索サービスへの接続解除 " on page 1372を参照してください。
ソフトウェア安全性評価サービスがオフライン	警告	×	Deep Security Managerノードはトレンドマイクロのソフトウェア安全性評価サービスに接続できないため、変更監視モジュールのファイル署名を比較できません。接続が復旧するまで、ローカルにキャッシュされたデータベースを使用します。Managerノードがインターネット接続されていること、およびプロキシ設定 (ある場合) が正しいことを確認してください。

アラート	初期設定の重要度	消去可能	説明
時計の変更の検出	警告	○	コンピュータで時計の変更が検出されました。時計が予期せず変更された場合は、コンピュータに問題がある可能性があります。アラートを消去する前に調査する必要があります。
クラウドコンピュータがクラウドアカウントで管理されていない	警告	○	Agentが1つ以上のAmazon WorkSpacesで稼働していますが、WorkSpaceが自身のAWSアカウントで無効に設定されています。WorkSpacesを有効にするには、上記の [AWSアカウントの編集] をクリックして、[Amazon WorkSpacesを含める] チェックボックスをオンにします。WorkSpacesがAWSアカウントのWorkSpacesフォルダに移動し、。
通信の問題の検出	警告	○	コンピュータで通信の問題が検出されました。通信の問題は、ネットワーク設定または負荷が原因で、コンピュータがDeep Security Managerとの通信を開始できないことを示しています。コンピュータからDeep Security Managerへの通信が確立できることを確認するとともに、システムイベントもチェックしてください。アラートを消去する前に、問題の原因を調査する必要があります。
コンピュータがアップデートを受信していない	警告	×	これらのコンピュータではアップデートの受信を停止しています。手動の操作が必要になる可能性があります。
コンピュータの再起動が必要	重大	○	Agentソフトウェアのアップデートは正常に完了しましたが、インストールを完了するにはコンピュータの再起動が必要です。アラートを消去するには、コンピュータを手動でアップデートする必要があります。
不正プログラム対策保護を完了するためにコンピュータの再起動が必要	重大	×	Agentの不正プログラム対策保護が、コンピュータの再起動が必要であることをレポートしました。コンピュータのシステムイベントを確認して、再起動の理由を特定してください。
アプリケーションコントロール保護に必要なコンピュータの再起動	重大	×	Agentのアプリケーションコントロールによる保護機能により、コンピュータを再起動する必要があることが報告されました。コンピュータのシステムイベントを確認して、再起動の理由を特定してください。

アラート	初期設定の重要度	消去可能	説明
変更監視保護のためのコンピュータの再起動が必要	重大	×	エージェントの変更監視保護により、コンピュータを再起動する必要があることが報告されました。コンピュータのシステムイベントを確認して、再起動の理由を特定してください。
設定が必要	警告	×	1台以上のコンピュータで、複数のインターフェースの種類を定義するポリシーを使用していますが、マッピングされていないインターフェースがあります。
Filter Driverとの接続失敗	重大	×	Filter Driverへの接続に失敗したことがApplianceからレポートされました。ESXiで実行されているFilter Driver、またはApplianceに設定上の問題がある可能性があります。ゲストを保護するには、ApplianceをFilter Driverに接続できる必要があります。問題の原因を調査し、解決してください。
CPUの重大しきい値の超過	重大	×	CPUの重大しきい値を超過しました。
CPUの警告しきい値の超過	警告	×	CPUの警告しきい値を超過しました。
重複するコンピュータの検出	警告	○	重複するコンピュータが有効化またはインポートされました。必要に応じて、重複するコンピュータを削除し、元のコンピュータを再有効化してください。
重複する一意のIDの検出	警告	×	重複したUUIDが検出されました。重複したUUIDを削除してください。
空のRelayグループの割り当て	重大	×	これらのコンピュータには空のRelayグループが割り当てられています。コンピュータに別のRelayグループを割り当てるか、空のRelayグループにRelayを追加してください。
イベントの抑制	警告	○	Agent/Applianceで予想外に大量のイベントが発生しました。その結果、潜在的なDoS攻撃を防止するために、1つ以上のイベントが記録されませんでした (抑制されました)。ファイアウォールイベントを調べ、抑制原因を確認してください。
イベントの切り捨て	警告	○	データファイルが大きくなりすぎてAgent/Applianceがイベントを保存できなくなったために、一部のイベントが失われました。これは、生成されるイベント数が予想外に増大したこと、またはAgent/ApplianceがDeep Security Managerにデータを送信できなかったことが原因である可能性があります。詳細については、コンピュータ上の「イベントの切り捨て」システムイベントのプロパティを参照してください。

アラート	初期設定の重要度	消去可能	説明
ソフトウェアの実行をブロック	警告	○	1台以上のコンピュータでソフトウェアの実行がブロックされました。詳細については、次のコンピュータのアプリケーション制御イベントを参照してください。
SNSメッセージの送信に失敗しました	重大	×	Amazon SNSにメッセージを転送できませんでした
Syslogメッセージの送信に失敗	警告	×	1台以上のSyslogサーバにメッセージを転送できませんでした。
ファイルで不正プログラムを検索できませんでした	警告	×	ファイルパスの長さまたはディレクトリの深さが上限を超えているため、ファイルで不正プログラムを検索できませんでした。コンピュータのシステムイベントを確認して、原因を特定してください。
ファイアウォールエンジンがオフライン	重大	×	Agent/Applianceにより、ファイアウォールエンジンがオフラインであることがレポートされました。Agent/Applianceのエンジンのステータスを確認してください。
ファイアウォールルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように選択されているファイアウォールルールに合致しました。
ファイアウォールルールの推奨	警告	○	Deep Security Managerは、ネットワークのコンピュータにファイアウォールルールを割り当てる必要があることを検出しました。この理由としては、新しいコンピュータにAgentがインストールされ、脆弱性のあるアプリケーションが検出されたか、以前は安全であると考えられていたインストール済みアプリケーションが新しい脅威として検出されたことが考えられます。コンピュータにファイアウォールルールを割り当てるには、[コンピュータの詳細] ダイアログボックスを開き、[ファイアウォールルール] タブをクリックし、ファイアウォールルールを割り当てます。
ハートビートサーバの失敗	警告	×	ハートビートサーバが正常に起動しませんでした。 ポート番号 の競合が原因である可能性があります。この問題が解決されるまで、Agent/ApplianceはManagerに接続できません。この問題を解決するには、ハートビートサーバ用に確保されているポート番号が別のサービスで使用されていないことを確認し、" Deep Security Managerの再起動 " on page 993 してください。ハートビートを使用しない場合は、[アラートの設定] セクションでこのアラートをオフにできます。

アラート	初期設定の重要度	消去可能	説明
非互換のAgent/Applianceバージョン	警告	×	Deep Security Managerは、本バージョンのManagerと互換性のない新しいバージョンのAgent/Applianceがインストールされたコンピュータを検出しました。Managerソフトウェアのアップグレードをお勧めします。
ディスク容量の不足	警告	○	Agent/Applianceで、古いログファイルを強制的に削除して新しいログファイル用に空きディスク容量を確保したことがレポートされました。侵入防御、ファイアウォール、およびAgent/Applianceのイベントの消失を防ぐため、必要な空きディスク容量をただちに確保してください。" 警告: ディスク容量の不足 " on page 1374を参照してください。
変更監視エンジンがオフライン	重大	×	Agent/Applianceが、変更監視エンジンが応答していないことをレポートしました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
変更監視情報の収集が遅延しています	警告	×	変更監視データ量が増加したため、変更監視情報を収集する速度が一時的に遅延しています。この間、一部のコンピュータでベースラインと整合性イベントの表示が最新ではなくなる可能性があります。変更監視データに遅延がなくなると、このアラートは自動的に消去されます。
変更監視ルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように選択されている変更監視ルールに合致しました。
変更監視ルールのコンパイルエラー	重大	×	コンピュータで変更監視ルールをコンパイルしているときに、エラーが発生しました。その結果、変更監視ルールが予期したとおりに動作しないことがあります。
変更監視ルールの推奨	警告	○	Deep Security Managerは、ネットワークのコンピュータに変更監視ルールを割り当てる必要があることを検出しました。コンピュータに変更監視ルールを割り当てるには、[コンピュータの詳細] ダイアログボックスを開き、[変更監視]→[変更監視ルール] ノードをクリックし、変更監視ルールを割り当てます。
変更監視ルールの設定が必要	警告	×	使用前に設定が必要な変更監視ルールが、1台以上のコンピュータに割り当てられています。このルールはコンピュータに送信されません。詳細については、変更監視ルールのプロパティを開き、[設定] タブを選択してください。
変更監視のTPMが無効です	警告	○	TPMが無効になっています。ハードウェアがインストールされていること、およびBIOSの設定が正しいことを確認してください。
変更監視のTPM	警	○	TPMのレジスタ値が変更されました。ESXiハイパーバイザの設定を変更していない場合は、攻撃を受

アラート	初期設定の重要度	消去可能	説明
レジスタ値が変更されました	告		けた可能性があります。
侵入防御エンジンがオフライン	重大	×	Agent/Applianceにより、侵入防御エンジンがオフラインであることがレポートされました。Agent/Applianceのエンジンのステータスを確認してください。
侵入防御ルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように設定されている侵入防御ルールに合致しました。
侵入防御ルールのコンパイルに失敗しました	重大	○	これは通常、侵入防御ルールの設定が間違っていることが原因です。ルール名はイベントの[プロパティ]画面で確認できます。この問題を解決するには、ルールを特定して割り当て解除するか、トレンドマイクロのサポートにお問い合わせください。
侵入防御ルールの設定が必要	警告	×	使用前に設定が必要な侵入防御ルールが、1台以上のコンピュータに割り当てられています。このルールはコンピュータに送信されません。詳細については、侵入防御ルールのプロパティを開き、[設定] タブを選択してください。
無効なシステム設定を検出	重大	×	1つ以上のシステム設定で無効な値が検出されました
レガシーのAgentソフトウェアが検出されました	警告	○	バージョンが9.5未満の現在サポートされていないソフトウェアが検出されました。最新のソフトウェアをインポートして置き換えてください。 詳細については、" Deep Security Agentソフトウェアの入手 " on page 372を参照してください。
セキュリティログ監視エンジンがオフライン	重大	×	Agent/Applianceにより、セキュリティログ監視エンジンの初期化に失敗したことがレポートされました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
セキュリティログ監視ルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように設定されているセキュリティログ監視ルールに合致しました。
セキュリティログ監視ルールの推奨	警告	○	Deep Security Managerは、ネットワークのコンピュータにセキュリティログ監視ルールを割り当てる必要があることを検出しました。コンピュータにセキュリティログ監視ルールを割り当てるには、[コンピュータの詳細] ダイアログボックスを開き、[セキュリティログ監視]→[セキュリティログ監視

アラート	初期設定の重要度	消去可能	説明
			ルール] ノードをクリックし、セキュリティログ監視ルールを割り当てます。
セキュリティログ監視ルールに設定が必要	警告	×	使用前に設定が必要なセキュリティログ監視ルールが、1台以上のコンピュータに割り当てられています。このルールはコンピュータに送信されません。詳細については、セキュリティログ監視ルールのプロパティを開き、[設定] タブを選択してください。
ディスク容量不足	警告	×	Deep Security Managerノードのディスク容量が残り10%未満です。古いファイルや不要なファイルを削除して空き容量を増やすか、ストレージ容量を追加してください。
メンテナンスモードが有効	警告	×	1台以上のコンピュータで、アプリケーションコントロールのメンテナンスモードが有効になっています。このモードを有効にすると、ブロックルールは引き続き適用されますが ([承認されていないソフトウェアを明示的に許可するまでブロック] を選択した場合)、ソフトウェアアップデートは許可され、その後自動的にルールセットのインベントリ部分に追加されます。各コンピュータでソフトウェアのアップデートが終了したら、承認されていないソフトウェアが誤ってルールセットに追加されないように、メンテナンスモードを無効にしてください。
Managerがオフライン	警告	×	Deep Security Managerノードがオフラインです。理由としては、コンピュータでハードウェアまたはソフトウェアの問題が発生したか、単純にネットワーク接続が切断されたことが考えられます。Managerのコンピュータのステータスを確認してください。
Managerの時刻が非同期	重大	×	各Managerノードの時計はデータベースの時計と同期されている必要があります。時計間の時刻の差が30秒を超える場合、Managerノードのタスクは正常に実行されません。Managerノードの時計をデータベースの時計と同期してください。
メモリの重大しきい値の超過	重大警告	×	メモリの重大しきい値を超過しました。
メモリの警告しきい値の超過	警告	×	メモリの警告しきい値を超過しました。
複数の有効化されたApplianceの検出	警告	○	同じESXi上のFilter Driverへの接続が複数確立されたことがApplianceからレポートしました。同じESXi上で有効化されたApplianceが複数実行されている可能性があります。この状況はサポートされていません。アラートを消去する前に、問題の原因を調査する必要があります。
ネットワークエンジンモードの	警告	×	「ネットワークエンジンモード」を「タップ」に設定できるのは、Agentバージョン5.2以降のみです。互換性の問題を解決するには、Agentの設定を確認してアップデートするか、Agentをアップグ

アラート	初期設定の重要度	消去可能	説明
非互換性			レードしてください。
新しいパターンファイルアップデートがダウンロード済みで利用可能	警告	×	セキュリティアップデートの一部として、新しいパターンファイルを利用できます。パターンファイルはDeep Securityにダウンロード済みですが、まだコンピュータに適用されていません。コンピュータにアップデートを適用するには、[管理]→[アップデート]→[セキュリティ]画面に移動してください。
新しいルールアップデートがダウンロード済みで利用可能	警告	×	セキュリティアップデートの一部として、新しいルールを利用できます。ルールはDeep Securityにダウンロード済みですが、まだポリシーに適用されておらず、コンピュータに送信されていません。アップデートを適用し、更新されたポリシーをコンピュータに送信するには、[管理]→[アップデート]→[セキュリティ]画面に移動してください。
新しいバージョンのDeep Security Managerが利用可能	警告	×	新しいバージョンのDeep Security Managerが利用可能です。トレンドマイクロのダウンロードセンター (https://help.deepsecurity.trendmicro.com/ja-jp/software.html) から最新バージョンをダウンロードしてください。
新しいバージョンのソフトウェアが利用可能	警告	×	新しいソフトウェアを利用できます。ダウンロードセンターからソフトウェアをダウンロードできます。
コンピュータ数がデータベースの上限を超過	警告	×	有効化されたコンピュータの数が、組み込みデータベースに対して推奨される上限を超過しています。さらにコンピュータが追加された場合はパフォーマンスの急速な低下が発生するため、現時点で他のデータベースオプション (OracleまたはSQL Server) を検討することを強くお勧めします。
保護モジュールライセンスが期限切れ	警告	○	保護モジュールライセンスが有効期限切れになりました。
保護モジュールライセンスがまもなく期限切れ	警告	×	保護モジュールライセンスはまもなく有効期限切れになります。このアラートは、[管理]→[ライセンス]画面でライセンスを変更すると削除されます。

アラート	初期設定の重要度	消去可能	説明
推奨設定	警告	○	Deep Security Managerは、1台のコンピュータのセキュリティ設定をアップデートする必要があることを検出しました。推奨されている変更点を確認するには、 コンピュータエディタ¹ を開き、モジュールの画面で未解決の推奨設定に関する警告を確認してください。割り当て済みのルールで、[割り当て/割り当て解除]をクリックして使用可能なルールのリストを表示してから、[割り当てに推奨される設定の表示]フィルタオプションを使用してフィルタします(安全に割り当てを解除できるルールを表示するには、[割り当て解除に推奨される設定の表示]を選択します)。
攻撃の予兆の検出: OSのフィンガープリント調査	警告	○	AgentまたはApplianceは、「フィンガープリント」調査によってコンピュータのOSを識別しようとする動作を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、 "警告: 攻撃の予兆の検出" on page 1374 を参照してください。
攻撃の予兆の検出: ネットワークまたはポートの検索	警告	○	AgentまたはApplianceが、ネットワークまたはポート検索特有のネットワークアクティビティを検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、 "警告: 攻撃の予兆の検出" on page 1374 を参照してください。
攻撃の予兆の検出: TCP Null検索	警告	○	AgentまたはApplianceで、TCP「null」の検索を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、 "警告: 攻撃の予兆の検出" on page 1374 を参照してください。
攻撃の予兆の検出: TCP SYNFIN検索	警告	○	AgentまたはApplianceで、TCP「SYNFIN」の検索を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、 "警告: 攻撃の予兆の検出" on page 1374 を参照してください。
攻撃の予兆の検出: TCP Xmas検索	警告	○	AgentまたはApplianceで、TCP「Xmas」の検索を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、 "警告: 攻撃の予兆の検出" on page 1374 を参照してください。
SAMLアイデンティティプロバ	重大	×	1つ以上のSAML IDプロバイダ証明書の期限が切れました。

¹コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

アラート	初期設定の重要度	消去可能	説明
イダ証明書の期限が切れました			
SAMLアイデンティティプロバイダ証明書がまもなく期限切れになります	警告	×	1つ以上のSAML IDプロバイダ証明書がまもなく期限切れになります。
SAPウイルス検索アダプタがインストールされていません	重大	×	Agentにより、SAPウイルス検索アダプタがインストールされていないことがレポートされました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
SAPウイルス検索アダプタが最新ではありません	重大	×	Agentにより、SAPウイルス検索アダプタが最新でないことがレポートされました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
不正プログラムの予約検索がスキップされました	警告	×	保留中の予約検索タスクがあるコンピュータで、不正プログラムの予約検索が開始されました。検索の頻度が高すぎる可能性があります。検索の頻度を低くするか、予約検索時に検索するコンピュータの台数を減らすことを検討してください。
ポリシー送信の失敗	重大	×	ポリシーを送信できない場合は、Agent/Applianceに問題がある可能性があります。該当するコンピュータを確認してください。
Smart Protection Serverとの接続失敗	警告	○	Smart Protection Serverへの接続に失敗しました。これは、設定の問題またはネットワーク接続が原因である可能性があります。
ソフトウェアパッケージが見つかりません	重大	×	1台以上のVirtual Applianceで、操作を正常に実行するためにAgentソフトウェアパッケージが必要です。各Applianceに対応するバージョンのRed Hat Enterprise Linux 6 (64ビット) Agentソフトウェア

アラート	初期設定の重要度	消去可能	説明
			アパッケージをインポートしてください。必要なバージョンを入手できない場合は、最新パッケージをインポートし、そのバージョンに合わせてApplianceをアップグレードしてください。
ソフトウェアアップデートをインポート可能	警告	×	新しいソフトウェアを利用できます。新しいソフトウェアをDeep Securityにインポートするには、[管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]に移動します。
通信不能	重大	×	Deep Security Managerは、設定された期間内にAgent/Aplianceのステータスを検索できませんでした。ネットワーク設定と該当するコンピュータの接続を確認してください。
Agentソフトウェアのアップグレード失敗	警告	○	Deep Security Managerが、コンピュータのAgentソフトウェアをアップグレードできませんでした。 Agent/Aplianceに問題がある可能性もありますが、Agentセルフプロテクションが有効になっている場合にもこのエラーが発生します。Deep Security Managerで、 [コンピュータエディタ] ¹ →[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
ソフトウェア変更を検出	警告	×	実行中のファイルシステム監視で、新しいソフトウェアがインストールされたこと、およびそのソフトウェアが設定されている許可またはブロックルールと一致しなかったことが、アプリケーションコントロールによって検出されました。システム管理者がソフトウェアをインストールしておらず、また他のユーザにソフトウェアのインストール権限が与えられていない場合は、セキュリティ侵害の可能性があります。ソフトウェアが起動を試みた場合、実行が許可されるかどうかはその時点でのロックダウン設定によって決まります。
未解決のソフトウェア変更数の	重大	×	ファイルシステムで検出されたソフトウェア変更数が上限を超えました。アプリケーションコントロールは引き続き既存のルールを適用しますが、これ以上の変更は記録されず、このコンピュータで

¹コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

アラート	初期設定の重要度	消去可能	説明
上限に達しました			のソフトウェアの変更は表示されなくなります。この状況を解決し、大量のソフトウェア変更が発生しないようにする必要があります。
Deep Security Managerソフトウェアのアップグレード推奨 (非互換のセキュリティアップデート)	警告	×	Deep Security Managerは、現在のバージョンのDeep Security Managerと互換性のないセキュリティアップデートを使用しているコンピュータを検出しました。Deep Security Managerソフトウェアのアップグレードをお勧めします。
Filter Driverのアップグレード推奨 (新しいバージョンが使用可能)	警告	×	Deep Security Managerは、使用可能な最新バージョンではないFilter DriverがインストールされたESXiサーバを検出しました。Filter Driverのアップグレードをお勧めします。
ユーザのロックアウト	警告	×	ユーザは手動で、不正ログオンが繰り返し試行された場合、ユーザのパスワードの期限が切れた場合、またはインポートされたもののロック解除されていない場合、ロックアウトされることがあります。
ユーザパスワードがまもなく有効期限切れ	警告	×	パスワードの有効期限の設定が有効になっており、7日以内にパスワードが期限切れになるユーザが1人以上います。
Virtual ApplianceとFilter Driverの互換性なし	警告	×	ApplianceがFilter Driverと互換性がありません。両方とも最新バージョンにアップグレードされていることを確認してください。
仮想マシンインタフェースの非同期	警告	×	Deep Security Virtual Applianceによって監視されている1つ以上の仮想マシンで、インタフェースがFilter Driverと同期していないことがレポートされました。これは、Applianceが仮想マシンのインタフェースを適切に監視していない可能性があることを意味しています。問題を解決するには、設定の変更や再起動などの手動操作を仮想マシンで実行しなければならないことがあります。

アラート	初期設定の重要度	消去可能	説明
保護されていないESXiサーバへの仮想マシンの移動	警告	<input type="radio"/>	有効化されたDeep Security Virtual ApplianceがないESXiサーバに、仮想マシンが移動されました。
別のESXiへの移動後に仮想マシンが保護されていない	警告	<input type="radio"/>	Applianceで保護されている仮想マシンが、別のESXiへの移動中または移動後に、保護されていませんでした。移動中にApplianceが再起動したか、電源がオフになったか、あるいは設定に問題がある可能性があります。アラートを消去する前に、問題の原因を調査する必要があります。
VMware Toolsがインストールされていない	重大	<input type="radio"/>	NSX環境内の保護されている仮想マシンにVMware Toolsがインストールされていない。NSX環境で仮想マシンを保護するにはVMware Toolsが必要です。
Webレピュテーションイベントアラート	警告	<input type="radio"/>	アラートを発するように設定されている1台以上のコンピュータで、Webレピュテーションイベントが発生しました。
AWSアカウントで無効にされたWorkSpaces	警告	<input type="radio"/>	Agentが1つ以上のAmazon WorkSpacesで稼働していますが、WorkSpacesが自身のAWSアカウントで無効に設定されています。WorkSpacesを有効にするには、上記の [AWSアカウントの編集] をクリックして、[Amazon WorkSpacesを含める] チェックボックスをオンにします。WorkSpacesがAWSアカウントのWorkSpacesフォルダに移動します。。

Agentイベント

ID	重要度	イベント	備考
特殊なイベント			
0	エラー	不明なAgent/Applianceイベント	
ドライバ関連のイベント			

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	備考
1000	エラー	エンジンを開けません	
1001	エラー	エンジンコマンドの失敗	
1002	警告	エンジンリストオブジェクトエラー	
1003	警告	オブジェクトの削除失敗	
1004	エラー	ドライバのアップグレードの停止	
1005	警告	ドライバのアップグレード中	
1006	エラー	ドライバのアップグレードで再起動が必要	
1007	警告	ドライバのアップグレード成功	
1008	エラー	サポートされないカーネル	
設定関連のイベント			
2000	情報	ポリシー送信	
2001	警告	無効なファイアウォールルール割り当て	
2002	警告	無効なファイアウォールステートフル設定	
2003	エラー	セキュリティ設定の保存失敗	
2004	警告	無効なインターフェース割り当て	
2005	警告	無効なインターフェース割り当て	
2006	警告	無効な処理	
2007	警告	無効なパケット方向	
2008	警告	無効なルール優先度	
2009	警告	認識できないIPアドレスの形式	
2010	警告	無効な送信元IPリスト	
2011	警告	無効な送信元ポートリスト	
2012	警告	無効な送信先IPリスト	
2013	警告	無効な送信先ポートリスト	
2014	警告	無効なスケジュール	
2015	警告	無効な送信元MACリスト	
2016	警告	無効な送信先MACリスト	
2017	警告	無効なスケジュール長	
2018	警告	無効なスケジュール文字列	
2019	警告	認識できないIPアドレスの形式	
2020	警告	オブジェクトが見つかりません	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	備考
2021	警告	オブジェクトが見つかりません	
2022	警告	無効なルールの割り当て	
2050	警告	ファイアウォールルールが見つかりません	
2075	警告	トラフィックストリームが見つかりません	
2076	警告	侵入防御ルールが見つかりません	
2077	警告	パターンリストが見つかりません	
2078	警告	トラフィックストリーム変換エラー	
2080	警告	条件付きファイアウォールルールが見つかりません	
2081	警告	条件付き侵入防御ルールが見つかりません	
2082	警告	空白の侵入防御ルール	
2083	警告	侵入防御ルールのXMLルール変換エラー	
2085	エラー	セキュリティ設定エラー	
2086	警告	サポートされていないIPマッチタイプ	
2087	警告	サポートされていないMACマッチタイプ	
2088	警告	無効なSSL資格情報	
2089	警告	SSL資格情報がありません	
2090	エラー	セキュリティ設定エラー	
2091	エラー	セキュリティ設定エラー	
ハードウェア関連のイベント			
3000	警告	無効なMACアドレス	
3001	警告	イベントデータの取得失敗	
3002	警告	過剰なインタフェース	
3003	エラー	外部コマンドの実行不能	
3004	エラー	外部コマンド出力の読み取り不能	
3005	エラー	OS呼び出しエラー	
3006	エラー	OS呼び出しエラー	
3007	エラー	ファイルエラー	
3008	エラー	コンピュータ固有のキーエラー	
3009	エラー	Agent/Applianceの予期しないシャットダウン	

ID	重要度	イベント	備考
3010	エラー	Agent/Applianceデータベースエラー	
3300	警告	イベントデータの取得失敗	Linuxエラー。
3302	警告	セキュリティ設定の取得失敗	Linuxエラー。
3303	エラー	ファイルマッピングエラー	Linuxエラー。ファイルタイプエラー。
3600	エラー	Windowsシステムディレクトリの取得失敗	
3601	警告	ローカルデータ読み取りエラー	Windowsエラー。
3602	警告	Windowsサービスエラー	Windowsエラー。
3603	エラー	ファイルマッピングエラー	Windowsエラー。ファイルサイズエラー。
3700	警告	異常な再起動の検出	Windowsエラー。
3701	情報	システムの前回起動時刻の変化	Windowsエラー。
通信関連のイベント			
4000	警告	無効なプロトコルヘッダ	コンテンツ長が範囲外です。
4001	警告	無効なプロトコルヘッダ	コンテンツ長がありません。
4002	情報	コマンドセッションの開始	
4003	情報	設定セッションの開始	
4004	情報	コマンドの受信	
4011	警告	Managerへの接続に失敗しました	
4012	警告	ハートビートの失敗	
Agent関連のイベント			
5000	情報	Agent/Applianceの開始	
5001	エラー	スレッド例外	
5002	エラー	オペレーションタイムアウト	
5003	情報	Agent/Applianceの停止	
5004	警告	時計の変更	
5005	情報	Agent/Applianceの監査開始	
5006	情報	Agent/Applianceの監査停止	
5007	情報	Appliance保護の変更	
5008	警告	Filter Driver接続の失敗	
5009	情報	Filter Driver接続の成功	
5010	警告	Filter Driverの情報イベント	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	備考
5100	情報	保護モジュールの配信開始	
5101	情報	保護モジュールの配信成功	
5102	エラー	保護モジュールの配信失敗	
5103	情報	保護モジュールのダウンロード成功	
5104	情報	保護モジュールの無効化開始	
5105	情報	保護モジュールの無効化成功	
5106	エラー	保護モジュールの無効化失敗	
5107	情報	Agentセルフプロテクションの有効化	
5108	情報	Agentセルフプロテクションの無効化	
5109	エラー	FIPS検証エラー	
5200	情報	ファイルバックアップ完了	
5201	エラー	ファイルバックアップ失敗	
ログ記録関連のイベント			
6000	情報	ログデバイスオープンエラー	
6001	情報	ログファイルオープンエラー	
6002	情報	ログファイル書き込みエラー	
6003	情報	ログディレクトリ作成エラー	
6004	情報	ログファイル検索エラー	
6005	情報	ログディレクトリオープンエラー	
6006	情報	ログファイル削除エラー	
6007	情報	ログファイルの名前変更エラー	
6008	情報	ログ読み取りエラー	
6009	警告	空き容量不足によるログファイルの削除	
6010	警告	イベントは抑制されました	
6011	警告	イベントの切り捨て	
6012	エラー	ディスク容量の不足	"警告: ディスク容量の不足" on page 1374を参照してください。
6013	警告	Agentの設定パッケージが大きすぎる	
攻撃関連、検索関連、調査関連のイベント			
7000	警告	OSのフィンガープリント調査	
7001	警告	ネットワークまたはポートの検索	
7002	警告	TCP Null検索	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	備考
7003	警告	TCP SYNFIN検索	
7004	警告	TCP Xmas検索	
セキュリティアップデートのダウンロードのイベント			
9050	情報	Agentでの不正プログラム対策コンポーネントのアップデート成功	
9051	エラー	Agentでの不正プログラム対策コンポーネントのアップデート失敗	
9100	情報	セキュリティアップデート成功	
9101	エラー	セキュリティアップデートの失敗	
9102	エラー	セキュリティアップデートの失敗	エラーメッセージに特定の情報が記録されました。
Relayのイベント			
9103	情報	Relay Webサーバの無効化	
9104	情報	Relay Webサーバの有効化	
9105	エラー	Relay Webサーバの有効化の失敗	
9106	エラー	Relay Webサーバの無効化の失敗	
9107	エラー	Relay Webサーバの失敗	
9108	情報	アップデート元に接続不能	
9109	エラー	コンポーネントのアップデートの失敗	
9110	エラー	不正プログラム対策のライセンスの期限切れ	
9111	情報	セキュリティアップデートのロールバック成功	
9112	エラー	セキュリティアップデートのロールバック失敗	
9113	情報	Relayによるすべてのパッケージの複製	
9114	エラー	Relayによるすべてのパッケージの複製に失敗	
9115	情報	Relay Webサーバからのダウンロードに失敗しました	
変更の検索のステータスに関するイベント			
9201	情報	変更の検索の開始	
9203	情報	変更の検索の異常終了	

ID	重要度	イベント	備考
9204	情報	変更の検索の一時停止	
9205	情報	変更の検索の再開	
9208	警告	変更の検索の開始失敗	
9209	警告	変更の検索の停止	
Smart Protection Serverのステータスに関するイベント			
9300	警告	Webレピュテーション用のSmart Protection Serverへの接続不能	"「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1346を参照してください。
9301	情報	Webレピュテーション用のSmart Protection Serverへの接続	"「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1346を参照してください。
9302	警告	Census、Good File Reputation、機械学習型検索サービスへの接続解除	
9303	情報	Census、Good File Reputation、機械学習型検索サービスへの接続	

システムイベント

システムイベントを表示するには、[イベントとレポート]→[イベント]の順に選択します。

システムイベントを設定するには、[管理]→[システム設定]→[システムイベント]タブの順に選択します。このタブでは、個々のイベントを記録するかどうか、また[SIEMサーバに転送](#)するかどうかを設定できます。[記録する]を選択した場合は、イベントがデータベースに保存されます。[記録する]を選択解除した場合は、[イベントとレポート]タブ (またはDeep Security Manager内) にイベントが表示されなくなり、イベントの転送も行われなくなります。

システム設定の変更かセキュリティインシデントかに応じて、[システムイベント]サブメニュー、またはイベントの保護モジュールに対応するサブメニュー ([不正プログラム対策イベント] など) に各ログが表示されます。

これらのイベントは、[コンピュータ]の[ステータス]列にも表示される場合があります。

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
0	エラー	不明なエラー	
100	情報	Deep Security Managerの開始	
101	情報	ライセンスの変更	
102	情報	Trend Micro Deep Securityユーザアカウントの変更	
103	警告	アップデートの確認の失敗	
104	警告	ソフトウェアの自動ダウンロードの失敗	
105	警告	スケジュールルールアップデートのダウンロードおよび適用の失敗	
106	情報	スケジュールルールアップデートのダウンロードおよび適用	
107	情報	ルールアップデートのダウンロードおよび適用	
108	情報	スクリプト実行	
109	エラー	スクリプト実行の失敗	
110	情報	システムイベントのエクスポート	
111	情報	ファイアウォールイベントのエクスポート	
112	情報	侵入防御イベントのエクスポート	
113	警告	スケジュールルールアップデートのダウンロード失敗	
114	情報	スケジュールルールアップデートのダウンロード	
115	情報	ルールアップデートのダウンロード	
116	情報	ルールアップデートの適用	
117	情報	Deep Security Managerのシャットダウン	
118	警告	オフラインのDeep Security Manager	
119	情報	Deep Security Managerのオンライン復帰	
120	エラー	ハートビートサーバの失敗	受信Agentハートビートを待機するDeep Security Manager内のサーバが起動しませんでした。

ID	重要度	イベント	説明または解決策
			Managerの 受信ハートビートポート番号 が、サーバ上の他のアプリケーションによって使用されていないことを確認してください。ポートが確保されると、Managerのハートビートサーバがそのポートにバインドされてエラーが解決します。
121	エラー	スケジューラの失敗	
122	エラー	Managerのメッセージスレッドの失敗	内部スレッドが失敗しました。このエラーの解決策はありません。このエラーが解決しない場合は、カスタマーサポートにお問い合わせください。
123	情報	Deep Security Managerの強制シャットダウン	
124	情報	ルールアップデートの削除	
130	情報	資格情報の生成	
131	警告	資格情報の生成の失敗	
140	情報	コンピュータの検出	
141	警告	コンピュータの検出の失敗	
142	情報	コンピュータの検出の要求	
143	情報	コンピュータの検出のキャンセル	
150	情報	システム設定の保存	
151	情報	ソフトウェアの追加	
152	情報	ソフトウェアの削除	
153	情報	ソフトウェアのアップデート	
154	情報	ソフトウェアのエクスポート	
155	情報	ソフトウェアプラットフォームの変更	
156	エラー	Agentインストーラのデジタル署名の検証に失敗しました	デジタル署名の確認に失敗したため、「<エージェント>.zip」が削除されました。この失敗は、ファイルが改ざんされている可能性を示しています。詳細: <detailed_message>

ID	重要度	イベント	説明または解決策
			<p>詳細については、トレンドマイクロのサポート担当者にお問い合わせください。</p> <p>詳細については、"ソフトウェアパッケージのデジタル署名の確認" on page 216を参照してください。</p>
160	情報	認証の失敗	
161	情報	ルールアップデートのエクスポート	
162	情報	セキュリティログ監視イベントのエクスポート	
163	情報	不正プログラム対策のイベントのエクスポート	
164	情報	セキュリティアップデート成功	
165	エラー	セキュリティアップデートの失敗	
166	情報	新規ソフトウェアの確認の成功	
167	エラー	新規ソフトウェアの確認の失敗	
168	情報	手動セキュリティアップデートの成功	
169	エラー	手動セキュリティアップデートの失敗	
170	エラー	Managerの利用可能ディスク容量の不足	<p>Managerのディスク空き容量が不足しているため、シャットダウンします。ディスク容量を拡張するか、使用していないファイルを削除してディスク容量を確保してから、"Deep Security Managerの再起動" on page 993をしてください。</p>
171	情報	不正プログラム対策のスパイウェアアイテムのエクスポート	
172	情報	Webレピュテーションイベントのエクスポート	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
173	情報	不正プログラム対策の検出ファイルリストのエクスポート	
174	情報	不正プログラム対策の不正変更対象アイテムのエクスポート	
180	情報	アラートの種類のアップデート	
190	情報	アラートの開始	
191	情報	アラートの変更	
192	情報	アラートの終了	
197	情報	アラートメールの送信	
198	警告	アラートメールの失敗	アラートメールを送信できませんでした。 SMTP設定 が正しく設定されていることを確認してください。
199	エラー	アラート処理の失敗	アラートが完全に処理されていないため、現在のアラートのステータスが正確ではない可能性があります。問題が解決しない場合は、サポート担当者にお問い合わせください。
248	情報	ソフトウェアアップデート: Relayの無効化要求	
249	情報	ソフトウェアアップデート: Relayの有効化要求	
250	情報	コンピュータの作成	
251	情報	コンピュータの削除	
252	情報	コンピュータのアップデート	
253	情報	コンピュータへのポリシーの割り当て	
254	情報	コンピュータの移動	
255	情報	有効化の要求	
256	情報	ポリシー送信の要求	
257	情報	ロック	
258	情報	ロック解除	
259	情報	無効化の要求	

ID	重要度	イベント	説明または解決策
260	情報	オープンポートの検索	
261	警告	オープンポートの検索の失敗	
262	情報	オープンポートの検索の要求	
263	情報	オープンポートの検索のキャンセル	
264	情報	Agentソフトウェアのアップグレード要求	
265	情報	Agentソフトウェアのアップグレードのキャンセル	
266	情報	警告/エラーのクリア	
267	情報	ステータスの確認の要求	
268	情報	イベントの取得の要求	
269	情報	クラウドコネクタへのコンピュータの追加	
270	エラー	コンピュータの作成の失敗	
271	情報	Agentソフトウェアのアップグレードのタイムアウト	
272	情報	Applianceソフトウェアのアップグレードのタイムアウト	
273	情報	セキュリティアップデート: セキュリティアップデートの確認とダウンロード要求	
274	情報	セキュリティアップデート: セキュリティアップデートのロールバック要求	
275	警告	重複するコンピュータ	
276	情報	アップデート: 概要情報	
277	情報	Agentソフトウェアの自動アップグレードがスキップされました	Agentは自動アップグレードの対象になっていましたが、アップグレードは実行されませんでした。詳細については、" Agentを有効化するとき自動的にアップグレードする " on page 397を参照してください。
278	情報	ソフトウェアアップデート: Agentソフトウェアのアップグレードを完了するには、再起動する必要があります	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
280	情報	コンピュータのエクスポート	
281	情報	コンピュータのインポート	
286	情報	コンピュータのログのエクスポート	
287	情報	コンピュータへのRelayグループの割り当て	
290	情報	グループの追加	
291	情報	グループの削除	
292	情報	グループのアップデート	
293	情報	インタフェース名の変更	
294	情報	コンピュータブリッジ名の変更	
295	情報	インタフェースの削除	
296	情報	インタフェースIPの削除	
297	情報	推奨設定の検索要求	
298	情報	推奨設定のクリア	
299	情報	コンピュータへの資産評価の割り当て	
300	情報	推奨設定の検索完了	
301	情報	Agentソフトウェアの配信の要求	
302	情報	Agentソフトウェアの削除の要求	
303	情報	コンピュータ名の変更	
304	情報	データセンターへのコンピュータの移動	Deep Security Managerでは、権限の問題によりVMの上位フォルダを特定できなかったため、仮想マシン（VM）がルートデータセンターフォルダに配置されました。Deep Security Managerの正しいフォルダにVMを表示するには、vCenter Server上のVMの権限を確認します。
305	情報	変更の検索の要求	
306	情報	ベースラインの再構築の要求	
307	情報	アップデートの要求のキャンセル	
308	情報	変更監視ルールのコンパイルの問題	
309	情報	変更監視ルールのコンパイルの問題の解決	
310	情報	ディレクトリの追加	

ID	重要度	イベント	説明または解決策
311	情報	ディレクトリの削除	
312	情報	ディレクトリのアップデート	
320	情報	ディレクトリ同期	
321	情報	ディレクトリ同期の完了	
322	エラー	ディレクトリ同期の失敗	
323	情報	ディレクトリ同期の要求	
324	情報	ディレクトリ同期のキャンセル	
325	情報	ユーザ同期	ユーザアカウントとMicrosoft Active Directoryとの同期が開始されました。
326	情報	ユーザ同期の完了	ユーザアカウントとMicrosoft Active Directoryとの同期が完了しました。
327	エラー	ユーザ同期の失敗	
328	情報	ユーザ同期の要求	
329	情報	ユーザ同期のキャンセル	
330	情報	SSL設定の作成	
331	情報	SSL設定の削除	
332	情報	SSL設定のアップデート	
333	情報	ホストのマージ完了	
334	エラー	ホストのマージ失敗	
338	警告	ディレクトリの同期の制限を超えました	Active Directory同期のグループメンバーの合計数に達しました。残りのメンバーをスキップします。
350	情報	ポリシーの作成	
351	情報	ポリシーの削除	
352	情報	ポリシーのアップデート	
353	情報	ポリシーのエクスポート	
354	情報	ポリシーのインポート	
355	情報	推奨設定の検索のキャンセル	
360	情報	VMware vCenterの追加	

ID	重要度	イベント	説明または解決策
361	情報	VMware vCenterの削除	
362	情報	VMware vCenterのアップデート	
363	情報	VMware vCenterの同期	
364	情報	VMware vCenterの同期の完了	
365	エラー	VMware vCenterの同期失敗	
366	情報	VMware vCenterの同期要求	
367	情報	VMware vCenterの同期キャンセル	
368	警告	インタフェースが非同期	Deep Security Virtual ApplianceからレポートされたインタフェースとvCenterからレポートされたインタフェースは異なります。通常、仮想マシンを再起動すると解決します。
369	情報	インタフェースが同期	
370	情報	Filter Driverのインストール完了	
371	情報	Filter Driverの削除完了	VMware ESXiサーバは、Filter Driverソフトウェアがインストールされる前の状態に復元されました。
372	情報	Filter Driverのアップグレード	
373	情報	Virtual Applianceの配置	
374	情報	Virtual Applianceのアップグレード完了	
375	警告	Virtual Applianceのアップグレードの失敗	
376	警告	保護されていないESXiへの仮想マシンの移動	
377	情報	保護されているESXiへの仮想マシンの移動	
378	警告	別のESXiへの移動後に仮想マシンが保護されていない	Deep Security Virtual ApplianceがないESXiに、仮想マシンが移動されました。
379	情報	別のESXiへの移動後に仮想マシンが未保護になる状態が解決	
380	エラー	オフラインのFilter Driver	ESXiサーバのFilter Driverがオフラインです。VMware vCenterコンソールを使用して、ハイパーバイザおよびESXiの問題をトラブルシューティングしてください。

ID	重要度	イベント	説明または解決策
381	情報	Filter Driverのオンライン復帰	
382	情報	Filter Driverのアップグレード要求	
383	情報	Applianceのアップグレード要求	
384	警告	ESXiの準備失敗	
385	警告	Filter Driverのアップグレード失敗	
386	警告	ESXiからのFilter Driver削除の失敗	
387	エラー	Filter Driverとの接続失敗	
388	情報	Filter Driverとの接続成功	
389	エラー	複数の有効化されたApplianceの検出	
390	情報	有効化されたApplianceの複数検出の解決	
391	エラー	ネットワーク設定とvCenterグローバル設定との非同期	
392	情報	ネットワーク設定とvCenterグローバル設定との同期	
393	エラー	不正プログラム対策エンジンがオフライン	不正プログラム対策保護モジュールが機能していません。これは、VMware環境が要件に一致していないことが原因である可能性があります。 "システム要件" on page 184 を参照してください。
394	情報	不正プログラム対策エンジンのオンライン復帰	
395	エラー	Virtual ApplianceとFilter Driverの互換性なし	
396	情報	Virtual ApplianceとFilter Driverの互換性がない状態の解決	
397	警告	VMware NSXコールバック認証失敗	
398	エラー	VMware Toolsがインストールされていない	
399	情報	VMware Toolsの未インストール解決	
410	情報	ファイアウォールルールの作成	

ID	重要度	イベント	説明または解決策
411	情報	ファイアウォールルールの削除	
412	情報	ファイアウォールルールのアップデート	
413	情報	ファイアウォールルールのエクスポート	
414	情報	ファイアウォールルールのインポート	
420	情報	ファイアウォールステートフル設定の作成	
421	情報	ファイアウォールステートフル設定の削除	
422	情報	ファイアウォールステートフル設定のアップデート	
423	情報	ファイアウォールステートフル設定のエクスポート	
424	情報	ファイアウォールステートフル設定のインポート	
460	情報	アプリケーションの種類を作成	管理者が新しいIPSネットワークのアプリケーション定義を設定しました。
461	情報	アプリケーションの種類を削除	管理者がIPSネットワークのアプリケーション定義を削除しました。
462	情報	アプリケーションの種類をアップデート	管理者が既存のIPSネットワークのアプリケーション定義を変更しました。
463	情報	アプリケーションの種類のエクスポート	管理者がIPSネットワークのアプリケーション定義をダウンロードしました。
464	情報	アプリケーションの種類をインポート	管理者がIPSネットワークのアプリケーション定義をアップロードしました。
470	情報	侵入防御ルールの作成	
471	情報	侵入防御ルールの削除	
472	情報	侵入防御ルールのアップデート	
473	情報	侵入防御ルールのエクスポート	
474	情報	侵入防御ルールのインポート	
480	情報	変更監視ルールの作成	
481	情報	変更監視ルールの削除	
482	情報	変更監視ルールのアップデート	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
483	情報	変更監視ルールのエクスポート	
484	情報	変更監視ルールのインポート	
490	情報	セキュリティログ監視ルールの作成	
491	情報	セキュリティログ監視ルールの削除	
492	情報	セキュリティログ監視ルールのアップデート	
493	情報	セキュリティログ監視ルールのエクスポート	
494	情報	セキュリティログ監視ルールのインポート	
495	情報	セキュリティログ監視デコーダの作成	
496	情報	セキュリティログ監視デコーダの削除	
497	情報	セキュリティログ監視デコーダのアップデート	
498	情報	セキュリティログ監視デコーダのエクスポート	
499	情報	セキュリティログ監視デコーダのインポート	
505	情報	コンテキストの作成	
506	情報	コンテキストの削除	
507	情報	コンテキストのアップデート	
508	情報	コンテキストのエクスポート	
509	情報	コンテキストのインポート	
510	情報	IPリストの作成	
511	情報	IPリストの削除	
512	情報	IPリストのアップデート	
513	情報	IPリストのエクスポート	
514	情報	IPリストのインポート	
520	情報	ポートリストの作成	
521	情報	ポートリストの削除	
522	情報	ポートリストのアップデート	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
523	情報	ポートリストのエクスポート	
524	情報	ポートリストのインポート	
525	情報	検索キャッシュ設定の作成	
526	情報	検索キャッシュ設定のエクスポート	
527	情報	検索キャッシュ設定のアップデート	
530	情報	MACリストの作成	
531	情報	MACリストの削除	
532	情報	MACリストのアップデート	
533	情報	MACリストのエクスポート	
534	情報	MACリストのインポート	
540	情報	プロキシの作成	
541	情報	プロキシの削除	
542	情報	プロキシのアップデート	
543	情報	プロキシのエクスポート	
544	情報	プロキシのインポート	
550	情報	スケジュールの作成	
551	情報	スケジュールの削除	
552	情報	スケジュールのアップデート	
553	情報	スケジュールのエクスポート	
554	情報	スケジュールのインポート	
560	情報	予約タスクの作成	
561	情報	予約タスクの削除	
562	情報	予約タスクのアップデート	
563	情報	予約タスクの手動実行	
564	情報	予約タスクの開始	
565	情報	バックアップの完了	
566	エラー	バックアップの失敗	
567	情報	未解決アラートの概要の送信中	

ID	重要度	イベント	説明または解決策
568	警告	未解決アラートの概要の送信失敗	
569	警告	メールの失敗	メール通知を送信できませんでした。 SMTP設定 が正しく設定されていることを確認してください。
570	情報	レポートの送信中	
571	警告	レポートの送信の失敗	
572	エラー	無効なReport Jar	
573	情報	資産評価の作成	
574	情報	資産評価の削除	
575	情報	資産評価のアップデート	
576	エラー	レポートのアンインストールの失敗	
577	エラー	レポートのアンインストール	
578	警告	設定が必要な変更監視ルール	
580	警告	アプリケーションの種類ポートリストの誤った設定	
581	警告	アプリケーションの種類ポートリストの誤った設定の解決	
582	警告	侵入防御ルールで設定が必要	
583	情報	侵入防御ルールで必要な設定の解決	
584	警告	アプリケーションの種類で設定が必要	IPSルールにはネットワークアプリケーション定義が必要で、定義するまでトラフィックを正しく検索できません。
585	情報	変更監視ルールで必要な設定の解決	
586	警告	セキュリティログ監視ルールで設定が必要	
587	情報	セキュリティログ監視ルールで必要な設定の解決	
588	警告	セキュリティログ監視ルールで必要なログファイル	
589	情報	セキュリティログ監視ルールで必要なログ	

ID	重要度	イベント	説明または解決策
		ファイルの解決	
590	警告	非推奨の予約タスク	
591	情報	Relayグループの作成	
592	情報	Relayグループのアップデート	
593	情報	Relayグループの削除	
594	情報	イベントベースタスクの作成	
595	情報	イベントベースタスクの削除	
596	情報	イベントベースタスクのアップデート	
597	情報	イベントベースタスクの開始	
600	情報	ユーザのログオン	
601	情報	ユーザのログオフ	
602	情報	ユーザのタイムアウト	
603	情報	ユーザのロックアウト	
604	情報	ユーザのロック解除	
605	情報	ユーザセッションの終了	
608	エラー	ユーザセッションの確認の失敗	認証が成功した後にセッションが開始されたことをDeep Security Managerで確認できませんでした。ユーザはログインページにリダイレクトされ、再認証を求められます。認証済みのセッションリストがクリアされた場合、これは正常な動作です。
609	エラー	ユーザによる無効な要求	Deep Security Managerが監査データへのアクセスを求める無効な要求を受け取りました (イベント)。アクセスは拒否されました。
610	情報	ユーザセッションの有効化	
611	情報	ユーザによるファイアウォールイベントの表示	
613	情報	ユーザによる侵入防御イベントの表示	
615	情報	ユーザによるシステムイベントの表示	
616	情報	ユーザによる変更監視イベントの表示	
617	情報	ユーザによるセキュリティログ監視イベントの表示	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
618	情報	ユーザによる検出ファイルの詳細表示	
619	情報	ユーザによる不正プログラム対策イベントの表示	
620	情報	ユーザによるWebレピュテーションイベントの表示	
621	情報	ユーザがテナントとしてログオン	
622	情報	プライマリテナントからのアクセスは有効	
623	情報	プライマリテナントからのアクセスは無効	
624	情報	プライマリテナントからのアクセスを許可	
625	情報	プライマリテナントからのアクセスは取り消し済み	
626	情報	プライマリテナントからのアクセスは期限切れ	
630	情報	Syslog設定の作成	
631	情報	Syslog設定の削除	
632	情報	Syslog設定のアップデート	
633	情報	Syslog設定のエクスポート	
634	情報	Syslog設定のインポート	
650	情報	ユーザの作成	
651	情報	ユーザの削除	
652	情報	ユーザのアップデート	
653	情報	ユーザパスワードの設定	
656	情報	APIキーの作成	
657	情報	APIキーの削除	
658	情報	APIキーのアップデート	
660	情報	役割の作成	
661	情報	役割の削除	
662	情報	役割のアップデート	
663	情報	役割のインポート	
664	情報	役割のエクスポート	

ID	重要度	イベント	説明または解決策
670	情報	連絡先の作成	
671	情報	連絡先の削除	
672	情報	連絡先のアップデート	
673	情報	APIキーのロックアウト	
674	情報	APIキーのロック解除	
675	エラー	APIキーセッションの有効化失敗	
676	エラー	APIキーによる無効な要求	
678	情報	APIキーの有効期限切れ	
680	情報	マスター暗号化キーの作成	詳細については、 masterkey パラメータを参照してください。
681	情報	マスター暗号化キーのエクスポート	詳細については、 masterkey パラメータを参照してください。
682	情報	マスター暗号化キーのインポート	詳細については、 masterkey パラメータを参照してください。
700	情報	Agentソフトウェアのインストール	
701	エラー	Agentソフトウェアのインストールの失敗	
702	情報	資格情報の生成	
703	エラー	資格情報の生成の失敗	
704	情報	Agent/Appliance有効化の完了	
705	エラー	Agent/Appliance有効化の失敗	Agentのセルフプロテクションが有効になっている場合に発生することがあります。Deep Security Managerの コンピュータエディタ ¹ で、[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザーによるAgent

¹コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ID	重要度	イベント	説明または解決策
			のアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
706	情報	ソフトウェアアップデート: Agentソフトウェアのアップグレード	
707	警告	ソフトウェアアップデート: Agentソフトウェアのアップグレードの失敗	アップグレードが失敗した理由の詳細については、イベント詳細を参照してください。
708	情報	Agent/Appliance無効化の完了	
709	エラー	Agent/Appliance無効化の失敗	
710	情報	イベントの取得	
711	情報	Agentソフトウェアの配信	
712	エラー	Agentソフトウェアの配信の失敗	Agentのセルフプロテクションが有効になっている場合に発生することがあります。Deep Security Managerの コンピュータエディタ ¹ で、[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
713	情報	Agentソフトウェアの削除	
714	エラー	Agentソフトウェアの削除の失敗	Agentのセルフプロテクションが有効になっている場合に発生することがあります。Deep Security Managerの コンピュータエディタ ² で、[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのア

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ID	重要度	イベント	説明または解決策
			ンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
715	情報	Agent/Applianceのバージョン変更	
716	情報	不明なAgentの再有効化の試行	Deep Security Managerに認識されていないAgentの再有効化が試行されました。通常、この問題は、先にコンピュータ上のAgentを削除せずにDeep Security Managerからコンピュータを削除した場合に発生します。詳細については、 「Agentの設定」 の「不明なAgentの再有効化の試行」を参照してください。
720	情報	ポリシー送信	Agent/Applianceがアップデートされました。
721	エラー	ポリシー送信の失敗	
722	警告	インタフェースの取得失敗	
723	情報	インタフェースの取得失敗の解決	
724	警告	ディスク容量の不足	Agentのディスク容量不足が検出されました。コンピュータの空き容量を増やしてください。 "警告: ディスク容量の不足" on page 1374を参照してください。
725	警告	イベントの抑制	
726	警告	Agent/Applianceイベントの取得失敗	ManagerがAgent/Applianceからイベントを取得できませんでした。Agent/Applianceでデータが失われたわけではありません。通常、このエラーは、イベントの転送中にネットワークが中断された場合に発生します。処理を再開するには、エラーをクリアして [ステータスの確認] を実行してください。
727	情報	Agent/Applianceイベントの取得失敗の解決	
728	エラー	イベントの取得失敗	ManagerがAgent/Applianceから監査データを取得できませんでした。Agent/Applianceでデータが失われたわけではありません。通常、このエラーは、

ID	重要度	イベント	説明または解決策
			イベントの転送中にネットワークが中断された場合に発生します。処理を再開するには、エラーをクリアして [今すぐイベントを取得] を実行してください。
729	情報	イベントの取得失敗の解決	
730	エラー	オフライン	Managerがコンピュータと通信できません。ただし通常は、コンピュータはオフラインのAgentの最新の設定に従って引き続き保護されています。「コンピュータおよびAgent/Applianceのステータス」および" 「オフライン」のAgent " on page 1541を参照してください。
731	情報	オンラインに復帰	
732	エラー	ファイアウォールエンジンがオフライン	ファイアウォールエンジンがオフラインであるため、トラフィックがフィルタリングされないまま送受信されています。この状態は、通常、ドライバのインストール中または確認中のエラーが原因で発生します。コンピュータのネットワークドライバの状態を調べて、正常に読み込まれていることを確認してください。
733	情報	ファイアウォールエンジンがオンライン復帰	
734	警告	コンピュータの時計の変更	コンピュータエディタまたはポリシーエディタ¹ の [設定]→[一般]→[ハートビート] エリアで指定された最大許容値を超える時計の変更がコンピュータで検出されました。コンピュータの時計が変更された原因を調査してください。
735	警告	誤った設定の検出	Agentの設定が、Managerのレコードで指示されて

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ID	重要度	イベント	説明または解決策
			いる設定と一致しません。これは通常、最近実行されたManagerまたはAgentバックアップの復元が原因です。設定の不一致が予期しないものである場合、調査する必要があります。
736	情報	ステータス確認の失敗の解決	
737	エラー	ステータスの確認の失敗	"エラー: ステータスの確認の失敗" on page 1354を参照してください。
738	エラー	侵入防御エンジンがオフライン	侵入防御エンジンがオフラインであるため、トラフィックがフィルタリングされないまま送受信されています。この状態は、通常、ドライバのインストール中または確認中のエラーが原因で発生します。コンピュータのネットワークドライバの状態を調べて、正常に読み込まれていることを確認してください。
739	情報	侵入防御エンジンがオンライン復帰	
740	エラー	Agent/Applianceエラー	
741	警告	異常な再起動の検出	
742	警告	通信の問題	AgentからManagerへステータスを送信中に問題が発生しました。通常、AgentからManagerへの通信で、ネットワークまたは負荷の輻輳が発生していることを示しています。この状態が解決しない場合、詳しい調査が必要です。
743	情報	通信の問題の解決	
745	警告	イベントの切り捨て	
748	エラー	セキュリティログ監視エンジンがオフライン	
749	情報	セキュリティログ監視エンジンのオンライン復帰	
750	警告	前回の自動再試行	
755	情報	Deep Security Managerのバージョン互換性の解決	

ID	重要度	イベント	説明または解決策
756	警告	Deep Security Managerのアップグレード推奨 (非互換のセキュリティアップデート)	<p>各セキュリティモジュールのルール（ファイアウォール、不正プログラム対策など）には、Deep Security Managerの最小バージョンがあります。ルールを実行するために必要です。</p> <p>現在のDeep Security Managerのバージョンは、サポートされているルールの最小バージョン数を下回っています。Deep Security Managerをアップグレードして警告をクリアし、ルールを実行してください。</p>
760	情報	Agent/Applianceバージョン互換性の解決	
761	警告	Agent/Applianceのアップグレード推奨	現在のDeep Security AgentまたはDeep Security Virtual Applianceのバージョンは、Deep Security Managerのサポートされている最小バージョンより小さいです。Agent/Appliance.のアップグレード
762	警告	Agent/Applianceのアップグレードが必要	
763	警告	非互換のAgent/Applianceバージョン	現在のDeep Security ManagerのバージョンがDeep Security AgentまたはDeep Security Virtual Applianceの最小サポートバージョンより小さい。マネージャーをアップグレードしてください。
764	警告	Agent/Applianceのアップグレード推奨 (非互換のセキュリティアップデート)	<p>セキュリティモジュールの各ルール（ファイアウォール、不正プログラム対策など）には、特定のDeep Security AgentまたはDeep Deep Security Agent固有のルールがあります。ルールを実行するために必要なDeep Security Virtual Applianceのバージョンです。</p> <p>現在のDeep Security AgentまたはDeep Security</p>

ID	重要度	イベント	説明または解決策
			Virtual Applianceのバージョンが、サポートされているルールの最小バージョン数を下回っています。Deep Security AgentまたはDeep Security Virtual Applianceをアップグレードして、警告をクリアしてルールを実行します。
765	エラー	コンピュータの再起動が必要	
766	警告	ネットワークエンジンモードの設定が非互換	
767	警告	ネットワークエンジンモードのバージョンが非互換	
768	警告	ネットワークエンジンモードの非互換性の解決	
770	警告	Agent/Applianceのハートビートの拒否	
771	警告	認識できないクライアントによる接続	"イベントID 771「認識できないクライアントによる接続」のトラブルシューティング" on page 1345を参照してください。
780	情報	推奨設定の検索失敗の解決	
781	警告	推奨設定の検索失敗	"トラブルシューティング: 推奨設定の検索失敗" on page 602を参照してください。
782	情報	ベースラインの再構築失敗の解決	
783	警告	ベースラインの再構築の失敗	
784	情報	セキュリティアップデート: セキュリティアップデートの確認とダウンロード成功	
785	警告	セキュリティアップデート: セキュリティアップデートの確認とダウンロード失敗	
786	情報	変更の検索失敗の解決	
787	警告	変更の検索の失敗	
790	情報	Agentからのリモート有効化の要求	

ID	重要度	イベント	説明または解決策
791	警告	Agentからのリモート有効化の失敗	
792	情報	不正プログラムの手動検索失敗の解決	
793	警告	不正プログラムの手動検索の失敗	不正プログラム検索に失敗しました。VMware vCenterのコンソールを使用して、検索に失敗した仮想マシンのステータスを確認してください。
794	情報	不正プログラムの予約検索失敗の解決	
795	警告	不正プログラムの予約検索の失敗	不正プログラムの予約検索に失敗しました。VMware vCenterのコンソールを使用して、検索に失敗した仮想マシンのステータスを確認してください。
796	警告	不正プログラムの予約検索タスクのスキップ	これは、以前の検索が完了しないうちに、コンピュータ上で不正プログラムの予約検索が開始された場合に発生します。通常、不正プログラムの予約検索の実行間隔が短かすぎることを示しています。
797	情報	不正プログラム検索のキャンセル失敗の解決	
798	警告	不正プログラム検索キャンセルの失敗	不正プログラム検索のキャンセルに失敗しました。VMware vCenterのコンソールを使用して、検索に失敗した仮想マシンのステータスを確認してください。
799	警告	不正プログラム検索の停止	不正プログラム検索が停止しました。VMware vCenterのコンソールを使用して、検索が停止した仮想マシンのステータスを確認してください。
800	情報	アラートの消去	
801	情報	エラーの消去	
803	警告	Agentの設定パッケージが大きすぎる	
804	エラー	侵入防御ルールのコンパイル失敗	
805	エラー	侵入防御ルールのコンパイル失敗	
806	エラー	侵入防御ルールのコンパイル失敗	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
850	警告	攻撃の予兆の検出: OSのフィンガープリント調査	"警告: 攻撃の予兆の検出" on page 1374
851	警告	攻撃の予兆の検出: ネットワークまたはポートの検索	"警告: 攻撃の予兆の検出" on page 1374
852	警告	攻撃の予兆の検出: TCP Null検索	"警告: 攻撃の予兆の検出" on page 1374
853	警告	攻撃の予兆の検出: TCP SYNFIN検索	"警告: 攻撃の予兆の検出" on page 1374
854	警告	攻撃の予兆の検出: TCP Xmas検索	"警告: 攻撃の予兆の検出" on page 1374
900	情報	Deep Security Managerの監査の開始	
901	情報	Deep Security Managerの監査のシャットダウン	
902	情報	Deep Security Managerのインストール	
903	警告	ライセンス関連設定の変更	
904	情報	診断ログが有効	
905	情報	診断ログの完了	
910	情報	診断パッケージの生成	
911	情報	診断パッケージのエクスポート	
912	情報	診断パッケージのアップロード	
913	エラー	自動診断パッケージのエラー	
914	情報	検出ファイルの削除の成功	
915	情報	検出ファイルの削除の失敗	
916	情報	検出ファイルのダウンロードの成功	
917	情報	検出ファイルのダウンロードの失敗	
918	情報	検出ファイル管理ユーティリティのダウンロードの成功	
919	情報	検出ファイルが見つかりません	
920	情報	使用状況情報の生成	
921	情報	使用状況情報パッケージのエクスポート	
922	情報	使用状況情報パッケージのアップロード	
923	エラー	使用状況情報パッケージのエラー	

ID	重要度	イベント	説明または解決策
924	警告	ファイルを分析または隔離できません (検出ファイル保存用のVMの最大ディスク容量を超過)	検出ファイルの保存に使用する仮想マシンの最大ディスク容量に達したため、不正プログラム対策モジュールでファイルを分析または隔離できませんでした。検出ファイルの設定で最大ディスク容量の設定を変更するには、コンピュータエディタまたはポリシーエディタを開き、[不正プログラム対策]→[詳細] タブに移動してください。
925	警告	ファイルを分析または隔離できません (検出ファイル保存用の最大ディスク容量を超過)	検出ファイルの保存に使用する最大ディスク容量に達したため、不正プログラム対策モジュールでファイルを分析または隔離できませんでした。検出ファイルの設定で最大ディスク容量の設定を変更するには、コンピュータエディタまたはポリシーエディタを開き、[不正プログラム対策]→[詳細] タブに移動してください。
926	警告	スマートスキャン用のSmart Protection Serverへの接続不能	"「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1346を参照してください。
927	情報	スマートスキャン用のSmart Protection Serverへの接続	
928	情報	検出ファイルの復元の成功	
929	警告	検出ファイルの復元の失敗	
930	情報	証明書の承諾	
931	情報	証明書の削除	
932	警告	Webレピュテーション用のSmart Protection Serverへの接続不能	"「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1346を参照してください。
933	情報	Webレピュテーション用のSmart Protection Serverへの接続	
934	情報	ソフトウェアアップデート: Windowsプラットフォーム用不正プログラム対策のアップデート成功	
935	エ	ソフトウェアアップデート: Windowsプラットフォーム用不正プログラム対策	"Windowsプラットフォーム用不正プログラム対策

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
	ラー	トフォーム用不正プログラム対策のアップデート失敗	のアップデート失敗" on page 1547
936	情報	Deep Discovery Analyzerへの検出ファイルの送信に成功しました。	
937	情報	Deep Discovery Analyzerへの検出ファイルの送信に失敗しました。	
938	情報	検出ファイルを送信キューに登録	
940	情報	自動タグルールを作成	
941	情報	自動タグルールの削除	
942	情報	自動タグルールのアップデート	
943	情報	タグの削除	
944	情報	タグの作成	
945	警告	Census、Good File Reputation、機械学習型検索サービスへの接続解除	
946	情報	Census、Good File Reputation、機械学習型検索サービスへの接続	
947	情報	FIPSモード有効	
948	情報	FIPSモード無効	
970	情報	コマンドラインユーティリティの開始	
978	情報	コマンドラインユーティリティの失敗	
979	情報	コマンドラインユーティリティのシャットダウン	Deep Security Managerが手動で停止されました。
980	情報	システム情報のエクスポート	
990	情報	Managerノードの追加	
991	情報	Managerノードの廃止	
992	情報	Managerノードのアップデート	
995	情報	ソフトウェア安全性評価サービスへの接続が復元	
996	警告	ソフトウェア安全性評価サービスに接続不能	
997	エ	タグ付けエラー	

ID	重要度	イベント	説明または解決策
	ラー		
998	エラー	システムイベント通知エラー	
999	エラー	内部ソフトウェアエラー	
1101	エラー	プラグインのインストールの失敗	
1102	情報	プラグインのインストール	
1103	エラー	プラグインのアップグレードの失敗	
1104	情報	プラグインのアップグレード	
1105	エラー	プラグインの起動の失敗	
1106	エラー	プラグインのアンインストールの失敗	
1107	情報	プラグインのアンインストール	
1108	情報	プラグイン起動	
1109	情報	プラグイン停止	
1110	エラー	ソフトウェアパッケージが見つかりません	エージェントソフトウェアパッケージが見つからないか、新しいパッケージが必要です。
1111	情報	ソフトウェアパッケージが見つかりました	
1500	情報	不正プログラム検索設定の作成	
1501	情報	不正プログラム検索設定の削除	
1502	情報	不正プログラム検索設定のアップデート	
1503	情報	不正プログラム検索設定のエクスポート	
1504	情報	不正プログラム検索設定のインポート	
1505	情報	ディレクトリリストの作成	
1506	情報	ディレクトリリストの削除	
1507	情報	ディレクトリリストのアップデート	
1508	情報	ディレクトリリストのエクスポート	

ID	重要度	イベント	説明または解決策
1509	情報	ディレクトリリストのインポート	
1510	情報	ファイル拡張子リストの作成	
1511	情報	ファイル拡張子リストの削除	
1512	情報	ファイル拡張子リストのアップデート	
1513	情報	ファイル拡張子リストのエクスポート	
1514	情報	ファイル拡張子リストのインポート	
1515	情報	ファイルリストの作成	
1516	情報	ファイルリストの削除	
1517	情報	ファイルリストのアップデート	
1518	情報	ファイルリストのエクスポート	
1519	情報	ファイルリストのインポート	
1520	情報	不正プログラムの手動検索の保留中	
1521	情報	不正プログラムの手動検索の開始	
1522	情報	不正プログラムの手動検索の完了	
1523	情報	不正プログラムの予約検索の開始	
1524	情報	不正プログラムの予約検索の完了	
1525	情報	不正プログラムの手動検索キャンセルの実行中	
1526	情報	手動不正プログラム検索キャンセル	<p>このイベントには次の原因があります。</p> <ul style="list-style-type: none"> • エージェントまたは不正プログラム対策サービスを再起動しています • スキャン中のコンピュータがシャットダウンまたは再起動中です。 • 誰かが手動で検索をキャンセルしました • その他の不明な理由 <p>詳細については、システムイベントの説明を参照し</p>

ID	重要度	イベント	説明または解決策
			てください。
1527	情報	不正プログラムの予約検索キャンセルの実行中	
1528	情報	不正プログラム検索予約のキャンセル	<p>このイベントには次の原因があります。</p> <ul style="list-style-type: none"> • エージェントまたは不正プログラム対策サービスを再起動しています • スキャン中のコンピュータがシャットダウンまたは再起動中です。 • 誰かが手動で検索をキャンセルしました • その他の不明な理由 <p>詳細については、システムイベントの説明を参照してください。</p>
1529	情報	不正プログラムの手動検索の一時停止	
1530	情報	不正プログラムの手動検索の再開	
1531	情報	不正プログラムの予約検索の一時停止	
1532	情報	不正プログラムの予約検索の再開	
1533	情報	不正プログラム対策のクリーンナップまたは復元タスクを完了するためにコンピュータの再起動が必要	
1534	エラー	不正プログラム対策保護を完了するためにコンピュータの再起動が必要	
1535	情報	不正プログラムのクリーンナップタスクの手動実行が必要	
1536	情報	不正プログラムのクイック検索の保留中	
1537	情報	不正プログラムのクイック検索の開始	
1538	情報	不正プログラムのクイック検索の完了	

ID	重要度	イベント	説明または解決策
1539	情報	不正プログラムのクイック検索キャンセルの実行中	
1540	情報	クイック不正プログラム検索キャンセル	<p>このイベントには次の原因があります。</p> <ul style="list-style-type: none"> • エージェントまたは不正プログラム対策サービスを再起動しています • スキャン中のコンピュータがシャットダウンまたは再起動中です。 • 誰かが手動で検索をキャンセルしました • その他の不明な理由 <p>詳細については、システムイベントの説明を参照してください。</p>
1541	情報	不正プログラムのクイック検索の一時停止	
1542	情報	不正プログラムのクイック検索失敗の解決	
1543	警告	不正プログラムのクイック検索の失敗	
1544	情報	不正プログラムのクイック検索の再開	
1545	情報	ファイルで不正プログラムを検索できませんでした	<p>ファイルパスが最大文字数を超えたため、不正プログラム対策がファイルを検索できませんでした。ファイルパスの最大長はOSとファイルシステムに応じて異なります。この問題を解決するには、ディレクトリパスにファイルを移動して、少ない文字数でファイル名を設定してください。</p>
1546	情報	ファイルで不正プログラムを検索できませんでした	<p>場所がディレクトリの深さの上限を超えたため、不正プログラム対策がファイルを検索できませんでした。この問題を解決するには、ネストするディレクトリの階層数を減らしてください。</p>
1547	情報	不正プログラムの予約検索タスクのキャンセル	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
1550	情報	Webレピュテーション設定のアップデート	
1551	情報	不正プログラム検索設定のアップデート	
1552	情報	変更監視設定のアップデート	
1553	情報	セキュリティログ監視設定のアップデート	
1554	情報	ファイアウォールステートフル設定のアップデート	
1555	情報	侵入防御設定のアップデート	
1600	情報	Relayグループのアップデートの要求	
1601	情報	Relayグループのアップデートの成功	
1602	エラー	Relayグループのアップデートの失敗	
1603	情報	セキュリティアップデート: セキュリティアップデートのロールバック成功	
1604	警告	セキュリティアップデート: セキュリティアップデートのロールバック失敗	
1605	情報	ホストへのファイルバックアップコマンドの送信成功	
1606	警告	ホストへのファイルバックアップコマンドの送信失敗	
1607	情報	ファイルバックアップ成功	
1608	エラー	ファイルをバックアップできませんでした	
1650	警告	不正プログラム対策保護がないか、期限切れ	
1651	情報	不正プログラム対策モジュールの準備完了	
1660	情報	ベースラインの再構築の開始	
1661	情報	ベースラインの再構築の一時停止	
1662	情報	ベースラインの再構築の再開	
1663	警告	ベースラインの再構築の失敗	
1664	警告	ベースラインの再構築の停止	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
1665	情報	ベースラインの再構築の完了	
1666	情報	変更の検索の開始	
1667	情報	変更の検索の一時停止	
1668	情報	変更の検索の再開	
1669	警告	変更の検索の失敗	
1670	警告	変更の検索の停止	
1671	情報	変更の検索の完了	
1675	エラー	変更監視エンジンがオフライン	
1676	情報	変更監視エンジンのオンライン復帰	
1677	エラー	TPMのエラー	
1678	情報	TPMのレジスタ値の読み込み	
1679	警告	TPMのレジスタ値の変更	
1680	情報	TPMチェックが無効	
1681	情報	TPM情報の信頼性なし	
1700	情報	Agentが検出されない	
1800	エラー	Deep Security Protectionモジュールの障害	
1801	情報	Deep Security Protectionモジュールが正常な状態に復帰	
1900	情報	クラウドアカウントの追加	
1901	情報	クラウドアカウントの削除	
1902	情報	クラウドアカウントのアップデート	
1903	情報	クラウドアカウント同期の実行中	
1904	情報	クラウドアカウント同期の完了	
1905	エラー	クラウドアカウント同期の失敗	
1906	情報	クラウドアカウント同期の要求	
1907	情報	クラウドアカウント同期のキャンセル	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
1908	情報	AWSアカウントの同期要求	
1909	情報	AWSアカウントの同期完了	
1910	エラー	AWSアカウントの同期失敗	
1911	情報	AWSアカウントの追加	
1912	情報	AWSアカウントの削除	
1913	情報	AWSアカウントのアップデート	
1914	情報	Azureアカウントの追加	
1915	情報	Azureアカウントの削除	
1916	情報	Azureアカウントのアップデート	
1917	情報	Azureアカウントの同期完了	
1918	エラー	Azureアカウントの同期失敗	
1919	情報	Azureアカウントの同期要求	
1920	警告	Azureアカウントの同期完了 (エラーあり)	
1921	情報	vCloudアカウントの追加	
1922	情報	vCloudアカウントの削除	
1923	情報	vCloudアカウントのアップデート	
1924	情報	vCloudアカウントの同期完了	
1925	エラー	vCloudアカウントの同期失敗	
1926	情報	vCloudアカウントの同期要求	
1927	情報	AWSアカウントへのコネクタのアップグレード要求	
1928	警告	AWSアカウントのアップデート失敗	
1929	情報	AWSアカウントへのコネクタのアップグレードの完了	
1950	情報	テナントの作成	
1951	情報	テナントの削除	
1952	情報	テナントのアップデート	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
1953	情報	テナントのデータベースサーバの作成	
1954	情報	テナントのデータベースサーバの削除	
1955	情報	テナントのデータベースサーバのアップデート	
1956	情報	テナントのエクスポート	
1957	エラー	テナントの初期化失敗	
1958	情報	テナント機能のアップデート	
2000	情報	検索キャッシュ設定オブジェクトの追加	
2001	情報	検索キャッシュ設定オブジェクトの削除	
2002	情報	検索キャッシュ設定オブジェクトのアップデート	
2102	情報	クレバーブリッジの数量がアップデートされました	
2103	警告	クレバーブリッジの数量がアップデートされていません	
2104	情報	クレバーブリッジの数量がリセットされました	
2105	警告	クレバーブリッジの数量がリセットされていません	
2106	情報	クレバーブリッジの課金日が設定されました	
2107	警告	クレバーブリッジの課金日が設定されていません	
2110	情報	クレバーブリッジから通知を受信しました	
2112	情報	アカウント残高がリセットされました	
2113	情報	Agentのインストールの要求	
2114	情報	AWS課金ジョブの開始	
2115	情報	AWS課金ジョブの完了	
2116	エラー	AWS課金エラー	AWS SDKを使用してDeep Security ManagerからAWSに課金使用状況レコードを送信した結果、SDK

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
			に例外が返されました。問題が解決しない場合は、サポート担当者に問い合わせてください。
2117	情報	資格の作成	
2118	情報	資格のアップデート	
2119	エラー	AWS Metering課金使用状況データの送信に失敗したためAgentの有効化に失敗	
2120	エラー	AWS課金エラー	AWS課金ジョブの実行中にDeep Security Managerでエラーが発生しました。問題が解決しない場合は、サポート担当者に問い合わせてください。
2200	情報	ソフトウェアアップデート: 不正プログラム対策モジュールのインストール開始	
2201	情報	ソフトウェアアップデート: 不正プログラム対策モジュールのインストール成功	このイベントは、アプリケーションコントロールまたは変更監視をインストールすることによってもトリガされます。これらのイベントは、不正プログラム対策と同じフレームワークを共有するためです。
2202	警告	ソフトウェアアップデート: 不正プログラム対策モジュールのインストール失敗	
2203	情報	ソフトウェアアップデート: 不正プログラム対策モジュールのダウンロード成功	
2204	情報	セキュリティアップデート: Agent/Applianceでのパターンファイルのアップデート成功	
2205	警告	セキュリティアップデート: Agent/Applianceでのパターンファイルのアップデート失敗	
2206	情報	セキュリティアップデート: Agent/Applianceでのパターンファイルアップデートがスキップされました	
2300	情報	ソフトウェアアップデート: Webレピュテーションモジュールのインストール開始	
2301	情報	ソフトウェアアップデート: Webレピュテー	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
		シヨンモジュールのインストール成功	
2302	警告	ソフトウェアアップデート: Webレピュテ シヨンモジュールのインストール失敗	
2303	情報	ソフトウェアアップデート: Webレピュテ シヨンモジュールのダウンロード成功	
2400	情報	ソフトウェアアップデート: ファイアウォ ールモジュールのインストール開始	
2401	情報	ソフトウェアアップデート: ファイアウォ ールモジュールのインストール成功	
2402	警告	ソフトウェアアップデート: ファイアウォ ールモジュールのインストール失敗	
2403	情報	ソフトウェアアップデート: ファイアウォ ールモジュールのダウンロード成功	
2500	情報	ソフトウェアアップデート: 侵入防御モ ジュールのインストール開始	
2501	情報	ソフトウェアアップデート: 侵入防御モ ジュールのインストール成功	
2502	警告	ソフトウェアアップデート: 侵入防御モ ジュールのインストール失敗	
2503	情報	ソフトウェアアップデート: 侵入防御モ ジュールのダウンロード成功	
2600	情報	ソフトウェアアップデート: 変更監視モ ジュールのインストール開始	
2601	情報	ソフトウェアアップデート: 変更監視モ ジュールのインストール成功	
2602	警告	ソフトウェアアップデート: 変更監視モ ジュールのインストール失敗	
2603	情報	ソフトウェアアップデート: 変更監視モ ジュールのダウンロード成功	
2700	情報	ソフトウェアアップデート: セキュリティロ グ監視モジュールのインストール開始	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
2701	情報	ソフトウェアアップデート: セキュリティログ監視モジュールのインストール成功	
2702	警告	ソフトウェアアップデート: セキュリティログ監視モジュールのインストール失敗	
2703	情報	ソフトウェアアップデート: セキュリティログ監視モジュールのダウンロード成功	
2800	情報	ソフトウェアアップデート: ソフトウェアの自動ダウンロード完了	
2801	エラー	ソフトウェアアップデート: ダウンロードセンターのインベントリ取得失敗	
2802	エラー	ソフトウェアアップデート: ダウンロードセンターからのソフトウェアのダウンロード失敗	
2803	情報	オンラインヘルプのアップデート開始	
2804	情報	オンラインヘルプのアップデート完了	
2805	情報	オンラインヘルプのアップデート成功	
2806	警告	オンラインヘルプのアップデート失敗	
2900	情報	ソフトウェアアップデート: Relayモジュールのインストール開始	
2901	情報	ソフトウェアアップデート: Relayモジュールのインストール成功	
2902	警告	ソフトウェアアップデート: Relayモジュールのインストール失敗	
2903	情報	ソフトウェアアップデート: Relayモジュールのダウンロード成功	
2904	情報	VMware NSX同期の完了	
2905	エラー	VMware NSX同期の失敗	
2906	情報	Agentセルフプロテクションの有効化	Deep Security Manager経由でAgentセルフプロテクションが有効化されました。
2907	情報	Agentセルフプロテクションの無効化	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
2908	情報	Agentセルフプロテクションの有効化	Deep Security Agentのコマンドラインを使用してAgentセルフプロテクションが有効化されました。
2909	情報	Agentセルフプロテクションの無効化	
2915	情報	データ移行完了	
2916	警告	データ移行完了 (エラーあり)	
2920	情報	Deep Discovery Analyzerからのレポートの取得完了	
2921	エラー	Deep Discovery Analyzerからのレポートの取得失敗	
2922	情報	Deep Discovery Analyzerへの送信の処理	
2923	エラー	Deep Discovery Analyzerへのファイル送信の失敗	
2924	情報	セキュリティアップデート: 不審オブジェクトの確認とアップデートに成功	
2925	エラー	セキュリティアップデート: 不審オブジェクトの確認とアップデートに失敗	
2926	警告	Deep Discovery Analyzerへの送信の処理待ち	
2930	情報	ファイルバックアップの保留中	
2931	情報	追加されたスマートフォルダ	
2932	情報	削除されたスマートフォルダ	
2933	情報	更新されたスマートフォルダ	
2934	エラー	Amazon SNSメッセージの送信失敗	
2935	情報	SNSメッセージの送信再開	
2936	情報	非アクティブなユーザの削除	
2937	情報	SAMLアイデンティティプロバイダの作成	
2938	情報	SAMLアイデンティティプロバイダのアップデート	
2939	情報	SAMLアイデンティティプロバイダの削除	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
2940	情報	SAMLサービスプロバイダのアップデート	
2941	エラー	ニュースのアップデートの失敗	
2942	情報	パフォーマンスプロファイルが作成されました	
2943	情報	パフォーマンスプロファイルがアップデートされました	
2944	情報	パフォーマンスプロファイルが削除されました	
2945	情報	システムのアップグレード開始	
2946	情報	システムのアップデート成功	
2947	エラー	システムのアップグレード失敗	
2948	情報	Managerノードのアップグレード開始	
2949	情報	Managerノードのアップデート成功	
2950	エラー	Managerノードのアップグレード失敗	マルチノード環境のノードがアップグレードに失敗しました。
2951	エラー	TICメッセージを送信できませんでした	管理下の検出および応答イベントを送信できませんでした。
2952	情報	TICメッセージの送信再開	
2953	情報	非アクティブなAgentのクリーンアップが正常に完了しました	非アクティブなAgentのクリーンアップにより、指定された期間にわたってオフラインまたは非アクティブになっているコンピュータが削除されました。非アクティブなAgentのクリーンアップの詳細については、" 非アクティブなAgentのクリーンアップによるオフラインコンピュータの削除の自動化 " on page 1523を参照してください。
2954	警告	記録日時が未来の日時になっているイベントを破棄しました	
2960	情報	Appliance (SVM) のアップグレードを要求	Deep Security Managerがアップグレード要求を受信しました。

ID	重要度	イベント	説明または解決策
2961	情報	Appliance (SVM) のアップグレード開始	Deep Security Managerによってアップグレード処理が実行されています。
2962	情報	Appliance (SVM) のアップグレードのキャンセル	Appliance SVMが使用不可のため、アップグレードを実行できませんでした。原因については、システムイベントの説明を参照してください。
2963	情報	Appliance (SVM) のアップグレード完了	Appliance SVMが新しいバージョンにアップグレードされ、正常に有効化されました。Appliance有効化の3分後に、すべてのゲスト仮想マシンが自動で有効化されます。
2964	警告	Appliance (SVM) のアップグレード失敗	Deep Security Managerで1つ以上のエラーが発生し、アップグレードプロセスが失敗しました。詳細については" 「Appliance (SVM) のアップグレード失敗」 システムイベントのトラブルシューティング" on page 1015 を参照してください。
2965	エラー	Appliance (SVM) のアップグレード完了 - 準備未完了	Appliance SVMが新しいバージョンにアップグレードされたものの、まだ有効化されていない状態であるか、Appliance SVMが有効化されたものの、ゲスト仮想マシンがまだ自動で有効化されていない状態です。詳細については、システムイベントの説明を参照してください。Applianceのインストールを確認し、Applianceまたはゲスト仮想マシンの有効化を手動で実行することが必要になる場合があります。
2969	情報	予約タスクのスキップ	
3000	情報	ソフトウェアアップデート: SAP Scannerのインストール開始	
3001	情報	ソフトウェアアップデート: SAP Scannerのインストール成功	
3002	エラー	ソフトウェアアップデート: SAP Scannerのインストール失敗	
3003	情報	ソフトウェアアップデート: SAP Scannerのダウンロード成功	

Trend Micro Deep Security On-Premise 12.0

ID	重要度	イベント	説明または解決策
3004	情報	SAP: ウイルス検索アダプタがインストールされています	
3005	エラー	SAP: ウイルス検索アダプタがインストールされていません	
3006	情報	SAP: ウイルス検索アダプタは最新です	
3007	情報	SAP: ウイルス検索アダプタが最新ではありません	
3008	情報	SAP: 不正プログラム対策モジュールの準備が完了しました	
3009	エラー	SAP: 不正プログラム対策モジュールの準備ができていません	
7000	情報	アプリケーションコントロールセキュリティイベントのエクスポート	管理者がアプリケーションコントロールイベントログをCSV形式でダウンロードしました。
7007	情報	ユーザがアプリケーションコントロールイベントを確認	管理者がアプリケーションコントロールアラートを消去しました。管理者ログインに成功した侵入者によってシステムが侵害された場合を除いて、これは正常な動作です。
7008	エラー	アプリケーションコントロールエンジンオフライン	Agentのアプリケーションコントロールエンジンをオンラインにできませんでした。このエラーは、カーネルがサポートされていないコンピュータでアプリケーションコントロールを有効にした場合に発生することがあります。
7009	情報	アプリケーションコントロールエンジンのオンライン復帰	Agentのアプリケーションコントロールエンジンが再起動されました。
7010	情報	アプリケーションコントロール設定のアップデート	Deep Security ManagerによってAgent上のアプリケーションコントロール設定がアップデートされました。
7011	情報	ソフトウェアアップデート: アプリケーションコントロールモジュールのインストール開始	Agentが、アプリケーションコントロールが選択されているDeep Security Managerからポリシーを受け取りましたが、アプリケーションコントロールエンジンがインストールされていないかアップデートが必要であることを検出したため、アプリケーショ

ID	重要度	イベント	説明または解決策
			ンコントロールエンジンのダウンロードを開始しました。コンピュータで初めてアプリケーションコントロールを有効にした場合、またはアプリケーションコントロールエンジンアップデートのリリース中にアプリケーションコントロールが無効にされていた場合、これは正常な動作です。
7012	情報	ソフトウェアアップデート: アプリケーションコントロールモジュールのインストール成功	Agentによってアプリケーションコントロールエンジンがインストールされました。また、アプリケーションコントロールエンジンは、変更監視機能によっても使用されます。
7013	エラー	ソフトウェアアップデート: アプリケーションコントロールモジュールのインストール失敗	Agentでアプリケーションコントロールエンジンをインストールできませんでした。これは正常な動作ではありません。
7014	情報	ソフトウェアアップデート: アプリケーションコントロールモジュールのダウンロード成功	Agentによるアプリケーションコントロールエンジンのダウンロードが完了しました。
7015	情報	アプリケーションコントロールルールセットのルールアップデート	従来のREST API がソフトウェアの許可またはブロックに使用されました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7020	情報	アプリケーションコントロールインベントリの取得	従来のREST API によってコンピュータの初期許可ルールがDeep Security Managerにアップロードされました。
7021	情報	アプリケーションコントロールインベントリ検索の開始	アプリケーションコントロールエンジンが有効化されましたが、そのコンピュータに許可ルールが存在しないことがAgentによって検知されたため、現在インストールされているソフトウェアに基づいて初期ルールの構築が開始されました。これは、アプリケーションコントロールを初めて有効にしたときの正常な動作です。このメッセージは、 従来のREST API を使用して許可ルールを置き換えるときには発生しません。

ID	重要度	イベント	説明または解決策
7022	情報	アプリケーションコントロールインベントリ検索の完了	Agentによるそのコンピュータの初期設定許可ルールの構築が完了しました。以降、許可またはブロックルールに登録されていないソフトウェアが新たに検出された場合は原因とアラート (設定されている場合) の対象になります。
7023	エラー	アプリケーションコントロールインベントリ検索の失敗	Agentはそのコンピュータの初期設定許可ルールを構築できませんでした。これは正常な動作ではありません。
7024	情報	アプリケーションコントロールソフトウェア変更の検出	管理者が [処理] タブでソフトウェアを許可またはブロックしたか、アプリケーションコントロールログメッセージで [ルールの変更] をクリックしてルールを変更しました。このメッセージは、 従来のREST API を使用して許可ルールを置き換えるときには発生しません。
7025	情報	アプリケーションコントロールインベントリ検索の要求	現在のルールを削除し、現在インストールされているソフトウェアに基づいてルールを再構築するように、管理者が手動で要求しました。複数のルールを同時に変更する必要がある場合、これは正常な操作です。
7026	情報	アプリケーションコントロールメンテナンスモードの開始要求	メンテナンスモードを有効にするコマンドが管理者により送信されたか、 従来のREST API により受信されました。
7027	情報	アプリケーションコントロールメンテナンスモードの停止要求	メンテナンスモードを無効にするコマンドが管理者により送信されたか、 従来のREST API により受信されました。
7028	情報	アプリケーションコントロールメンテナンスモードの開始	メンテナンスモードが有効化されました。このモードが有効な場合、アップデートまたは新規にインストールされたソフトウェアは、アップデートを許可する既知のソフトウェアとして許可ルールに自動的に追加されます。ブロックルールは、この間も引き続き適用されます。
7029	情報	アプリケーションコントロールメンテナンスモードの停止	メンテナンスモードが無効化されました。メンテナ

ID	重要度	イベント	説明または解決策
			ンスモードの停止中は、新規または変更されたソフトウェアが見つかり、明示的に許可またはブロックするまで「承認されていないソフトウェア」として処理されます。
7030	情報	アプリケーションコントロールインベントリ検索のキャンセル	Agentによって初期設定許可ルールの構築が開始されましたが、管理者によってキャンセルされました。
7031	エラー	アプリケーションコントロールルールセットの送信失敗	アプリケーションコントロールの共有ルールセットをAgentにダウンロードできませんでした。ネットワーク接続が切断されたか (AgentとRelay間のファイアウォールやプロキシなど)、Agentの空きディスク容量が十分でない可能性があります。
7032	情報	アプリケーションコントロールルールセットの送信成功	アプリケーションコントロールの共有ルールセットがAgentにダウンロードされました。管理者または 従来のREST API によってソフトウェアが許可またはブロックされた場合や、別の共有ルールセットが適用された場合の正常な動作です。
7033	情報	アプリケーションコントロールルールセットの作成	従来のREST API によって、アプリケーションコントロールルールセットが作成されました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7034	情報	アプリケーションコントロールルールセットのアップデート	従来のREST API により、アプリケーションコントロールルールセットに従ってソフトウェアが許可またはブロックされました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7035	情報	アプリケーションコントロールルールセットの削除	従来のREST API により、アプリケーションコントロールルールセットが削除されました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7036	情報	アプリケーションコントロールメンテナンスモードの期間リセット要求	管理者がメンテナンスモードの有効期間を変更しました。

ID	重要度	イベント	説明または解決策
7037	エラー	新しく適用されたルールセットによって、実行中のプロセスの一部は再起動時にブロックされます。	管理者が新しいルールセットを適用しましたが、ブロックルール内に現在実行中のプロセスがいくつか存在します。アプリケーションコントロールはプロセスを終了しますが、設定に応じてこのサービスをリブートまたは再起動すると、アラートが表示されるか、サービスがブロックされてしまいます。プロセスは承認されない場合は、プロセスを手動で終了する必要があります。承認してもプロセスがルールセットに見つからない場合は、プロセスをルールセットに追加する必要があります。
7038	エラー	未解決のソフトウェア変更数の上限に達しました	ファイルシステムで検出されたソフトウェア変更数が上限を超えました。アプリケーションコントロールは引き続き既存のルールを適用しますが、これ以上の変更は記録されず、このコンピュータでのソフトウェアの変更は表示されなくなります。この状況を解決し、大量のソフトウェア変更が発生しないようにする必要があります。
7040	エラー	アプリケーションコントロールルールセットに互換性がありません	アプリケーションコントロールルールセットを1台以上のコンピュータに割り当てることができませんでした。これは、インストールされているAgentのバージョンでこのルールセットがサポートされていないためです。通常、ハッシュベースのルールセットが古いDeep Security Agentに割り当てられていることが問題です。ハッシュベースのルールセットと互換性があるのは、Deep Security Agent 11.0以降のみです。Deep Security Agent 10.xでは、ファイルベースのルールセットのみをサポートしています(詳細については、" Deep Security Agent 10と11におけるファイルの比較方法の相違点 " on page 695 を参照してください)。この問題を解決するには、Deep Security Agentをバージョン11.0以降にアップグレードしてください。ローカルルールセットを使用している場合は、Agentのアプリケー

ID	重要度	イベント	説明または解決策
			ションコントロールをリセットする方法もあります。また、共有ルールセットを使用している場合は、共有ルールセットを使用するすべてのAgentをDeep Security Agent 11.0以降にアップグレードするまで、Deep Security 10.xで作成した共有ルールセットを使用します。
7041	情報	アプリケーションコントロールルールセットをアップグレードしました	アプリケーションコントロールルールセットがファイルベースのルールセットからハッシュベースのルールセットにアップグレードされました(詳細については、" Deep Security Agent 10と11におけるファイルの比較方法の相違点 " on page 695を参照してください)。
7042	情報	アプリケーションコントロールソフトウェアインベントリが削除されました	

アプリケーションコントロールイベント

イベントに関する全般的なベストプラクティスについては、"[Deep Securityのイベント](#)" on page 1116を参照してください。

Deep Securityでキャプチャされたアプリケーションコントロールイベントを確認するには、[イベントとレポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント]の順に選択します。

アプリケーションコントロールイベントで表示される情報

[アプリケーションコントロールイベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

Trend Micro Deep Security On-Premise 12.0

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- イベント: イベントの名前。
- ルール: イベント詳細を表示して、ルールの許可とブロックを切り替えることができます。
- ルールセット: イベントに関連付けられているルールセット。
- 処理: イベントをトリガさせた処理。
- 理由: イベントがトリガされた理由。
- 繰り返しカウント: 集約されるイベントの数。
- タグ: このイベントに関連付けられたイベントのタグ。
- パス: 影響を受けたファイルへのパス。
- ファイル: イベントの影響を受けたファイル。
- ユーザ名: 承認されていないソフトウェアの実行を担当したユーザ。
- イベント送信元: イベントの送信元であるDeep Securityコンポーネント。
- MD5:MD5ハッシュ。
- SHA1:SHA-1ハッシュ。
- SHA256:SHA-256ハッシュ。
- グループ: グループの名前。
- グループID: グループのID。
- ユーザID: ファイルの所有者のユーザID。
- プロセスID: 実行処理を実行するプロセスのID。
- プロセス名: 実行処理を実行するプロセス。

アプリケーションコントロールイベント一覧

注意: アプリケーションコントロールに関連するシステムイベントについては、"[システムイベント](#)" on page 1271を参照してください。

イベント
承認されていないソフトウェアの実行を許可
承認されていないソフトウェアの実行をブロック
ソフトウェアの実行をルールでブロック

不正プログラム対策イベント

イベントに関する全般的なベストプラクティスについては、"[Deep Securityのイベント](#)" on page 1116を参照してください。

Deep Securityでキャプチャされた不正プログラム対策イベントを確認するには、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]の順に選択します。

不正プログラム対策イベントで表示される情報

[不正プログラム対策イベント]画面には次の列が表示されます。[列]をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ (コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 感染ファイル: 感染ファイルの場所と名前。
- タグ: このイベントに関連付けられたイベントのタグ。
- 不正プログラム: 検出された不正プログラムの名前。

- 実行された処理: イベントに関連付けられた不正プログラム検索設定で指定された処理の結果が表示されます。
 - 駆除: 不正プログラムの種類に応じて、プロセスを終了したか、レジストリ、ファイル、Cookie、またはショートカットを削除しました。
 - 駆除失敗: 不正プログラムを駆除できませんでした。理由にはさまざまなものが考えられます。
 - 削除: 感染ファイルが削除されました。
 - 削除失敗: 感染ファイルを削除できませんでした。理由にはさまざまなものが考えられます。たとえば、ファイルが別のアプリケーションによってロックされている、CD上にある、または使用中である場合です。可能な場合、感染ファイルが解放された時点で削除されます。
 - 隔離: 検出ファイルフォルダに感染ファイルを隔離しました。
 - 隔離失敗: 感染ファイルを隔離できませんでした。理由にはさまざまなものが考えられます。たとえば、ファイルが別のアプリケーションによってロックされている、CD上にある、または使用中である場合です。可能な場合、感染ファイルが解放された時点で隔離されます。ポリシーまたはコンピュータエディタの [不正プログラム対策] → [詳細] タブで指定された「検出ファイルの保存に使用される最大ディスク容量」を超過した可能性もあります。
 - アクセス拒否: システムからファイルを削除せずに、感染ファイルにアクセスできないようにしました。
 - 放置: 何も処理を行わず、不正プログラムの検出のみをログに記録しました。
- 検索の種類: 不正プログラムを検出した検索の種類 (リアルタイム、予約、手動)。
- イベント送信元: イベントが発生したDeep Securityシステムのコンポーネントを示します。
- 理由: 不正プログラムが検出されたときに有効だった不正プログラム検索設定です。
- 主要なウイルスの種類: 検出された不正プログラムの種類。値には、ジョーク、トロイの木馬、テスト、スパイウェア、パッカー、一般的なプログラム、その他があります。それぞれの不正プログラムの詳細については、不正プログラム対策イベントの詳細を参照するか、["不正プログラムの防止" on page 722](#)を参照してください。
- 対象: 不正プログラムが操作を試みた対象のファイル、プロセス、またはレジストリキー (ある場合)。不正プログラムの対象が複数に及ぶ場合、このフィールドの値は「Multiple」になります。

- 対象の種類: この不正プログラムが操作を試みたシステムリソースの種類。ファイルシステム、プロセス、Windowsレジストリなどです。
- コンテナID: 不正プログラムが検出されたDockerコンテナのID。
- コンテナイメージ名: 不正プログラムが検出されたDockerコンテナのイメージ名。
- コンテナ名: 不正プログラムが検出されたDockerコンテナの名前。
- ファイルMD5: ファイルのMD5ハッシュ。

不正プログラム対策イベント一覧





ID	重要度	イベント
9001	情報	不正プログラム検索の開始
9002	情報	不正プログラム検索の完了
9003	情報	不正プログラム検索の異常終了
9004	情報	不正プログラム検索の一時停止
9005	情報	不正プログラム検索の再開
9006	情報	不正プログラム検索のキャンセル
9007	警告	不正プログラム検索キャンセルの失敗
9008	警告	不正プログラム検索開始の失敗
9009	警告	不正プログラム検索の停止
9010	エラー	ファイルを分析または隔離できません (検出ファイル保存用のVMの最大ディスク容量を超過)
9011	エラー	ファイルを分析または隔離できません (検出ファイル保存用の最大ディスク容量を超過)
9012	警告	スマートスキャン用のSmart Protection Serverへの接続不能
9013	情報	スマートスキャン用のSmart Protection Serverへの接続
9014	警告	不正プログラム対策保護を完了するためにコンピュータの再起動が必要
9016	情報	不正プログラム対策コンポーネントのアップデート成功
9017	エラー	不正プログラム対策コンポーネントのアップデート失敗
9018	エラー	ファイルで不正プログラムを検索できませんでした
9019	エラー	ディレクトリで不正プログラムを検索できませんでした

ファイアウォールイベント

イベントに関する全般的なベストプラクティスについては、"[Deep Securityのイベント](#)" on page 1116を参照してください。

Deep Securityでキャプチャされたファイアウォールイベントを確認するには、[イベントとレポート]→[イベント]→[ファイアウォールイベント]の順に選択します。

ファイアウォールイベントのアイコン:

-  単一イベント
-  データ付き単一イベント
-  折りたたみイベント
-  データ付き折りたたみイベント

注意: イベントの折りたたみは、同じ種類のイベントが数回続けて発生したときに実行されます。これによりディスク容量を節約でき、ログメカニズムに負荷をかけるDoS攻撃から防御することができます。

ファイアウォールイベントで表示される情報

[ファイアウォールイベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ (コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由: この画面のログエントリが、ファイアウォールルールによって生成されたか、またはファイアウォールステートフル設定によって生成されたかを示します。エントリがファイアウォールルールによって生成された場合、列エントリには、

「ファイアウォールルール:」と表示され、続いてファイアウォールルールの名前が表示されます。それ以外の場合、列エントリには、ログエントリを生成したファイアウォールステートフル設定の内容が表示されます。

- タグ: このイベントに適用されているイベントタグ。
- 処理: ファイアウォールルールまたはファイアウォールステートフル設定によって実行された処理。処理には、許可、拒否、強制的に許可、ログのみがあります。
- ランク: ランク付けシステムでは、侵入防御およびファイアウォールイベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、侵入防御ルールとファイアウォールルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、侵入防御イベントまたはファイアウォールイベントを表示するときに、イベントをランクでソートできます。
- 方向: パケットの方向 (受信または送信)。
- インタフェース: パケットが経由するインタフェースのMACアドレス。
- フレームの種類: 対象となるパケットのフレームの種類。値は、[IPV4]、[IPV6]、[ARP]、[REVARP]、および [その他: XXXX] (XXXXはフレームの種類を示す4桁の16進コード) のいずれかになります。
- プロトコル: 値は、[ICMP]、[ICMPV6]、[IGMP]、[GGP]、[TCP]、[PUP]、[UDP]、[IDP]、[ND]、[RAW]、[TCP+UDP]、および [その他: nnn] (nnnは、3桁の10進値) のいずれかになります。
- フラグ: パケットに設定されたフラグ。
- 送信元IP: パケットの送信元IP。
- 送信元MAC: パケットの送信元MACアドレス。
- 送信元ポート: パケットの送信元ポート。
- 送信先IP: パケットの送信先IP。
- 送信先MAC: パケットの送信先MACアドレス。
- 送信先ポート: パケットの送信先ポート。
- パケットサイズ: バイト単位のパケットのサイズ。
- 繰り返しカウント: イベントが連続して繰り返された回数。

- 時間 (マイクロ秒): コンピュータ上でイベントが発生した時間 (マイクロ秒)。
- イベント送信元: イベントの送信元であるDeep Securityコンポーネント。

注意: ログのみルールは、対象のパケットが、拒否ルールまたはそのパケットを除外する許可ルールによって、それ以降に停止されない場合にログエントリのみを生成します。この2つのルールのいずれかによってパケットが停止される場合は、ログのみルールではなく、これらのルールがログエントリを生成します。以降のルールでパケットを停止しない場合は、ログのみルールがエントリを生成します。

ファイアウォールイベント一覧

ID	イベント	備考
100	セッション情報なし	既存の接続に関連付けられていないパケットを受信しました。
101	不正なフラグ	パケットに設定されたフラグが無効です。このイベントは、現在の接続 (存在する場合) のコンテキスト内で意味をなさないフラグ、または無意味な組み合わせのフラグであることを示しています。 接続コンテキストを評価するには「ファイアウォールステートフル設定」がオンになっている必要があります。
102	不正なシーケンス	シーケンス番号が無効なパケットまたはデータサイズが範囲外のパケットが検出されました。
103	不正なACK	確認応答番号が無効なパケットが検出されました。
104	内部エラー	
105	CEフラグ	パケットに輻輳フラグが設定されていたり、ポリシーの回避技術対策でTCP輻輳フラグプロパティがログまたは拒否に設定されているカスタム設定を使用したりしています (" 回避技術対策の設定 " on page 827を参照)。
106	不正なIP	パケットの送信元IPが無効です。
107	不正なIPデータグラム長	IPヘッダで指定されている長さよりも短いIPデータグラム長です。
108	フラグメント化	フラグメント化されたパケットが検出されました。フラグメント化されたパケットは許可されていません。
109	不正なフラグメントオフセット	

ID	イベント	備考
110	最初のフラグメントが最小サイズ未満	<p>フラグメント化されたパケットが検出されました。最初のフラグメントのサイズがTCPパケット (データなし) のサイズよりも小さくなっています。</p> <p>パケットヘッダに次の設定が指定されている場合、パケットは破棄されます。</p> <ul style="list-style-type: none"> フラグメントオフセット = 0 (フラグメントはパケットの最初のフラグメントです) 合計長 (最大組み合わせヘッダ長) < 120バイト (デフォルトの許容最小フラグメントサイズ) <p>このイベントの再発を防止するには、最小フラグメントサイズプロパティの値を低くするようにポリシーのネットワークエンジンの詳細設定を行うか、この監視をオフにするように0に設定します ("ネットワークエンジン設定" on page 612の「ネットワークエンジンの詳細オプション」を参照)。</p>
111	範囲外のフラグメント	フラグメント化されたパケットシーケンスに指定されているオフセットが、データグラムの最大サイズ範囲を超えています。
112	最小オフセット値以下のフラグメント	フラグメント化されたパケットが検出されました。フラグメントのサイズがTCPパケット (データなし) のサイズよりも小さくなっています。
113	IPv6パケット	IPv6パケットが検出されました。IPv6ブロックが有効になっています。「ネットワークエンジンの詳細オプション」の「バージョン9以降のAgentとApplianceでIPv6をブロック」プロパティ (" ネットワークエンジン設定 " on page 612を参照) を参照してください。
114	受信接続の上限	受信接続数が最大許容数を超えました。" TCPパケットインスペクション " on page 880の「TCPステートフルインスペクションを有効にする」プロパティを参照してください。
115	送信接続の上限	送信接続数が最大許容数を超えていました。" TCPパケットインスペクション " on page 880の「TCPステートフルインスペクションを有効にする」プロパティを参照してください。
116	SYN送信の上限	単一コンピュータからのハーフオープン接続数がファイアウォールステートフル設定に指定された数を超えています。" TCPパケットインスペクション " on page 880の「単一コンピュータからのハーフオープン接続数の上限」プロパティを参照してください。
118	不明なIPバージョン	IPv4またはIPv6以外のIPパケットが検出されました。
119	不正なパケット情報	
120	内部エンジンエラー	システムメモリの不足。システムリソースを追加してこの問題を修正します。

ID	イベント	備考
121	許可されていないUDP応答	コンピュータに許可されていない受信UDPパケットは拒否されます。
122	許可されていないICMP応答	ファイアウォールステートフル設定でICMPステートフルが有効になっています。いずれの「強制的に許可」ルールにも一致しない未許可のパケットを受信しました。
123	ポリシーで未許可	パケットはいずれの「許可」ルールまたは「強制的に許可」ルールにも一致しないため黙示的に拒否されます。
124	不正なポートコマンド	FTP制御チャンネルのデータストリームで無効なFTPポートコマンドが検出されました。
125	SYN Cookieエラー	SYN Cookieの保護メカニズムでエラーが発生しました。
126	不正なデータオフセット	データオフセットパラメータが無効です。
127	IPヘッダなし	パケットIPヘッダが無効または不完全です。
128	読み取り不能なイーサネットヘッダ	このイーサネットフレームに含まれるデータがイーサネットヘッダよりも少なくなっています。
129	未定義	
130	送信元および送信先IPが同一	送信元IPと送信先IPが同じです。
131	不正なTCPヘッダ長	
132	読み取り不能なプロトコルヘッダ	読み取り不能なTCP、UDP、またはICMPヘッダがパケットに含まれています。
133	読み取り不能なIPv4ヘッダ	読み取り不能なIPv4ヘッダがパケットに含まれています。
134	不明なIPバージョン	IPバージョンを認識できません。
135	不正なアダプタ設定	無効なアダプタ設定を受信しました。
136	重複しているフラグメント	このパケットのフラグメントは以前に送信されたフラグメントと重複しています。
138	切断された接続	すでに切断された接続に属するパケットを受信しました。

ID	イベント	備考
	上のパケット	
139	再送の破棄	<p>ネットワークエンジンが、同じTCP接続ですでに受信したデータと重複しているTCPパケットを検出しましたが、すでに受信したデータと一致しません。(ネットワークエンジンは、エンジンの接続バッファ内の処理待ちパケットデータと再送信されたパケットのデータを比較します。)</p> <p>ネットワークエンジンは、処理するTCP接続ごとにデータストリームを順番に再構築します。受信パケットのシーケンス番号と長さにより、このデータストリームの特定の領域が決まります。ログの注記用フィールドは、TCPストリームで変更した次のコンテンツの場所を示します。prev-full、prev-part、next-full、およびnext-part。</p> <ul style="list-style-type: none"> 「prev-full」と「prev-part」:変更領域は、順番に整理されたデータストリームの再送信パケットをすぐに処理するパケット内にあります。「prev-full」は、変更領域が順番に整理されたデータストリームの再送信パケットをすぐに処理するパケット内に完全に含まれることを示します。それ以外の場合の注記は「prev-part」です。 「next-full」と「next-part」:変更領域は、順番に整理されたデータストリームの再送信パケットのすぐ後に続くパケット内にあります。「next-full」は、変更領域が順番に整理されたデータストリームの再送信パケットのすぐ後に続くパケット内に完全に含まれることを示します。それ以外の場合の注記は「next-part」です。
140	未定義	
141	ポリシーで未許可 (オープンポート)	
142	新しい接続の開始	
143	無効なチェックサム	
144	無効なフック	
145	IPペイロードがゼロ	
146	IPv6ソースがマ	

ID	イベント	備考
	ルチキャスト	
147	無効なIPv6アドレス	
148	最小サイズ以下のIPv6のフラグメント	
149	無効なトランスポートヘッダ長	
150	メモリ不足	
151	最大TCP接続数	TCP接続の最大数が超えました。 "イベント: 最大TCP接続数" on page 1371 を参照してください。
152	最大UDP接続数	
200	リージョンサイズの超過	リージョン (編集リージョン、URIなど) が閉じられずに、バッファの最大許容サイズ (7570バイト) を超えました。これは、通常、データがプロトコルに適合していないために発生します。
201	メモリ不足	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続によってバッファ (最大2,048) や一致リソース (最大128) が一度に要求された場合、1つのIPパケットにおける一致数 (最大2,048) を超過した場合、または単にシステムのメモリが不足した場合に発生することがあります。
202	編集回数の超過	パケットの単一リージョンにおける最大編集回数 (32回) を超えました。
203	編集範囲の超過	リージョンのサイズを最大許容サイズ (8,188バイト) よりも増やそうとする編集が試行されました。
204	パケットの最大一致数を超過	パケット内でパターンに一致する地点が2,048箇所を超えています。この制限に達するパケットは通常ガベージパケットまたは回避パケットであるため、エラーが返されて接続が破棄されます。
205	エンジンのコールスタック数の超過	
206	ランタイムエラー	ランタイムエラーです。
207	パケットの読み込みエラー	パケットデータの読み込み中に発生した低レベルの問題です。
257	Fail-Open:拒否 (ログに記録)	破棄する必要のあるパケットを記録し、Fail-Open機能がオンでインラインモードの場合には記録しません。
300	サポートされていない暗号化	不明またはサポートされていない暗号化スイートが要求されました。
301	マスターキーの	マスターシークレットから、暗号化キー、MACシークレット、および初期化ベクタを生成できません。

ID	イベント	備考
	生成エラー	
302	レコードレイヤメッセージ (準備ができていません)	SSL状態エンジンで、セッションの初期化前にSSLレコードが検出されました。
303	ハンドシェークメッセージ (準備ができていません)	SSL状態エンジンで、ハンドシェークのネゴシエーション後にハンドシェークメッセージが検出されました。
304	ハンドシェークメッセージの障害	適切にフォーマットされたハンドシェークメッセージが、誤った順序で検出されました。
305	メモリの割り当てエラー	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続によってバッファ (最大2,048) や一致リソース (最大128) が一度に要求された場合、1つのIPパケットにおける一致数 (最大2,048) を超過した場合、または単にシステムのメモリが不足した場合に発生することがあります。
306	サポートされていないSSLバージョン	クライアントがSSL V2バージョンのネゴシエーションを試行しました。
307	プレマスターキーの復号時のエラー	ClientKeyExchangeメッセージからプレマスターシークレットを復号できません。
308	クライアントによるロールバックの試行	クライアントが、ClientHelloメッセージに指定されたバージョンより古いバージョンのSSLプロトコルへのロールバックを試行しました。
309	更新エラー	キャッシュされたセッションキーでSSLセッションが要求されましたが、該当するセッションキーが見つかりませんでした。
310	鍵の交換エラー	サーバが一時的に生成されたキーを使用してSSLセッションを確立しようとしています。
311	SSLキー交換の上限を超過	キー交換の同時要求数が上限を超えました。
312	鍵サイズの超過	マスターの秘密鍵がプロトコルIDで指定されたサイズを超えています。
313	ハンドシェーク内の不正なパラメータ	ハンドシェークプロトコルのデコード中に無効または不正な値が検出されました。

ID	イベント	備考
314	利用可能なセッションなし	
315	未サポートの圧縮方法	
316	サポートされていないアプリケーション層プロトコル	不明、またはサポートされていないSSLアプリケーション層プロトコルが要求されました。
385	Fail-Open:拒否(ログに記録)	破棄する必要のあるパケットを記録し、Fail-Open機能がオンでタップモードの場合には記録しません。
500	URIパスの深さが超過	区切り文字「/」が多すぎます。パスの深さは最大100です。
501	無効なトラバーサル	ルートより上位に「../」を使用しようとしてしました。
502	URIに使用できない文字	URIに無効な文字が使用されています。
503	不完全なUTF8シーケンス	UTF8シーケンスの途中でURIが終了しました。
504	無効なUTF8の符号化	無効または規定外のエンコードが試行されました。
505	無効な16進の符号化	%nnのnnが16進数ではありません。
506	URIパス長の超過	パス長が512文字を超えています。
507	不正な文字の使用	無効な文字を使用しています。
508	二重デコードの攻撃コード	二重デコードの攻撃コードです (%25xx、%25%xxdなど)。
700	不正なBase64コンテンツ	Base64形式でエンコードされるはずのパケットコンテンツが正しくエンコードされませんでした。
710	破損したDeflate/GZIPコンテンツ	Base64形式でエンコードされるはずのパケットコンテンツが正しくエンコードされませんでした。

ID	イベント	備考
711	不完全な Deflate/GZIP コンテンツ	不完全な Deflate/GZIP コンテンツです
712	Deflate/GZIP チェックサムエラー	Deflate/GZIP チェックサムエラーです。
713	未サポートの Deflate/GZIP 辞書	サポートされていない Deflate/GZIP 辞書です。
714	サポートされていない GZIP ヘッダ形式/方法	サポートされていない GZIP ヘッダ形式または方法です。
801	プロトコルデコード検索の上限を超過	プロトコルデコードルールには検索または PDU オブジェクトの制限が定義されていますが、オブジェクトを見つける前に制限に達しました。
802	プロトコルデコードの制約エラー	プロトコルデコードルールによってデコードされたデータが、プロトコルコンテンツの制約を満たしていません。
803	プロトコルデコードエンジンの内部エラー	
804	プロトコルデコードの構造の超過	プロトコルデコードルールで、型の最大ネスト深度 (16) を超える型定義とパケットコンテンツが検出されました。
805	プロトコルデコードのスタックエラー	ルールのプログラミングエラーが原因で、反復が発生したか、またはネストされたプロシージャコールが使用されようとしていました。
806	データの無限ループエラー	

侵入防御イベント

イベントに関する全般的なベストプラクティスについては、"[Deep Securityのイベント](#)" on page 1116を参照してください。

Deep Securityでキャプチャされた侵入防御イベントを確認するには、[イベントとレポート]→[イベント]→[侵入防御イベント]の順に選択します。

侵入防御イベントで表示される情報

[侵入防御イベント]画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由: このイベントに関連付けられた侵入防御ルール。
- タグ: イベントに付けられたタグ。
- アプリケーションの種類: このイベントの原因となった侵入防御ルールに関連付けられたアプリケーションの種類。
- 処理: 侵入防御ルールが実行する処理 (ブロックまたはリセット)。ルールが検出のみモードの場合、処理名の前に「検出のみ:」が付きます。

注意: Deep Security 7.5 SP1より前に作成された侵入防御ルールでは、挿入、置換、削除処理も実行することができましたが、現在これらの処理は実行されません。これらの処理の実行を試みる古いルールが実行された場合、ルールが検出のみモードで適用されたことを示すイベントが記録されます。

- ランク: ランク付けシステムでは、侵入防御およびファイアウォールイベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、侵入防御ルールとファイアウォールルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、侵入防御イベントまたはファイアウォールイベントを表示するときに、イベントをランクでソートできます。
- 重要度: 侵入防御ルールの重要度。
- 方向: パケットの方向 (受信または送信)。
- フロー: このイベントを引き起こしたパケットが、侵入防御ルールで監視しているトラフィックと同じ方向に進んでいたか (「接続フロー」)、または反対方向に進んでいたか (「リバースフロー」)。

Trend Micro Deep Security On-Premise 12.0

- インタフェース: パケットが通過したインタフェースのMACアドレス。
- フレームの種類: 対象となるパケットのフレームの種類。値は、[IPV4]、[IPV6]、[ARP]、[REVARP]、および [その他:XXXX] (XXXXはフレームの種類を示す4桁の16進コード) のいずれかになります。
- プロトコル: 値は、[ICMP]、[ICMPV6]、[IGMP]、[GGP]、[TCP]、[PUP]、[UDP]、[IDP]、[ND]、[RAW]、[TCP+UDP]、および [その他: nnn] (nnnは、3桁の10進値) のいずれかになります。
- フラグ: パケットに設定されたフラグ。
- 送信元IP: パケットの送信元IP。
- 送信元MAC: パケットの送信元MACアドレス。
- 送信元ポート: パケットの送信元ポート。
- 送信先IP: パケットの送信先IP。
- 送信先MAC: パケットの送信先MACアドレス。
- 送信先ポート: パケットの送信先ポート。
- パケットサイズ: バイト単位のパケットのサイズ。
- 繰り返しカウント: イベントが連続して繰り返された回数。
- 時間 (マイクロ秒): コンピュータ上でイベントが発生した時間 (マイクロ秒)。
- イベント送信元: イベントの送信元であるDeep Securityコンポーネント。

侵入防御イベントの追加情報の表示。

侵入防御イベントを[エクスポート](#)する場合、エクスポートされたデータには上記のフィールドと、Deep Security Managerコンソールには表示されない追加のフィールドが含まれます。唯一の例外は、Severityフィールドです。このフィールドはCSVファイルでは使用できません。

- Note : CVEコードなど、イベントに意味のある文字列。
- 終了時刻 : パケットが最後に確認された時刻。
- バッファ内位置 : パケット内の位置。

- ストリーム内の位置：TCP / IPストリーム内のパケットの位置。
- データフラグ：データフラグの値の詳細については、次の表を参照してください。

コード	フラグ	備考
0x01	dataTruncated	データをログに記録できなかったことを示します。
0x02	logOverflow	このエントリの後にログがオーバーフローしました。
0x04	suppressed	このエントリの後にしきい値の抑制が発生したことをログに記録します。
0x08	haveData	パケットデータがログに記録されます。
0x10	refData	DataIdがログに記録されます。パケットペイロードはこのイベントに記録されません。ペイロードは、0x08フラグと同じデータインデックスを持つイベントでのみログに記録されます。
0x20	haveRawPkt	データは完全な生のパケットです。

- Data Index：パケットデータの一意のID (dataId)。dataIdが同じレコードはすべて同じパケットのものです。
- Data：パケットのペイロード。
- Original IP (XFF)：クライアントの元のIPアドレスを表示します。このフィールドのデータを取得するには、ルール 1006450-Enable X-Forwarded-For HTTP Header Loggingを有効にします。

侵入防御イベント一覧

ID	イベント	備考
200	リージョンサイズの超過	リージョン (編集リージョン、URIなど) が閉じられずに、バッファの最大許容サイズ (7570バイト) を超えました。これは、通常、データがプロトコルに適合していないために発生します。
201	メモリ不足	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続が一度に行われた場合、または単にシステムのメモリが不足した場合に発生することがあります。
202	編集回数の超過	パケットの単一リージョンにおける最大編集回数 (32回) を超えました。
203	編集範囲の超過	リージョンのサイズを最大許容サイズ (8,188バイト) よりも増やそうとする編集が試行されました。
204	パケットの最大一致数を超過	パケット内でパターンに一致する地点が2,048箇所を超えています。この制限に達するパケットは通常ガベージパケットまたは回避パケットであるため、エラーが返されて接続が破棄されます。
205	エンジンのコールスタック	(備考はありません)

ID	イベント	備考
	ク数の超過	
206	ランタイムエラー	ランタイムエラーです。
207	パケットの読み込みエラー	パケットデータの読み込み中に発生した低レベルの問題です。
258	Fail-Open:リセット	リセットする必要がある接続を記録し、Fail-Open機能がオンでインラインモードの場合には記録しません。
300	サポートされていない暗号化	不明またはサポートされていない暗号化スイートが要求されました。
301	マスターキーの生成エラー	マスターシークレットから、暗号化キー、MACシークレット、および初期化ベクタを生成できません。
302	レコードレイヤメッセージ (準備ができていません)	SSL状態エンジンで、セッションの初期化前にSSLレコードが検出されました。
303	ハンドシェイクメッセージ (準備ができていません)	SSL状態エンジンで、ハンドシェイクのネゴシエーション後にハンドシェイクメッセージが検出されました。
304	ハンドシェイクメッセージの障害	適切にフォーマットされたハンドシェイクメッセージが、誤った順序で検出されました。
305	メモリの割り当てエラー	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続が一度に行われた場合、または単にシステムのメモリが不足した場合に発生することがあります。
306	サポートされていないSSLバージョン	クライアントがSSL V2バージョンのネゴシエーションを試行しました。
307	プレマスターキーの復号時のエラー	ClientKeyExchangeメッセージからプレマスターシークレットを復号できません。
308	クライアントによるロールバックの試行	クライアントが、ClientHelloメッセージに指定されたバージョンより古いバージョンのSSLプロトコルへのロールバックを試行しました。
309	更新エラー	キャッシュされたセッションキーでSSLセッションが要求されましたが、該当するセッションキーが見つかりませんでした。
310	鍵の交換エラー	サーバが一時的に生成されたキーを使用してSSLセッションを確立しようとしています。
311	SSLキー交換の上限を超過	キー交換の同時要求数が上限を超えました。
312	鍵サイズの超過	マスターの秘密鍵がプロトコルIDで指定されたサイズを超えています。
313	ハンドシェイク内の不正なパラメータ	ハンドシェイクプロトコルのデコード中に無効または不正な値が検出されました。
314	利用可能なセッションな	(備考はありません)

ID	イベント	備考
	し	
315	未サポートの圧縮方法	(備考はありません)
316	サポートされていないアプリケーション層プロトコル	不明、またはサポートされていないSSLアプリケーション層プロトコルが要求されました。
386	Fail-Open:リセット	リセットする必要がある接続を記録し、Fail-Open機能がオンでタップモードの場合には記録しません。
500	URIパスの深さが超過	区切り文字「/」が多すぎます。パスの深さは最大100です。
501	無効なトラバーサル	ルートより上位に「../」を使用しようとしてしました。
502	URIに使用できない文字	URIに無効な文字が使用されています。
503	不完全なUTF8シーケンス	UTF8シーケンスの途中でURIが終了しました。
504	無効なUTF8の符号化	無効または規定外のエンコードが試行されました。
505	無効な16進の符号化	%nnのnnが16進数ではありません。
506	URIパス長の超過	パス長が512文字を超えています。
507	不正な文字の使用	無効な文字を使用しています。
508	二重デコードの攻撃コード	二重デコードの攻撃コードです (%25xx、%25%xxdなど)。
700	不正なBase64コンテンツ	Base64形式でエンコードされるはずの packets コンテンツが正しくエンコードされませんでした。
710	破損したDeflate/GZIPコンテンツ	Base64形式でエンコードされるはずの packets コンテンツが正しくエンコードされませんでした。
711	不完全なDeflate/GZIPコンテンツ	不完全なDeflate/GZIPコンテンツです
712	Deflate/GZIPチェックサムエラー	Deflate/GZIPチェックサムエラーです。
713	未サポートのDeflate/GZIP辞書	サポートされていないDeflate/GZIP辞書です。
714	サポートされていないGZIPヘッダ形式/方法	サポートされていないGZIPヘッダ形式または方法です。
801	プロトコルデコード検索の上限を超過	プロトコルデコードルールには検索またはPDUオブジェクトの制限が定義されていますが、オブジェクトを見つける前に制限に達しました。
802	プロトコルデコードの制約エラー	プロトコルデコードルールによってデコードされたデータが、プロトコルコンテンツの制約を満たしていません。

ID	イベント	備考
803	プロトコルデコードエンジンの内部エラー	(備考はありません)
804	プロトコルデコードの構造の超過	プロトコルデコードルールで、型の最大ネスト深度 (16) を超える型定義とパケットコンテンツが検出されました。
805	プロトコルデコードのスタックエラー	ルールのプログラミングエラーが原因で、反復が発生したか、またはネストされたプロシージャコールが使用されようとしていました。
806	データの無限ループエラー	

変更監視イベント

イベントに関する全般的なベストプラクティスについては、"[Deep Securityのイベント](#)" on page 1116を参照してください。

Deep Securityでキャプチャされた変更監視イベントを確認するには、[イベントとレポート]→[イベント]→[変更監視イベント]の順に選択します。

変更監視イベントで表示される情報

[変更監視イベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ (コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由: このイベントに関連付けられた変更監視ルール。
- タグ: このイベントに適用されているイベントタグ。
- 変更: 変更監視ルールによって検出された変更。値は、「作成」、「アップデート」、「削除」、または「拡張子変更」のいずれかです。

- ランク: ランク付けシステムでは、イベントの重要度を数値化できます。コンピュータに「資産評価」を、ルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、イベントをランクでソートできます。
- 重要度: 変更監視ルールの重要度
- 種類: イベントの発生元であるエンティティの種類
- キー: イベントの発生元であるパスおよびファイル名またはレジストリキー
- ユーザ: ファイルの所有者のユーザID
- プロセス: イベントの発生元であるプロセス
- イベント送信元: イベントの送信元であるDeep Securityコンポーネント

変更監視イベント一覧

ID	重要度	イベント	備考
8000	情報	完全なベースラインの作成	Agentに対してベースラインを作成するよう要求があった場合、またはAgentの変更監視ルールが0からnになり、その結果ベースラインが作成された場合に作成されます。このイベントには、検索にかかった時間 (ミリ秒) およびカタログ化されたエンティティ数の情報が含まれます。
8001	情報	部分的なベースラインの作成	Agentのセキュリティ設定で変更監視ルールが1つ以上変更された場合に作成されます。このイベントには、検索にかかった時間 (ミリ秒) およびカタログ化されたエンティティ数の情報が含まれます。
8002	情報	変更の検索の完了	Agentに対して完全または部分的な手動検索が要求された場合に作成されます。このイベントには、検索にかかった時間 (ミリ秒) およびカタログ化された変更数の情報が含まれます。ファイルシステムドライバまたは通知に基づく変更に対する継続検索では、8002イベントは生成されません。
8003	エラー	変更監視ルール内の不明な環境変数	ルールで <code>\${env.EnvironmentVar}</code> が使用されていて、「EnvironmentVar」が既知の環境変数でない場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、および不明な環境変数の名前が含まれます。
8004	エラー	変更監視ルール内の不正なベース値	無効な基本ディレクトリまたはキーがルールに含まれる場合に作成されます。たとえば、基本ディレクトリが「c:\foo\d:\bar」のFileSetを指定すると、このイベントが生成されます。または、環境変数の置き換えによって無効な値が生成される場合もあります。このイベントには、

ID	重要度	イベント	備考
			該当する変更監視ルールIDと名前、および無効な基本値が含まれます。
8005	エラー	変更監視ルール内の不明なエンティティ	変更監視ルールで不明なEntitySetが検出された場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、および検出された不明なEntitySet名のカンマ区切りのリストが含まれます。
8006	エラー	変更監視ルール内のサポートされていないエンティティ	変更監視ルールで既知のサポートされないEntitySetが検出された場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、および検出されたサポートされないEntitySet名のカンマ区切りのリストが含まれます。RegistryKeySetなどの一部のEntitySetの種類はプラットフォームに固有です。
8007	エラー	変更監視ルール内の不明な機能	変更監視ルールで不明な機能が検出された場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、エンティティセットの種類 (FileSetなど)、および検出された不明な機能名のカンマ区切りのリストが含まれます。有効な機能値の例は、「whereBaseInOtherSet」、「status」、および「executable」です。
8008	エラー	変更監視ルール内のサポートされていない機能	変更監視ルールで既知のサポートされない機能が検出された場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、エンティティセットの種類 (FileSetなど)、および検出されたサポートされない機能名のカンマ区切りのリストが含まれます。Windowsサービスの状態を表す「status」などの一部の機能値はプラットフォームに固有です。
8009	エラー	変更監視ルール内の不明な属性	変更監視ルールで不明な属性が検出された場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、エンティティセットの種類 (FileSetなど)、および検出された不明な属性名のカンマ区切りのリストが含まれます。有効な属性値の例は、「created」、「lastModified」、および「inodeNumber」です。
8010	エラー	変更監視ルール内のサポートされていない属性	変更監視ルールで既知のサポートされない属性が検出された場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、エンティティセットの種類 (FileSetなど)、および検出されたサポートされない属性名のカンマ区切りのリストが含まれます。「inodeNumber」などの一部の属性値はプラットフォームに固有です。
8011	エラー	変更監視ルール内のエンティティセットの不明な属性	変更監視ルールで不明なEntitySet XML属性が検出された場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、エンティティセットの種類 (FileSetなど)、および検出された不明なEntitySet属性名のカンマ区切りのリストが含まれます。<FileSet base="c:\foo"> の代わりに <FileSet dir="c:\foo"> を記述した場合にこのイベントが記録されます。
8012	エラー	変更監視ルール内の不明なレジストリ文字列	ルールが存在しないレジストリキーを参照している場合に作成されます。このイベントには、該当する変更監視ルールIDと名前、および不明なレジストリ文字列の名前が含まれます。

ID	重要度	イベント	備考
8013	エラー	WQLSetが無効です。名前空間またはWQLクエリが見つかりませんでした。	変更監視ルールXMLの形式が正しくないため、WQLクエリ内に名前空間が見つからないことを示しています。WQLクエリを使用および監視するカスタム変更監視ルールが使用される、高度な事例でのみ発生します。
8014	エラー	WQLSetが無効です。不明なプロバイダ値が使用されています。	(備考はありません)
8015	警告	適用できない変更監視ルール	プラットフォームの不一致、存在しないターゲットディレクトリやファイル、サポートされていない機能など、いくつかの理由によって発生する可能性があります。
8016	警告	2番目に最適な変更監視ルール検出	(備考はありません)
8050	エラー	正規表現をコンパイルできませんでした。無効なワイルドカードが使用されています。	(備考はありません)

セキュリティログ監視イベント

イベントに関する全般的なベストプラクティスについては、"[Deep Securityのイベント](#)" on page 1116を参照してください。

Deep Securityでキャプチャされたセキュリティログ監視イベントを確認するには、[イベントとレポート]→[イベント]→[セキュリティログ監視イベント]の順に選択します。

セキュリティログ監視イベントで表示される情報

[セキュリティログ監視イベント]画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

Trend Micro Deep Security On-Premise 12.0

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ (コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由: このイベントに関連付けられたセキュリティログ監視ルール。
- タグ: イベントに付けられたタグ。
- 説明: ルールの説明。
- ランク: ランク付けシステムでは、イベントの重要度を数値化できます。コンピュータに「資産評価」を、セキュリティログ監視ルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、イベントをランクでソートできます。
- 重要度: セキュリティログ監視ルールの重要度。
- グループ: ルールの所属先グループ。
- プログラム名: プログラム名。イベントのSyslogヘッダから取得されます。
- イベント: イベントの名前。
- 場所: ログの生成元。
- 送信元IP: パケットの送信元IP。
- 送信元ポート: パケットの送信元ポート。
- 送信先IP: パケットの送信先IP。
- 送信先ポート: パケットの送信先ポート。
- プロトコル: 値は、[ICMP]、[ICMPV6]、[IGMP]、[GGP]、[TCP]、[PUP]、[UDP]、[IDP]、[ND]、[RAW]、[TCP+UDP]、および [その他: nnn] (nnnは、3桁の10進値) のいずれかになります。
- 処理: イベント内で実行された処理
- 送信元ユーザ: イベント内の送信元ユーザ。
- 送信先ユーザ: イベント内の送信先ユーザ。

Trend Micro Deep Security On-Premise 12.0

- イベントホスト名: イベント発生元のホスト名。
- ID: イベントからIDとしてデコードされたID。
- ステータス: イベント内のデコードされたステータス。
- コマンド: イベント内で呼び出されるコマンド。
- URL: イベント内のURL。
- データ: イベントから抽出されたその他のデータ。
- システム名: イベント内のシステム名。
- 一致したルール: 一致したルールの数。
- イベント送信元: イベントの送信元であるDeep Securityコンポーネント。

セキュリティログ監視のセキュリティイベント一覧

注意: セキュリティログ監視に関連するシステムイベントについては、"[システムイベント](#)" on page 1271を参照してください。

ID	重要度	イベント
8100	エラー	セキュリティログ監視エンジンのエラー
8101	警告	セキュリティログ監視エンジンの警告
8102	情報	セキュリティログ監視エンジンの初期化

Webレピュテーションイベント

イベントに関する全般的なベストプラクティスについては、"[Deep Securityのイベント](#)" on page 1116を参照してください。

Deep SecurityでキャプチャされたWebレピュテーションイベントを確認するには、[イベントとレポート]→[イベント]→[Webレピュテーションイベント]に移動します。

Webレピュテーションイベントで表示される情報

[Webレピュテーションイベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ (コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- URL: このイベントをトリガしたURL。
- タグ: このイベントに関連付けられたイベントのタグ。
- リスク: このイベントをトリガしたURLのリスクレベル。「不審」、「非常に不審」、「危険」、「未評価」、「管理者によるブロック」などがあります。
- ランク: イベントの重要度を数値化する手段。コンピュータの資産評価にルール的重要度を乗算して計算されます("イベントのランク付けによる重要度の数値化" on page 1139を参照)。
- イベント送信元: イベントが発生したDeep Securityシステムのコンポーネントを示します。

許可するURLのリストにURLを追加する

イベントをトリガしたURLを許可するURLのリストに追加するには、イベントを右クリックして [許可リストに追加] を選択します (許可およびブロックのリストを表示または編集するには、メインの [Webレピュテーション] 画面の [除外] タブに進みます)。

共通イベント、アラート、およびエラーのトラブルシューティング

このセクションでは、共通イベント、アラート、およびエラーの一部についてトラブルシューティングのヒントを紹介します。

- "ファイアウォールモジュールが無効であるにも関わらず、ファイアウォールイベントが発生する理由" on page 1345
- "イベントID 771 「認識できないクライアントによる接続」のトラブルシューティング" on page 1345

- イベント: 設定パッケージが大きすぎる ("設定パッケージの最大サイズ" on page 834を参照)
- "「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1346
- "エラー: 有効化に失敗" on page 1347
- "エラー: サポートされていないAgentバージョン" on page 1351
- "エラー: 機能「dpi」のインストール失敗: 使用不可: フィルタ" on page 1355
- "エラー: インタフェースが非同期" on page 1356
- "エラー: 仮想マシンを有効化した後に「変更監視エンジンがオフライン」およびその他のエラーが発生する" on page 1356
- "エラー: モジュールのインストール失敗 (Linux)" on page 1365
- "エラー: このコンピュータに1つ以上のアプリケーションの種類の競合がある" on page 1366
- "エラー: クラウドアカウントに接続できない" on page 1368
- "エラー: インスタンスのホスト名を解決できない" on page 1370
- "エラー: 不正プログラム検索エンジンオフライン" on page 1351
- "エラー: ステータスの確認の失敗" on page 1354
- "エラー: セキュリティログ監視ルールに必要なログファイル" on page 1364
- "アラート: 変更監視情報の収集が遅延しています" on page 1370
- "アラート: Managerノードのメモリの警告しきい値を超過しました" on page 1371
- "アラート: Managerの時刻が非同期" on page 1370
- "警告: 攻撃の予兆の検出" on page 1374
- "警告: ディスク容量の不足" on page 1374

ファイアウォールモジュールが無効であるにも関わらず、ファイアウォールイベントが発生する理由

侵入防御またはWebレピュテーションを有効にしている場合、一部のファイアウォールイベントが表示されることがあります。これは、侵入防御モジュールおよびWebレピュテーションモジュールによる監視でファイアウォールのステートフル設定メカニズムが利用されるためです。

イベントID 771 「認識できないクライアントによる接続」のトラブルシューティング

Deep Security AgentまたはDeep Security Virtual ApplianceがManagerへの接続を試行したものの、[コンピュータ]画面の保護されているコンピュータのリストにコンピュータの名前が存在しない場合に、Deep Security ManagerにイベントID 771 「認識できないクライアントによる接続」が表示されます。

よくある原因は次のとおりです。

- クローン仮想マシンまたはクラウドインスタンス ([クローンAgentの再有効化] を有効にしていない)。
- Deep Security Agentを無効にする前に [コンピュータ]画面から削除したコンピュータ ([不明なAgentの再有効化] を有効にしていない)。AgentソフトウェアはManagerへの接続を定期的に試行し続けるため、ソフトウェアをアンインストールするか、コンピュータを無効にするまでこのイベントが毎回生成されます。
- vCenter、AWS、Azureなど、コネクタの同期の中断。たとえば、VMware ESXiホストが電源障害により正常にシャットダウンされなかった場合、仮想マシンの情報が正確に同期されない可能性があります。

解決策は原因ごとに異なります。

Deep Security Agentをアンインストールする

認識できないコンピュータを保護しない場合は、Deep Security Agentソフトウェアを無効にするか、アンインストールすることでこのイベントを発生しないようにできます。"[Deep Securityのアンインストール](#)" on page 1501を参照してください。

コンピュータまたはクローンを再有効化する

コンピュータを保護する場合は、Deep Security Managerでコンピュータを有効化します。再有効化により、Agentの証明書が再確立されるため、Managerが[コンピュータ]のリストで証明書を認証し、コンピュータを認識できるようになります。"[Agentからのリモート有効化](#)" on page 434を参照してください。

VMwareコネクタの同期の中断を修正する

1. Deep Security Managerで、[コンピュータ]に進みます。
2. vCenterコネクタを削除します。
3. VMware vSphereで、Deep Security Virtual Appliance (DSVA) をリセットします。

これにより、以下から情報が削除されます。

```
/var/opt/ds_agent/guests
```

4. Deep Security ManagerにvCenterを再度追加します。
5. 仮想マシンを再度有効化します。

「Smart Protection Serverへの接続不能」エラーのトラブルシューティング

不正プログラム対策またはWebレピュテーションのモジュールを使用していると、「スマートスキャン用のSmart Protection Serverへの接続不能」または「Webレピュテーション用のSmart Protection Serverへの接続不能」のエラーがDeep Security Managerコンソールに表示される場合があります。エラーを修正するには、次のトラブルシューティングのヒントを試してください。

エラーの詳細を確認する

エラーメッセージをダブルクリックして、サーバが接続するURLなどの詳細情報を表示します。次のようなエラーがあります。

Trend Micro Deep Security On-Premise 12.0

- タイムアウトになる。
- ホスト名を解決できない。

コマンドプロンプトでnslookupを使用して、DNS名がIPアドレスに解決されるかどうかを確認します。URLが解決されない場合は、ローカルサーバでDNSの問題が発生します。

telnetクライアントを使用して、ポート80と443でURLへの接続をテストします。接続できない場合は、すべてのファイアウォールやセキュリティグループなどが、それぞれのポートでURLへの送信トラフィックを許可していることを確認します。

Deep Security Virtual Applianceの問題

Deep Security Virtual Applianceでエラーが発生した場合:

1. Virtual Applianceのインターネット接続を確認します。
2. Virtual Applianceのポート80でインターネットと双方向接続できることを確認します。
3. Virtual Applianceにメモリが十分に割り当てられていることを確認します。メモリ要件の詳細については、"[Deep Security Virtual Applianceのサイジング](#)" on page 189を参照してください。

エラー: 有効化に失敗

「有効化に失敗」アラートをトリガするイベントがあります。

- "[プロトコルエラー](#)" on the next page
- "[ホスト名解決不能](#)" on the next page
- "[エージェント/アプライアンスがありません](#)" on page 1349
- "[ポートのブロック](#)" on page 1349
- "[重複するコンピュータ](#)" on page 1350
- "[プロキシ経由のエンドポイント](#)" on page 1351
- "[再インストールが必要です](#)" on page 1351

プロトコルエラー

通常、このエラーは、Deep Security Managerを使用してDeep Security Agentを有効にする際に、ManagerがAgentと通信できなかった場合に発生します。Agentが使用する通信方向により、このエラーのトラブルシューティングに使用する必要のある方法が決定されます ("[AgentとManagerの通信](#)" on page 400を参照)。

Agentから開始

AgentがAgentからの通信を使用するには、AgentコンピュータからAgentを有効にする必要があります ("[Agentを有効化する](#)" on page 461を参照)。

双方向の通信

エラーが発生して、Agentが双方向の通信を使用する場合は、次のトラブルシューティング手順を実行します。

1. Agentがコンピュータにインストール済みで稼働していることを確認します。
2. ManagerとAgent間のポートが空いていることを確認します ("[ポート番号、URL、およびIPアドレス](#)" on page 190と"[ファイアウォールルールの作成](#)" on page 850を参照)。

ホスト名解決不能

エラー「有効化に失敗 (ホスト名解決不能)」は、DNSのホスト名が解決不能な場合、またはAgentからのリモート有効化を使用せずに、Deep Security ManagerからAgentを有効化した場合に発生することがあります。

Agentが双方向またはManagerから開始の場合、DNSのホスト名は解決可能です。Deep Security ManagerのDNSがホストを解決できるかどうかを確認します。

お使いのコンピュータがクラウドアカウントを使用している場合は、常にエージェントが開始するアクティベーションを使用することをお勧めします。Agentからの通信用のポリシーールールの設定方法、およびインストールスクリプトを使用したAgentのインストール方法については、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on page 408を参照してください。

エージェント/アプライアンスがありません

このエラーメッセージは、保護対象のコンピュータにAgentソフトウェアがインストールされていないことを示しています。

"[Deep Security Agentソフトウェアの入手](#)" on page 372を参照してください。

ポートのブロック

ds_agent.logで「有効化に失敗」イベントが次のエラーメッセージとともに記録されている場合、

- 2018-06-25 17:52:14.000000: [Error/1] | CHTTPServer::AcceptSSL(<IP>:<PORT>) - BIO_do_handshake() failed - peer closed connection. | http\HTTPServer.cpp:246:DsaCore::CHTTPServer::AcceptSSL | 1E80:1FEC:ActivateThread
- 2018-06-25 17:52:14.143355: [dsa.Heartbeat/5] | Unable to reach a manager. | .\dsa\Heartbeat.lua:149:(null) | 1E80:1FEC:ActivateThread
- 2018-06-25 17:52:14.000000: [Info/5] | AgentEvent 4012 | common\DomainPrivate.cpp:493:DsaCore::DomPrivateData::AgentEventWriteHaveLock | 1E80:1FEC:ActivateThread
- 2018-06-25 17:52:14.143355: [Cmd/5] | Respond() - sending status line of 'HTTP/1.1 400 OK' | http\HTTPServer.cpp:369:DsaCore::CHTTPServer::Respond | 1E80:1D7C:ConnectionHandlerPool_0011

そして次のメッセージがパケットキャプチャソフトウェア (pcap) に表示される場合、

- [TCP Retransmission] <Ephemeral Port> -> 443 [SYN, ECN, CWR]
- [TCP Retransmission] <Ephemeral Port> -> 443 [SYN]

Deep Security AgentとManagerが通信を確立する際に使用されたポートがブロックされていた可能性があります。AgentとManagerの間で使用される通信ポートには、たとえば次のものがあります。

AgentとManagerの通信の種類	送信元 / ポート	送信先 / ポート
Agentからの通信	Deep Security Agent / エフェメラルポート	Deep Security Manager / 4119
Agentからの通信	Deep Security Agent / エフェメラルポート	Deep Security Manager / 443
Managerからの通信	Deep Security Manager / エフェメラルポート	Agent / 4118

上の表から分かるように、エフェメラルポートはAgentとManagerの間の送信トラフィックの送信元ポートとして使用されます。エフェメラルポートがブロックされている場合は、Agentを有効化できなくなり、ハートビートが機能しなくなります。送信先ポートのいずれかがブロックされている場合も、同様の問題が発生します。

この問題を解決するには、次の手順に従います。

- ネットワーク設定で、クライアントの送信ポート (エフェメラルポート) の制限を削除する。
- Deep Security Managerへのポート4119または443へのアクセスを許可します。
- Managerからの通信を使用している場合は、ポート4118でDeep Security Agentへの受信アクセスを許可する。

ポートの詳細については、"[ポート番号、URL、およびIPアドレス](#)" on page 190を参照してください。

重複するコンピュータ

このエラーは、通常、既存の名前を使用してコンピュータをアクティベートした場合、または別のコネクタですでにアクティブなコンピュータを使用している場合に発生します。

この問題を解決するには、次のいずれかの方法を使用できます。

- 重複しているコンピュータのいずれかを削除し、必要に応じて残りのコンピュータを再度有効にしてください。
- Deep Security Managerから、の[管理]→[システム設定]→[エージェント][]の順に選択し、エージェントが開始するアクティベーションの設定を選択します。同じ名前のコンピュータがすでに存在する場合は、既存のコンピュータを再度アク

ティベートするか、同じ名前の新しいコンピュータをアクティベートするか、またはアクティベーションを許可しないオプションがあります。詳細については、"[Agentからのリモート有効化](#)" on page 434を参照してください。

プロキシ経由のエンドポイント

プロキシを使用している場合は、Deep Security Managerで Support> Deployment Scripts に移動し、プロキシでフィールドをアップデートしてから、エージェントを再度有効にします。詳細については、"[インストールスクリプトを使用したコンピュータの追加と保護](#)" on page 498を参照してください。

再インストールが必要です

Deep Security Agentがアクティベートされていない場合は、"[Deep Security Agentをアンインストールする](#)" on page 1503をアンインストールしてから、[Deep Security Agent](#)を再インストールする必要があります。

エラー: サポートされていないAgentバージョン

「サポートされていないAgentバージョン」というエラーメッセージは、コンピュータに現在インストールされているAgentのバージョンがDeep Security Managerでサポートされていない場合に表示されます。

サポートされていないAgentでも、Deep Security Managerから最後に受け取ったポリシー設定に基づいてコンピュータは保護されますが、最新の脅威に迅速に対応できるように、Agentをアップグレードすることをお勧めします。詳細については、"[Deep Security Agentのアップグレード](#)" on page 998を参照してください。

エラー：不正プログラム検索エンジンオフライン

ヒント: 「不正プログラム対策エンジンがオフライン」エラーのよくある原因と確認方法については、次のWebサイトも参照してください。

Deep Security Agentの場合: <https://success.trendmicro.com/jp/solution/000286892>

Deep Security Virtual Applianceの場合: <https://success.trendmicro.com/jp/solution/000159761>

このエラーはさまざまな理由で発生します。この問題を解決するには、使用している保護のモードに対応した次の手順に従います。

- ["Agentベースの保護" below](#)
- ["Agentレスによる保護" on the next page](#)

不正プログラム対策モジュールの概要については、["不正プログラムの防止" on page 722](#)を参照してください。

Agentベースの保護

1. Deep Security Managerで、同じマシンのその他のエラーを確認します。エラーが存在する場合は、通信やDeep Security Agentのインストールに失敗したなど、不正プログラム対策エンジンがオフラインになっているその他の問題がある可能性があります。
2. エージェントからDeep Security Relayおよびマネージャへの通信を確認します。
3. Deep Security Managerで、問題が発生したAgentの詳細を表示します。不正プログラム対策のポリシーまたは設定が有効になっていること、および検索ごとの設定（リアルタイム検索、手動検索、予約検索）が有効でアクティブであることを確認します。（["不正プログラム対策の有効化と設定" on page 730](#)。）
4. Agentを再インストールして再有効化する前に、無効化してアンインストールします。詳細については、["Deep Securityのアンインストール" on page 1501](#)と["Agentの有効化" on page 430](#)を参照してください。
5. Deep Security Managerで、該当コンピュータの [アップデート] セクションに移動します。セキュリティアップデートが存在しており、最新であることを確認します。そうでない場合は、[セキュリティアップデートのダウンロード] をクリックして、アップデートを開始します。
6. 他のウイルス対策製品との競合があるかどうかを確認します。競合がある場合は、他の製品とDeep Security Agentをアンインストールし、Deep Security Agentを再起動してから再インストールしてください。

エージェントがWindowsの場合：

1. 次のサービスが実行されていることを確認します。
 - Trend Micro Deep Security Agent
 - Trend Micro Solution Platform

2. 次のコマンドを実行して、不正プログラム対策に関連するすべてのドライバが適切に実行されていることを確認します。

- # sc query AMSP
- # sc query tmcomm
- # sc query tmactmon
- # sc query tmevtmgr

ドライバが実行されていない場合は、トレンドマイクロのサービスを再起動します。再起動してもサービスが実行されない場合は、さらに次の手順を実行します。

3. インストール方法を確認します。zipファイルではなく、MSIのみをインストールします。
4. Agentの手動での削除と再インストールが必要になる場合があります。詳細については、[「エラー: モジュールのインストール失敗 \(Linux\)」](#)を参照してください。
5. インストールされたComodo証明書が問題の原因になる場合があります。この問題を解決するには、[「証明書の問題により、不正プログラム対策機能がオフラインになる」](#)を参照してください。

エージェントがLinuxにインストールされている場合：

1. Agentが実行されていることを確認するには、コマンドラインで次のコマンドを入力します。
 - service ds_agent status
2. Linuxサーバを使用している場合、カーネルがサポートされていない場合があります。詳細については、["エラー: モジュールのインストール失敗 \(Linux\)" on page 1365](#)を参照してください。

これらの手順に従っても問題が解決しない場合は、診断パッケージを作成して、サポートにお問い合わせください。詳細については、["診断パッケージとログの作成" on page 1573](#)を参照してください。

Agentレスによる保護

1. Deep Security Managerで、vcenterおよびnsxとの同期を確認します。[Computers]セクションで、Vcenterを右クリックして[Properties]に移動します。[接続テスト]をクリックします。[NSX] タブをクリックして、接続をテストします。証明書が変更されている場合は、[証明書の追加/アップデート]をクリックします。

2. NSXマネージャにログオンし、vCenterと適切に同期していることを確認します。
3. vSphere Clientにログインして、[Network & Security]→[Installation]→[Service Deployments] の順に選択します。
Trend Micro Deep SecurityおよびGuest Introspectionのエラーを確認して、検出されたエラーをすべて解決します。
4. vSphere Clientで、[Network & Security]→[Service Composer] の順に選択します。セキュリティポリシーが適切なセキュリティグループに割り当てられていることを確認します。
5. VMware ToolsがDeep Securityと互換性があることを確認します。詳細については、[「VMware ToolsとDeep Security Virtual Applianceの組み合わせにおけるトラブル事例」](#)を参照してください。
6. File Introspection Driver (vsepflt) がターゲット仮想マシンにインストールされ、実行されていることを確認します。コマンドプロンプトで管理者として「sc query vsepflt」を実行します。
7. vCloud DirectorのカatalogまたはvAppテンプレートから配信されたインスタンスおよび仮想マシンにはすべて同じBIOS UUIDが付与されます。Deep Securityでは、BIOS UUIDによって個々の仮想マシンを識別するため、vCenterに重複した値があると、「不正プログラム対策エンジンがオフライン」エラーが発生します。この問題を解決するには、[「VM BIOS UUIDs are not unique when virtual machines are deployed from vApp templates \(2002506\)」](#)を参照してください。
8. 問題が解決しない場合は、次の情報を含むサポートケースを開きます。
 - 各Deep Security Managerの診断パッケージ詳細については、「[診断パッケージとログの作成](#)」 on page 1573を参照してください。
 - Deep Security Virtual Applianceの診断パッケージ
 - 影響を受ける仮想マシンのvCenterサポートバンドル

エラー: ステータスの確認の失敗

Deep Security ManagerコンソールからコンピュータのAgent/Applianceのステータスを確認できます。[コンピュータ]画面でコンピュータを右クリックして、[処理]→[ステータスの確認] の順にクリックします。

「ステータスの確認の失敗」エラーが表示されたら、このエラーメッセージを開いて詳細な説明を確認します。

説明にプロトコルエラーが表示されている場合は、通常、通信問題が原因です。いくつかの原因が考えられます。

- コンピュータ (またはコンピュータに割り当てられたポリシー) がAgentからの通信または双方向の通信用に設定されているかを確認します。エージェントが開始した通信を使用している場合は、「ステータスの確認」操作は失敗します。
- Deep Security ManagerがAgentと通信できることを確認します。ManagerがAgentにアクセスできる必要があります。"[ポート番号、URL、およびIPアドレス](#)" on page 190を参照してください。
- Agentコンピュータのリソースを確認します。メモリ、CPU、またはディスク容量が不足すると、このエラーが発生します。

説明にSQLITE_IOERR_WRITE[778]と表示された場合: ディスクI/Oエラー、Agentコンピュータに問題がある可能性があります。ディスクがいっぱいか、書き込みが制限されていることが最も一般的な問題です。

エラー: 機能「dpi」のインストール失敗: 使用不可: フィルタ

「機能「dpi」のインストール失敗:使用不可:フィルタ」というエラーメッセージは、OSカーネルバージョンがネットワークドライバでサポートされていないことを示しています。このエラーは、通常、侵入防御、Webレピュテーション、またはファイアウォールをインストールする場合に、Deep Security Agentでトラフィックを調査できるようにネットワークドライバも一緒にインストールされるために発生します。同じ状況でエンジンオフラインアラートが生成されることもあります。

アップデートを随時提供できるように、トレンドマイクロでは、さまざまなOSベンダからの新しいカーネルのリリースを常にチェックし、品質保証テストが完了次第、それらのカーネルに対応したアップデートをリリースしています。

対応するOSカーネルバージョン用のアップデートが利用可能になると、必要なモジュールが自動的にインストールされます。

追加情報

これは、侵入防御、Webレピュテーション、およびファイアウォールにのみ影響します。それ以外の保護モジュール (不正プログラム対策、変更監視、およびセキュリティログ監視) はすべて正常に動作します。

サポートされているOSカーネルバージョンを確認するには、[「Deep Security 9.6 Supported Linux Kernels」](#)にアクセスし、該当するOSの配信情報を参照してください。

エラー:仮想マシンを有効化した後に「変更監視エンジンがオフライン」およびその他のエラーが発生する

Deep Security Virtual Applianceで保護される仮想マシンを有効化すると、Deep Security Managerには以下のエラーが表示されます。これらのエラーは、有効化が正常に実行された場合でも表示されます。

- 不正プログラム対策エンジンがオフライン
- ベースラインの再構築の失敗 (AgentまたはApplianceのエラー)
- 変更監視エンジンがオフライン

次のトラブルシューティングタスクを実行した場合でも、問題は未解決のままになります。

- vSphere Endpointがインストール済みであることを確認します。
- 最新のVMware Toolsがインストールされていることを確認します。
- VMCIドライバとVSEPFLTドライバが仮想マシンにインストールされていて稼働中であることを確認します。
- DSMコンソールでvCenterを同期します。
- Deep Security Virtual Applianceを無効化してから再度有効化します。
- 問題が発生している特定の仮想マシンを無効にしてから再度有効にします。
- VMware Toolsを再インストールします。

これらのエラーが表示されるのは、仮想マシンのハードウェアがバージョン7以上を実行していないためです。この問題を解決するには、[仮想マシンを最新のハードウェアバージョンにアップグレードする](#)必要があります。

エラー:インタフェースが非同期

このエラーは、Deep Security Managerのデータベースに格納されているゲスト仮想マシン (VM) のネットワークインタフェース情報が、Deep Security Virtual Applianceから報告されたインタフェース情報と異なる場合 (たとえば、MACアドレスが異なる場

合)に発生します。

この問題の根本原因を確認するには、どの段階で情報が同期されなくなったかを特定する必要があります。

最初に、Deep Security Managerで生成されたエラーメッセージを確認して、問題が発生している仮想マシンとインタフェースを特定します。

仮想マシンのインタフェースを確認する

1. 仮想マシンにログインします。
2. コマンドプロンプトを開きます。
3. コマンドを入力し、すべてのネットワークインタフェースの情報を表示します。たとえば、Windowsでは次のコマンドを入力します。 `ipconfig /all`
4. すべてのNICとMACアドレスを検証して、NICに正しいドライバが適用されていて、正常に動作していることを確認します。

vCenterで仮想マシンのインタフェース情報を確認する

vCenter ServerのManaged Object Reference (MoRef) から仮想マシンのインタフェース情報を確認します。

1. `https://<VC_SERVER>/mob/?moid=<OBJECT_ID>`にアクセスして、仮想マシンのMOBに移動します。
たとえば、次のようなURLになります。 `https://192.168.100.100/mob/?moid=vm-1136&doPath=config`
指定する項目は次のとおりです。

<VC_SERVER> は、vCenter ServerのFQDNまたはIPです。

=<OBJECT_ID>は、確認するオブジェクトのIDです。

VC MOBへのアクセスの詳細については、[「Looking up Managed Object Reference \(MoRef\) in vCenter Server」](#)を参照してください。

2. [Config]→[extraConfig["ethernet0.filter0……"]]→[hardware] に移動して、すべてのNICとMACアドレスを確認します。
3. MACアドレスを[仮想マシンのOSのMAC](#)と比較します。

Deep Security Managerでvmxファイルと仮想マシンのインタフェース情報を確認する

1. vCenter Serverデータストアのブラウザを使用して、仮想マシンのvmxファイルをダウンロードします。
2. メモ帳などのテキストエディタを使用して、vmxファイルを開きます。
3. IP、uuid.bios、およびMACアドレスを確認します。

次に例を示します。

```
Check virtual computer UUID
- uuid.bios = "42 23 d6 5d f2 d5 22 41-87 41 86 83 ea 2f 23 ac"
Check EPSec Settings
- VFILE.globaloptions = "svmip=169.254.50.39 svmport=8888"
- scsi0:0.filters = "VFILE"
Check DvFilter Settings
- ethernet0.filter0.name = "dvfilter-dsa"
- ethernet0.filter0.onFailure = "failOpen"
- ethernet0.filter0.param0 = "4223d65d-f2d5-2241-8741-8683ea2f23ac"
- ethernet0.filter0.param2 = "1"
- ethernet0.filter0.param1 = "00:50:56:A3:02:D8"
```

4. Deep Security Managerのダッシュボードに移動して、該当する仮想マシン→[インタフェース]の順にダブルクリックし、IPアドレスとMACアドレスを確認します。
5. IPアドレスとMACアドレスを前述の結果と比較します。

Deep Security Virtual Applianceの仮想マシンのインタフェース情報を確認する

1. vCenter Serverデータストアのブラウザを使用して、仮想マシンの該当するvmxファイルをダウンロードします。
2. メモ帳などのテキストエディタを使用して、vmxファイルを開きます。

3. uuid.biosの値を確認します。
4. Deep Security Virtual Applianceのコンソールにログオンし、<Alt>+<F2> キーを押してコマンドモードに切り替え、Deep Security Virtual Applianceのユーザ名とパスワードを入力します。
5. 次のコマンドを実行して、仮想マシンのネットワークインタフェースがDeep Security Virtual Applianceで認識されたかどうかを確認します (注意:\$suuidは実際のBIOS UUIDに置き換えます。)

```
cd /var/opt/ds_agent/guests/$suuid
```

```
>/opt/ds_guest_agent/ratt if
```

6. ifconfig -aコマンドを実行して、Deep Security Virtual ApplianceのNIC設定とIPが正しく設定されていることを確認します。
7. IPアドレスとMACアドレスを前述の結果と比較します。

回避策

前述のいずれかの項目が同期されていない場合は、その問題を修正する必要があります。

回避策1

有効化した仮想マシンのクローンを作成するときに、クローンコンピュータの電源をオンにして有効化すると、「インタフェースが非同期」アラートが表示されることがあります。回避策としては、クローンとして作成したコンピュータの電源をオンにする前にdvfilterの設定を消去します。

- ethernet0.filter0.name = "dvfilter-dsa"
- ethernet0.filter0.onFailure = "failOpen"
- ethernet0.filter0.param0 = "4223d65d-f2d5-2241-8741-8683ea2f23ac"
- ethernet0.filter0.param2 = "1"
- ethernet0.filter0.param1 = "00:50:56:A3:02:D8"

回避策2

1. 仮想マシンを一時停止してから、もう一度電源をオンにします。
2. Deep Security Virtual Applianceを再起動します。
3. 仮想マシンを無効化してから、もう一度有効化します。

回避策3

vMotionで仮想マシンを保護対象のESXiホストに移行して、警告メッセージを消去します。

注意: vCenterをDeep Security Managerに常に接続しておく必要があります。そうしないと、インタフェースの同期が失われる問題が繰り返し発生します。

詳細なトラブルシューティング手順

1. ["Deep Security Virtual Applianceの仮想マシンのインタフェース情報を確認する"](#) on page 1358で[IPアドレスとMACアドレスを確認した](#)前述の手順の結果を入力します。
2. [仮想マシンのインタフェースがDeep Security Virtual Applianceによって認識されたことを確認](#)した前述の手順から、rattif.txtファイルを取得します。
3. 次のコマンドからの出力を取得します。

```
$ ls -alR > /home/dsva/ls.txt
$ netstat -an > /home/dsva/netstat.txt
$ ps auxww > /home/dsva/ps.txt
$ lsof > /home/dsva/lsof.txt
$ ifconfig -a > /home/dsva/ifconfig.txt
$ cp /var/log/syslog /home/dsva/syslog.txt
```

4. [Deep Security Manager、Deep Security Agent、およびDeep Security Virtual Applianceの診断パッケージ](#)を取得します。
5. 次のファイルを収集して、[トレンドマイクロのテクニカルサポートに送信](#)します。

- rattif.txt
- ls.txt
- netstat.txt
- ps.txt
- lsof.txt
- ifconfig.txt
- syslog.txt

ratt ifコマンドの出力で仮想マシンのMACアドレスを確認できない場合は、次の回避策を実行してください。

1. vCenterでテンプレートから仮想マシンを配置します。
2. 既存のNICを削除します。
3. 仮想マシンの電源をオンにします (ログオンする必要はありません)。
4. 仮想マシンの電源をオフにします。
5. 新しいNICを追加します。
6. 仮想マシンの電源をオンにします。

エラー: 侵入防御ルールのコンパイルに失敗しました

このエラーはさまざまな理由で発生します。実際にエラーであるかどうかを確認するには、以下の手順に従います。

ポリシーを再送信する

1. Deep Security Managerで [コンピュータ] をクリックします。
2. エラーが発生したコンピュータを右クリックします。
3. [処理]→[ポリシーの送信] の順に選択します。

ステータスを再確認する

1. Deep Security Managerで [コンピュータ] をクリックします。
2. エラーが発生したコンピュータを右クリックします。
3. [処理]→[警告/エラーのクリア] の順に選択します。
4. 警告とエラーがクリアされたら、[処理]→[ステータスの確認] の順に選択します。

上記の手順を実行した後もエラーが発生する場合は、以下の方法で問題を解決します。

- ["侵入防御のベストプラクティスを適用する" below](#)
- ["ルールを管理する" below](#)
- ["個々のポートからアプリケーションの種類の割り当てを解除する" on the next page](#)

これらの方法でもエラーが解決しない場合は、テクニカルサポートにお問い合わせください。

侵入防御のベストプラクティスを適用する

「侵入防御ルールのコンパイルに失敗しました」エラーは、容量、メモリ、CPUなどのリソースがマシンに不足していることが原因で発生する可能性があります。この問題を解決するには、["侵入防御のパフォーマンスに関するヒント" on page 832](#)を参照し、設定を調整します。

ルールを管理する

「侵入防御ルールのコンパイルに失敗しました」エラーは、割り当てられている侵入防御ルールの数が推奨値を超えている場合に発生する可能性があります。エンドポイントに割り当てられている侵入防御ルールの数が400を超えないようにしてください。不要なルールを割り当てないようにするため、[推奨設定の検索](#)で推奨される侵入防御ルールのみを適用することをお勧めします。侵入防御ルールを手動で適用する場合は、単一のポートに追加されるアプリケーションの種類が多くなりすぎないように、ポリシーではなくコンピュータにルールを適用します。

この問題を解決するには、割り当てられているルールの数を減らします。

1. 割り当て方法に応じて、侵入防御ルールにアクセスします。以下のいずれかの方法を実行します。
 - コンピュータレベルでルールが割り当てられている場合は、[コンピュータ] タブに移動し、コンピュータを右クリックして [詳細] を選択します。
 - ポリシーレベルでルールが割り当てられている場合は、[ポリシー] タブに移動し、ポリシーを右クリックして [詳細] を選択します。
2. [侵入防御] に移動し、[推奨設定の検索] をクリックします。
3. 検索が完了したら、[割り当て/割り当て解除] をクリックします。ウィンドウの上部で、[割り当て解除を推奨] を使用してルールを絞り込みます。

IPS Rules

4. ルールの割り当てを解除するには、ルール名の横にあるチェックボックスをオンにします。複数のルールの割り当てをまとめて解除するには、ShiftキーまたはControlキーを使用して複数のルールを選択します。
5. 削除する1つまたは複数のルールを右クリックして、[ルールの割り当て解除]→[すべてのインタフェースから] の順に選択し、[OK] をクリックします。ウィンドウを閉じます。
6. [コンピュータ] タブでコンピュータを右クリックし、[処理]→[警告/エラーのクリア] の順に選択します。侵入防御エンジンによって、ルールのコンパイルが自動的に実行されます。このプロセスにかかる時間は、Deep Security ManagerとAgent間のハートビート間隔と通信設定によって異なります。

ヒント: ポリシーを通じて侵入防御ルールを適用していて、どのコンピュータにルールが適用されているのかが不明な場合は、**ポリシーエディタ**¹を開いて、[概要]→[このポリシーを使用しているコンピュータ] の順に選択します。

個々のポートからアプリケーションの種類を割り当てを解除する

「侵入防御ルールのコンパイルに失敗しました」エラーは、個々のポートに割り当てられているアプリケーションの種類が多すぎる場合に発生する可能性があります。現時点では、1つのポートに割り当てることができるアプリケーションの種類は8個までです。

¹ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

この問題を解決するには、次の手順に従い、ポートに割り当てられているアプリケーションの種類を削除します。

1. 問題が発生しているルールを確認するには、エラーをダブルクリックしてイベント表示ツールを開きます。
2. [コンピュータ] タブに進みます。
3. 侵入防御ルールの設定に問題があるコンピュータを右クリックし、[詳細] を選択します。
4. [侵入防御] に移動します。
5. [割り当て/割り当て解除] をクリックします。設定に問題があるルールの名前を検索バーに入力します。
6. ルールを右クリックし、[アプリケーションの種類プロパティ] を選択します。
7. [継承] チェックボックスをオフにします。
8. ポートを削除し、新しいポートを入力します。
9. [適用]→[OK] の順にクリックします。

エラー: セキュリティログ監視ルールで必要なログファイル

セキュリティログ監視ルールで監視対象のファイルの場所を追加する必要がある場合、または不要なセキュリティログ監視ルールを追加し、監視対象のファイルがマシンに存在しない場合は、**コンピュータエディタ**¹または**ポリシーエディタ**²で次のエラーが発生します。

このエラーを解決するには、次の操作を実行します。

1. [セキュリティログ監視ルールで必要なログファイル] エラーをクリックします。エラーの詳細が含まれるウィンドウが表示されます。[説明] の下に、エラーの原因となったルールの名前が一覧表示されます。
2. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[ルール]→[セキュリティログ監視ルール] に進み、エラーの原因のルールを見つけます。
3. ルールをダブルクリックします。ルールのプロパティウィンドウが表示されます。
4. [設定] タブに進みます。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

ファイルの場所が必要な場合:

1. [監視するログファイル]の下に場所を入力し、[追加]をクリックします。
2. [OK]をクリックします。Agentがポリシーを受け取ると、エラーがクリアされます。

リストされたファイルが保護対象マシンに存在しない場合:

1. **コンピュータエディタ**¹または**ポリシーエディタ**²の[セキュリティログ監視]に進みます。
2. [割り当て/割り当て解除]をクリックします。
3. 不要なルールを見つけて、チェックボックスをオフにします。
4. [OK]をクリックします。Agentがポリシーを受け取ると、エラーがクリアされます。

このエラーを回避するために、推奨ルールの推奨設定の検索を実行するには:

1. Deep Security Managerで、[コンピュータ]に進みます。
2. 検索するコンピュータを右クリックし、[処理]→[推奨設定の検索]の順にクリックします。
3. **コンピュータエディタ**³または**ポリシーエディタ**⁴の保護モジュールの[一般]タブで結果を確認します。

エラー: モジュールのインストール失敗 (Linux)

「モジュールのインストール失敗」というエラーメッセージは、OSのカーネルバージョンがDeep Securityネットワークドライバまたはファイルシステムフックでサポートされていないことを示しています。同じ状況でエンジンオフラインアラートが生成されることもあります。互換性のあるネットワークドライバがないことが、このエラーの主な原因です。

侵入防御、Webレピュテーション、またはファイアウォールを適用すると、Deep Security Agentでトラフィックを調査できるようにネットワークドライバがインストールされます。不正プログラム対策および変更監視は、ファイルシステムフックモ

¹コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して[詳細]をクリック) します。

²ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して[詳細]をクリック) します。

³コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して[詳細]をクリック) します。

⁴ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して[詳細]をクリック) します。

Trend Micro Deep Security On-Premise 12.0

ジュールをインストールします。このモジュールは、ファイルシステムの変更をリアルタイムで監視するために必要です (予約検索には同じファイルシステムフックは必要ありません)。

アップデートが開発中である可能性があります。トレンドマイクロは、多数のベンダの新しいカーネル リリースを常にチェックし、品質保証テストが完了次第、それらのカーネルに対応したアップデートをリリースしています。お使いのカーネルバージョンのサポート予定については、テクニカルサポートにお問い合わせください (ログインして右上の [サポート] をクリック)。

モジュールのサポートアップデートは、利用可能になると自動的にシステムにインストールされます。

サポートされているOSカーネルのバージョンについては、"[Deep Security AgentのLinuxカーネルサポート](#)" on page 183を参照してください。

エラー:このコンピュータに1つ以上のアプリケーションの種類の競合がある

このエラーメッセージは、Deep Security Agentをアップデートする際に、Deep Security Managerの [侵入防御イベント] タブに表示されます。

このコンピュータには1つ以上のアプリケーションの種類の競合があります。1つのアプリケーションの種類に関連付けられている1つ以上の侵入防御ルールは、他のアプリケーションの種類に関連付けられている1つ以上の侵入防御ルールに依存しています。2つのアプリケーションの種類が異なるポートを使用しているため、この競合が発生しています。

競合しているアプリケーションの種類を以下に示します。

```
[A] "Web Application Tomcat" Ports:[80,8080,4119]
```

```
[B] "Web Server Common" Ports:[80,631,8080,7001,7777,7778,7779,7200,7501,8007,8004,4000,32000,5357,5358,9000]
```

```
[A] "Web Server Miscellaneous" Ports:[80,4000,7100,7101,7510,8043,8080,8081,8088,8300,8500,8800,9000,9060,19300,32000,3612,10001,8093,8094]
```

```
[B] "Web Server Common" Ports:[80,631,8080,7001,7777,7778,7779,7200,7501,8007,8004,4000,32000,5357,5358,9000]"
```

解決方法

競合を解決するには、アプリケーションの種類Bで使用されているポート番号を編集し、アプリケーションの種類Aで使用されているポート番号を追加します。2つのアプリケーションの種類 (Web Application TomcatとWeb Server Miscellaneous) は両方とも、アプリケーションの種類Web Server Commonに依存しています。そのため、この2つのアプリケーションの種類に指定されているポートはWeb Server Commonのポートにも指定されている必要があります。

この3つのアプリケーションの種類のポート番号を統合すると、次のようになります。

80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200,7501,7510,7777,7778,7779,
8004,8007,8043,8080,8081,8088,8093,8094,8300,8500,8800,9000,9060,10001,19300,32000

これをWeb Server Commonのポートリストに追加すると、[イベント] タブに次のメッセージが表示されます。アプリケーションの種類のポートリストの誤った設定は解決されました。

ポートを統合する

1. Deep Security Managerにログオンし、[ポリシー]→[ルール]→[侵入防御ルール] に移動します。
2. 検索ボックスでWeb Server Commonを検索し、アプリケーションの種類Web Server Commonをダブルクリックします。
3. [一般]→[詳細]→[アプリケーションの種類]→[編集]→[Web Server Common] に移動します。
4. [一般]→[接続]→[ポート] に移動し、[編集] をクリックして、すべてのポートを次エントリで置き換えます。
80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200,
7501,7510,7777,7778,7779,8004,8007,8043,8080,8081,8088,8093,
8094,8300,8500,8800,9000,9060,10001,19300,32000
5. [OK] をクリックします。

継承オプションを無効にする

セキュリティプロファイルで侵入防御の継承オプションを無効にすることをお勧めします。無効にすることで、アプリケーションの種類に対する変更は、現在のセキュリティプロファイルにのみ反映されます。

Trend Micro Deep Security On-Premise 12.0

1. Deep Security Managerにログオンし、[セキュリティプロファイル] に移動します。
2. 右側の画面で、セキュリティプロファイルをダブルクリックします。
3. [DPI] セクションに移動し、[継承] をクリックして選択解除します。
4. [OK] をクリックします。

IPSルール1000128を確認します。

1. [アプリケーションの種類プロパティ] を右クリックします。
2. [継承] をクリックして選択解除します。
3. 現在継承されているポートリストに、[Deep Security Manager GUIの待機ポート番号](#)が含まれていることを確認します。含まれていない場合は、Web Server Commonのポートグループにこのポートを追加します。
4. [継承] をクリックします。

エラー: クラウドアカウントに接続できない

Amazonクラウドアカウントを追加するときに、「クラウドアカウントに接続できない」というエラーが発生することがあります。これには以下の原因が考えられます。

- キーIDまたはシークレットが無効である
- 権限が正しくない
- ネットワーク接続で障害が発生した

AWSアカウントのアクセスキーIDまたは秘密アクセスキーが無効である

解決方法

入力したセキュリティ資格情報が正しいことを確認します。

Deep Securityで使用するアカウントに間違ったAWS IAMポリシーが適用されている

解決方法

AWSアカウントにアクセスし、そのアカウントのIAMポリシーを確認します。

AWS IAMポリシーで次の権限が割り当てられている必要があります。

- Effect:許可
- AWS Service:Amazon EC2
- [Actions] として次を選択します。
 - DescribeImages
 - DescribeInstances
 - DescribeTags
- Amazon Resource Name (ARN): *

NAT、プロキシ、またはファイアウォールのポートが開いていないか、設定が正しくない

このエラーは、AWS MarketplaceのAMIを使用して新しいDeep Security Managerを導入する場合など、いくつかのケースで発生します。

Deep Security Managerは、[必要なポート番号](#)でインターネット (特にAmazonクラウド) に接続する必要があります。

解決方法

次の作業が必要となる場合があります。

- AMIとインターネットの間のファイアウォール/ルータでNATまたはポート転送を設定する
- AMIの外部IPアドレスを取得する

安定したネットワーク接続も必要です。ネットワーク接続が断続的に途切れる場合も、このエラーメッセージが表示されることがあります。

エラー: インスタンスのホスト名を解決できない

「インスタンスのホスト名を解決できない」というエラーメッセージは、Agentからのリモート有効化を使用せずに、Deep Security ManagerからAgentを有効化した場合に発生することがあります。

常に [Agentからのリモート有効化] を使用することを推奨します。Agentからの通信用のポリシーールールの設定方法、およびインストールスクリプトを使用したAgentのインストール方法については、"[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" on page 408を参照してください。

アラート:変更監視情報の収集が遅延しています

このアラートは、変更監視情報の収集速度が一時的に遅延していることを示します。この遅延は、AgentからDeep Security Managerに送信される変更監視データ量の増加によるものです。この間、一部のコンピュータでベースラインと変更監視イベントの表示が最新ではなくなる可能性があります。

このアラートは、変更監視データの収集が遅延しなくなったときに自動的に消去されます。

変更監視の詳細については、"[変更監視の設定](#)" on page 887を参照してください。

アラート: Managerの時刻が非同期

Deep Security Managerオペレーティングシステムのシステム時刻は、データベースコンピュータの時刻と同期する必要があります。このアラートは、コンピュータの時刻が30秒以上同期していないときに、Managerコンソールの [アラートステータス] ウィジェットに表示されます。

時刻を同期するには、次の設定を適用します。

Trend Micro Deep Security On-Premise 12.0

- データベースとすべてのManagerノードが同じタイムゾーンを使用するように設定します。
- データベースとすべてのManagerノードの時刻が同じタイムソースで同期していることを確認します。
- ManagerがLinuxオペレーティングシステムで稼働している場合は、ntpdデーモンが実行されていることを確認します。

アラート: Managerノードのメモリの警告しきい値を超過しました

メモリの警告しきい値の超過 または メモリの重大しきい値の超過 alertsが Deep Security に表示され、ホストのメモリ使用量が一定量を超えたことが通知されます。警告アラートは、ホストのメモリの70%が使用されていることを示し、重大なアラートは使用率が85%を超えていることを示します。

この問題を解決するには、予期せず大量のメモリを消費するプロセスがあるかどうかを判断します。

- 検出されたプロセスがDeep Security Managerでない場合は、プロセスをホストから削除するか、または削除します。Deep Security Managerは専用のホストコンピュータで実行する必要があります。
- プロセスがDeep Security Managerの場合は、ホストメモリの量を増やしてください。ガイドラインについては、"[サイジング](#)" on page 184 を参照してください。

注意: 初期設定では、Deep Security Managerの最大ヒープサイズは4GBです。つまり、Deep Security Managerは最大4 GBのヒープを割り当てます。ただし、JVMはヒープだけでなく非ヒープも割り当てます。その結果、Deep Security Managerプロセスの最大合計メモリサイズは4GBより大きくなります。

注意: ホストがVMの場合は、そのVMのすべてのゲストメモリを予約することを強くお勧めします。

イベント: 最大TCP接続数

Deep Securityは保護対象コンピュータへの最大TCP接続数を許可するように設定されています。接続数が最大数を超えた場合は、ネットワークトラフィックが中断し、最大TCP接続数ファイアウォールイベントが発生します。接続が中断しないようにするには、最大TCP接続イベントが発生したコンピュータの最大許容TCP接続数を増やします。

注意: 侵入防御モジュールにより、TCP接続の許容数を適用するネットワークエンジンが有効になります。

1. Deep Security Managerで、[ポリシー] をクリックします。
2. 対象のコンピュータに影響するように設定するポリシーを決定します。"[ポリシー、継承、およびオーバーライド](#)" on [page 587](#)を参照してください。
3. 設定するポリシーを開くには、ポリシーをダブルクリックします。
4. 左側画面で、[設定] をクリックして、[詳細] タブをクリックします。
5. [ネットワークエンジンの詳細設定] エリアで、[継承] が選択されている場合、チェックボックスをクリアして変更を有効にします。
6. ニーズに応じて、[最大TCP接続数] プロパティの値を10000以上に増やします。
7. [保存] をクリックします。

警告: Census、Good File Reputation、機械学習型検索サービスへの接続解除

Census、Good File Reputationサービス、機械学習型検索は、Trend Micro Smart Protection Networkによってホストされるセキュリティサービスです。これらのサービスは、Deep Securityの挙動監視、機械学習型検索、プロセスメモリ検索の機能の正常な運用に必要です。

サービスと機能が対応する表を次に示します。

サービス名	対象機能
Global Censusサービス	挙動監視 、 機械学習型検索
Good File Reputationサービス	挙動監視 、 機械学習型検索 、 プロセスメモリ検索
機械学習型検索サービス	機械学習型検索

アラートが表示された場合、

Census、Good File Reputation、機械学習型検索サービスへの接続解除

いくつかの原因が考えられます。

- ["原因1: AgentまたはRelay有効化済みAgentがインターネットにアクセスできない" below](#)
- ["原因2: プロキシは有効化されているが、適切に設定されていない" below](#)

原因1: AgentまたはRelay有効化済みAgentがインターネットにアクセスできない

AgentまたはRelay有効化済みAgentがインターネットにアクセスできない場合は、上記のサービスにアクセスできません。

解決策:

- ファイアウォールポリシーをチェックして、送信HTTPおよびHTTPSポート (初期設定は80または443) が開いていることを確認します。
- このポートを開くことができない場合、他の解決策については、["インターネットにアクセスできない エージェントを設定する" on page 413](#)を参照してください。

原因2: プロキシは有効化されているが、適切に設定されていない

Census、Good File Reputationサービス、機械学習型検索には、プロキシを使用するとアクセスできます。

プロキシが有効化されているかどうかをチェックして、適切に設定されていることを確認するには、次の手順を実行します。

1. **コンピュータまたはポリシーエディタ¹**を開きます。
2. 左側で [設定] をクリックします。
3. メイン画面で [一般] タブをクリックします。
4. Census、Good File Reputationサービスおよび機械学習型検索向けのネットワーク設定というタイトルの見出しを探します。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

5. プロキシが指定されている場合、[編集] をクリックして、[プロキシプロトコル]、[アドレス]、[ポート]、およびオプションの [ユーザ名] と [パスワード] が正しいことを確認します。

警告: ディスク容量の不足

「ディスク容量の不足」警告は、Deep Security AgentまたはApplianceが稼働するコンピュータのディスク容量が少なくなり、イベントをこれ以上保存できない可能性があることを示します。警告を開いてその詳細を表示すると、AgentまたはApplianceの場所、残りの空き容量、AgentまたはApplianceに必要な容量が表示されます。

この問題を修正するには、影響を受けるドライブまたはシステムを確認し、不要なデータを消去します。

注意: AgentまたはApplianceは、ドライブの容量がなくなっても、インスタンスを保護し続けますが、イベントの記録は停止されます。

ヒント

- Deep Security AgentまたはApplianceが原因で警告が発生した場合、同一ファイルシステムを共有する別のプログラムにも容量の問題が発生します。
- Deep Security Agentはログファイルを自動的に切り捨て、ローテーションします。
- Deep Security Agentは自身のログファイルをクリーンアップしますが、他のアプリケーションのログファイルはクリーンアップしません。
- Deep Security Managerは「ディスク容量の不足」警告を自動的に消去しませんが、Deep Security Managerから手動で消去できます。

警告: 攻撃の予兆の検出

攻撃の予兆の検出機能は、潜在的な攻撃またはネットワークの機密情報収集活動の早期警告として機能します。

攻撃の予兆の検出の種類

Deep Securityはいくつかの種類 of 攻撃の予兆を検出できます。

- OSのフィンガープリント調査:AgentまたはApplianceはコンピュータのOSを見つけようとする動作を検出します。
- ネットワークまたはポートの検索:AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしていることを検出した場合、ネットワークまたはポート検索をレポートします。通常、AgentまたはApplianceのコンピュータは、コンピュータ自身宛てのトラフィックのみを監視するため、ポート検索が最も一般的に検出されます。コンピュータまたはポート検索の検出で使用される統計的な分析方法は「TAPS」アルゴリズムから導出されたもので、2006年にIPCCCで発表された「Connectionless Port Scan Detection on the Backbone」で提案されました。
- TCP Null検索:AgentまたはApplianceはフラグが付いていないパッケージを検出します。
- TCP SYNFIN検索:AgentまたはApplianceはSYNフラグおよびFINフラグの付いたパケットのみを検出します。
- TCP Xmas検索:AgentまたはApplianceは、FINフラグ、URGフラグ、およびPSHフラグの付いたパケット、または値0xFF (想定されるすべてのフラグ) を含むパケットを検出します。

推奨処理

攻撃の予兆の検出アラートを受信したら、このアラートをダブルクリックして、検出を実行しているIP アドレスなどの詳細を表示します。次に、上記の推奨処理のいずれかを実行できます。

- アラートは不正ではない検索によって発生する場合があります。アラートに記載されているIPアドレスがわかっており、トラフィックに問題がない場合は、IPアドレスを偵察許可リストに追加できます。

- a. **コンピュータまたはポリシーエディタ**¹で、[ファイアウォール]→[攻撃の予兆]の順に選択します。
 - b. [検出を実行しないIPリスト]にリスト名を追加する必要があります。リスト名がまだ指定されていない場合は、リスト名を選択します。
 - c. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト]を選択すると、リストを編集できます。IPアドレスを編集および追加するリストをダブルクリックします。
- 特定の期間、ソースIPからのトラフィックをブロックするようにAgentおよびApplianceに指示できます。分数を設定するには、**コンピュータまたはポリシーエディタ**²で、[ファイアウォール]→[攻撃の予兆]の順に選択し、[トラフィックのブロック]の値を適切な検索の種類に変更します。
 - ファイアウォールまたはセキュリティグループを使用すると、受信IPアドレスをブロックできます。

注意: Deep Security Managerは「攻撃の予兆の検出」アラートを自動的に消去しませんが、Deep Security Managerから手動で消去できます。

攻撃の予兆の検索に関する詳細については、"[ファイアウォールの設定](#)" on page 866を参照してください。

ユーザの作成と管理

Deep Securityにはユーザ、役割、および連絡先があり、[管理]→[ユーザ管理]で作成および管理できます。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

²これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- ユーザは、一意のユーザ名とパスワードを使用してDeep Security Managerにログオンできる、Deep Securityのアカウント所有者です。"[Active Directoryと同期する](#)" [below](#)ことや、"[ユーザを個別に追加または編集する](#)" [on the next page](#)ことができます。
- 役割は、Deep Security Manager内でデータを表示したり、処理を実行したりするための権限の集まりです。各ユーザには役割が割り当てられます。"[ユーザロールの定義](#)" [on page 1382](#)を参照してください。
- 連絡先にはユーザアカウントが割り当てられていないため、Deep Security Managerにログオンすることはできませんが、連絡先をメール通知や予約レポートの受信者として指定することはできます。"[レポートのみを受信できるユーザの追加](#)" [on page 1406](#)を参照してください。

Active Directoryと同期する

Active Directoryを使用してユーザを管理する場合は、Deep SecurityとActive Directoryを同期してユーザリストを統合できます。そうすると、ユーザはディレクトリに保存されたパスワードを使用してDeep Security Managerにログオンできます。

注意: Active DirectoryのユーザアカウントをDeep Securityのユーザまたは連絡先としてDeep Securityにインポートするには、Active Directoryのユーザアカウントに属性値userPrincipalNameが設定されている必要があります。userPrincipalName属性は、Active Directoryのアカウント所有者の「ユーザログオン名」に相当します。

注意: FIPSモードでDeep Securityを使用している場合は、Active Directoryと同期する前にActive DirectoryのSSL証明書をインポートする必要があります。"[信頼された証明書の管理](#)" [on page 424](#)を参照してください。

1. Deep Security Managerで、[管理]→[ユーザ管理]→[ユーザ] の順にクリックします。
2. [ディレクトリとの同期] をクリックしてディレクトリとの同期ウィザードを表示します。
3. ディレクトリサーバのアドレスとアクセス資格情報を入力して [次へ] をクリックします。Active Directoryへの接続が試行されます。

注意: FIPSモードでDeep Securityを使用している場合は、[信頼された証明書] セクションの [接続テスト] をクリックして、Active DirectoryのSSL証明書がDeep Security Managerに正常にインポートされたかどうかを確認します。

[Active Directoryグループの選択]画面が表示されます。

4. Active Directoryグループ名またはグループ名の一部を検索フィールドに入力し、<Enter>キーを押します。[>>]ボタンを使用してグループを[Groups to]グループに移動します。マネージャは、これらのActive Directoryグループ内のユーザをマネージャの ユーザリストにインポートします。ユーザのインポートが完了すると、定期的にディレクトリとの同期を行ってリストを最新の状態にするための予約タスクの作成オプションが表示されます。

初期設定では、インポートされたユーザはDeep Security Managerにログオンできません。ユーザがDeep Security Managerにログオンできるようにするには、ユーザのプロパティを変更する必要があります。

注意: Active Directoryとの同期によって追加されたユーザをDeep SecurityManagerから削除し、その後Active Directoryと再同期した場合、そのユーザがActive Directoryに残っていると、再びそのユーザがユーザリストに表示されます。

ユーザを個別に追加または編集する

1. Deep Security Managerで、[管理]→[ユーザ管理]→[ユーザ] の順にクリックします。
2. [新規] をクリックして新しいユーザを追加するか、既存のユーザアカウントをダブルクリックして設定を編集します。
3. 次を含む、ユーザの一般的なプロパティを指定します。
 - ユーザ名: ユーザがDeep Security Managerのログイン画面に入力するユーザ名。
 - パスワードとパスワードの確認入力: ダイアログボックスに表示されるパスワード要件に注意してください。パスワード要件はユーザのセキュリティ設定で設定できます ("[ユーザパスワードルールの適用](#)" on page 1081を参照してください)。
 - 名前: (オプション) アカウント所有者の名前。
 - 説明: (オプション) アカウントの説明。

- 役割: リストを使用して、定義済みの役割をこのユーザに割り当てます。また、ユーザを右クリックして [役割の割り当て] をクリックすると、ユーザリストから役割をユーザに割り当てることもできます。

注意: Deep Security Managerには、Full AccessとAuditorという定義済みの2つの役割が用意されています。Full Accessの役割では、コンピュータ、コンピュータグループ、ポリシー、ルールなどの作成、編集、削除をはじめとする、Deep Securityシステムの管理に関するすべての特権がユーザに付与されます。Auditorの役割では、Deep Securityシステムのすべての情報を表示する権限がユーザに付与されます。ただし、パスワード、連絡先情報、表示設定などの個人情報設定以外は変更できません。[役割] リストから [新規] を選択して、さまざまなレベルのシステムアクセス権を持つ役割を作成または変更できます。

- 言語: ユーザのログイン時にインターフェースに使用される言語。
 - タイムゾーン: ユーザのタイムゾーン。Deep Security Managerで日時を表示する際に使用されるタイムゾーンです。
 - 時刻の形式: Deep Security Managerでの時刻の表示形式。12時間形式または24時間形式を使用できます。
 - パスワードの有効期限なし: このオプションを選択すると、ユーザのパスワードが無期限になります。それ以外の場合は、ユーザのセキュリティ設定で指定したとおりに期限が切れます ("[ユーザパスワードルールの適用](#)" on page 1081 を参照してください)。
4. 多要素認証 (MFA) を有効にするには、[多要素認証の有効化] をクリックします。ユーザに対してMFAがすでに有効になっている場合は、[多要素認証の無効化] をクリックすると無効にできます。詳細については、"[多要素認証の設定](#)" on page 1083を参照してください。
 5. [連絡先情報] タブをクリックし、ユーザの連絡先情報を入力し、そのユーザが主担当者であるかどうかを指定できます。[アラートメールを受信] チェックボックスをオンにして、アラートがトリガされたときにメール通知を受信するユーザのリストにこのユーザを追加することもできます。
 6. また、[設定] タブで設定を編集することもできます。ただし、この値を大きくすると、Deep Security Managerのパフォーマンスに影響します。変更を加えて、その結果に満足できない場合は、[初期設定に戻す] (タブの下部) をクリックして、この画面のすべての設定を初期設定値に戻すことができます。

モジュール

- ライセンス許可されていないモジュールを非表示: この設定では、このユーザに対してライセンス許可されていないモジュールをグレー表示ではなく非表示にするかどうかを決定します。このオプションは、[管理]→[システム設定]→[詳細] タブでグローバルに設定できます。

更新頻度

- ステータスバー: この設定では、コンピュータの検出や検索などのさまざまな操作中にDeep Security Managerのステータスバーを更新する頻度を決定します。
- アラートリスト/概要: リストビューまたは概要ビューの [アラート] 画面のデータを更新する頻度。
- コンピュータのリスト: [コンピュータ] 画面のデータを更新する頻度。

注意: [前回成功したアップデート] 列の値は、画面が手動でリロードされるまで再計算されません。

- コンピュータの詳細: 必要に応じて、個々のコンピュータのプロパティページを最新の情報で更新する頻度。

リストビュー

- 各ページの最後のタグフィルタを保存: [イベント] 画面では、表示されたイベントをタグごとにフィルタできます。このリストビューの設定では、[イベント] 画面から移動して戻ったときに [タグ] のフィルタ設定を保持するかどうかを決定します。
- 各ページの最後の期間フィルタを保存: [イベント] 画面では、表示されたイベントを期間またはコンピュータごとにフィルタできます。これらのリストビューの設定では、[イベント] 画面から移動して戻ったときに [期間] および [コンピュータ] のフィルタ設定を保持するかどうかを決定します。
- 各ページの最後のコンピュータフィルタを保存: [イベント] 画面では、表示されたイベントを期間またはコンピュータごとにフィルタできます。これらのリストビューの設定では、[イベント] 画面から移動して戻ったときに [期間] および [コンピュータ] のフィルタ設定を保持するかどうかを決定します。
- 各ページの最後の詳細検索を保存: この設定では、[イベント] 画面で「詳細検索」を実行した場合、この画面から移動して戻ったときに検索結果を保持するかどうかを決定します。

- 1ページに表示するアイテム数: アイテムのリストを表示する画面の各ページに、一定数のアイテムが表示されます。次のページを表示するには、レイアウトコントロールを使用する必要があります。各ページに表示されるリストアイテムの数を変更する場合は、この設定を使用します。
- データベースから取得する最大アイテム数: この設定では、データベースから取得して表示できるアイテムの数を制限します。これにより、データベースクエリから返された大量の結果を表示しようとしてDeep SecurityManagerが停止する状況を回避できます。この制限を超える結果がクエリで生成される場合は、一部の結果のみ表示されることを示すメッセージが画面の一番上に表示されます。

注意: この値を大きくすると、Deep Security Managerのパフォーマンスに影響します。

レポート

- PDF暗号化の有効化: このオプションを選択すると、PDF形式でエクスポートされたレポートが [レポートのパスワード] でパスワードで保護されます。

ユーザのパスワードを変更する

ユーザのパスワードを変更するには、[管理]→[ユーザ管理]→[ユーザ] の順に選択してユーザを右クリックし、[パスワード設定] をクリックします。現在のパスワードと新しいパスワードを入力するように求められます。

ユーザをロックアウトする/ロックアウトをリセットする

ログオン時にユーザが間違ったパスワードを何回も入力すると、自動的にロックされます。この状況を解決して、ユーザがログインできるようにするには、"[ロックアウトされたユーザ名のロック解除](#)" on page 1408を参照してください。

ユーザに関連付けられたシステムイベントを表示する

ユーザに関連付けられたシステムイベントを表示するには、[管理]→[ユーザ管理]→[ユーザ]の順に選択してユーザを右クリックし、[システムイベントの表示]をクリックします。

ユーザを削除する

Deep Security Managerからユーザアカウントを削除するには、[管理]→[ユーザ管理]→[ユーザ]の順に選択してユーザをクリックし、[削除]をクリックします。

注意: Active Directoryとの同期によって追加されたユーザをDeep Security Managerから削除し、その後Active Directoryと再同期した場合、そのユーザがActive Directoryに残っていると、再びそのユーザがユーザリストに表示されます。

ユーザロールの定義

Deep Securityでは、役割に基づいたアクセス制御 (RBAC) を使用して、Deep Securityのさまざまな部分に対するユーザ権限を制限します。アクセス権限と編集権限は、ユーザにではなく、役割に関連付けられます。Deep Security Managerのインストールが完了したら、ユーザごとに個別のアカウントを作成して役割を割り当てます。役割は、各ユーザのアクティビティを業務に必要な範囲に制限します。個々のユーザのアクセス権限と編集権限を変更するには、ユーザに別の役割を割り当てるか、役割自体を編集する必要があります。

役割がコンピュータとポリシーに対して持つアクセス権限は、コンピュータとポリシーのサブセットに限定することもできます。たとえば、ユーザに対して、既存のすべてのコンピュータの表示は許可するが、特定のグループ内のコンピュータ以外の編集を許可しないようにできます。

Deep Securityには、次の2つの役割が事前に設定されています。



- Full Access: Full Accessの役割では、コンピュータ、コンピュータグループ、ポリシー、ルール、不正プログラム検索設定などの作成、編集、削除を含むDeep Securityシステムの管理に関するすべての権限がユーザに付与されます。
- Auditor: Auditorの役割では、Deep Securityシステムのすべての情報を表示する権限がユーザに付与されます。ただし、パスワード、連絡先情報、ダッシュボードレイアウト設定などの個人情報設定以外は変更できません。

注意: Deep Security Managerのオプションは、付与されたアクセスレベルに応じて、表示および編集可能、表示可能ですが無効、非表示のいずれかになります。事前に定義された役割で付与されている権限のリスト、および新しい役割を作成する際の権限の初期設定については、"[Full Access、Auditor、および新規の各役割の初期設定](#)" on page 1395を参照してください。

新しい役割を作成して、Deep Securityのオブジェクト (特定のコンピュータ、セキュリティルールのプロパティ、システム設定など) をユーザが編集または表示できないように制限することができます。

ユーザアカウントを作成する前に、ユーザの役割、およびそれらの役割がアクセスする必要があるDeep Securityのオブジェクトとアクセスの種類 (表示、編集、作成など) を確認します。役割を作成したら、ユーザアカウントを作成して特定の役割を割り当てることができます。

注意: Full Accessの役割を複製して変更する方法で新しい役割を作成しないでください。新しい役割に目的とする権限のみを確実に付与するには、ツールバーの [新規] をクリックして新しい役割を作成します。新しい役割の権限は、初期設定では最も制限された状態で設定されます。後に必要な権限のみを付与できます。Full Accessの役割を複製してから制限を適用すると、不要な権限を与える危険があります。

[新規] () または [プロパティ] () をクリックして、6つのタブ ([一般]、[コンピュータの権限]、[ポリシーの権限]、[ユーザ権限]、[その他の権限]、および [割り当て対象]) がある [役割のプロパティ] 画面を表示します。

役割を追加または編集する

1. Deep Security Managerで、[管理]→[ユーザ管理]→[役割] の順に選択します。
2. 新しい役割を追加する場合は [新規] をクリックし、設定を編集する場合は既存の役割をダブルクリックします。

3. 次を含む、役割の一般的なプロパティを指定します。
 - 名前: [役割] 画面と、ユーザ追加時に使用できる役割のリストに表示される役割の名前
 - 説明: (オプション) 役割の説明。
 - アクセスの種類: この役割のユーザに、Deep Security Manager、Deep Security ManagerのWebサービスAPI (従来のSOAP APIとREST APIに適用)、あるいはその両方へのアクセス権を付与するかどうかを選択します。
 - **注意:** 従来のSOAPおよびREST WebサービスAPIを有効にするには、[管理]→[システム設定]→[詳細]→[SOAP WebサービスAPI] の順に選択します。
4. 表示、編集、削除、アラート消去、イベントのタグ付けなどの権限をある役割のユーザに付与するには、[コンピュータの権限] 画面を使用します。これらの権限は、すべてのコンピュータおよびコンピュータグループに適用できます。また、権限の付与を特定のコンピュータに制限することもできます。アクセス権を制限する場合は、[選択したコンピュータ] オプションを選択し、この役割のユーザにアクセス権を付与するコンピュータグループとコンピュータの横にあるチェックボックスをオンにします。
5. **注意:** こうした権限の制限は、Deep Security Managerのコンピュータに対するユーザのアクセス権だけでなく、イベントやアラートなどの情報の表示にも影響します。メール通知も同様に、ユーザがアクセス権を持つデータに関連する場合のみ送信されます。

一般	コンピュータの権限	ポリシーの権限	ユーザ権限	その他の権限	割り当て対象
コンピュータとグループの権限					
ユーザに許可される処理:					
	<input checked="" type="checkbox"/> 表示	}	<input checked="" type="radio"/> すべてのコンピュータ		
	<input type="checkbox"/> 編集		<input type="radio"/> 選択したコンピュータ		
	<input type="checkbox"/> 削除				
	<input type="checkbox"/> アラートの消去				
	<input type="checkbox"/> アイテムのタグ付け				
<div style="border: 1px solid gray; padding: 5px;"> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> コンピュータ <input checked="" type="checkbox"/> vCenter - 172.16.122.85 <ul style="list-style-type: none"> <input checked="" type="checkbox"/> ホストおよびクラスタ <ul style="list-style-type: none"> <input checked="" type="checkbox"/> New Datacenter <input checked="" type="checkbox"/> 仮想マシン <ul style="list-style-type: none"> <input checked="" type="checkbox"/> New Datacenter <ul style="list-style-type: none"> <input checked="" type="checkbox"/> 検出された仮想マシン <ul style="list-style-type: none"> <input checked="" type="checkbox"/> (JP_WS2012_x64_DSM) </div>					
<input checked="" type="checkbox"/> 選択されていないコンピュータおよびデータ (イベントやレポートなど) を表示 <input checked="" type="checkbox"/> コンピュータに関連していないイベントおよびアラートを表示 <input type="checkbox"/> 選択したグループ内に新しいコンピュータを作成 <input type="checkbox"/> 選択したグループ内にサブグループを追加または削除					
詳細な権限					
<input type="checkbox"/> コンピュータファイルをインポート					
<input type="checkbox"/> ディレクトリを追加、削除、および同期					
<input type="checkbox"/> VMware vCenterを追加、削除、および同期					
<input type="checkbox"/> クラウドアカウントの追加、削除、および同期を許可					
<input type="button" value="OK"/> <input type="button" value="キャンセル"/> <input type="button" value="適用"/>					

次に示す4つの基本オプションを使用できます。

- 選択されていないコンピュータおよびデータ (イベントやレポートなど) を表示: この役割のユーザの編集、削除、またはアラート消去の権限が制限されている場合でも、このチェックボックスをオンにすることで他のコンピュータに関する情報の表示 (変更は不可) を許可できます。
- コンピュータに関連していないイベントおよびアラートを表示: システムイベント (ユーザがロックされた、新しいファイアウォールルールが作成された、IPリストが削除されたなど) のような、コンピュータ関連以外の情報をこの役割のユーザが表示できるようにするには、このオプションを設定します。

注意: 前述の2つの設定は、ユーザがアクセスできるデータに影響します。この2つの設定は、ユーザがコンピュータに変更を加える機能は制限したまま、アクセス権を持たないコンピュータに関連する情報を表示可能にするかどうかを制御します。それらのコンピュータに関連するメール通知を受信するかどうかにも含まれます。

- 選択したグループ内に新しいコンピュータを作成: この役割のユーザが、アクセス可能なコンピュータグループに新しいコンピュータを作成できるようにするには、このオプションを設定します。
- 選択したグループ内にサブグループを追加または削除: この役割のユーザが、アクセス可能なコンピュータグループ内にサブグループを作成および削除できるようにするには、このオプションを設定します。

[詳細な権限] セクションで以下を有効にすることもできます。

- コンピュータファイルをインポート: この役割のユーザが、Deep Security Managerの [コンピュータのエクスポート] オプションで作成されたファイルを使用してコンピュータをインポートできるようにします。
- ディレクトリを追加、削除、および同期: この役割のユーザが、MS Active DirectoryなどのLDAPベースのディレクトリを使用して管理されているコンピュータを追加、削除、および同期できるようにします。
- VMware vCenterを追加、削除、および同期: この役割のユーザが、VMware vCenterを追加、削除、および同期できるようにします。
- クラウドアカウントの追加、削除、および同期を許可: この役割のユーザが、クラウドプロバイダを追加、削除、および同期できるようにします。

6. 表示、編集、および削除の権限をある役割のユーザに与えるには、[ポリシーの権限] タブを使用します。これらの権限は、すべてのポリシーに適用することも、特定のポリシーに制限することもできます。アクセス権を制限する場合は、[選択したポリシー] をクリックし、この役割のユーザにアクセス権を与えるポリシーの横にあるチェックボックスをオンにします。

一般 コンピュータの権限 **ポリシーの権限** ユーザ権限 その他の権限 割り当て対象

ポリシーの権限

ユーザに許可される処理:

表示
 編集
 削除

すべてのポリシー
 選択したポリシー:

ポリシー
 Base Policy
 Deep Security
 Deep Security Manager
 Deep Security Virtual Appliance
 Linux Server
 Solaris Server
 Windows
 Windows 10 Desktop
 Windows 7 Desktop
 Windows 8 Desktop
 Windows Anti-Malware Protection
 Windows Mobile Laptop
 Windows Server 2000
 Windows Server 2003
 Windows Server 2008
 選択されていないポリシーを表示
 ポリシーの作成

詳細な権限

ポリシーのインポートを許可

OK キャンセル 適用

「子」ポリシーを持つポリシーへの権限を許可すると、その子ポリシーに対する権限も自動的に付与されます。

次に示す2つの基本オプションを使用できます。

- 選択されていないポリシーを表示: この役割のユーザの編集または削除の権限が制限されている場合でも、このチェックボックスをオンにすることで他のポリシーに関する情報の表示 (変更は不可) を許可できます。
- ポリシーの作成: この役割のユーザが新しいポリシーを作成できるようにするには、このオプションを設定します。

[詳細な権限] セクションで以下を有効にすることもできます。

- ポリシーのインポートを許可: この役割のユーザが、Deep Security Managerの [ポリシー] タブの [エクスポート] オプションで作成したファイルを使用してポリシーをインポートできるようにします。

7. [ユーザ権限] タブのオプションを使用して、管理者アカウントの権限を定義できます。

一般	コンピュータの権限	ポリシーの権限	ユーザ権限	その他の権限	割り当て対象
ユーザ権限					
ユーザに許可される処理:					
<input checked="" type="radio"/> 自身のパスワードと連絡先情報のみを変更					
<input type="radio"/> 同等以下のアクセス権を持つユーザを作成および管理					
<input type="radio"/> すべての役割およびユーザを完全に管理					
<input type="radio"/> カスタム					
<input type="button" value="OK"/> <input type="button" value="キャンセル"/> <input type="button" value="適用"/>					

- 自身のパスワードと連絡先情報のみを変更: この役割のユーザは、自身のパスワードと連絡先情報のみを変更できません。
- 同等以下のアクセス権を持つユーザを作成および管理: この役割のユーザは、同等以下のアクセス権を持つユーザを作成および管理できます。この役割を持つユーザの権限を1つでも上回る場合、この役割のユーザはそのユーザを作成または管理できません。
- すべての役割およびユーザを完全に管理: この役割のユーザは、ユーザと役割を制限なしで作成および管理できます。このオプションの使用には、十分な注意が必要です。このオプションを役割に割り当てると、別の制限付きの権限を持つユーザが、Deep Security Managerのすべての要素への無制限のフルアクセス権を持つユーザを作成し、そのユーザとしてログオンできるようになるおそれがあります。
- カスタム: [カスタム] を選択して、[カスタム権限] セクションのオプションを使用すると、ユーザが他のユーザおよび役割を表示、作成、編集、または削除する権限をさらに制限できます。[同等以下の権限を持つユーザのみを操作] オプションを選択すると、特定のユーザに対して一部のオプションが制限される場合があります。

[同等以下の権限を持つユーザのみを操作] オプションでは、この役割のユーザの権限をさらに制限します。ユーザは、自身と同等または下位の権限を持つユーザに対する変更のみ行うことができます。この役割のユーザは、役割を作成、編集、削除できなくなります。このオプションを選択すると、[カスタム権限] セクションの以下のオプションが制限されます。

- 新規ユーザを作成できます: 同等または下位の権限を持つユーザの作成のみ可能です。
 - ユーザプロパティを編集できます: 同等または下位の権限を持つユーザの編集、またはパスワードの設定やリセットのみ可能です。
 - ユーザを削除できます: 同等または下位の権限を持つユーザの削除のみ可能です。
8. [その他の権限] タブでは、Deep Securityの特定の機能、またはその機能の特定の処理にのみにアクセスできるように役割の権限を制限できます。たとえば、管理者が複数いる場合、誤って他の管理者の作業内容を上書きすることがないように各管理者の権限を制限できます。初期設定では、各役割は各機能に対して「表示のみ」または「非表示」に設定されています。

す。アクセスを細かく変更またはカスタマイズするには、リストから [カスタム] を選択します。

一般	コンピュータの権限	ポリシーの権限	ユーザ権限	その他の権限	割り当て対象
その他の権限					
	アラート			表示のみ	▼
	アラート設定			表示のみ	▼
	IPリスト			表示のみ	▼
	ポートリスト			表示のみ	▼
	スケジュール			表示のみ	▼
	システム設定 (グローバル)			非表示	▼
	システム情報			非表示	▼
	診断			表示のみ	▼
	タグ付け			表示のみ	▼
	タスク			非表示	▼
	マルチテナントの管理			表示のみ	▼
	検索キャッシュ設定の管理			表示のみ	▼
	連絡先			非表示	▼
	ライセンス			非表示	▼
	アップデート			非表示	▼
	資産評価			表示のみ	▼
	証明書			表示のみ	▼

OK キャンセル 適用

9. [割り当て対象] タブには、この役割が割り当てられたユーザのリストが表示されます。役割が正しく機能していることをテストする場合は、新しいユーザを作成し、そのユーザとしてログインして機能を検証します。

Full Access、Auditor、および新規の各役割の初期設定

次の表は、Full Accessの役割とAuditorの役割に対する権限の初期設定を示しています。また、[役割] 画面のツールバーで [新規] をクリックして新しい役割を作成するときの権限の設定についても示します。

権限	役割別の設定		
	Full Accessの役割	Auditorの役割	新規役割の初期設定
一般	Full Accessの役割	Auditorの役割	新規役割の初期設定
DSMユーザインタフェースへのアクセス	許可	許可	許可
WebサービスAPIへのアクセス	許可	許可	不許可
コンピュータの権限	Full Accessの役割	Auditorの役割	新規役割の初期設定
表示	許可、すべてのコンピュータ	許可、すべてのコンピュータ	許可、すべてのコンピュータ
編集	許可、すべてのコンピュータ	不許	不許

権限	役割別の設定		
		可、すべてのコンピュータ	可、すべてのコンピュータ
削除	許可、すべてのコンピュータ	不許可、すべてのコンピュータ	不許可、すべてのコンピュータ
アラートの消去	許可、すべてのコンピュータ	不許可、すべてのコンピュータ	不許可、すべてのコンピュータ
アイテムのタグ付け	許可、すべてのコンピュータ	不許可、すべてのコンピュータ	不許可、すべてのコンピュータ
選択されていないコンピュータおよびデータ (イベントやレポートなど) を表示	許可	許可	許可、すべてのコンピュータ

権限	役割別の設定		
			タ
コンピュータに関連していないイベントおよびアラートを表示	許可	許可	許可、すべてのコンピュータ
選択したグループ内に新しいコンピュータを作成	許可	不許可	不許可
選択したグループ内にサブグループを追加または削除	許可	不許可	不許可
コンピュータファイルをインポート	許可	不許可	不許可
クラウドアカウントの追加、削除、および同期を許可	許可	不許可	不許可
ポリシーの権限	Full Accessの役割	Auditorの役割	新規役割の初期設定
表示	許可、すべてのポリシー	許可、すべてのポリシー	許可、すべてのポリシー

権限	役割別の設定		
編集	許可、すべてのポリシー	不許可、すべてのポリシー	不許可、すべてのポリシー
削除	許可、すべてのポリシー	不許可、すべてのポリシー	不許可、すべてのポリシー
選択されていないポリシーの表示	許可	許可	許可
新規ポリシーの作成	許可	不許可	不許可
ポリシーのインポート	許可	不許可	不許可
ユーザ権限 (この後の「ユーザ権限に関する注意」を参照)	Full Accessの役割	Auditorの役割	新規役割の初期設定
ユーザの表示	許可	許可	不許可
ユーザの作成	許可	不許可	不許可
ユーザプロパティの編集	許可	不許可	不許可

権限	役割別の設定		
ユーザの削除	許可	不許可	不許可
役割の表示	許可	許可	不許可
役割の作成	許可	不許可	不許可
役割のプロパティの編集	許可	不許可	不許可
役割の削除	許可	不許可	不許可
権限の委任	許可	不許可	不許可
その他の権限	Full Accessの役割	Auditor の役割	新規役割の初期設定
アラート	完全 (グローバルアラートを消去可能)	表示のみ	表示のみ
アラート設定	完全 (アラート設定を編集可能)	表示のみ	表示のみ
IPリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
ポートリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
スケジュール	完全 (作成、編集、および削除可能)	表示の	表示の

Trend Micro Deep Security On-Premise 12.0

権限	役割別の設定		
		み	み
システム設定 (グローバル)	完全 (システム設定 (グローバル) を表示、編集可能)	表示のみ	非表示
診断	完全 (診断パッケージを作成可能)	表示のみ	表示のみ
タグ付け	完全 (タグ付け (コンピュータに属さない項目)、タグ削除、所有していない自動タグルールをアップデート、所有していない自動タグルールを実行、および所有していない自動タグルールを削除可能)	表示のみ	表示のみ
タスク	完全 (タスクを表示、追加、編集、削除、および実行可能)	表示のみ	非表示
マルチテナントの管理	完全	非表示	表示のみ
検索キャッシュ設定の管理	完全	表示のみ	表示のみ
連絡先	完全 (連絡先を表示、作成、編集、および削除可能)	表示のみ	非表示
ライセンス	完全 (ライセンスを表示および変更可能)	表示のみ	非表示
アップデート	完全 (ソフトウェアを追加、編集、および削除可能。コンポーネントのアップデートを表示可能。アップデートコンポーネントをダウンロード、インポート、および適用可能。Deep Securityルールアップデートを削除	表示のみ	非表示

権限	役割別の設定		
	可能)		
資産評価	完全 (資産評価を作成、編集、および削除可能)	表示のみ	表示のみ
証明書	完全 (SSL証明書を作成および削除可能)	表示のみ	表示のみ
Relayグループ	完全	表示のみ	表示のみ
プロキシ	完全	表示のみ	表示のみ
SAML IDプロバイダ	完全	非表示	非表示
不正プログラム検索設定	完全 (不正プログラム検索設定を作成、編集、および削除可能)	表示のみ	表示のみ
検出ファイル	完全 (検出ファイルを削除およびダウンロード可能)	表示のみ	表示のみ
Webレピュテーション設定	完全	表示のみ	表示のみ
ディレクトリリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
ファイルリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ

権限	役割別の設定		
ファイル拡張子リスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
ファイアウォールルール	完全 (ファイアウォールルールを作成、編集、および削除可能)	表示のみ	表示のみ
ファイアウォールステートフル設定	完全 (ファイアウォールステートフル設定を作成、編集、および削除可能)	表示のみ	表示のみ
侵入防御ルール	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
アプリケーションの種類	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
MACリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
コンテキスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
変更監視ルール	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
セキュリティログ監視ルール	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
セキュリティログ監視デコーダ	完全 (作成、編集、および削除可能)	表示のみ	表示のみ

[自身のパスワードと連絡先情報のみを変更] オプションに対応するカスタム設定を次の表に示します。

[自身のパスワードと連絡先情報のみを変更] オプションに対応するカスタム設定	
ユーザ	
ユーザを表示できます	不許可
新規ユーザを作成できます	不許可
ユーザプロパティを編集できます (ユーザは常に自分のアカウントの選択プロパティを編集できます)	不許可
ユーザを削除できます	不許可
役割	
役割を表示できます	不許可
新規の役割を作成できます	不許可
役割のプロパティを編集できます (警告: この権限を付与すると、この役割を持つユーザが自分の権限を編集できるようになります)	不許可
役割を削除できます	不許可
権限の委任	
同等以下の権限を持つユーザのみを操作	不許可

[同等以下のアクセス権を持つユーザを作成および管理] オプションに対応するカスタム設定を次の表に示します。

[同等以下のアクセス権を持つユーザを作成および管理] オプションに対応するカスタム設定	
ユーザ	
ユーザを表示できます	許可
新規ユーザを作成できます	許可
ユーザプロパティを編集できます (ユーザは常に自分のアカウントの選択プロパティを編集できます)	許可
ユーザを削除できます	許可
役割	
役割を表示できます	不許可
新規の役割を作成できます	不許可
役割のプロパティを編集できます (警告: この権限を付与すると、この役割を持つユーザが自分の権限を編集できるようになります)	不許可
役割を削除できます	不許可
権限の委任	
同等以下の権限を持つユーザのみを操作	許可

[すべての役割およびユーザを完全に管理] オプションに対応するカスタム設定を次の表に示します。

[すべての役割およびユーザを完全に管理] オプションに対応するカスタム設定	
ユーザ	
ユーザを表示できます	許可
新規ユーザを作成できます	許可
ユーザプロパティを編集できます (ユーザは常に自分のアカウントの選択プロパティを編集できます)	許可
ユーザを削除できます	許可
役割	
役割を表示できます	許可
新規の役割を作成できます	許可
役割のプロパティを編集できます (警告: この権限を付与すると、この役割を持つユーザが自分の権限を編集できるようになります)	許可
役割を削除できます	許可
権限の委任	
同等以下の権限を持つユーザのみを操作	該当なし

レポートのみを受信できるユーザの追加

「連絡先」とは、Deep Security Managerにログオンできないが、予約タスクを使用して定期的にレポートを受信できるユーザのことです。連絡先には、既存の役割にマッピングする「アクセス許可」レベルを割り当てることができます。連絡先にレポートが送信される場合、同じレベルのユーザがアクセスできない情報はそのレポートに含まれません。たとえば、3名の連絡先を週次の概要レポートの受信者として指定した場合、各連絡先が使用するコンピュータの権限に応じて、3つのレポートの内容がまったく異なるものになる場合があります。

連絡先を追加または編集する

1. Deep Security Managerで、[管理]→[ユーザ管理]→[連絡先]の順に選択します。
2. 新しい連絡先を追加する場合は [新規] をクリックし、既存の連絡先の設定を編集する場合はその連絡先をダブルクリックします。
3. [一般情報] セクションで、この連絡先の名前、説明、および優先する言語を指定します。
4. [連絡先情報] セクションで、レポート配布リストにこの連絡先が含まれている場合にレポートの送信先となるメールアドレスを入力します (詳細については、[レポートの生成] 画面を参照してください)。
5. [アクセス許可] セクションで役割を指定し、この連絡先が参照できる情報を決定します。たとえば、この連絡先にコンピュータレポートを送信するように予約すると、役割でアクセスが許可されている、コンピュータに関する情報だけがレポートに含まれます。
6. エクスポートされるPDF形式のレポートをパスワードで保護するには、[パスワードで保護されたレポート] セクションで [このユーザが生成したレポートをパスワードで保護する] を選択し、[レポートのパスワード] を指定します。

連絡先を削除する

Deep Security Managerから連絡先を削除するには、[管理]→[ユーザ管理]→[連絡先]の順に選択して連絡先をクリックし、[削除] をクリックします。

ユーザ向けのAPIキーの作成

Deep Security Manager APIを使用するには、APIキーが必要になります。

注意: APIキーは、Deep Security Manager 11.1以降で提供されている新しい"[Deep Security APIを使用したタスクの自動化](#)" [on page 478](#)でのみ使用できます。

注意: トレンドマイクロでは、APIを使用してDeep Security Managerにアクセスする必要があるすべてのユーザに対して、1つのAPIキーのみを作成することをお勧めします。

ヒント: APIキーの作成は、Deep Security APIを使用して自動化できます。自動化の例については、Deep Security Automation Centerにあるガイド [「Create and Manage API Keys」](#) を参照してください。

新しいAPIキーを作成するには、次の手順に従います。

1. [管理]→[ユーザ管理]→[APIキー] の順に移動します。
2. [新規] をクリックします。
3. [プロパティ] ウィンドウで、APIキーの [名前] と [説明] を入力します。
4. [役割] リストをクリックして、役割を選択します。[監査担当者] を選択するとAPIを介したDeep Security Managerへの読み取り専用アクセス権限が付与され、[Full Access] を選択すると読み取りアクセス権限および書き込みアクセス権限の両方が付与されます。より詳細に定義された役割をAPIキーのユーザに割り当てる必要がある場合は、[新規] を選択して役割を定義することもできます。手順の詳細については、"[ユーザロールの定義](#)" [on page 1382](#)を参照してください。
5. [言語] を選択します。
6. タイムゾーンを選択します。
7. 必要に応じて [有効期限] を選択し、APIキーの有効期限を選択します。
8. [OK] をクリックします。

9. [秘密鍵の値] をコピーします。

注意: 秘密鍵の値はこのときにしか表示されないため、必ずコピーしておいてください。

既存のAPIキーをロックアウトする

既存のAPIキーが第三者に漏えいした場合は、次の手順でロックアウトすることができます。

1. ロックアウトするAPIキーをダブルクリックします。
2. 必要に応じ、[ロックアウト (認証を拒否)] を選択してAPIキーの使用をブロックします。
3. [OK] をクリックします。

ロックアウトされたユーザ名のロック解除

間違ったパスワードを使用してDeep Security Managerに何回もログオンすると、ユーザアカウントはロックアウトされます。ロックアウトされないログオン試行の許容回数は、[管理]→[システム設定]→[セキュリティ]→[ログオン失敗の許容回数 (ロックアウト前)] で設定します。

次の状況に応じて、ユーザをそれぞれの方法でロック解除できます。

- 管理者ユーザが利用可能な場合、"[管理者としてユーザのロックを解除する](#)" [below](#)を参照してください。
- すべての管理ユーザがロックアウトされた場合は、"[コマンドラインから管理ユーザのロックを解除する](#)" [on the next page](#)を参照してください。

管理者としてユーザのロックを解除する

1. 作業管理者のユーザ名とパスワードを使用してDeep Security Managerにログインします。
2. [管理]→[ユーザ管理]→[ユーザ] の順に選択します。ロック解除するユーザを選択して右クリックし、[プロパティ] をクリックします。

3. ウィザードで、[一般]→[ログオン資格情報]の順に選択します。[ロックアウト (ログオンを拒否)] チェックボックスの選択を解除します。
4. [保存] をクリックします。

コマンドラインから管理ユーザのロックを解除する

1. ローカルコマンドラインインタフェースに移動します。

Deep Security ManagerがWindowsの場合、`..\Program Files\Trend Micro\Deep security Manager`ディレクトリに移動します。

Deep Security ManagerがLinuxの場合、`/opt/dsm`ディレクトリに移動します。

2. 次のコマンドを入力します。

```
dsm_c -action unlockout -username <username>
```

SAMLシングルサインオン (SSO) を実装する

注意: FIPSモードが有効な場合、SAMLシングルサインオンは利用できません。"[FIPS 140-2のサポート](#)" on page 1457を参照してください。

SAMLシングルサインオンを実装するには、"[SAMLシングルサインオンを設定する](#)" on page 1412 または "[SAMLシングルサインオンをAzure Active Directoryで設定する](#)" on page 1419で設定します。

SAMLとシングルサインオンとは

Security Assertion Markup Language (SAML) は、当事者間でのユーザ識別情報の安全な交換を可能にする、オープンな認証標準です。SAMLは、1回のユーザログインを複数のアプリケーションとサービスにわたって機能させる技術である、シングルサイ

ンオンをサポートしています。Deep Securityでは、SAMLシングルサインオンを実装することで、組織のポータルにログオンするユーザが、既存のDeep SecurityアカウントなしでDeep Securityにシームレスにログオンできるようになります。

Deep SecurityでのSAMLシングルサインオンの仕組み

信頼関係を確立する

SAMLシングルサインオンでは、両当事者(IDプロバイダとサービスプロバイダ)の間で信頼関係が確立されます。IDプロバイダのディレクトリサーバにはユーザID情報が保存されています。サービスプロバイダ(この場合はDeep Security)は、IDプロバイダのユーザIDを使用して独自の認証とアカウント作成を行います。

IDプロバイダとサービスプロバイダは、SAMLメタデータドキュメントを交換することで、信頼を確立します。

注意: 現時点では、Deep SecurityはSAML 2.0 IDプロバイダ (IdP) で開始されたログインフローのHTTP POSTバインディングのみをサポートし、サービスプロバイダ (SP) で開始されたログインフローはサポートしません。

ユーザIDからDeep Securityアカウントを作成する

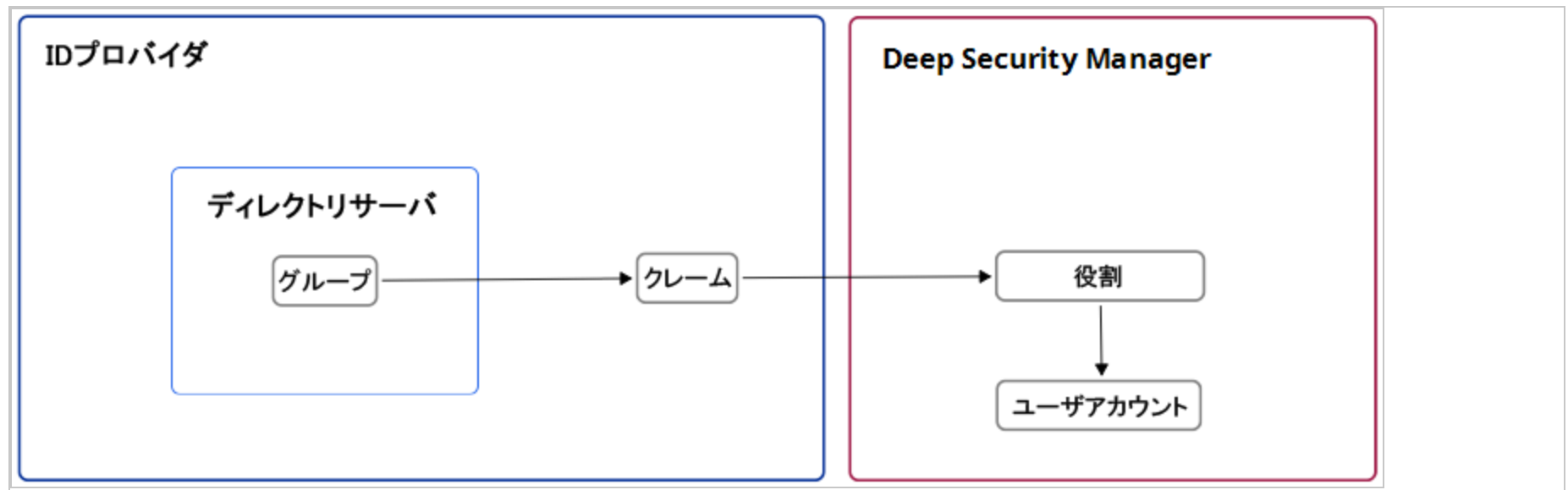
Deep SecurityとIDプロバイダがSAMLメタデータドキュメントを交換して信頼関係を確立すると、Deep SecurityはIDプロバイダのディレクトリサーバ上のユーザIDにアクセスできるようになります。ただし、Deep Securityが実際にユーザIDからアカウントを作成する前に、アカウントの種類を定義し、データ形式を変換するための手順を導入する必要があります。これは、グループ、役割、クレームを使用して実行されます。

グループと役割は、Deep Securityユーザアカウントのテナントとアクセス許可を指定します。グループは、IDプロバイダのディレクトリサーバ上に作成されます。IDプロバイダは、1つ以上のグループにユーザIDを割り当てます。役割はDeep Security Managerで作成されます。各Deep Securityアカウントの種類にはグループと役割の両方が必要で、アクセス許可とテナントの割り当てが一致している必要があります。

各ユーザの種類に一致するグループと役割を用意したら、グループデータ形式をDeep Securityが理解できる形式に変換する必要があります。これは、IDプロバイダによりクレームを使用して実行されます。クレームには、グループデータ形式を一致するDeep Securityの役割に変換するための手順が含まれています。

ヒント: Deep Securityで必要となる"[SAMLクレームの構造](#)" on page 1415について確認してください。

このプロセスを次に示します。



Deep SecurityでSAMLシングルサインオンを実装する

SAMLメタデータドキュメントの交換により、Deep SecurityとIDプロバイダとの間で信頼関係が確立されると、一致するグループと役割が作成され、グループデータを役割に変換するためのクレームが導入されて、Deep SecurityはSAMLシングルサインオンを使用して組織のポータルからログオンするユーザに対してDeep Securityアカウントを自動的に作成できるようになります。

SAMLシングルサインオンの実装の詳細については、"[SAMLシングルサインオンを設定する](#)" on the next pageを参照してください。

SAMLシングルサインオンを設定する

注意: FIPSモードが有効な場合、SAMLシングルサインオンは利用できません。"[FIPS 140-2のサポート](#)" on page 1457を参照してください。

SAMLシングルサインオンを使用するようDeep Securityを設定すると（組織のポータルにサインインするSSO）、ユーザは、既存のDeep Securityアカウントがない状態でDeep Securityにシームレスにログインできます。また、SAMLシングルサインオンを使用すると、次のようなユーザ認証アクセス制御機能を実装できます。

- パスワード強度または変更の強制
- ワンタイムパスワード (OTP)
- 2要素認証 (2FA) または多要素認証 (MFA)

Deep SecurityのSAML標準実装の詳細については、"[SAMLシングルサインオン \(SSO\) を実装する](#)" on page 1409を参照してください。Azure Active DirectoryをIDプロバイダとして使用している場合は、"[SAMLシングルサインオンをAzure Active Directoryで設定する](#)" on page 1419を使用したSAMLシングルサインオンの設定を参照してください。

注意: 現時点では、Deep SecurityはSAML 2.0 IDプロバイダ (IdP) で開始されたログインフローのHTTP POSTバインディングのみをサポートし、サービスプロバイダ (SP) で開始されたログインフローはサポートしません。

Deep SecurityでSAMLシングルサインオンを使用するには、次の手順を実行する必要があります。

1. "[設定前の要件を設定する](#)" on the next page
2. "[Deep SecurityをSAMLサービスプロバイダとして設定する](#)" on the next page
3. "[Deep SecurityでSAMLを設定する](#)" on page 1414
4. "[IDプロバイダの管理者に情報を提供する](#)" on page 1415
5. "[SAMLクレームの構造](#)" on page 1415
6. "[SAMLシングルサインオンをテストする](#)" on page 1418
7. "[サービスとIDプロバイダの設定](#)" on page 1419

設定前の要件を設定する

1. Deep Security Managerが正常に動作していることを確認します。
2. IDプロバイダの管理者に次のことを問い合わせます。
 - ディレクトリサーバグループをDeep Securityルールにマッピングするための名前付け規則を設定します。
 - IDプロバイダSAMLメタデータドキュメントを取得します。
 - 必要なユーザ認証アクセス制御機能をポリシーに追加するよう依頼します。

Deep SecurityでのSAMLシングルサインオンの動作がすでにテストされている次のIDプロバイダがサポートされています。

- Active Directoryフェデレーションサービス (ADFS)
- Okta
- PingOne
- Shibboleth

Deep SecurityをSAMLサービスプロバイダとして設定する

注意: マルチテナントのDeep Securityインストール環境でDeep SecurityをSAMLサービスプロバイダとして設定できるのは、プライマリテナントの管理者だけです。

1. Deep Security Managerで、[管理]→[ユーザ管理]→[IDプロバイダ]→[SAML]の順に選択します。
2. [開始] をクリックします。
3. エンティティID および サービス名を入力し、をクリックします。[次へ]をクリックします。

注意: [エンティティID] はSAMLサービスプロバイダの一意の識別子です。SAMLの仕様ではエンティティIDがエンティティのドメイン名を含むURLであることが推奨されており、業界の慣習として、エンティティIDにはSAMLメタデータ

URLを使用します。SAMLメタデータは、Deep Security Managerの / samlエンドポイントから配信されるため、例の値は `https://<DSMServerIP:4119>/saml` です。

4. 証明書のオプションを選択し、[次へ] をクリックします。SAMLサービスプロバイダの証明書は現時点では使用されていませんが、サービスプロバイダが開始したログオン機能やシングルサインアウト機能をサポートするために将来使用されます。証明書をインポートするには、PKCS #12キーストアファイルとパスワードを入力するか、新しい自己署名証明書を作成します。
5. 証明書の詳細の概要が表示されるまで手順を実行し、[Finish] をクリックします。

Deep SecurityでSAMLを設定する

IDプロバイダSAMLメタデータドキュメントをインポートする

注意: Deep Securityアカウントには、管理者権限と「SAML IDプロバイダの作成」権限の両方が必要です。

1. [管理] 画面で、[ユーザ管理]→[アイデンティティプロバイダ]→[SAML] に移動します。
2. [開始] をクリックします。
3. [ファイルの選択] をクリックし、IDプロバイダによって提供されたSAMLメタデータドキュメントを選択して、[次へ] をクリックします。
4. IDプロバイダの [名前] を入力し、[完了] をクリックします。
[役割] 画面が表示されます。

SAMLユーザのDeep Securityの役割を作成する

想定されるユーザの種類ごとに役割を作成する必要があります。各役割は、IDプロバイダのディレクトリサーバに対応するグループがあり、グループのアクセス権限およびテナントの割り当てと一致する必要があります。

IDプロバイダのSAML統合では、グループのメンバーシップをSAMLクレームに変換するメカニズムが用意されます。クレームルールの詳細は、IDプロバイダに付属するドキュメントを確認してください。

役割の作成方法については、"[ユーザロールの定義](#)" on page 1382の定義を参照してください。

IDプロバイダの管理者に情報を提供する

Deep Security ManagerサービスプロバイダSAMLメタデータドキュメントをダウンロードする

1. [管理] 画面で、[ユーザ管理]→[アイデンティティプロバイダ]→[SAML] に移動します。
2. SAMLサービスプロバイダの下の [ダウンロード] をクリックします。
Deep SecurityサービスプロバイダSAMLメタデータドキュメント (ServiceProviderMetadata.xml) がダウンロードされます。

URNおよびDeep Security SAMLメタデータドキュメントをIDプロバイダの管理者に送信する

IDプロバイダの管理者には、Deep SecurityのサービスプロバイダSAMLメタデータドキュメント、IDプロバイダのURN、および作成したDeep Securityの各役割のURNを指定する必要があります。

ヒント:

役割のURNを確認するには、[管理]→[ユーザ管理]→[役割] の順に選択し、[URN] 列を参照します。

IDプロバイダのURNを確認するには、[管理]→[ユーザ管理]→[アイデンティティプロバイダ]→[SAML]→[アイデンティティプロバイダ] の順に選択し、[URN] 列を参照します。

IDプロバイダの管理者が、Deep Securityの役割に対応するグループと、グループメンバーシップをSAMLクレームに変換するために必要なルールを作成していることを確認したら、SAMLシングルサインオンの設定は完了です。

注意: IDプロバイダの管理者には、必要に応じて、Deep Securityが必要とする"[SAMLクレームの構造](#)" belowについての情報を提供できます。

SAMLクレームの構造

次のSAML要求はDeep Securityでサポートされています。

Trend Micro Deep Security On-Premise 12.0

- "Deep Securityユーザ名 (必須)" below
- "Deep Securityユーザの役割 (必須)" below
- "最大セッション期間 (オプション)" on the next page
- "言語設定 (オプション)" on page 1418

Deep Securityユーザ名 (必須)

クレームには、Name属性が<https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionNameAttribute>エレメントと、1つのAttributeValueエレメントが含まれるSAMLアサーションが必要です。Deep Security ManagerはAttributeValueをDeep Securityユーザ名として使用します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName">
        <AttributeValue>alice</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

Deep Securityユーザの役割 (必須)

クレームには、Name属性が<https://deepsecurity.trendmicro.com/SAML/Attributes/RoleAttribute>エレメントと、1~10個のAttributeValueエレメントが含まれるSAMLアサーションが必要です。Deep Security Managerは、この属性値を使用して、ユーザのテナント、IDプロバイダ、役割を確認します。1つのアサーションには複数のテナントの役割が含まれる場合があります。

SAMLデータの例 (簡略版)

注意: 読みやすいようにAttributeValueエレメントに改行を入れていますが、クレームでは1行にする必要があります。

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/Role">
        <AttributeValue>urn:tmds:identity:[pod ID]:[tenant ID]:saml-provider/[IDP name],
          urn:tmds:identity:[pod ID]:[tenant ID]:role/[role name]</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

最大セッション期間 (オプション)

クレームに `https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration` の Name 属性と整数値の AttributeValue 要素を含む Attribute 要素が含まれているSAMLアサーションがある場合、セッションはその時間 (秒) が経過すると自動的に終了します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration">
        <AttributeValue>28800</AttributeValue>
      </Attribute>
    </AttributeStatement>
```

```
</Assertion>  
</samlp:Response>
```

言語設定 (オプション)

要求に `https://deepsecurity.trendmicro.com/SAML/attributes/PreferredLanguage` という Name 属性の Attribute 要素が含まれ、サポートされている言語のいずれかと同じ文字列値の AttributeValue 要素が含まれている SAML アサーションがある場合、Deep Security Manager はこの値を使用してユーザの優先言語を設定します。

次の言語がサポートされます。

- `en-US` (米国英語)
- `ja-JP` (日本語)

SAML データの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">  
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">  
    <AttributeStatement>  
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/PreferredLanguage">  
        <AttributeValue>en-US</AttributeValue>  
      </Attribute>  
    </AttributeStatement>  
  </Assertion>  
</samlp:Response>
```

SAML シングルサインオンをテストする

ID プロバイダサーバのシングルサインオンのログイン画面に移動し、そこから Deep Security Manager にログインします。正しく設定されている場合、Deep Security Manager コンソールにリダイレクトされます。SAML シングルサインオンが機能していない場合は、次の手順に従います。

設定を確認する

1. "設定前の要件を設定する" on page 1413セクションを確認します。
2. ユーザが正しいディレクトリグループに属していることを確認します。
3. IDプロバイダと役割のURNがIDプロバイダのフェデレーションサービスで正しく設定されていることを確認します。

診断パッケージを作成する

1. [管理]→[システム情報]の順に選択し、[診断ログ]をクリックします。
2. [SAMLに関する問題]を選択し、[保存]をクリックします。
3. ログを生成します。IDプロバイダ経由でDeep Security Managerにログインし、問題を再現します。
4. ログインが失敗したら、[管理]→[システム情報]に移動し、診断パッケージの作成をクリックして診断パッケージを生成します。
5. 診断パッケージが作成されたら、<https://success.trendmicro.com/jp/contact-support>に移動してテクニカルサポートケースを開き、ケースの作成時に診断パッケージをアップロードします。

サービスとIDプロバイダの設定

サーバ証明書とIDプロバイダ証明書の有効期限を事前に通知するタイミングや、SAMLシングルサインオン経由で追加された非アクティブなユーザアカウントを自動的に削除するまでの期間を設定できます。

これらの設定を変更するには、[管理]→[システム設定]→[セキュリティ]→[アイデンティティプロバイダ]に移動します。

SAMLシングルサインオンをAzure Active Directoryで設定する

Deep SecurityのSAML標準の実装の詳細については、"[SAMLシングルサインオン \(SSO\) を実装する](#)" on page 1409の実装を参照してください。他のIDプロバイダとの設定手順については、"[SAMLシングルサインオンを設定する](#)" on page 1412を参照してください。

注意:

- FIPSモードが有効な場合、SAMLシングルサインオンは利用できません。"[FIPS 140-2のサポート](#)" on page 1457 \
- 現時点では、Deep Securityではのみがサポートされています。では、SAML 2.0アイデンティティプロバイダのHTTP POSTバインドのみがサポートされます (IdP)-はログインフローを開始し、サービスプロバイダは開始しませんでした (SP)-はログオンフローを開始しました)。

誰がこのプロセスに関与していますか？

通常、Deep Security ManagerでSAMLシングルサインオンにAzure Active Directoryを使用するように設定するには、2人必要です (SSO): a Deep Security管理者とAzure Active Directory管理者)。

Deep Securityの管理者には、SAML IDプロバイダ 権限が完全に設定されているか、カスタム (で新しいSAML IDプロバイダの作成可能な が有効) に設定されたDeep Securityの役割が割り当てられている必要があります。

Azure Active Directoryを使用してDeep SecurityでSAMLシングルサインオンを設定する手順と、各手順を実行する担当者の手順は次のとおりです。

ステップ	実行者
" Deep SecurityをSAMLサービスプロバイダとして設定する " on the next page	Deep Security管理者
" Deep SecurityサービスプロバイダのSAMLメタデータドキュメントをダウンロードする " on the next page	Deep Security管理者
" Azure Active Directoryを設定する " on the next page	Azure Active Directory管理者
" Deep SecurityでSAMLを設定する " on page 1422	Deep Security管理者
" Azure Active Directoryで役割を定義する " on page 1423	Azure Active Directory管理者

Deep SecurityをSAMLサービスプロバイダとして設定する

注意: マルチテナントのDeep Securityインストール環境でDeep SecurityをSAMLサービスプロバイダとして設定できるのは、プライマリテナントの管理者だけです。

1. Deep Security Managerで、[管理]→[ユーザ管理]→[IDプロバイダ]→[SAML]の順に選択します。
2. [開始] をクリックします。
3. エンティティID および サービス名を入力し、をクリックします。[次へ]をクリックします。

注意: [エンティティID] はSAMLサービスプロバイダの一意的識別子です。SAMLの仕様ではエンティティIDがエンティティのドメイン名を含むURLであることが推奨されており、業界の慣習として、エンティティIDにはSAMLメタデータURLを使用します。SAMLメタデータは、Deep Security Managerの/ samlエンドポイントから配信されるため、例の値は `https://<DSMServerIP:4119>/saml` です。

4. 証明書のオプションを選択し、[次へ] をクリックします。SAMLサービスプロバイダの証明書は現時点では使用されていませんが、サービスプロバイダが開始したログオン機能やシングルサインアウト機能をサポートするために将来使用されます。証明書をインポートするには、PKCS #12キーストアファイルとパスワードを入力するか、新しい自己署名証明書を作成します。
5. 証明書の詳細の概要が表示されるまで手順を実行し、[Finish]をクリックします。

Deep SecurityサービスプロバイダのSAMLメタデータドキュメントをダウンロードする

Deep Security Managerの の管理ページで、[ユーザ管理]→[IDプロバイダ]→[SAML]の順に選択し、[Download]をクリックします。このファイルは、 `ServiceProviderMetadata.xml` としてダウンロードされます。このファイルをAzure Active Directory管理者に送信します。

Azure Active Directoryを設定する

このセクションの手順は、Azure Active Directory管理者が実行します。

以下の手順の実行方法の詳細については、[Azure Active Directory](#) の非ギャラリーアプリケーションへのシングルサインオンの設定を参照してください。

1. Azure Active Directoryポータルで、ギャラリー以外の新しいアプリケーションを追加します。
2. アプリケーションのシングル・サインオンを設定します。Deep Security Managerからダウンロードされたメタデータファイル `ServiceProviderMetadata.xml` をアップロードすることをお勧めします。また、応答URL (Deep Security Manager URL + / `saml`) を入力することもできます。
3. SAML要求を設定します。Deep Securityには次の2つが必要です。
 - `https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName`
Deep Securityのユーザ名となる一意のユーザIDです。たとえば、User Principal Name (UPN) を使用できます。
 - `https://deepsecurity.trendmicro.com/SAML/Attributes/Role`
形式は「IDP URN、役割URN」です。IDPはまだDeep Security Managerに作成されていません。このSAMLクレームは、後で "[Azure Active Directoryで役割を定義する](#)" on the next page で役割を定義するで設定できます。

"[SAMLクレームの構造](#)" on page 1424で説明されているように、その他の任意のクレームを設定することもできます。

4. フェデレーションメタデータXML ファイルをダウンロードし、Deep Security管理者に送信してください。

Deep Securityで複数の役割が定義されている場合は、これらの手順を繰り返して役割ごとに個別のアプリケーションを作成します。

Deep SecurityでSAMLを設定する

Azure Active Directoryメタデータドキュメントをインポートする

1. Deep Security Managerで、[[管理]→[ユーザ管理]→[アイデンティティプロバイダ]→[SAML]]の順に選択します。
2. [の開始]または[新しい]をクリックします。
3. [ファイルの選択] の順に選択し、Azure Active DirectoryからダウンロードしたフェデレーションメタデータXMLファイルを選択して、[次へ] の順にクリックします。
4. IDプロバイダの [名前] を入力し、[完了] をクリックします。

Rolesのページに移動します。

Trend Micro Deep Security On-Premise 12.0

SAMLユーザのDeep Securityの役割を作成する

Deep Securityの[管理]→[ユーザ管理]→[役割の の管理]画面に、組織の適切な役割が含まれていることを確認します。ユーザには、自分の業務を職務の遂行に必要なもの限定する役割を割り当てる必要があります。役割の作成方法については、"[ユーザロールの定義](#)" on page 1382の定義を参照してください。Deep Securityの各役割には、対応するAzure Active Directoryアプリケーションが必要です。

URNを取得する

Deep Security Managerで、次の情報を収集します。この情報は、Azure Active Directory管理者に提供する必要があります。

- アイデンティティプロバイダURNIDプロバイダのURNを表示するには、の[管理]→[ユーザ管理]→[IDプロバイダ]→[SAML]→[IDプロバイダ]に移動し、[URN]列を選択します。
- Azure Active Directoryアプリケーションに関連付けるDeep Securityの役割のURN。ロールURNを表示するには、の[管理]→[ユーザ管理]→[ロール]の順に選択し、[URN]列を選択します。複数の役割を持つ場合は、役割ごとにURNが必要になります。役割ごとに個別のAzure Activeアプリケーションが必要なためです。

Azure Active Directoryで役割を定義する

このセクションの手順は、Azure Active Directory管理者が実行する必要があります。

Azure Active Directoryでは、前のセクションで識別したアイデンティティプロバイダのURNと役割のURNを使用して、Azureアプリケーションで「役割」属性を定義します。これは、「IDP URN、役割URN」の形式で指定してください。「Deep Securityユーザの役割（"[SAMLクレームの構造](#)" on the next page セクションの）」が必要です。」を参照してください。

Azure Active Directoryの[検証]ボタンを使用してセットアップをテストするか、新しいアプリケーションをユーザに割り当ててテストします。

サービスとIDプロバイダの設定

サーバ証明書とIDプロバイダ証明書の有効期限を事前に通知するタイミングや、SAMLシングルサインオン経由で追加された非アクティブなユーザアカウントを自動的に削除するまでの期間を設定できます。

これらの設定を変更するには、[管理]→[システム設定]→[セキュリティ]→[アイデンティティプロバイダ]に移動します。

SAMLクレームの構造

次のSAML要求はDeep Securityでサポートされています。

- ["Deep Securityユーザ名 \(必須\)" below](#)
- ["Deep Securityユーザの役割 \(必須\)" on the next page](#)
- ["最大セッション期間 \(オプション\)" on the next page](#)
- ["言語設定 \(オプション\)" on page 1426](#)

Deep Securityユーザ名 (必須)

クレームには、Name属性が<https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionNameAttribute>エレメントと、1つのAttributeValueエレメントが含まれるSAMLアサーションが必要です。Deep Security ManagerはAttributeValueをDeep Securityユーザ名として使用します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName">
        <AttributeValue>alice</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```



```
</AttributeStatement>
</Assertion>
</samlp:Response>
```

Deep Securityユーザの役割 (必須)

クレームには、Name属性が<https://deepsecurity.trendmicro.com/SAML/Attributes/RoleAttribute>エレメントと、1~10個のAttributeValueエレメントが含まれるSAMLアサーションが必要です。Deep Security Managerは、この属性値を使用して、ユーザのテナント、IDプロバイダ、役割を確認します。1つのアサーションには複数のテナントの役割が含まれる場合があります。

SAMLデータの例 (簡略版)

注意: 読みやすいようにAttributeValueエレメントに改行を入れていますが、クレームでは1行にする必要があります。

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/Role">
        <AttributeValue>urn:tmds:identity:[pod ID]:[tenant ID]:saml-provider/[IDP name],
          urn:tmds:identity:[pod ID]:[tenant ID]:role/[role name]</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

最大セッション期間 (オプション)

クレームに <https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration> の Name 属性と整数値の AttributeValue 要素を含む Attribute 要素が含まれているSAMLアサーションがある場合、セッションはその時間 (秒) が経過すると自動的に終了します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration">
        <AttributeValue>28800</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

言語設定 (オプション)

要求に `https://deepsecurity.trendmicro.com/SAML/attributes/PreferredLanguage` という Name 属性の Attribute 要素が含まれ、サポートされている言語のいずれかと同じ文字列値の AttributeValue 要素が含まれているSAMLアサーションがある場合、Deep Security Managerはこの値を使用してユーザの優先言語を設定します。

次の言語がサポートされます。

- en-US (米国英語)
- ja-JP (日本語)

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/PreferredLanguage">
        <AttributeValue>en-US</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

```
</Attribute>  
</AttributeStatement>  
</Assertion>  
</samlp:Response>
```

Deep Security Managerの移動とカスタマイズ

ニーズに合わせて使用環境に関する役立つ情報が表示されるようにDeep Security Managerコンソールをカスタマイズできます。

- "スマートフォルダによるコンピュータの動的なグループ化" below
- "ダッシュボードのカスタマイズ" on page 1104
- "アクティブなDeep Security Managerノードの表示" on page 1444
- "ライセンス情報の確認" on page 988

スマートフォルダによるコンピュータの動的なグループ化

スマートフォルダはコンピュータの動的なグループで、保存した検索クエリで定義します。グループをクリックするたびに、一致するコンピュータが検索されます。コンピュータをOSやAWSプロジェクトタグなどの属性でグループ化して表示したい場合は、スマートフォルダを利用できます。

ヒント: プログラムを介してリソースを検索する場合は、Deep Security APIを使用してリソースの検索を自動化できます。例については、Deep Security Automation Centerにあるガイド [「Search for Resources」](#) を参照してください。

スマートフォルダを作成するには、次の項目を定義します。

1. 検索対象のコンピュータのプロパティ (1)
2. 一致条件を定義する演算子 (2)
3. 検索する値 (3)



スマートフォルダを作成する

1. [コンピュータ]→[スマートフォルダ]の順に選択します。
2. [スマートフォルダの作成]をクリックします。

初期設定の空の検索条件グループ (ルールグループ) が表示されます。最初にこのグループを設定する必要があります。追加または異なる一致条件を定義する必要がある場合は、後からルールグループを追加できます。

3. スマートフォルダの名前を入力します。
4. 最初のリストで、一致するすべてのコンピュータに設定されているプロパティ ([OS] など) を選択します ("検索可能なプロパティ" on page 1433を参照)。

AWSタグを選択した場合は、タグの名前も入力します。

5. 完全一致、類似、または一致しないコンピュータを選択する [演算子](#) を選択します ([次の文字列を含む] など)。

注意: 一部の演算子はすべてのプロパティには使用できません。

6. 検索語句のすべてまたは一部を入力します。

注意: ワイルドカード文字はサポートされていません。

ヒント: 複数の単語を入力した場合、それぞれの単語が個別に比較されるのではなく、1つのフレーズとして比較されます。プロパティの値に別の順序の単語が含まれている場合や、一部の単語しか含まれていない場合は、一致しません。いずれかの単語に一致させるには、[ルールの追加] と [または] をクリックして、別の値を追加します (1つのルールに1つの単語)。

7. コンピュータが複数のプロパティに一致する必要がある場合は、[ルールの追加] と [および] をクリックします。手順4~6を繰り返します。

さらに複雑なスマートフォルダを作成するには、複数の検索条件を連結します。[グループの追加] をクリックし、[および] または [または] をクリックします。Repeat steps 4-7.

たとえば、オンプレミスとクラウド (AWS、Azure、vCloudなど) の両方にLinuxコンピュータが配置されている場合は、次の条件に基づく3つのルールグループを使用して、それらのコンピュータをすべて含むスマートフォルダを作成できます。

- a. ローカルの物理コンピュータのOS
- b. AWSタグ
- c. vCenterまたはvCloud名

および または + ルールグループの追加

および または + ルールの追加 × グループの削除

OS 次の文字列を含む Linux ×

OS 次の文字列を含む Red Hat ×

および または + ルールの追加 × グループの削除

AWS タグ タグキー: 次の文字列に等しい OS タグ値: 次の文字列: Amazon Linux ×

AWS タグ タグキー: 次の文字列に等しい OS タグ値: 次の文字列: Red Hat ×

および または + ルールの追加 × グループの削除

vCenter 名前 次の文字列を含む Linux ×

vCenter 名前 次の文字列を含む Red Hat ×

ヒント: スマートフォルダを保存する前にクエリの結果をテストするには、[プレビュー]をクリックします。

8. [保存] をクリックします。
9. 確認するため、新しいスマートフォルダをクリックします。想定するコンピュータがすべて含まれていることを確認しま

す。


ヒント: スマートフォルダの処理速度を上げるには、不要なAND演算を削除し、サブフォルダの階層を減らします。クエリが複雑なほどパフォーマンスは低下します。

また、クエリに一致すべきでないコンピュータが除外されていることも確認してください。スマートフォルダのクエリを編集する必要がある場合は、そのスマートフォルダをダブルクリックします。

注意: アカウントの役割に権限がない場合は、一部のコンピュータが表示されないか、またはコンピュータのプロパティを編集できません。詳細については、"[ユーザロールの定義](#)" on page 1382を参照してください。

スマートフォルダを編集する

スマートフォルダのクエリを編集する必要がある場合は、そのスマートフォルダをダブルクリックします。

検索条件のルールまたはルールグループを並べ替えるには、ルールまたはグループにカーソルを合わせ、カーソルがに変わったら、ルールまたはグループを目的の位置までドラッグします。

スマートフォルダのクローンを作成する

既存のスマートフォルダを新しいスマートフォルダのテンプレートとして複製および変更するには、元のスマートフォルダを右クリックして [スマートフォルダの複製] を選択します。

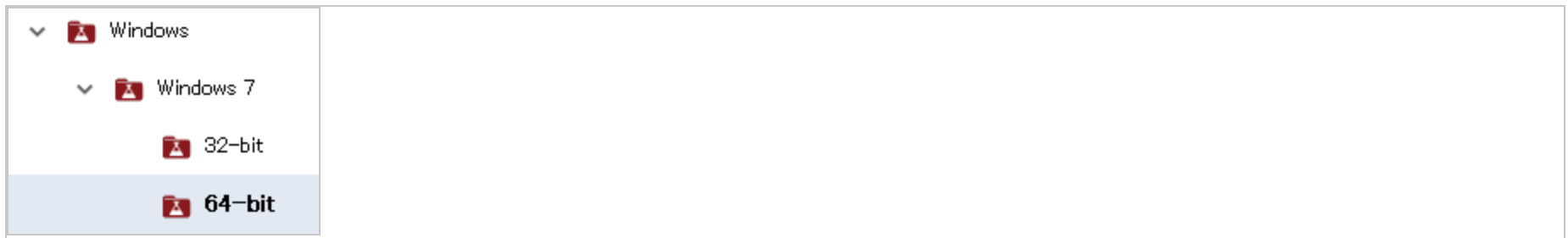
サブフォルダを使用して検索を絞り込む

サブフォルダを使用して、スマートフォルダの検索結果を絞り込むことができます。

スマートフォルダは、10階層までネストできます。

- スマートフォルダ1
 - サブフォルダ2
 - サブフォルダ3 ...(以下同様)

たとえば、すべてのWindowsコンピュータを対象としたスマートフォルダがあり、32ビットまたは64ビットのWindows 7を実行するコンピュータに絞り込みたいとします。そのためには、親である「Windows」フォルダの下にWindows 7用の子スマートフォルダを作成します。次に、その「Windows 7」フォルダの下に2つの子スマートフォルダ（「32ビット」と「64ビット」）を作成します。



1. スマートフォルダを右クリックし、[子スマートフォルダの作成] を選択します。
2. 子スマートフォルダのクエリグループまたはルールを編集します。[保存] をクリックします。
3. 新しいスマートフォルダをクリックします。想定するコンピュータがすべて含まれていることを確認します。また、クエリに一致すべきでないコンピュータが除外されていることも確認してください。

サブフォルダを自動作成する

注意: AWSコンピュータにのみ該当します。

Amazonのクラウドを使用する場合は、子フォルダを手動で作成する代わりに、AWSタグの値ごとにサブフォルダを自動で作成できます。コンピュータにAWSタグを適用する方法については、Amazonのガイドの [「Amazon Ec2リソースにタグを付ける」](#) を参照してください。

注意: 親フォルダの下にある手動で作成された既存の子フォルダが、AWSタグベースのサブフォルダで置き換えられます。

1. スマートフォルダグループの下にある [特定のAWSタグキーの値ごとにサブフォルダを自動的に作成:] チェックボックスをオンにします。
2. AWSタグの名前を入力します。このタグの値ごとにサブフォルダが自動作成されます。
3. [保存] をクリックします。

ヒント: 使用されなくなったAWSタグ値がある場合は、空のサブフォルダが表示されることがあります。これを削除するには、スマートフォルダを右クリックし、[スマートフォルダの同期] を選択します。

検索可能なプロパティ

プロパティとは、検索する一部またはすべてのコンピュータが持つ属性です。スマートフォルダには、選択したプロパティがあり、その値が一致するコンピュータが表示されます。

注意: 検索では、vCenter、AWS、Azureなどではなく、*Deep Security Manager*に表示されているプロパティを正確に入力してください。値が正確でないとスマートフォルダのクエリは一致しません。

プロパティの正確な値を確認するには、(特に指定のないかぎり) [コンピュータ] に進み、左側のナビゲーションペインを確認します。

一般

プロパティ	説明	データタイプ	例
ホスト名	コンピュータのホスト名です。[コンピュータ]→[詳細]の[ホスト名]に表示されます。	文字列	ca-staging-web1
コンピュータの表示名	Deep Securityでのコンピュータの表示名 (存在する場合) です。[コンピュータ]→[詳細]の[表示名]に表示されます。	文字列	nginxTest

プロパティ	説明	データタイプ	例
フォルダ名	コンピュータに割り当てられているグループです。	文字列	US-East
OS	コンピュータのOSです。[コンピュータ]→[詳細]の[プラットフォーム]に表示されます。	文字列	Microsoft Windows 7 (64ビット) Service Pack 1 Build 7601
IPアドレス	<p>コンピュータのIPアドレスです。</p> <p>Deep Security ManagerでIPアドレスを見つけることができます。各IPを見つける方法は次のとおりです。</p> <ul style="list-style-type: none"> • [追加]→[AWSアカウントの追加] または [追加]→[Azureアカウントの追加] を使用してDeep Securityに追加されたAWSインスタンスまたはAzure仮想マシン: AWSまたはAzureコンピュータの詳細画面に移動し、[一般] タブの [仮想マシンの概要] セクションまでスクロールします。AWS IPアドレスは次のフィールドで確認できます。 <ul style="list-style-type: none"> • プライベートIPアドレス • パブリックIP (PIP) アドレス <p>注意: [追加]→[コンピュータの追加] を使用してAWSまたはAzureコンピュータを追加した場合、そのIPは物理コンピュータと同じ場所にあります。</p>	IPv4/IPv6アドレス、またはIPv4範囲	172.20.1.5-172.20.1.55 2001:db8:face::5

プロパティ	説明	データタイプ	例
	<ul style="list-style-type: none"> 物理コンピュータ (AWS、Azure、vCenter、vCloud以外): コンピュータの詳細画面に移動し、左側の [インタフェース] をクリックします。 <p>注意: 静的IPアドレスではなく「DHCP」と表示される場合は、スマートフォルダのクエリに一致しません。</p> <ul style="list-style-type: none"> vCenterまたはvCloud 仮想マシン: vCenterコンピュータの詳細画面に移動し、[一般] タブで [仮想マシンの概要] セクションまでスクロールします。vCenterまたはvCloudのIPアドレスは [IPアドレス] フィールドに表示されます。 		
ポリシー	コンピュータに割り当てられているDeep Securityポリシーです。[コンピュータ]→[詳細] に表示されます。	文字列 (ドロップダウンリストのオプション)	ベースポリシー
有効化済み	コンピュータがDeep Security Managerで有効化されているかどうかを示します。[コンピュータ]→[詳細] に表示されます。	ブール	○
Dockerホスト	コンピュータに Docker がインストールされているかどうかを示します。[コンピュータ]→[詳細] に表示されます。	ブール	×
コンピュータの種類	コンピュータの種類です。物理コンピュータ、Amazon EC2インスタンス、Amazon WorkSpaces、vCenter仮想マシン、Azureインスタンス、Azure ARMインスタンスのオプションがあります。	文字列 (ドロップダウンリストのオプション)	例: 物理コンピュータ、Amazon EC2インスタンス

Trend Micro Deep Security On-Premise 12.0

プロパティ	説明	データタイプ	例
前回成功した推奨設定の検索	指定した時間内にコンピュータで推奨設定の検索に成功したかどうかを示します。[コンピュータ]→[詳細]→[一般]→[侵入防御] または [変更監視] または [セキュリティログ監視]→[推奨設定] には、前回の推奨設定の検索の日付および結果が表示されます。	日付演算子ドロップダウンリスト、文字列、日付単位ドロップダウンリスト	次の期間より古い、7、日
Agentの前の通信	指定した期間内にAgentがDeep Security Managerと通信したかどうかを示します。前回の通信日は、[コンピュータ]→[詳細]→[一般]→[前の通信] に表示されます。	日付演算子ドロップダウンリスト、文字列、日付単位ドロップダウンリスト	次の期間より古い、3、日
オフラインのAgent	Agentがオフラインかどうかを示します。これは、[コンピュータ]→[詳細]→[一般]→[前の通信] に [管理対象 (オフライン)] または [オフライン] として表示されます。	ブール	○
ホスト作成日	そのコンピュータがDeep Security Managerに追加された日付です。	文字列 (日付)	2019/03/15

AWS

プロパティ	説明	データタイプ	例
タグ	コンピュータのAWSタグのキー:値のペアです。[コンピュータ]→[詳細]→[概要]→[一般] の [仮想マシンの概要] の下の [クラウドインスタンスのメタデータ] に表示されます。	文字列	タグキー: env タグ値: staging

プロパティ	説明	データタイプ	例
	タグ名とその値を入力します。大文字と小文字が区別されます。		
セキュリティグループ名	コンピュータに関連付けられているAWSセキュリティグループ名です。[コンピュータ]→[詳細]→[概要]→[一般]の[仮想マシンの概要]の下の[セキュリティグループ]に表示されます。	文字列	SecGrp1
セキュリティグループID	コンピュータのAWSセキュリティグループIDです。[コンピュータ]→[詳細]→[概要]→[一般]の[仮想マシンの概要]の下の[セキュリティグループ]に表示されます。	文字列	sg-12345678
AMI ID	コンピュータのAmazon Machine AMI IDです。[コンピュータ]→[詳細]→[概要]→[一般]の[仮想マシンの概要]の下の[AMI ID]に表示されます。	文字列	ami-23c44a56
アカウントID	コンピュータに関連付けられている12桁の AWSアカウントID です。[コンピュータ]の[Amazonアカウント]を右クリックし、[プロパティ]を選択すると表示されます。 コンピュータはサブフォルダに分けて表示されます。	文字列	123456789012

プロパティ	説明	データタイプ	例
アカウント名	<p>コンピュータに関連付けられているAWSアカウントのエイリアスです。[コンピュータ]の[AWSクラウドコネクタ]を右クリックし、[プロパティ]を選択すると表示されます。</p> <p>コンピュータはサブフォルダに分けて表示されます。</p>	文字列	MyAccount-123
リージョンID	<p>コンピュータのAWSリージョン接尾辞です。</p> <p>コンピュータはサブフォルダに分けて表示されます。</p>	文字列	us-east-1
リージョン名	<p>コンピュータに関連付けられているAWSリージョン名です。</p> <p>コンピュータはサブフォルダに分けて表示されます。</p>	文字列	米国東部 (オハイオ)
VPC ID	<p>コンピュータのVirtual Private Cloud (VPC) IDです。</p> <p>エイリアスがある場合はフォルダ名にはエイリアスが使用され、VPC IDはカッコ内に表示されます。エイリアスがない場合は、VPC IDがフォルダ名になります。</p> <p>コンピュータはサブフォルダに分けて表示されます。</p>	文字列	vpc-3005e48a
サブネットID	<p>コンピュータに関連付けられているVirtual Private Cloud (VPC) サブネットIDです。</p>	文字列	subnet-b1c2e468

プロパティ	説明	データタイプ	例
	エイリアスがある場合はフォルダ名にはエイリアスが使用されVPCサブネットIDはカッコ内に表示されます。エイリアスがない場合は、VPCサブネットIDがフォルダ名になります。 コンピュータはサブフォルダに分けて表示されます。		
ディレクトリID	Amazon WorkSpacesに関連付けられたユーザーエントリがあるAWSディレクトリのIDです。ディレクトリIDは [コンピュータ]→[詳細]→[仮想マシンの概要] の [Workspaceディレクトリ] フィールドに表示されます。フィールドの形式は<directory_alias>(<directory_ID>) です。例: myworkspacedir(d-9367232d89)	文字列	d-9367232d89

Azure

プロパティ	説明	データタイプ	例
サブスクリプション名	<p>注意: Deep Security Manager 12.0以降、Subscription名は収集されなくなりました。以前のバージョンのマネージャから情報が取得された場合は、プロパティのドロップダウンリストに引き続き表示されます。</p> <p>コンピュータに関連付けられているAzureサブスクリプションアカウントIDです。[コンピュータ] の [Azure] を右クリックし、[プロパティ] を選択すると表示されます。</p>	文字列	MyAzureAccount

プロパティ	説明	データタイプ	例
	コンピュータはサブフォルダに分けて表示されます。		
リソースグループ	コンピュータに関連付けられているリソースグループです。	文字列	MyResourceGroup

vCenter

プロパティ	説明	データタイプ	例
名前	コンピュータに関連付けられているvCenterです。 コンピュータはサブフォルダに分けて表示されます。	文字列	vCenter - lab13-vc.example.com
データセンター	コンピュータに関連付けられているvCenterデータセンターです。 コンピュータはサブフォルダに分けて表示されます。	文字列	lab13-datacenter
フォルダ	コンピュータのvCenterフォルダです。 コンピュータはサブフォルダに分けて表示されます。	文字列	db_dev
親ESXのホスト名	コンピュータのゲスト仮想マシンが実行されているESXiハイパーバイザのホスト名です。[コンピュータ]に表示されます。	文字列	lab13-esx2.example.com
カスタム属性	コンピュータに割り当てられているvCenterカスタム属性です。[コンピュータ]→[詳細]の[仮想マシンの概要]に表示されます。	文字列 (カンマ区切り)	env, production

プロパティ	説明	データタイプ	例
		の属性名と値)	

vCloud

プロパティ	説明	データタイプ	例
名前	コンピュータに関連付けられているvCloudです。 コンピュータはサブフォルダに分けて表示されます。	文字列	vCloud-lab23
データセンター	コンピュータに関連付けられているvCloudデータセンターです。 コンピュータはサブフォルダに分けて表示されます。	文字列	lab13- datacenter
vApp	コンピュータに関連付けられているvCloudデータセンターフォルダです。 コンピュータはサブフォルダに分けて表示されます。	文字列	db_dev

フォルダ

プロパティ	説明	データタイプ	例
名前	Microsoft Active DirectoryまたはLDAPディレクトリのホスト名です。 コンピュータはサブフォルダに分けて表示されます。	文字列	ad01.example.com
フォルダ	コンピュータのMicrosoft Active DirectoryまたはLDAPフォルダ名です。 コンピュータはサブフォルダに分けて表示されます。	文字列	台

演算子

スマートフォルダの演算子は、一致するコンピュータが検索語句と同一のプロパティ値、類似のプロパティ値、または異なるプロパティ値を持つかどうかを示します。すべての演算子をすべてのプロパティに使用できるわけではありません。

演算子	説明	使用例
次の文字列に等しい	完全に一致するコンピュータのみが検出されます。	「OS」プロパティで「Windows」を指定した検索クエリでは、「Windows 7」または「Microsoft Windows」のコンピュータは検出されません。
次の文字列に等しくない	一致しないコンピュータがすべて検出されます。	「OS」プロパティで「Amazon Linux (64ビット)」を指定した検索クエリでは、Amazon Linux 64ビット以外のすべてのコンピュータが検出されます。
次の文字列を含む	検索語句を含むコンピュータがすべて検出されます。	「IPアドレス」プロパティで「203.0.113」を指定した検索クエリでは、203.0.113.xxxサブネット上にあるすべてのコンピュータが検出されます。
次の文字列を含まない	検索語句を含まないコンピュータが検出されます。	「OS」プロパティで「Windows」を指定した検索クエリでは、OS名に「Windows」がないコンピュータが検出されます。
任意の値	選択したプロパティのすべてのコンピュータが検出されます。	「グループ名」プロパティの検索クエリでは、そのグループに属するすべてのコンピュータが検出されます。
範囲内	指定した開始範囲と終了範囲の間のすべてのコンピュータが検出されます。	「IPアドレス」プロパティで開始範囲に「10.0.0.0」、終了範囲に「10.255.255.255」を指定した検索クエリでは、IPアドレスが10.0.0.0～10.255.255.255の範囲にあるすべてのコンピュータが検出されます。

演算子	説明	使用例
範囲外	指定した開始範囲と終了範囲の間にないすべてのコンピュータが検出されます。	「IPアドレス」プロパティで開始範囲に「10.0.0.0」、終了範囲に「10.255.255.255」を指定した検索クエリでは、IPアドレスが10.0.0.0～10.255.255.255の範囲外のすべてのコンピュータが検出されます。
はい	選択したプロパティのすべてのコンピュータが検出されます。	「Docker」プロパティで「はい」を選択した検索クエリでは、Dockerサービスが実行されているすべてのコンピュータが検出されます。
いいえ	選択したプロパティを持たないすべてのコンピュータが検出されます。	「Docker」プロパティで「いいえ」を選択した検索クエリでは、Dockerサービスが実行されていないすべてのコンピュータが検出されます。
次の期間より古い	プロパティで指定した日付よりも前のすべてのコンピュータが検出されます。 日、週、時間、または分といった演算子と組み合わせて使用します。	[前回成功した推奨設定の検索] プロパティで「次の期間より古い」、「7」、「日」を指定した検索クエリでは、8日以前に推奨設定の検索に成功したコンピュータが検出されます。
次の期間より新しい	プロパティで指定した日付よりも後のすべてのコンピュータが検出されます。 日、週、時間、または分といった演算子と組み合わせて使用します。	[前回成功した推奨設定の検索] プロパティで「次の期間より新しい」、「1」、「月」を指定した検索クエリでは、1か月よりも前に推奨設定の検索に成功したコンピュータが検出されます。
なし	プロパティと一致しないすべて	[前回成功した推奨設定の検索] プロパティで「なし」を指定した検索クエリで

演算子	説明	使用例
	てのコンピュータが検出されます。	は、推奨設定の検索に成功したことの無いコンピュータが検出されます。

アクティブなDeep Security Managerノードの表示

すべてのアクティブなDeep Security Managerノードのリストを表示するには、[管理]→[Managerノード]の順に選択します ("複数のノードでのDeep Security Managerの実行" on page 270も参照)。

Managerノードの1つの詳細を表示するには、リスト内の行をダブルクリックします。[プロパティ]ウィンドウが表示されます。

- ホスト名: Deep Security Managerがインストールされているコンピュータのホスト名
- 説明: Managerノードの説明。
- パフォーマンスプロファイル: Deep Security Managerのパフォーマンスは、CPU数、使用可能な帯域幅、データベースの応答性など、いくつかの要因に影響されます。Managerのパフォーマンスの初期設定は、多くのインストール環境に適するように設計されています。ただし、パフォーマンスが低下する場合は、1つ以上のDeep Security Managerノードに割り当てられているパフォーマンスプロファイルを変更するよう、サポート担当者から提案されることがあります(設定の変更はサポート担当者が必要と判断した場合にのみ行ってください)。

注意: 以下の各表の「エンドポイントのディスクおよびネットワークにおける同時ジョブ数」には、不正プログラム検索、変更監視検索、攻撃の予兆検索、コンピュータへのポリシーのアップデートの送信、およびセキュリティアップデートの配布が含まれます。

- アグレッシブ: このパフォーマンスプロファイルは、Deep Security Managerが専用サーバにインストールされている場合に適しています。たとえば、次の表にアグレッシブパフォーマンスプロファイルを使用している場合に、同時処理が各Managerノードにどのように分散されるかを示します。

処理	2コアシステム	8コアシステム
有効化	10	20
アップデート	25	50
推奨設定の検索	5	12
ステータスの確認	100	100
AgentまたはApplianceからのハートビート	アクティブ20 処理待ち40	アクティブ50 処理待ち40
エンドポイントのディスクおよびネットワークにおける同時ジョブ数	50	50
ESXi1台あたりのエンドポイントのディスクおよびネットワークにおける同時ジョブ数	3	3

- 標準: このパフォーマンスプロファイルは、Deep Security Managerとデータベースが同じコンピュータ上にある場合に適しています。たとえば、次の表に標準パフォーマンスプロファイルを使用している場合に、同時処理が各Managerノードにどのように分散されるかを示します。

処理	2コアシステム	8コアシステム
有効化	5	10
アップデート	16	46
推奨設定の検索	3	9
ステータスの確認	65	100
AgentまたはApplianceからのハートビート	アクティブ20 処理待ち40	アクティブ50 処理待ち40
エンドポイントのディスクおよびネットワークにおける同時ジョブ数	50	50
ESXi1台あたりのエンドポイントのディスクおよびネットワークにおける同時ジョブ数	3	3

- 無制限のディスクおよびネットワークの使用量: この設定は「アグレッシブ」と同じですが、コンピュータのディスクおよびネットワークを使用する場合の制限はありません。

処理	2コアシステム	8コアシステム
有効化	10	20
アップデート	25	25
推奨設定の検索	5	12

処理	2コアシステム	8コアシステム
ステータスの確認	100	100
AgentまたはApplianceからのハートビート	アクティブ20 処理待ち40	アクティブ50 処理待ち40
エンドポイントのディスクおよびネットワークにおける同時ジョブ数	無制限	無制限
ESXi1台あたりのエンドポイントのディスクおよびネットワークにおける同時ジョブ数	無制限	無制限

注意: 同時にアップデートできるコンポーネントの数は、すべてのパフォーマンスプロファイルで、Relayグループあたり100個に制限されています。

- ステータス: 現在ログインしているDeep Security Managerノードから見てノードの状態がオンラインかどうか、アクティブかどうかを示します。
- オプション: 廃止するManagerノードを選択できます。ノードを廃止するには、そのノードが、アンインストール済みまたはサービス停止中であり、オフラインになっている必要があります。

詳細なシステム設定のカスタマイズ

上級者向けのいくつかの機能は、[管理]→[システム設定]→[詳細] から設定できます。

ヒント: システム設定の変更は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド [「Configure Policy, Computer, and System Settings」](#) を参照してください。

プライマリテナントアクセス

初期設定では、プライマリテナントはDeep Security環境にアクセスできます。

ただし、プライマリテナントが該当する環境の [プライマリテナントアクセス] の設定を有効にしている場合、プライマリテナントによるDeep Security環境へのアクセスを禁止したり、指定した期間だけアクセスを許可したりできます。

ロードバランサ

注意: FIPSモードが有効な場合、ロードバランサ設定は使用できません。"[FIPS 140-2のサポート](#)" on page 1457を参照してください。

Agentには、Deep Security ManagerとDeep Security Relayのリストが設定されています。ManagerやRelayが複数インストールされた環境で[ロードバランサ](#)が配置されていない場合、Agentはランダムなラウンドロビンシーケンスを使用してManagerやRelayに自動的に接続します。

ネットワークのスケラビリティを高めるには、ManagerやRelayの手前にロードバランサを配置すると効果的です。ロードバランサのホスト名と[ポート番号](#)を設定すると、Agentで現在使用されているIPアドレスまたはホスト名とポート番号がオーバーライドされます。

スクリプトジェネレータは、接続しているDeep Security Managerのアドレスを使用します。そのため、いずれかのDeep Security Managerノードで障害が発生した場合やメンテナンスやアップグレードのために停止しているときもスクリプトは機能します。

注意: Agentのハートビートポート番号とのSSLまたはTLSセッションでは相互認証が使用されるため、このセッションがロードバランサで終端しないようにする必要があります。SSLインスペクションが終端する場合 (SSLオフロードを使用する場合など)、セッションが中断します。

マルチテナントモード

1. マルチテナントモードの有効化 を選択します。
2. 表示されるウィザードで、マルチテナントのアクティベーションコード を入力し、次へ をクリックします。
3. ライセンスモードとして次のいずれかを選択します。
 - プライマリテナントからライセンスを継承: すべてのテナントでプライマリテナントと同じライセンスを使用します。
 - テナント単位のライセンス: 初回ログイン時にテナント自身がライセンスを入力します。

4. 次へ をクリックします。

Deep Security Managerプラグイン

プラグインとは、Deep Security Manager用のモジュール、レポート、およびその他のアドオンを指します。トレンドマイクロでは、新規または追加のバージョンのプラグインを必要に応じて生成し、自己インストール型のパッケージとして配布する場合があります。

SOAP WebサービスAPI

従来のSOAP API Webサービスを有効または無効にします。WSDL (Web Services Description Language) には、画面のパネルに表示されるURLからアクセスできます。APIの詳細については、"[Deep Security APIを使用したタスクの自動化](#)" on page 478を参照してください。

注意: WebサービスAPIにアクセスするには、適切なアクセス権限を持つ役割をユーザに割り当てる必要があります。役割を設定するには、[管理]→[ユーザ管理]→[役割] の順に選択し、役割のプロパティを開いて [WebサービスAPIへのアクセスを許可] を選択します。

ステータス監視API

従来のREST APIのステータス監視APIを有効または無効にします。このAPIは、Deep Security Manager (個々のManagerノードを含む) のステータス情報 (CPUやメモリの使用率、処理待ちのジョブ数、データベースの合計サイズおよびテナント固有のデータベースサイズなど) のクエリに使用されます。APIの詳細については、"[Deep Security APIを使用したタスクの自動化](#)" on page 478を参照してください。

エクスポート

エクスポートファイルの文字エンコード:Deep Security Managerからデータファイルをエクスポートするときに使用する文字エンコードを指定します。このエンコードは選択した言語の文字をサポートしている必要があります。

エクスポートする診断パッケージの言語:サポート担当者から、Deep Security診断パッケージを生成して送信するよう求められる場合があります。この設定は診断パッケージの言語を指定します。診断パッケージは [管理]→[システム情報] で生成します。

Whois

Whoisは、ログに記録された侵入防御イベントやファイアウォールイベントを確認する際に、IPアドレスに関連付けられたドメイン名の確認に使用できます。検索URLを次のように入力します。[IP] には、検索するIPアドレスを指定します。

例: [http://reports.internic.net/cgi/whois?whois_nic=\[IP\]&type=nameserver](http://reports.internic.net/cgi/whois?whois_nic=[IP]&type=nameserver)

ライセンス

新規ユーザに対してライセンス許可されていないモジュールを非表示:以降に作成されるユーザに対して、ライセンス許可されていないモジュールをグレー表示ではなく非表示にする場合に指定します。この設定は、[管理]→[ユーザ管理]→[ユーザ]→[プロパティ] 画面の設定でユーザごとに上書きできます。

保存済みの検索キャッシュ設定のリストを表示するには、[検索キャッシュ設定の表示] をクリックします。検索キャッシュ設定は、仮想化された環境における不正プログラム検索および変更の検索の効率を最大化するためにVirtual Applianceで使用される設定です。詳細については、"[Virtual Applianceの検索キャッシュ](#)" on page 899を参照してください。

推奨設定の検索中のCPU使用率

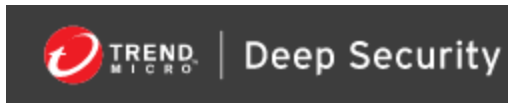
推奨設定の検索に使用するCPUリソース量を制御します。CPU使用率が想定以上に高くなった場合は、設定を下げて状況を改善するようにしてください。その他のパフォーマンス制御については、[管理]→[Managerノード]→[プロパティ]→[パフォーマンスプロファイル] を参照してください。

NSX

Deep SecurityがVMware NSX環境の仮想マシンの保護に使用され、複数のDeep Security Managerノードにインストールされている場合に、どのDeep Security ManagerノードがNSX Managerと通信するかを決定します。Deep SecurityとNSX環境の統合の詳細については、"[Deep Securityのインストールまたはアップグレード](#)" on page 223を参照してください。複数のDeep Security Managerノードの詳細については、"[複数のノードでのDeep Security Managerの実行](#)" on page 270を参照してください。

ロゴ

ログイン画面、Deep Security ManagerのGUIの右上、およびレポートの上部に表示されるDeep Securityのロゴを置き換えることができます。使用できるのは、幅320ピクセル×高さ35ピクセル、ファイルサイズ1MB未満のPNGファイルです。Deep Security Managerのinstallfilesディレクトリにテンプレートが用意されています。



[ロゴのインポート] をクリックして独自のロゴをインポートするか、または [ロゴのリセット] をクリックして初期設定のロゴにリセットします。

Manager AWS ID

クロスアカウントアクセスを設定できます。次のいずれかを選択します。

- Managerインスタンスロールを使用: クロスアカウントアクセスを設定するためのより安全なオプションです。このオプションを選択する前に、sts:AssumeRole権限を設定したポリシーをDeep Security Managerのインスタンスロールに関連付けておきます。このオプションは、Deep Security Managerにインスタンスロールがない場合は表示されません。また、Azure MarketplaceまたはオンプレミスインストールのDeep Security Managerを使用している場合も表示されません。

- AWSアクセスキーを使用: このオプションを選択する場合は、キーを作成し、sts:AssumeRole権限を設定したポリシーを関連付けておきます。オプションを選択したら、[アクセスキー]と[秘密鍵]を入力します。このオプションは、Azure MarketplaceまたはオンプレミスインストールのDeep Security Managerを使用している場合は表示されません。

アプリケーションコントロール

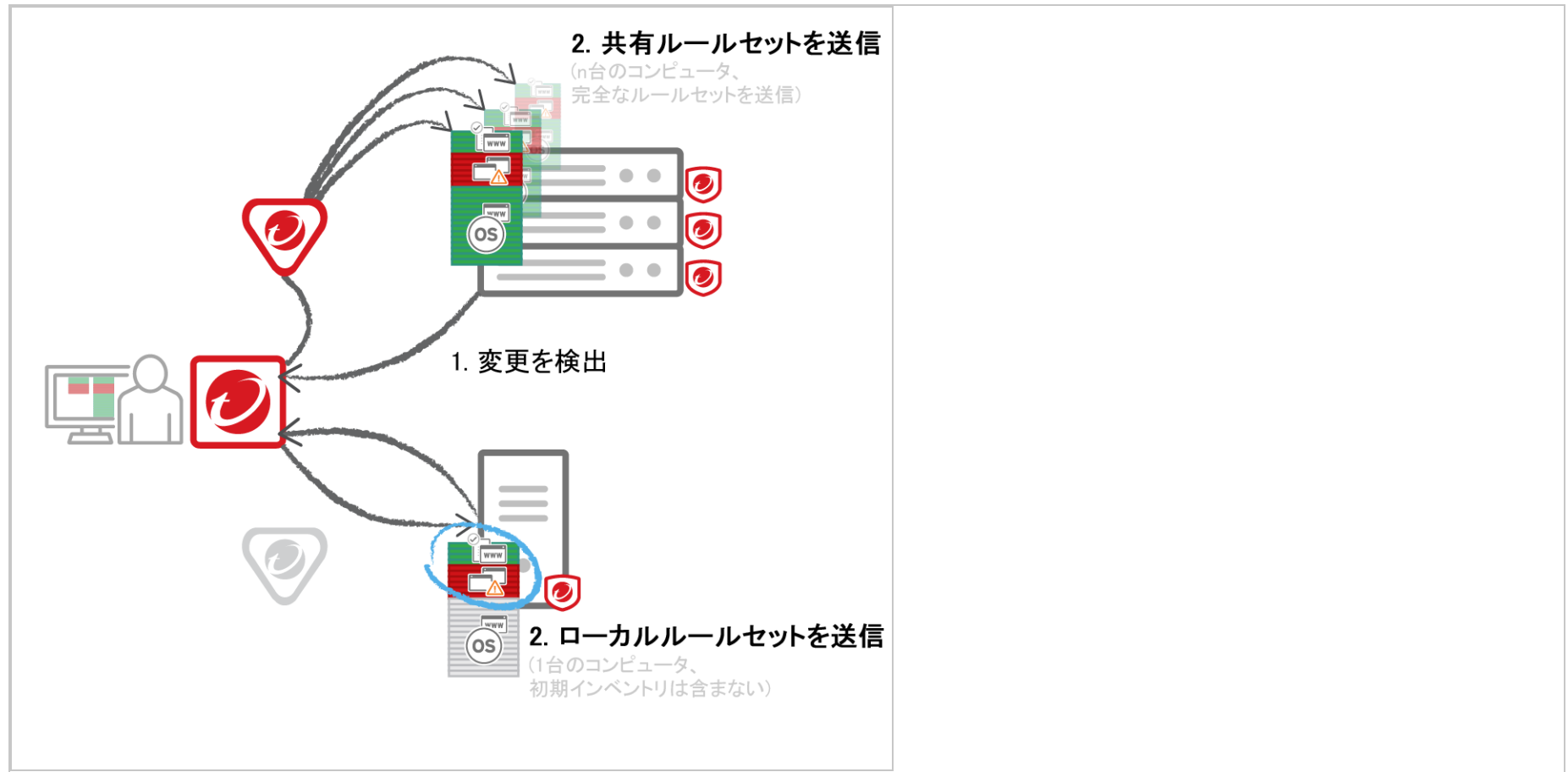
[アプリケーションコントロール](#)ルールセットを作成または変更するたびに、使用するすべてのコンピュータに配布する必要があります。共有ルールセットはローカルルールセットよりも大きくなります。また、共有ルールセットはさまざまなサーバにも適用されることがあります。ルールセットをManagerから同時に直接ダウンロードすると、負荷が大きくなり、パフォーマンスが低下する可能性があります。グローバルルールセットの注意事項も同じです。

Deep Security Relayを使用すると、この問題を解決できます。(Relayの設定の詳細については、「["Relayによるセキュリティとソフトウェアのアップデートの配布" on page 438](#)」を参照してください。)

マルチテナント環境を使用しているかどうかによって、手順が異なります。

単一テナント環境

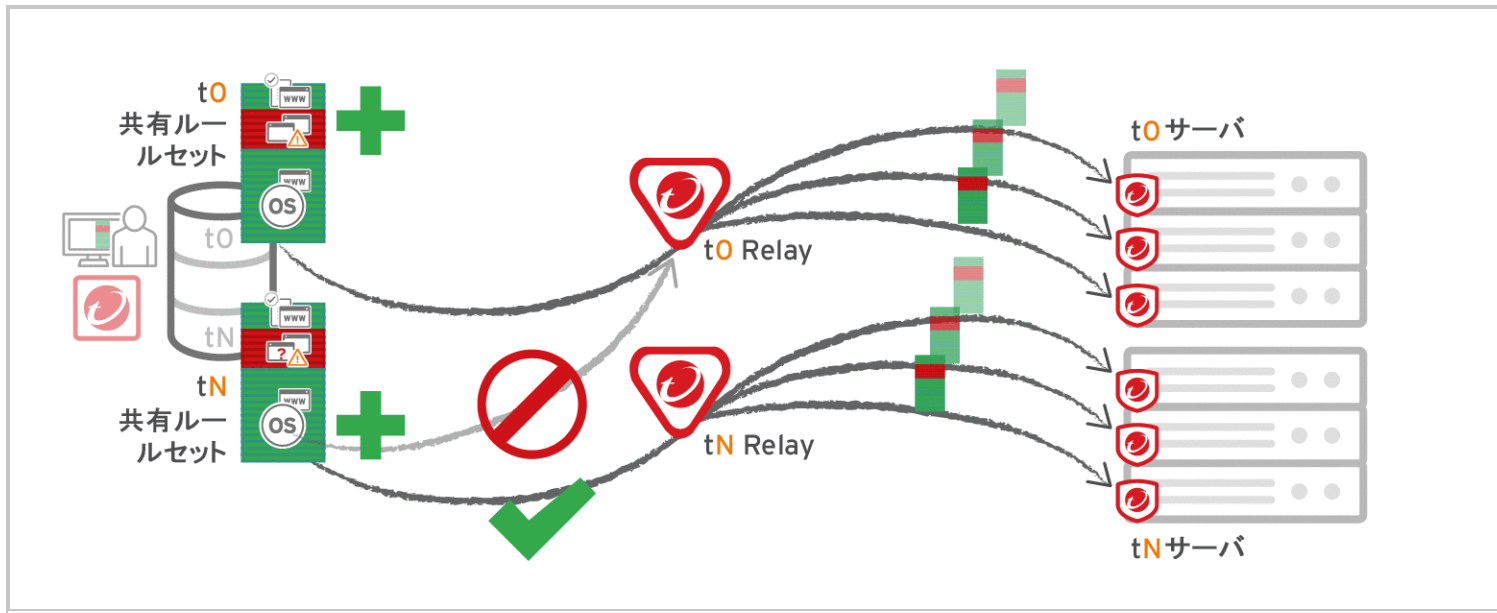
[管理]→[システム設定]→[詳細]の順に選択し、[アプリケーションコントロールルールセットをRelayから提供する]を選択します。



マルチテナント環境

プライマリテナント (t0) は他のテナント (tN) の設定にアクセスできないため、t0 RelayにはtNアプリケーションコントロールルールセットが設定されません。(IPSのような他の機能には、テナントではなくトレンドマイクロのルールセットが設定されるため、この注意事項は関係ありません。)

他のテナント (tN) は独自の[Relayグループ](#)を作成してから [アプリケーションコントロールルールセットをRelayから提供する] を選択する必要があります。



警告:

Relayの使用前に使用環境との互換性を確認します。以前にダウンロードしたルールセットがAgentに現在適用されていない場合、新しいアプリケーションコントロールルールを受信しないと、コンピュータはアプリケーションコントロールで保護されません。アプリケーションコントロールルールセットのダウンロードに失敗した場合は、[ルールセットダウンロード失敗イベント](#)が、[Manager](#)および[Agent](#)で記録されます。

Relayのパフォーマンスが変化したり、アプリケーションコントロールルールセットのダウンロードが中断し、Relayが必要になる場合があります。プロキシの場所、マルチテナント、グローバル/共有ルールセットかローカルルールセットかによって異なります。

必須	パフォーマンス向上	パフォーマンス低下	有効にしない
[Agent]→[プロキシ]	共有ルール	ローカル	プライマリ以外のテナント (tN) が初期設定のプライマリ (t0) Relayが

必須	パフォーマンス向上	パフォーマンス低下	有効にしない
<p>シ]→[Manager]</p> <p>注意: Deep Security Agent 10.0以前では、プロキシ経由でのRelayへの接続がサポートされていませんでした。プロキシが原因でルールセットダウンロードに失敗した場合、およびAgentがRelayまたはManagerにアクセスするためのプロキシを必要とする場合は、次のいずれかを実行する必要があります。</p>	<p>セット</p> <p>グローバル</p> <p>ルールセット</p>	<p>ルールセット</p>	<p>ループを使用する場合のマルチテナント設定:</p> <ul style="list-style-type: none"> • [Agent (tN)]→[DSR (t0)]→[DSM (tN)] • [Agent (tN)]→[プロキシ]→[DSR (t0)]→[DSM (tN)]

必須	パフォーマンス向上	パフォーマンス低下	有効にしない
<ul style="list-style-type: none">• Agentソフトウェアをアップデートして、プロキシを設定する。• プロキシをバイパスする。• Relayを追加して、[アプリケーションコントロールルールセットをRelayから提供する]を選択する。			

コンプライアンスの推進

トレンドマイクロは、複数のセキュリティコントロールを1つの製品に統合してコンプライアンスを推進し、包括的な監査とサポートを提供します。詳細については、トレンドマイクロのWebサイトにある [「Regulatory Compliance」](#) を参照してください。

要件に応じて、次を参照してください。

- "Deep SecurityによるPCI DSS要件への対応" below
- "Common Criteriaの設定" on the next page
- "GDPR" on the next page
- "FIPS 140-2のサポート" on the next page
- AWS Config Rulesの設定
- "Deep Securityでの脆弱性管理検索トラフィックのバイパス" on page 1470
- "Deep SecurityでのTLS 1.2の使用" on page 1472
- "TLS 1.2の強力な暗号化スイートの有効化" on page 1491

Deep SecurityによるPCI DSS要件への対応

Payment Card Industry Data Security Standard (PCI DSS) は、カード所有者のデータの安全を促進する情報セキュリティ基準です。Deep Securityを使用すると、PCI DSSに従ってPCIデータを保護できます。

ヒント: 各種方法に関する情報:

- AWSでPCI DSSへの準拠を推進する方法については、[「Accelerating PCI Compliance in AWS using Deep Security」](#) を参照してください。
- TLS 1.2を有効にしてPCIに準拠する方法については、["Deep SecurityでのTLS 1.2の使用" on page 1472](#)または["TLS 1.2の強力な暗号化スイートの有効化" on page 1491](#)を参照してください。

Common Criteriaの設定

Deep Security 20は、Common Criteria認定を取得する最新バージョンです。詳細については、このページの上部にあるドロップダウンリストに移動し、Deep Security 20 Long-Term Supportを選択してください。

GDPR

欧州連合 (EU) の一般データ保護規則 (GDPR) では、EU市民のデータを処理している世界各地の組織に対し、データ処理の管理方法の見直しとデータ保護を強化するための計画の実施が義務付けられています。GDPRとトレンドマイクロの詳細については、[トレンドマイクロのGDPRへの準拠](#)に関するWebサイトを参照してください。

Deep Securityでの個人情報データの収集の詳細については、"[プライバシーと個人データの収集に関する規定](#)" on page 78を参照してください。

FIPS 140-2のサポート

連邦情報処理標準 (FIPS) は暗号化モジュールの一連の標準です。FIPSの詳細情報については、[アメリカ国立標準技術研究所 \(NIST\) のWebサイト](#)を参照してください。Deep Securityには、FIPS 140-2標準に準拠するモードで暗号化モジュールを実行できる設定が用意されています。トレンドマイクロは、[Java暗号化モジュール](#)と[ネイティブ暗号化モジュール \(OpenSSL\)](#) の認証を取得しています。

FIPS以外のモードとFIPSモードで実行するDeep Securityインストールにはいくつかの違いがあります ("[FIPSモードでDeep Securityを操作する場合の違い](#)" on the next pageを参照)。

ヒント: Deep Security Manager SSL証明書を置き換える場合は、置き換えてからFIPSモードを有効にします。FIPSモードの有効化後に証明書を置き換える必要がある場合は、FIPSモードを無効にし、"[Deep Security Manager TLS証明書の置き換え](#)" on page 1057の手順を実行してから、FIPSモードを再び有効にします。

FIPS 140-2モードでDeep Securityを操作するには、次の手順を実行する必要があります。

1. ["FIPSモードでDeep Securityを操作する場合の違い"](#) [below](#)を参照して、必要なDeep Security機能がFIPS 140-2モードで操作する場合に利用可能になるようにします。
2. Deep Security ManagerおよびDeep Security Agentが["FIPSモードのシステム要件"](#) [on the next page](#)に一致していることを確認します。
3. ["Deep Security ManagerでFIPSモードを有効にする"](#) [on page 1460](#)。
4. Deep Security ManagerはSSLを使用して外部サービス (Active Directory、vCenter、またはNSX Managerなど) に接続する必要がある場合は、["FIPSモードで外部サービスに接続する"](#) [on page 1461](#)を参照してください。
5. ["保護しているコンピュータのOSのFIPSモードを有効にする"](#) [on page 1462](#)。
6. ["保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする"](#) [on page 1462](#)
7. ["Deep Security Virtual ApplianceでFIPSモードを有効にする"](#) [on page 1463](#)。
8. RHEL 7.0 GAなど、Linuxカーネルのいくつかのバージョンでは、FIPSモードを有効にするためにSecure Bootを有効にする必要があります。手順については、["Agent向けのLinux Secure Bootのサポート"](#) [on page 427](#)を参照してください。

また、このセクションでは、["FIPSモードを無効にする"](#) [on page 1469](#)手順についても説明します。

FIPSモードでDeep Securityを操作する場合の違い

次のDeep Security機能は、FIPSモードで操作する場合には使用できません。

- ["VMware vCloudでホストされる仮想マシンの追加"](#) [on page 545](#)の説明に従った、VMware vCloudでホストされた仮想マシンへの接続。また、[管理]→[システム設定]→[Agent]→[AgentレスによるvCloud保護] 設定も使用できません。
- マルチテナント環境
- ロードバランサ設定 ([管理]→[システム設定]→[詳細]→[ロードバランサ])
- Deep Security Scanner (SAP Netweaverに統合)
- Connected Threat Defense機能

Trend Micro Deep Security On-Premise 12.0

- SAML 2.0を介したIDプロバイダサポート
- SMTPを設定する場合、STARTTLSオプションを使用できません。

FIPSモードのシステム要件

Deep Security Managerの要件

FIPSモードを有効にしたDeep Security Managerの要件は、次の例外を除き、["システム要件" on page 184](#)の記載内容と同じです。

サポートは次のOSに限定されます。

- Red Hat Enterprise Linux 7 (64ビット)
- Windows Server 2016 (64ビット)
- Windows Server 2012または2012 R2 (64ビット)

サポートは次のデータベースに限定されます。

- PostgreSQL 9.6 (["PostgreSQLデータベースでFIPSモードを使用する" on page 1463](#)を参照)
- Microsoft SQL Server 2016 Enterprise Edition (["Microsoft SQL ServerデータベースでFIPSモードを使用する" on page 1467](#)を参照)
- Microsoft SQL Server 2014 Enterprise Edition (["Microsoft SQL ServerデータベースでFIPSモードを使用する" on page 1467](#)を参照)
- Microsoft SQL Server 2012 Enterprise Edition (["Microsoft SQL ServerデータベースでFIPSモードを使用する" on page 1467](#)を参照)

注意: SSL接続でFIPSモードを有効にしても、Oracle Databaseはサポートされません。

注意: Microsoft SQL Serverの名前付きパイプはサポートされません。

Deep Security Agentの要件

FIPSモードを有効にしたDeep Security Agentの要件は、"[システム要件](#)" on page 184の記載内容と同じです。FIPSモードは、一部のOSのみでサポートされています。この機能をサポートしているOSについては、"[各プラットフォームでサポートされている機能](#)" on page 183を参照してください。

Deep Security Virtual Applianceの要件

Virtual ApplianceでFIPSモードをサポートするための要件は、次のとおりです。

- Deep Security Manager 11.0 Update 3以降
- Deep Security Virtual Appliance 10.0または11.0以降
- Deep Security Agent 11.0 for RedHat_EL7以降 (Applianceの組み込みのAgentとして使用されます)

Applianceのシステム要件の詳細については、"[システム要件](#)" on page 184を参照してください。

Deep Security ManagerでFIPSモードを有効にする

WindowsでDeep Security ManagerのFIPSモードを有効にする

1. Microsoft管理コンソールの [サービス] 画面を使用して「Trend Micro Deep Security Manager」サービスを停止します。
2. Windowsコマンドラインで、Deep Security Managerの作業用フォルダ (例: `C:\Program Files\Trend Micro\Deep Security Manager`) に移動します。
3. 次のコマンドを入力してFIPSモードを有効にします。

```
dsm_c -action enablefipsmode
```

4. Deep Security Managerサービスを再起動します。

LinuxでDeep Security ManagerのFIPSモードを有効にする

1. Deep Security Managerコンピュータでコマンドラインを開き、`/opt/dsm`などのDeep Security Managerの作業フォルダに移動します。
2. 次のコマンドを入力してDeep Security Managerサービスを停止します。

```
service dsm_s stop
```

3. 次のコマンドを入力してFIPSモードを有効にします。

```
dsm_c -action enablefipsmode
```

4. 次のコマンドを入力してDeep Security Managerサービスを再起動します。

```
service dsm_s start
```

FIPSモードで外部サービスに接続する

Deep Security ManagerをFIPSモードで操作し、SSL接続を使用して外部サービス (Active Directory、vCenter、またはNSX Managerなど) に接続する場合は、外部サービスのSSL証明書をManagerにインポートしてから接続する必要があります。証明書をインポートする手順については、"[信頼された証明書の管理](#)" on page 424を参照してください。

Active Directoryからコンピュータをインポートする手順については、"[Microsoft Active Directoryからのコンピュータグループの追加](#)" on page 549を参照してください。

ユーザ情報とActive Directoryを同期する手順については、"[ユーザの作成と管理](#)" on page 1376を参照してください。

VMware vCenterをDeep Security Managerに追加する手順については、"[vCenter - FIPSモードを追加する](#)" on page 515を参照してください。

保護しているコンピュータのOSのFIPSモードを有効にする

WindowsでFIPSモードを有効にする手順については、Microsoftサポートサイト [「システム暗号化: 使用して FIPS 準拠アルゴリズムを暗号化、ハッシュ、署名の"Windows XP およびそれ以降のバージョンの Windows のセキュリティ設定の効果」](#) を参照してください。

RHEL 7またはCentOS 7でFIPSモードを有効にする手順については、Red Hatのドキュメント [「米連邦政府の標準および規制」](#) および [「How can I make RHEL 6 or RHEL 7 FIPS 140-2 compliant?」](#) を参照してください。

保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする

注意: この手順は、Deep Security ManagerでFIPSモードを有効化した後にインストールしたDeep Security 11.0以降のAgentでは必要ありません。この場合、FIPSモードはすでにAgentに対して有効になっています。

Windows AgentのFIPSモードを有効にする

1. Windowsシステムのルートフォルダ (C:\Windowsなど) で、`ds_agent.ini`という名前のファイルを探します。テキストエディタでファイルを開くか、すでにファイルがない場合には新しいファイルを作成します。
2. 次の行をファイルに追加します。

```
FIPSMODE=1
```

3. Deep Security Agentサービスを再起動します。

RHEL 7またはCentOS 7 AgentのFIPSモードを有効にする

1. `/etc/`で、`ds_agent.conf`という名前のファイルを探します。テキストエディタでファイルを開くか、すでにファイルがない場合には新しいファイルを作成します。
2. 次の行をファイルに追加します。

```
FIPSMODE=1
```

Trend Micro Deep Security On-Premise 12.0

3. Deep Security Agentを再起動します。

SysV initスクリプトの使用：

```
/etc/init.d/ds_agent restart
```

systemdコマンドの使用：

```
systemctl restart ds_agent
```

Deep Security Virtual ApplianceでFIPSモードを有効にする

1. <DSVA_root>/etc/で、`ds_agent.conf`という名前のファイルを探します。テキストエディタでファイルを開くか、すでにファイルがない場合には新しいファイルを作成します。
2. 次の行をファイルに追加します。

```
FIPSMode=1
```

3. コマンドラインからApplianceを再起動します。

SysV initスクリプトの使用：

```
/etc/init.d/ds_agent restart
```

systemdコマンドの使用：

```
systemctl restart ds_agent
```

PostgreSQLデータベースでFIPSモードを使用する

Deep Security ManagerデータベースとしてPostgreSQLを使用する場合は、"[Deep Security Managerで使用するデータベースの準備](#)" on page 206とに記載されている要件に加えて、別の要件があります。

FIPSモードで、キーストアにBCFKSタイプを指定する必要があります。javaの初期設定キーストア (C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\security\cacertsまたは/opt/dsm/jre/lib/security/cacerts) を直接変換する代わりに、初期設定のキーストアを別の場所にコピーし、SSL接続の初期設定のキーストアとして使用します。

1. PostgreSQL環境を作成する
2. 「server.crt」 ファイルをPostgreSQLサーバからコピーし、<Deep Security Managerのインストールフォルダ>に貼り付けます。
3. Deep Security Managerをインストールします。
4. ["Deep Security ManagerでFIPSモードを有効にする" on page 1460](#)。
5. 初期設定のJava cacertsファイルをDeep Security Managerのルートインストールフォルダにコピーします。

Windowsの場合:

```
copy "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\security\cacerts" "C:\Program Files\Trend Micro\Deep Security Manager\cacerts"
```

Linuxの場合:

```
cp "/opt/dsm/jre/lib/security/cacerts" "/opt/dsm/cacerts"
```

6. KeystoreファイルをJKSからBCFKSに変換します。次のコマンドにより、Deep Security Managerのインストールフォルダにcacerts.bcfksファイルが作成されます。

Windowsの場合:

```
cd C:\Program Files\Trend Micro\Deep Security Manager\jre\bin
```

```
keytool -importkeystore -srckeystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts" -srcstoretype JKS -deststoretype BCFKS -destkeystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks" -srcstorepass <changeit> -deststorepass <changeit> -providerpath "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -providerclass com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
```


Trend Micro Deep Security On-Premise 12.0

<changeit>の部分は、適切な値に置き換えてください。

Linuxの場合:

```
cd /opt/dsm/jre/bin
```

```
keytool -importkeystore -srckeystore "/opt/dsm/cacerts" -srcstoretype JKS -deststoretype BCFKS -  
destkeystore "/opt/dsm/cacerts.bcfks" -srcstorepass <changeit> -deststorepass <changeit> -  
providerpath "/opt/dsm/jre/lib/ext/ccj-3.0.0.jar" -providerclass  
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
```

<changeit>の部分は、適切な値に置き換えてください。

7. 証明書をインポートします ("Deep Security Manager root folder/server.crt")。

Windowsの場合:

```
cd C:\Program Files\Trend Micro\Deep Security Manager\jre\bin
```

```
keytool -import -alias psql -file "C:\Program Files\Trend Micro\Deep Security  
Manager\server.crt" -keystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks"  
-storepass <changeit> -provider  
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath "C:\Program  
Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -storetype BCFKS
```

<changeit>の部分は、適切な値に置き換えてください。

Linuxの場合:

```
cd /opt/dsm/jre/bin
```

```
keytool -import -alias psql -file "/opt/dsm/server.crt" -keystore "/opt/dsm/cacerts.bcfks" -  
storepass <changeit> -provider
```

Trend Micro Deep Security On-Premise 12.0

```
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath  
"/opt/dsm/jre/lib/ext/ccj-3.0.0.jar" -storetype BCFKS
```

<changeit>の部分は、適切な値に置き換えてください。

8. Deep Securityインストーラは、`vmoptions`ファイルを使用してJVMパラメータを割り当てることができます。

Windowsの場合、`Deep Security Manager.vmoptions` という名前のファイルをインストールフォルダに作成し、次のテキストをファイルに追加します。

注意: ファイル拡張子が `.vmoptions` であることを確認してください。

```
-Djavax.net.ssl.keyStoreProvider=CCJ
```

```
-Djavax.net.ssl.trustStore=C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks
```

```
-Djavax.net.ssl.trustStorePassword=<changeit>
```

```
-Djavax.net.ssl.keyStoreType=BCFKS
```

```
-Djavax.net.ssl.trustStoreType=BCFKS
```

<changeit>の部分は、適切な値に置き換えてください。

Linuxの場合、インストールフォルダに `dsm_s.vmoptions` という名前のファイルを作成して、そのファイルに次の文字列を追加します。

```
-Djavax.net.ssl.keyStoreProvider=CCJ
```

```
-Djavax.net.ssl.trustStore=/opt/dsm/cacerts.bcfks
```

```
-Djavax.net.ssl.trustStorePassword=<changeit>
```

```
-Djavax.net.ssl.keyStoreType=BCFKS
```

Trend Micro Deep Security On-Premise 12.0

```
-Djavax.net.ssl.trustStoreType=BCFKS
```

<changeit>の部分は、適切な値に置き換えてください。

9. <Deep Security Managerのディレクトリ>\webclient\webapps\ROOT\WEB-INF\dsm.propertiesファイルをテキストエディタで開いて次の文字列を追加します。

```
database.PostgreSQL.connectionParameters=ssl=true
```

10. テキストエディタで/opt/postgresql/data/postgresql.confファイルを開いて、次の文字列を追加します。

```
ssl= on
```

```
ssl_cert_file= 'server.crt'
```

```
ssl_ksy_file= 'server.key'
```

11. PostgreSQLを再起動してから、Deep Security Managerサービスを再起動します。
12. 接続を確認します。

```
cd /opt/postgresql/bin
```

```
./psql -h 127.0.0.1 -Udsm dsm
```

プロンプトが表示されたら、パスワードを入力します。次のように表示されます。

```
dsm=> select a.client_addr, a.application_name, a.username, s.* from pg_stat_ssl s join pg_stat_activity a using (pid) where a.datname='dsm';
```

Microsoft SQL ServerデータベースでFIPSモードを使用する

Deep Security ManagerデータベースとしてMicrosoft SQL Serverを使用する場合は、FIPSモードを有効化する前に以下の手順に従ってデータベースSSL暗号化を設定する必要があります。

Trend Micro Deep Security On-Premise 12.0

1. Deep Security Managerサービスを停止します。
2. SQL Server証明書を使用してBCFKSKeystoreファイルを作成します。C:\Program Files\Trend Micro\Deep Security Manager\jre\bin内でキーツールを使用できます。
3. 次のコマンドを使用してSQL Server証明書 (C:\sqlserver_cert.cer) を新しいKeystoreファイル (C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks) にインポートします。

注意: Deep Security Managerパッケージにccj-3.0.0.jarファイルが含まれない場合は、jarファイルをFIPSページから取得します。

```
keytool -import -alias mssql -file "C:\sqlserver_cert.cer" -keystore "C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks" -storepass <changeit> -provider com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -storetype BCFKS
```

<changeit>の部分は、適切な値に置き換えてください。

インポートプロセス中に、[はい] を選択してこの証明書を信頼します。

4. Keystoreファイルの作成に成功すると、次のコマンドを使用してキーストアに記載された証明書を表示できるようになります。

```
keytool -list -v -keystore "C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks" -provider com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider -providerpath "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\ext\ccj-3.0.0.jar" -storetype BCFKS -storepass <changeit>
```

<changeit>の部分は、適切な値に置き換えてください。

5. テキストエディタでC:\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.propertiesファイルを開き、次の行を追加してSSL/TLSおよびFIPS設定を有効にします。

```
database.SqlServer.encrypt=true
```

```
database.SqlServer.trustServerCertificate=false
```

```
database.SqlServer.fips=true
```

```
database.SqlServer.trustStorePassword=<changeit>
```

```
database.SqlServer.fipsProvider=CCJ
```

```
database.SqlServer.trustStoreType=BCFKS
```

```
database.SqlServer.trustStore=C:\Program Files\Trend Micro\Deep Security Manager\mssql_  
keystore.bcfks
```

<changeit>の部分は、適切な値に置き換えてください。

6. 必要に応じて、SQLサーバ/クライアント接続プロトコルを名前付きパイプからTCP/IPに変更することもできます。これにより、Deep Security 10.2へのアップグレード後にFIPSをサポートできるようになります。
 - a. SQL Server構成マネージャで、[SQL Serverネットワーク構成]→[MSSQLSERVERのプロトコル]を選択し、[TCP/IP]を有効にします。
 - b. [SQL Native Client 11.0の構成]→[クライアントプロトコル]に移動し、[TCP/IP]を有効にします。
 - c. Microsoftから提供される手順に従って、SQL Serverデータベースのインスタンスで暗号化された接続を有効にします。[「データベースエンジンへの暗号化接続の有効化」](#)を参照してください。
 - d. dsm.propertiesファイルを編集し、database.sqlserver.driver=MSJDBCおよびdatabase.SqlServer.namedPipe=falseを変更します。
7. Deep Security Managerサービスを再起動します。
8. ["Deep Security ManagerでFIPSモードを有効にする" on page 1460](#)。

FIPSモードを無効にする

1. Deep Security ManagerのFIPSモードを無効にするには、有効化の際に使用した手順 (["Deep Security ManagerでFIPSモードを有効にする" on page 1460](#)を参照) に従いますが、手順3で次のコマンドを使用します。

```
dsm_c -action disablefipsmode
```

2. Deep Security AgentのFIPSモードを無効にするには、有効化の際に使用した手順 ("[保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする](#)" on page 1462を参照) に従いますが、`FIPSMODE=1`の代わりに`FIPSMODE=0`を使用します。

Deep Securityでの脆弱性管理検索トラフィックのバイパス

(PCI準拠等の目的で) QualysやNessusなどの脆弱性管理プロバイダを使用している場合、このプロバイダの検索トラフィックをバイパスし、そのまま許可するようにDeep Securityを設定する必要があります。

- "[脆弱性検索プロバイダのIP範囲またはアドレスから新しいIPリストを作成する](#)" below
- "[受信および送信検索トラフィック用のファイアウォールルールを作成する](#)" on the next page
- "[新規ファイアウォールルールをポリシーに割り当てて、脆弱性検索をバイパスする](#)" on page 1472

これらのファイアウォールルールを新規ポリシーに割り当てると、Deep Security ManagerはIPリストに追加したIPからのトラフィックをすべて無視します。

Deep Securityは、脆弱性管理プロバイダのトラフィックについては、ステートフルの問題または脆弱性の有無を検索せず、そのまま許可します。

脆弱性検索プロバイダのIP範囲またはアドレスから新しいIPリストを作成する

脆弱性検索プロバイダから受け取ったIPアドレスを手元に用意します。

1. Deep Security Managerで、[ポリシー]に進みます。
2. 左側の画面で [リスト]→[IPリスト] の順に展開します。
3. [新規]→[新規IPリスト] の順にクリックします。
4. 「Qualys IP list」など、新規IPリストの [名前] を入力します。
5. 脆弱性管理プロバイダから受け取ったIPアドレスを、1行に1つずつ [IP] ボックスに貼り付けます。
6. [OK] をクリックします。

受信および送信検索トラフィック用のファイアウォールルールを作成する

IPリストの作成後、受信トラフィック用と送信トラフィック用の2つのファイアウォールルールを作成する必要があります。

それぞれ、次のように名前を付けます。

<プロバイダ名> Vulnerability Traffic - Incoming

<プロバイダ名> Vulnerability Traffic - Outgoing

1. メインメニューで [ポリシー] をクリックします。
2. 左側の画面で [ルール] を展開します。
3. [ファイアウォールルール]→[新規]→[新規ファイアウォールルール] の順にクリックします。
4. 脆弱性管理プロバイダとの間で送受信するTCPおよびUDP接続の受信および送信をバイパスする、最初のルールを作成します。

ヒント: 以下に記載しない設定については、初期設定のままにします。

名前: (推奨) <プロバイダ名> Vulnerability Traffic - Incoming

処理: バイパス

プロトコル: 任意

パケット送信元: [IPリスト] を選択し、前の手順で作成した新しいIPリストを指定します。

5. 2番目のルールを作成します。

名前: <プロバイダ名> Vulnerability Traffic - Outgoing

処理: バイパス

プロトコル:任意

パケット送信先: [IPリスト] を選択し、前の手順で作成した新しいIPリストを指定します。

新規ファイアウォールルールをポリシーに割り当てて、脆弱性検索をバイパスする

脆弱性管理プロバイダによって検索されるコンピュータですでに使用されているポリシーを特定します。

ポリシーを個別に編集し、ファイアウォールモジュールでルールを割り当てます。

1. メインメニューで [ポリシー] をクリックします。
2. 左側の画面で [ポリシー] をクリックします。
3. 右側の画面で、各ポリシーをダブルクリックしてポリシー詳細を開きます。
4. 左側の画面のポップアップで [ファイアウォール] をクリックします。
5. [割り当てられたファイアウォールルール] で [割り当て/割り当て解除] をクリックします。
6. 左上のリストにすべてのファイアウォールルールが表示されていることを確認します。
7. 検索ウィンドウを使用し、作成したルールを探して選択します。
8. [OK] をクリックします。

Deep SecurityでのTLS 1.2の使用

Deep Security Manager 11.1以降の新規インストールでは、初期設定でTLS 1.2が強制されます。

対応が必要であるかどうかは、以下の表で確認してください。

注意: TLS 1.2のA+評価の強力な暗号化スイートのみを有効にする場合は、"TLS 1.2の強力な暗号化スイートの有効化" on

page 1491」を参照してください。強力な暗号化スイートを使用すると、互換性の問題が発生することがあります。

目的	現在の環境	対応
Deep Security Manager 11.1以上の新規インストール	10.0以降のDeep Security Agent、Relay、Virtual Applianceのみ	なし 初期設定で、TLS 1.2は、すべてのコンポーネント間で使用され、ManagerとRelay上で強制されます。
	10.0未満のDeep Security Agent、Relay、Virtual Applianceを含む	(推奨)すべてのコンポーネントを、TLS 1.2をサポートする10.0以上のバージョンにアップグレードしてください。「 "TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1479 」を参照してください。お使いの環境のセキュリティを強化するための最良の方法です。 古いコンポーネントとの下位互換性を確保するために、初期のTLS 1.0を有効にすることもできます。「 "初期のTLS (1.0) を有効にする" on page 1487 」を参照してください。
Deep Security Manager 11.1以上へのアップグレード	10.0以降のDeep Security Agent、Relay、Virtual Applianceのみ	(推奨)環境のセキュリティを強化するためにTLS 1.2の強制を有効にします。「 "TLS 1.2を強制する" on page 1482 」を参照してください。 何もしないという選択肢もあります。以前の環境にあったTLS設定はすべて維持されます。これまでTLS 1.2を強制する設定になっていた場合は、その設定がアップグレード後も維持されます。逆に、強制する設定を無効にしていた場合も、それらの設定が維持されます。
	10.0未満	(推奨)すぐに対応する必要はありませんが、古いコンポーネントは、TLS 1.2がサポートさ

目的	現在の環境	対応
	のDeep Security Agent、Relay、Virtual Applianceを含む	<p>れる10.0以上にアップグレードし、TLS 1.2を強制することを検討してください。「"TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1479」および「"TLS 1.2を強制する" on page 1482」を参照してください。お使いの環境のセキュリティを強化するための最良の方法です。</p> <p>何もしないという選択肢もあります。以前の環境にあったTLS設定はすべて維持されます。以前TLS 1.0が許可されていた場合は、アップグレード後も許可されます。</p>

このページのトピック:

- ["TLS 1.2のアーキテクチャ" below](#)
- ["TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1479](#)
- ["TLS 1.2を強制する" on page 1482](#)
- ["初期のTLS \(1.0\) を有効にする" on page 1487](#)
- ["TLS 1.2が強制されているかどうかを確認する" on page 1489](#)
- ["TLS 1.2の強制後のAgent、Virtual Appliance、Relayのインストールに関するガイドライン" on page 1489](#)

TLS 1.2のアーキテクチャ

下の図は、Deep SecurityアーキテクチャにおけるTLS通信を示しています。

図1は、TLS 1.2が強制されているときのTLS通信を示しています (新しい11.1以上のDeep Security Manager環境では、これが初期設定となります)。図に示されているとおり、バージョン9.6のAgentも古いサードパーティのアプリケーションも、Deep Security Managerと通信できなくなります。

Trend Micro Deep Security On-Premise 12.0

図2は、TLS 1.2が強制されていない場合のTLS通信を示しています。図に示されているとおり、10.0以降のAgentはTLS 1.2を介してDeep Security Managerと通信しますが、バージョン9.6のAgentは初期のTLSを介して通信します。同様に、新しいサードパーティのアプリケーションではTLS 1.2が使用されていますが、古いアプリケーションでは初期のTLSが使用されています。

図1: TLS 1.2の強制あり

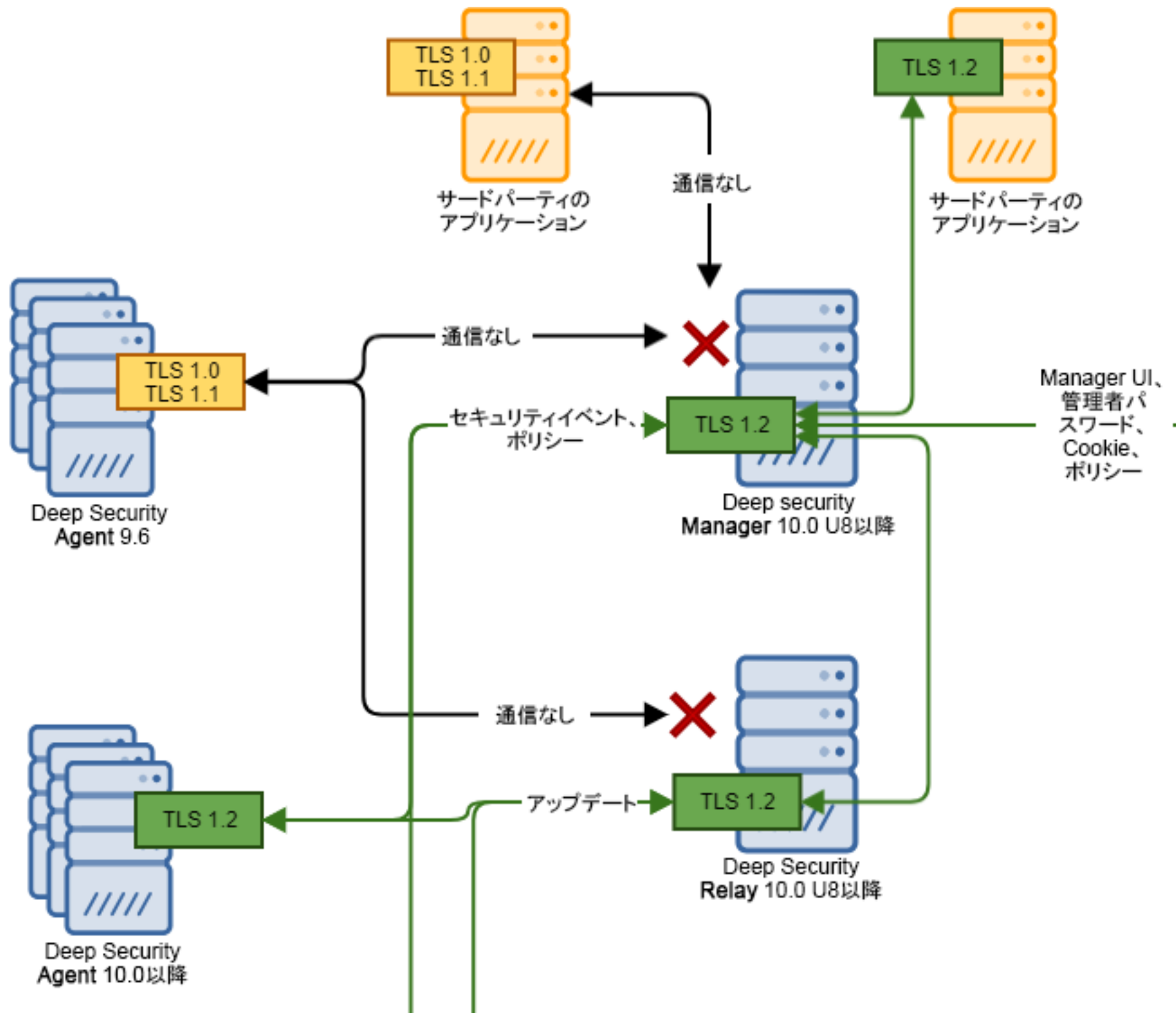
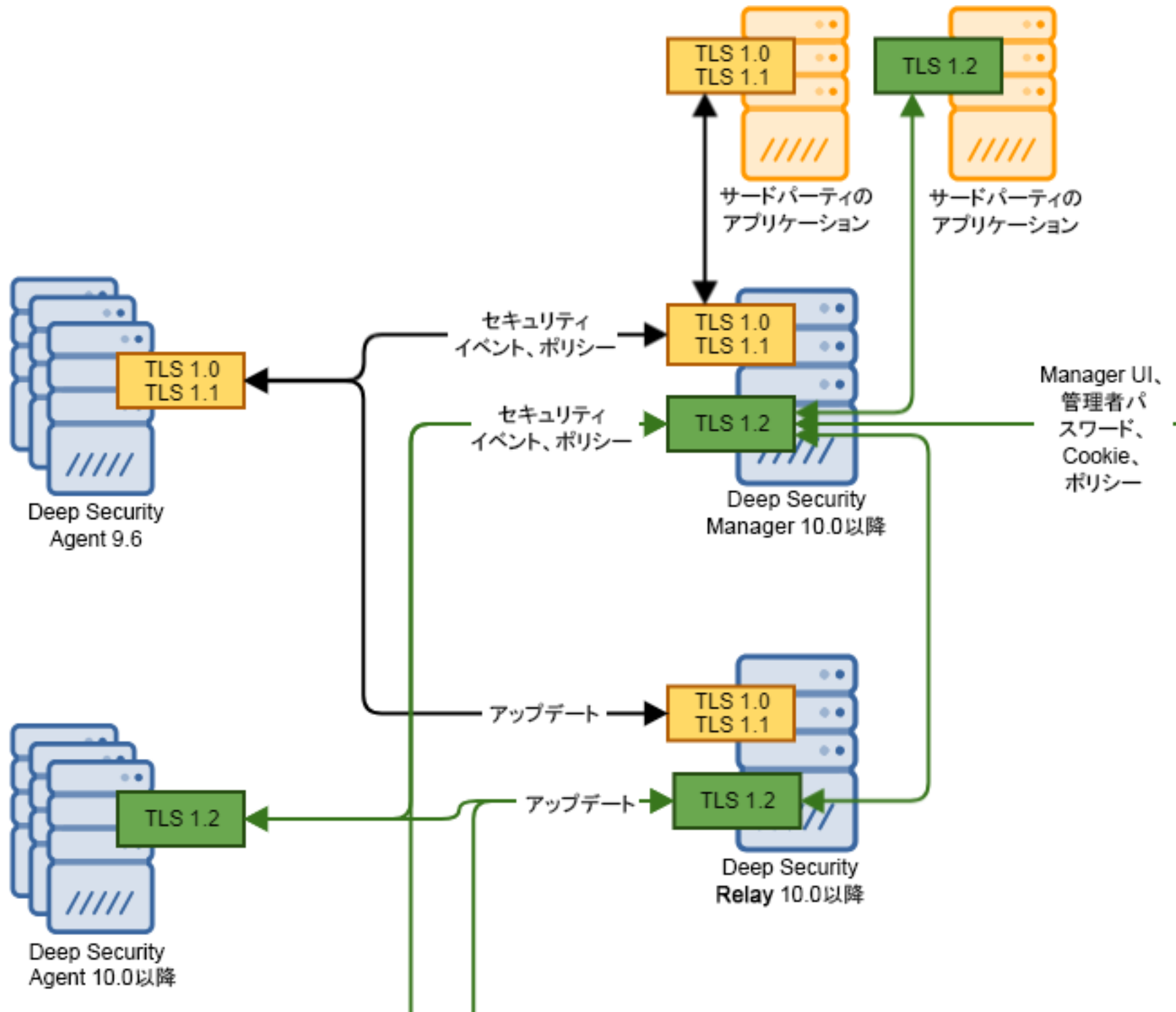


図2: TLS 1.2の強制なし



TLS 1.2を使用するようにコンポーネントをアップグレードする

Deep SecurityコンポーネントでTLS 1.2を使用する場合、個々のコンポーネントでTLS 1.2がサポートされていることを確認してください。

以下の手順に従って、Deep SecurityのコンポーネントがTLS 1.2をサポートしていることを確認し、必要に応じてそれらをアップグレードします。

注意: TLS 1.2を強制して初期のTLSが使用されないようにするには、「["TLS 1.2を強制する" on page 1482](#)」を参照してください。

Deep Security Managerを確認してアップグレードする

- 次のいずれかのバージョンのDeep Security Managerを使用していることを確認します。別のバージョンを使用している場合はアップグレードしてください。
 - Managerで["TLS 1.2を強制する" on page 1482](#)予定がある場合は、Deep Security Manager 10.0 Update 8以降を使用します。TLS 1.2の強制をサポートしているのは、10.0 Update 8以降のManagerのみです。
 - Managerで["TLS 1.2を強制する" on page 1482](#)予定がない場合は、Deep Security Manager 10.0以降を使用します。TLS 1.2通信をサポートしているのは、10.0以降のManagerのみです。
- アップグレード手順については、「["Deep Securityのインストールまたはアップグレード" on page 223](#)」を参照してください。

Deep Security Managerデータベースを確認する

- Deep Security ManagerデータベースとしてMicrosoft SQL Serverを使用する場合は、データベースでTLS 1.2がサポートされていることを確認し、サポートされていない場合は、データベースをアップグレードします。解説については、[こちらのMicrosoftのWebサイト](#)を参照してください。
- PostgreSQLデータベースを使用している場合は、TLS 1.2がサポートされているため、何もする必要はありません。

Trend Micro Deep Security On-Premise 12.0

- Oracleデータベースを使用している場合は、データベースとManager間の通信でTLSではなく、Oracleのネイティブの暗号化がサポートされているため、何もする必要はありません。
- 初期設定では、データベース (SQL Server、PostgreSQL、またはOracle) とDeep Security Manager間の通信は暗号化されていません。[暗号化は手動で有効にすることが](#)できます。

Deep Security Agentを確認する

- 既存のDeep Security Agentがある場合は、バージョンが10.0以降であることを確認します。TLS 1.2をサポートしているのは、10.0以降のAgentのみです。

注意: アップグレードされていないAgent (10.0より以前のAgent) が残っていると、そのAgentは初期のTLSを介して通信するため、初期のTLSを有効にする必要があります。詳細については、「["初期のTLS \(1.0\) を有効にする" on page 1487](#)」を参照してください。

Agentをアップグレードするには

1. Deep Security Managerに最新のDeep Security Agentソフトウェアを手動または自動でインポートします。詳細については、「["Deep Security Agentのアップグレード" on page 998](#)」を参照してください。
2. Deep Security Agentをアップグレードします。
 - Agentを自動的にアップグレードするには、「["Agentのアップグレードを開始する" on page 1000](#)」を参照してください。
 - Agentを手動でアップグレードするには、「["Agentを手動でアップグレードする" on page 1001](#)」を参照してください。

Deep Security Relayを確認する

- 次のいずれかのバージョンのDeep Security Relayを使用していることを確認します。別のバージョンを使用している場合はアップグレードしてください。

Trend Micro Deep Security On-Premise 12.0

- Relayで"[TLS 1.2を強制する](#)" on the next page 予定がある場合は、Deep Security Relay 10.0 Update 8以降を使用します。TLS 1.2の強制をサポートしているのは、10.0 Update 8以降のRelayのみです。
- Relayで"[TLS 1.2を強制する](#)" on the next page 予定がない場合は、Deep Security Relay 10.0以降を使用します。TLS 1.2通信をサポートしているのは、10.0以降のRelayのみです。

Relayをアップグレードするには、Agentのアップグレードと同じ手順に従います。

1. Deep Security Managerに最新のDeep Security Relayソフトウェアを手動または自動でインポートします。詳細については、"[Deep Security Agentのアップグレード](#)" on page 998を参照してください。
2. Relayをアップグレードします。
 - Relayを自動的にアップグレードするには、「"[Agentのアップグレードを開始する](#)" on page 1000」を参照してください。
 - Relayを手動でアップグレードするには、「"[Agentを手動でアップグレードする](#)" on page 1001」を参照してください。

Deep Security Virtual Applianceを確認する

Deep Security Virtual Appliance 10.0以降を使用していることを確認してください。

Applianceをアップグレードするには

1. 一時的に[初期のTLS \(1.0\) を有効](#)にします。
2. Applianceを10.0以上にアップグレードします ("[既存のAppliance SVMを自動的にアップグレードする](#)" on page 1010」を参照)。新しいVirtual ApplianceではTLS 1.2がサポートされます。
3. アップグレードが完了したら、[TLS 1.2の強制を再び有効](#)にします。

注意: Virtual Applianceに必要なvSphereおよびNSXソフトウェアの最小バージョンでは、TLS 1.2はすでにサポートされています。詳細については、"[システム要件](#)" on page 184を参照してください。

TLS 1.2を強制する

このセクションのトピック:

- ["TLS 1.2を強制できるコンポーネント" below](#)
- ["TLS 1.2を強制した場合の動作" below](#)
- ["初期設定でTLS 1.2が強制されるかどうか" on the next page](#)
- ["TLS 1.2の強制が可能になる場合の条件" on the next page](#)
- ["Deep Security ManagerでTLS 1.2を強制する" on the next page](#)
- ["Deep Security RelayでTLS 1.2を強制する" on page 1484](#)
- ["ManagerのGUIポート \(4119\) でのみTLS 1.2を強制する" on page 1484](#)
- ["TLS 1.2の強制をテストする" on page 1485](#)

TLS 1.2を強制できるコンポーネント

TLS 1.2を強制できるコンポーネントは次のとおりです。

- Deep Security Manager
- Deep Security Relay

TLS 1.2を強制した場合の動作

TLS 1.2を強制すると、ManagerとRelayで初期のTLS接続が許可されなくなり、初期のTLSの使用を試みるアプリケーションは、アクセスが拒否されて正常に機能しなくなります。

TLS 1.2を強制しない場合、ManagerとRelayで初期のTLSに加えてTLS 1.2接続も許可されます。そのため、古いアプリケーションと新しいアプリケーションの両方が接続できます。

初期設定でTLS 1.2が強制されるかどうか

- Deep Security Manager 11.1以上をアップグレードではなく新規インストールした場合、初期設定でTLS 1.2が強制されません。
- 既存のDeep Security Managerを11.1以上にアップグレードした場合は、既存のTLS設定が維持されます。つまり、それまでTLSを強制していなかった場合、アップグレード後も強制されません。逆に、強制していた場合は、引き続き強制されます。

TLS 1.2の強制が可能になる場合の条件

TLS 1.2を強制できるのは、Deep Security Agentすべてが、TLS 1.2がサポートされているバージョンである10.0以降にアップグレードされている場合のみです。

Deep Security ManagerでTLS 1.2を強制する

1. 開始前の準備:
 - Deep Security Managerのバージョンが10.0 Update 8以上であることを確認してください。TLS 1.2を強制するためには、このバージョンが必要です。
 - その他すべてのコンポーネントがTLS 1.2をサポートしていることを確認します。「["TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1479](#)」を参照してください。
2. Deep Security Managerコンピュータで、次の[dsm_cコマンド](#)を実行します。

```
dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
```

TLSのバージョンが表示されます。それが、現在Deep Security Managerで許可される最小のTLSバージョンとなります。

3. 次の[dsm_cコマンド](#)を実行します。

```
dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1.2
```

Trend Micro Deep Security On-Premise 12.0

このコマンドによって、最小TLSバージョンが1.2に設定されます。これでDeep Security ManagerがTLS 1.2接続を許可し、TLS 1.0接続を禁止するようになりました。

Deep Security Managerサービスが自動的に再開されます。

Deep Security RelayでTLS 1.2を強制する

1. 開始前の準備:

- Deep Security Relayのバージョンが10.0 Update 8以上であることを確認してください。TLS 1.2を強制するためには、このバージョンが必要です。
- すべてのコンポーネントがTLS 1.2をサポートしていることを確認します。「["TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1479](#)」を参照してください。
- [Deep Security ManagerでTLS 1.2を強制する](#)設定になっていることを確認します。

2. Relayに関連するポリシーを再送信します。

- a. Deep Security Managerで、[コンピュータ] をクリックし、コンピュータのリストで対象とするRelayを見つけます。どのRelayかわからない場合は、上部にある [管理] をクリックします。左側の [アップデート] を展開し、[Relayの管理] をクリックします。メイン画面でRelayグループを展開し、該当するRelayを表示します。
- b. コンピュータのリストでRelayをダブルクリックします。
- c. メイン画面で [処理] タブをクリックします。
- d. [ポリシーの送信] をクリックしてポリシーを再送信します。
- e. 各Relayにポリシーを再送信します。

ManagerのGUIポート (4119) でのみTLS 1.2を強制する

["Deep Security ManagerでTLS 1.2を強制する" on the previous page](#)および["Deep Security RelayでTLS 1.2を強制する" above](#)で説明したとおり、Deep Security ManagerおよびRelayで完全な強制が不可能な場合にのみ、このセクションを読んでください。

このセクションでは、ポート4119の最小TLSバージョンをTLS 1.2に設定する方法について説明します。通常、ポート4119で接続するアプリケーションは、WebブラウザとDeep Security APIクライアントです。TLS 1.2をサポートしていない古いDeep Securityコンポーネントは引き続き、TLS 1.0を使用してManagerに接続できます (初期設定ではポート4120を使用)。

1. Deep Security Managerで次の`dsm_c`コマンドを実行してTLS 1.0を有効にします。

```
dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1
```

Deep Security Managerが、古いAgentやアプリケーションからのTLS 1.0接続を許可するようになりました。

2. ManagerのGUIポート (4119) で初期のTLSを無効にします (すでに無効になっている可能性があります)。
 - a. Deep Security Managerのインストールディレクトリのルートにある`configuration.properties`ファイルを開きます。
 - b. `serviceName=`の下にある`protocols=`設定を探します。

この設定は、WebブラウザおよびDeep SecurityAPI クライアントのサーバとして機能しているDeep Security Managerへの接続に使用可能なプロトコルを定義しています。

- c. `protocols=`設定がある場合は、ポート4119でTLS 1.2のみが許可されるように、この設定を削除します。
 - d. ファイルを保存します。
3. Deep Security Managerサービスを再起動します。

TLS 1.2の強制をテストする

1. 初期TLS 1.2を強制したDeep Securityコンポーネントで、次のnmapコマンドを実行します。

```
nmap --script ssl-enum-ciphers <ds_host> -p <ds_port> -Pn
```

指定する項目は次のとおりです。

- `<ds_host>`は、ManagerまたはRelayのIPアドレスまたはホスト名に置き換えます。
- `<ds_port>`は、TLSが使用されている待機ポートに置き換えます。Managerの場合は4119、Relayの場合は4122、Agentの場合は4118です (Managerからの有効化を使用した場合)。

Trend Micro Deep Security On-Premise 12.0

この応答ではTLS 1.2のみが表示されます。応答の例は次のとおりです。

```
PORT STATE SERVICE
443/tcp open https
| ssl-enum-ciphers:
| | TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
| compressors:
```

初期のTLS (1.0) を有効にする

初期設定では、初期のTLS (1.0) が無効になっています。Deep Security Manager 11.1以上をアップグレードではなく新規インストールした場合で、かつ以下に該当する場合は、自分で有効にする必要があります。

- 10.0より前のAgentを使用している。この場合、サポートされるのは初期のTLSだけです。お使いのOSで10.0以上のAgentが利用できるかどうかについては、[こちらを参照](#)してください。
- 古いサードパーティコンポーネントを使用していて、Deep Security Managerとの通信に初期のTLSを使用する必要がある。
- 現在サポート対象外となっている、10.0より前のバージョンのDeep Security Virtual Applianceを使用している。

初期のTLS (1.0) を有効にするには、以下の手順に従います。

Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする

1. Deep Security Managerコンピュータで、次の[dsm_cコマンド](#)を実行します。

```
dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
```

TLSのバージョンが表示されます。それが、現在Deep Security Managerで許可される最小のTLSバージョンとなります。

2. 次のdsm_cコマンドを実行します。

```
dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1
```

このコマンドによって、最小TLSバージョンが1.0に設定されます。

Deep Security ManagerでTLS 1.0が再び有効になりました。

Deep Security Managerサービスが自動的に再開されます。

3. Relayに関連するポリシーを再送信します。
 - a. Deep Security Managerで、[コンピュータ] をクリックし、コンピュータのリストで対象とするRelayを見つけます。どのRelayかわからない場合は、上部にある [管理] をクリックします。左側の [アップデート] を展開し、[Relayの管理] をクリックします。メイン画面でRelayグループを展開し、該当するRelayを表示します。
 - b. コンピュータのリストでRelayをダブルクリックします。
 - c. メイン画面で [処理] タブをクリックします。
 - d. [ポリシーの送信] をクリックしてポリシーを再送信します。
 - e. 各Relayにポリシーを再送信します。

RelayでTLS 1.0が再び有効になりました。

ManagerのGUIポートでTLS 1.0を有効にする (4119)

以前ManagerのGUIポート (4119) でのみTLS 1.2を強制しており、今後はそのポートで初期のTLS 1.0を再び有効にしたい場合は、このセクションをお読みください。

1. 「["Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする" on the previous page](#)」の手順に従ってください。これにより、GUIポート (4119) でTLS 1.0が再び有効になります。

インストールスクリプトでTLS 1.0を有効にする

Deep Security AgentとDeep Security Relayは、[インストールスクリプト](#)を使用してインストールできます。これらのスクリプトに次のように変更を加える必要があります。

1. インストール先がWindows XP、2003、2008のいずれかである場合は、インストールスクリプトから次の行を削除します。

```
#requires -version 4.0
```

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
```

TLS 1.2ではPowerShell 4.0が必要ですが、Windows XP、2003、2008ではPowerShell 4.0がサポートされません。

2. インストール先がRed Hat Enterprise Linux 6である場合は、インストールスクリプトから次のタグを削除します。

```
--tls1.2
```

Red Hat Enterprise Linux 6の初期設定では、TLS 1.2をサポートしないcurl 7.19が使用されます。

3. それ以外のサポート対象のOSがインストール先である場合は、インストールスクリプトをそのままにしてください。

TLS 1.2が強制されているかどうかを確認する

Deep Security ManagerでTLS 1.2が強制されているかどうか分からない場合は、以下の手順に従って確認してください。

1. Deep Security Managerコンピュータでコマンドプロンプトを開き、次の[dsm_cコマンド](#)を実行します。

```
dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
```

Managerで許可される最小バージョンのTLSプロトコルが表示されます。TLS 1.2と表示された場合は、TLS 1.2が強制されています。TLS 1.0と表示された場合、初期のTLSは許可されていますが、TLS 1.2は強制されていません。

RelayでTLS 1.2が強制されているかどうかを確認するのは、もっと難しくなります。「["Deep Security RelayでTLS 1.2を強制する" on page 1484](#)」または「["Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする" on page 1487](#)」に従い、お使いのTLS設定をポリシーを通じてRelayに強制した場合、それらのTLS設定がRelayに適用されます。ポリシーを通じてTLS設定を強制しなかった場合は、Relayの初期設定のTLS設定が適用されます。Relayの初期設定は、そのバージョンによって異なります。11.1以上のRelayを使用している場合は、初期設定でTLS 1.2が強制されます。11.1より前のRelayの初期設定では、TLS 1.2が強制されません。

TLS 1.2の強制後のAgent、Virtual Appliance、Relayのインストールに関するガイドライン

このセクションでは、TLS 1.2を強制した後でAgent、Virtual Appliance、およびRelayをインストールする場合の特別な注意事項について説明します。[初期のTLS \(1.0\)](#) を有効にした場合、特に注意事項はないため、このセクションを読む必要はありません。

このセクションのトピック:

- ["TLS 1.2が強制されているときのAgent、Virtual Appliance、およびRelayのインストールに関するガイドライン"](#) below
- ["TLS 1.2の強制後にインストールスクリプトを使用する場合のガイドライン"](#) below

TLS 1.2が強制されているときのAgent、Virtual Appliance、およびRelayのインストールに関するガイドライン

- 10.0以上のAgent、Virtual Appliance、およびRelayをインストールする必要があります。TLS 1.2をサポートしているのは、10.0以上のAgentとRelayのみです。
- 9.6以前のAgentまたはRelayをインストールする必要がある場合は、[初期のTLS \(1.0\) を有効にする](#)必要があります。

TLS 1.2の強制後にインストールスクリプトを使用する場合のガイドライン

TLS 1.2が強制されている場合、[インストールスクリプト](#)を使用して、10.0以上のAgentとRelayをインストールできます。ここでは、インストールスクリプトを確実に機能させるためのガイドラインを示します。

1. WindowsコンピュータにAgentまたはRelayをインストールする場合は、TLS 1.2をサポートしているPowerShell 4.0以降を使用します。
2. LinuxにAgentまたはRelayをインストールする場合は、TLS 1.2をサポートしているcurl 7.34.0以降を使用します。
3. インストール先がWindows XP、2003、2008のいずれかである場合

または

インストール先がRed Hat Enterprise Linux 6である場合

これらのOSはTLS 1.2をサポートしていないため、["初期のTLS \(1.0\) を有効にする"](#) on page 1487にしたうえで、[インストールスクリプトに変更を加える](#)必要があります。

TLS 1.2の強力な暗号化スイートの有効化

強力な暗号化スイートを有効にすることで、Deep Securityコンポーネントとのすべての通信を安全に行えるようになります。悪意のあるユーザーが、弱い暗号化スイートを使用した通信チャンネルを介してシステムへの接続を作成できると、その暗号化スイートの既知の脆弱性を悪用して、システムや情報の安全性を脅かすことになります。

このページでは、TLS 1.2の強力な暗号化スイートを使用するように、Deep Security Manager、Deep Security Agent、およびDeep Security Relayをアップデートする方法について説明します。これらの暗号スイートには+ (A+) の詳細評価があり、[このページ](#)の表にリストされています。

注意: 強力な暗号化スイートを有効にするには、すべてのDeep Securityコンポーネントを12.0以降にアップグレードする必要があります。アップグレードできない場合 (たとえば、12.0 Agentが対応していないOSを使用している場合) は、代わりに["Deep SecurityでのTLS 1.2の使用" on page 1472](#)を参照してください。

手順1: ["Deep Securityコンポーネントをアップデートする" below](#)

手順2: ["TLS 1.2の強力な暗号化スイートを有効にするためのスクリプトを実行する" on the next page](#)

手順3: ["スクリプトの動作を確認する" on page 1493](#)

["TLS 1.2の強力な暗号化スイートを無効にする" on page 1497](#)

Deep Securityコンポーネントをアップデートする

以下に記載された順にすべてのコンポーネントをアップデートしてください。しなかった場合、AgentはRelayやManagerと通信できなくなります。

1. すべてのManagerインスタンスを12.0以降のバージョンにアップデートします。アップグレード手順については、["Deep Securityのインストールまたはアップグレード" on page 223](#)を参照してください。

2. すべてのRelayを12.0以降にアップデートします。Relayをアップグレードするには、Agentのアップグレードと同じ手順に従います。
 - a. Managerに最新のRelayソフトウェアを手動または自動でインポートします。詳細については、"[Deep Security Agentのアップグレード](#)" on page 998を参照してください。
 - b. Relayをアップグレードします。
 - Relayを自動的にアップグレードするには、「["Agentのアップグレードを開始する"](#) on page 1000」を参照してください。
 - Relayを手動でアップグレードするには、「["Agentを手動でアップグレードする"](#) on page 1001」を参照してください。
3. すべてのAgentを12.0以降にアップデートします。Agentをアップグレードするには
 - a. Managerに最新のAgentソフトウェアを手動または自動でインポートします。詳細については、"[Deep Security Agentのアップグレード](#)" on page 998を参照してください。
 - b. Deep Security Agentをアップグレードします。
 - Agentを自動的にアップグレードするには、「["Agentのアップグレードを開始する"](#) on page 1000」を参照してください。
 - Agentを手動でアップグレードするには、「["Agentを手動でアップグレードする"](#) on page 1001」を参照してください。

TLS 1.2の強力な暗号化スイートを有効にするためのスクリプトを実行する

1. <https://github.com/deep-security/ops-tools/tree/master/deepsecurity/manager>にある `EnableStrongCiphers12.script` ファイルを以下の場所にコピーします。
 - Windowsの場合: `<Manager_root>\Scripts`
 - Linuxの場合: `<Manager_root>/Scripts`

この場合、`<Manager_root>`は、Managerのインストールディレクトリのパスに置き換えます。初期設定では次のようになっています。

- C:\Program Files\Trend Micro\Deep Security Manager (Windows)
- /opt/dsm/ (Linux)

注意: \Scripts ディレクトリが表示されない場合は、作成してください。

2. Managerにログインします。
3. 上部の [管理] をクリックします。
4. 左側で、[予約タスク] をクリックします。
5. メイン画面で、[新規] をクリックします。
6. [新規予約タスクウィザード] が表示されます。
7. [種類] リストで [スクリプトの実行] を選択します。[1回のみ] を選択します。[次へ] をクリックします。
8. 初期設定の日付、時刻、およびタイムゾーンをそのままにし、[次へ] をクリックします。
9. [スクリプト] で、[EnableStrongCiphers.script] を選択します。[次へ] をクリックします。
10. [名前] には、スクリプトの名前 (たとえば、Enable Strong Cipher Suites) を入力します。[タスクの有効化] が選択されていることを確認します。[[完了] でタスクを実行] をクリックします。[完了] をクリックします。

スクリプトが実行されます。

11. Deep Security Managerサービスを再起動します。

Agent、Relay、およびManagerは、TLS 1.2の強力な暗号化スイートのみを使用して相互に通信を行うようになりました。

スクリプトの動作を確認する

スクリプトの動作と、TLS 1.2の強力な暗号化スイートのみが許可されていることを確認するには、一連のnmapコマンドを実行する必要があります。

- ["nmapを使用してManagerを確認する" on the next page](#)
- ["nmapを使用してRelayを確認する" on page 1495](#)
- ["nmapを使用してAgentを確認する" on page 1496](#)

nmapを使用してManagerを確認する

次のコマンドを実行します。

```
nmap --script ssl-enum-ciphers -p 4119 <Manager_FQDN>
```

出力は次のようになります。強力な暗号化スイートは中段付近で確認できます。

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:51 EST
Nmap scan report for <DSM FQDN> (X.X.X.X)
Host is up (0.0049s latency).
PORT STATE SERVICE
4119/tcp open  assuria-slm
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256k1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256k1) - A
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256k1) - A
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256k1) - A
| compressors:
| NULL
| cipher preference: client
|_ least strength: A
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
```

nmapを使用してRelayを確認する

次のコマンドを実行します。

```
nmap --script ssl-enum-ciphers -p 4122 <Relay_FQDN>
```

出力は次のようになります。強力な暗号化スイートは中段付近に記述されています。

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:49 EST
```

```
Nmap scan report for <DSR FQDN> (X.X.X.X)
```

```
Host is up (0.0045s latency).
```

```
PORT STATE SERVICE
```

```
4122/tcp open unknown
```

```
| ssl-enum-ciphers:
```

```
| TLSv1.2:
```

```
| ciphers:
```

```
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
```

```
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
```

```
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
```

```
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
```

```
| compressors:
```

```
| NULL
```

```
| cipher preference: server
```

```
|_ least strength: A
```

```
Nmap done: 1 IP address (1 host up) scanned in 31.02 seconds
```

nmapを使用してAgentを確認する

次のコマンドを実行します。

```
nmap --script ssl-enum-ciphers -p 4118 <Agent_FQDN>
```

出力は次のようになります。

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:50 EST
```

```
Nmap scan report for <DSA FQDN> (X.X.X.X)
```

```
Host is up (0.0048s latency).
```

```
PORT STATE SERVICE
```

```
4118/tcp open netscript
```

```
| ssl-enum-ciphers:
```

```
| TLSv1.2:
```

```
| ciphers:
```

```
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
```

```
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
```

```
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
```

```
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
```

```
| compressors:
```

```
| NULL
```



```
| cipher preference: server
```

```
|_ least strength: A
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
```

TLS 1.2の強力な暗号化スイートを無効にする

すべてのAgent、Relay、およびManagerをアップグレードする前に誤ってスクリプトを実行してしまった場合には、次の手順に従って以前の状態に戻すことができます。

1. <Manager_root>にあるconfiguration.propertiesファイルを開き、ciphersで始まる行を削除します。次のような行です。

```
ciphers=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
```

2. protocols フィールドに値TLSv1とTLSv1.1を追加します。プロパティは最終的には次のようになります。

```
protocols = TLSv1, TLSv1.1, TLSv1.2
```

3. ファイルを保存して、閉じます。
4. <Manager_root>\jre\lib\security\にあるjava.securityファイルを開き、jdk.tls.disabledAlgorithms から次の2つのプロトコルを削除します。

```
TLSv1, TLSv1.1
```

5. Deep Security Managerで、次のdsm_cコマンドを実行します。

```
dsm_c -action changesetting -name settings.configuration.restrictRelayMinimumTLSProtocol -value TLSv1
```

```
dsm_c -action changesetting -name settings.configuration.enableStrongCiphers -value false
```

Trend Micro Deep Security On-Premise 12.0

システムが再度通信できるようになります。TLS 1.2の強力な暗号化スイートを有効にする必要がある場合は、すべてのコンポーネントをアップグレードしてからスクリプトを実行するようにしてください。

Deep Security Managerとの通信の問題が解決しない場合は、次の`dsm_c`コマンドを追加で実行してください。

```
dsm_c -action changesetting -name settings.configuration.MinimumTLSProtocolNewNode -value TLSv1
```

Deep Securityの暗号化アルゴリズムのアップグレード

Deep Security 9.6 SP1以前のバージョンでは、Deep Security ManagerとDeep Security Agent間の通信はRSA-1024とSHA-1を使用して保護されます。Deep Security 10.0以降では、より安全なアルゴリズムであるRSA-2048とDSA-256が初期設定で使用されます。

Deep Security 10.0以降を新規にインストールした場合はRSA-2048とDSA-256が使用されますが、以前のバージョンからDeep Security 10.0以降にアップグレードした場合は、暗号化アルゴリズムを別途アップグレードしないかぎり以前のアルゴリズムが引き続き使用されます。

ここでは、Deep Security 10.0以降へのアップグレード後にアルゴリズムをアップグレードする方法について説明します。下記の手順に従って設定を変更すると、Deep Security Managerによって、Manager自体と管理下のすべてのAgent用に新しい証明書が生成されます。生成された新しい証明書は、その後AgentがDeep Security Managerに接続したときにManagerからAgentに送信されます。

Windowsでアルゴリズムをアップグレードする

1. Microsoft管理コンソールの [サービス] 画面を使用して「Trend Micro Deep Security Manager」サービスを停止します。
2. Windowsコマンドラインで、Deep Security Managerの作業用フォルダ (例: `C:\Program Files\Trend Micro\Deep Security Manager`) に移動します。

3. dsm_cコマンドとパラメータを使用して、新しい設定に変更します。次に例を示します。

```
dsm_c -action changesetting -name settings.security.defaultSignatureAlg -value "SHA256withRSA"
```

```
dsm_c -action changesetting -name settings.security.defaultKeyLength -value "2048"
```

```
dsm_c -action changesetting -name settings.security.forceCertificateUpdate -value "true"
```

4. エラーが表示されないことを確認し、Trend Micro Deep Security Managerサービスを再起動します。

Linuxでアルゴリズムをアップグレードする

1. コマンドラインで、Deep Security Managerサービスが実行されているディレクトリに移動し、次のコマンドを実行してサービスを停止します。

```
service dsm_s stop
```

2. Linuxコマンドラインで、Deep Security Managerの作業用フォルダ (例: /opt/dsm) に移動します。
3. dsm_cコマンドとパラメータを使用して、新しい設定に変更します。次に例を示します。

```
./dsm_c -action changesetting -name settings.security.defaultSignatureAlg -value "SHA256withRSA"
```

```
./dsm_c -action changesetting -name settings.security.defaultKeyLength -value "2048"
```

```
./dsm_c -action changesetting -name settings.security.forceCertificateUpdate -value "true"
```

4. エラーが表示されないことを確認し、Trend Micro Deep Security Managerサービスを再起動します。

複数ノード環境でアルゴリズムをアップグレードする

複数のノードでDeep Security Managerを実行している場合は、いずれかのノードでdsm_cコマンド (上記を参照) を実行し、次に他の各ノードで手動で「Trend Micro Deep Security Manager」サービスを再起動して変更を反映します。

マルチテナント環境でアルゴリズムをアップグレードする

Deep Security 10.0では、アルゴリズムはテナントごとに設定されています。そのため、dsm_cコマンドでテナント名 (-tenantname) またはテナントID (-tenantid) を指定して、各テナントについて個別に設定をアップデートする必要があります。テナントIDが5のテナントの設定を変更する例を次に示します。

```
dsm_c -action changesetting -name settings.security.defaultSignatureAlg -value "SHA256withRSA" -tenantid 5
```

```
dsm_c -action changesetting -name settings.security.defaultKeyLength -value "2048" -tenantid 5
```

```
dsm_c -action changesetting -name settings.security.forceCertificateUpdate -value "true" -tenantid 5
```

Microsoft SQL Server ExpressデータベースのEnterpriseへの移行

Microsoft SQL Server Expressは、ごく限られた構成でのみサポートされます (詳細については、"[Microsoft SQL Server Express に関する注意事項](#)" on page 216を参照してください)。Microsoft SQL Server Expressデータベースを使用していて、制限が厳しすぎる場合には、[サポートされているデータベース](#)に移行できます。

1. Deep Security Managerサービスを終了して、データベースへの書き込みを停止します。

Deep Security Agentは、Managerの停止中も引き続き現在の保護ポリシーを適用します。イベントは保持され、Deep Security Managerがオンラインに戻ると送信されます。

2. データベースをバックアップします。
3. 次のデータベース接続設定ファイルをバックアップします。

```
[Deep Securityのインストールディレクトリ]/webclient/webapps/ROOT/WEB-INF/dsm.properties
```

4. データベースを新しいデータベースエンジンに移動します。バックアップを復元します。
5. 移行後のデータベースに接続するよう、dsm.propertiesを編集します。

```
database.SqlServer.user
```

```
database.name
```

```
database.SqlServer.instance
```

```
database.SqlServer.password
```

```
database.type
```

```
database.SqlServer.server
```

初期設定のインスタンスを使用している場合は、`database.SqlServer.instance`設定を削除できます。

`database.SqlServer.password`にはパスワードをプレーンテキストで入力できます。Deep Security Managerサービスの開始時に、パスワードは次のように暗号化されます。

```
database.SqlServer.password=!CRYPT!20DE3D96312D6803A53C0D1C691FE6DEB7476104C0A
```

6. Deep Security Managerサービスを再起動します。
7. データベースへの再接続が成功したことを確認するために、Deep Security Managerにログインします。

既存の保護対象のコンピュータとイベントログが表示されます。管理者のログインやポリシーの変更などの新しいイベントが発生すると、それらのイベントが追加されます。再接続できない場合は、データベースユーザアカウントに新しいデータベースサーバに対する権限が付与されていることを確認してください。

Deep Securityのアンインストール

有効化されたAgentまたはRelayをコンピュータから手動でアンインストールした場合、コンピュータはソフトウェアがアンインストールされたことをDeep Security Managerに通知しません。Deep Security Managerの [コンピュータ] 画面で、コンピュータのステータスは状況に応じて「管理対象 (オフライン)」のように表示されます。これを避けるには、Deep Security Managerで次のいずれかを実行します。

- アンインストールする前にAgentまたはRelayを無効化します。
- アンインストールした後にリストからコンピュータを削除します。

Deep Security Relayをアンインストールする

Deep Security Relayは、Relay機能を有効にしたAgentです。そのため、Relayを削除するには、Agentをアンインストールする必要があります。

Relayをアンインストールする (Windows)

注意: WindowsでDeep Security AgentやRelayをアップデートまたはアンインストールする際は、Agentセルフプロテクションを無効にしておく必要があります。この操作を行うには、Deep Security Managerで、**コンピュータエディタ**¹の [設定]→[一般] に移動します。[Agentセルフプロテクション] で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。

Windowsの [コントロール パネル] で、プログラムの追加/削除 を選択します。[Trend Micro Deep Security Agent] をダブルクリックして、[削除] をクリックします。

次のコマンドを使用して、コマンドラインからアンインストールすることもできます。

```
msiexec /x <package name including extension>
```

サイレントアンインストールを実行する場合は、/quietを追加します。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Relayをアンインストールする (Linux)

Relayと、Red Hatパッケージマネージャ (rpm) を使用するプラットフォーム (CentOS、Amazon Linux、Oracle Linux、SUSE、CloudLinuxなど) に作成された設定ファイルを完全に削除するには、次のコマンドを入力します。

```
# sudo rpm -ev ds_agent
Stopping ds_agent: [ OK ]
Unloading dsa_filter module [ OK ]
```

Relay有効化済みAgentのインストール前にiptablesが有効になっていた場合は、Relay有効化済みAgentをアンインストールするときに再度有効になります。

注意: Deep Security Managerの管理対象コンピュータのリストからRelay有効化済みAgentを削除し、さらにRelayグループから削除してください。

Deep Security Agentをアンインストールする

Agentをアンインストールする (Windows)

注意: WindowsでDeep Security AgentやRelayをアップデートまたはアンインストールする際は、Agentセルフプロテクションを無効にしておく必要があります。この操作を行うには、Deep Security Managerで、**コンピュータエディタ**¹の [設定]→[一般] に移動します。[Agentセルフプロテクション] で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。

¹コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Trend Micro Deep Security On-Premise 12.0

1. [コンピュータ] 画面に移動し、コンピュータを右クリックして [処理]→[無効化] を選択し、Deep Security Managerを使用してAgentを無効化します。

Deep SecurityManagerがAgentとやり取りできないためにAgentを無効化できない場合は、次の手順に進む前に以下を実行する必要があります。

```
C:\Program Files\Trend Micro\Deep Security Agent>dsa_control --selfprotect 0
```

2. コントロールパネルに移動して [プログラムのアンインストール] を選択します。Trend Micro Deep Security Agentを探して、[アンインストール] を選択します。

次のコマンドを使用して、コマンドラインからアンインストールすることもできます。

```
msiexec /x <package name including extension>
```

サイレントアンインストールを実行する場合は、/quietを追加します。

Agentをアンインストールする (Linux)

Linuxのバージョンでグラフィカルパッケージ管理ツールが用意されている場合は、ds_agentパッケージを探して、このツールを使用してパッケージを削除します。それ以外の場合は、以下のコマンドラインの手順を使用します。

Agentと、Red Hatパッケージマネージャ (rpm) を使用するプラットフォーム (CentOS、Amazon Linux、Oracle Linux、SUSE、CloudLinuxなど) に作成された設定ファイルを完全に削除するには、次のコマンドを入力します。

```
# sudo rpm -ev ds_agent
Stopping ds_agent: [ OK ]
Unloading dsa_filter module [ OK ]
```

Deep Security Agentのインストール前に、iptablesが有効になっていた場合は、Deep Security Agentをアンインストールするときに再度有効になります。

Trend Micro Deep Security On-Premise 12.0

Debianパッケージマネージャ (dpkg) を使用するプラットフォーム (DebianやUbuntuなど) の場合は、次のコマンドを入力します。

```
$ sudo dpkg -r ds-agent  
Removing ds-agent...  
Stopping ds_agent: .[OK]
```

Agentをアンインストールする (Solaris 10)

次のコマンドを入力します。

```
pkgrm ds-agent
```

(アンインストール後に再起動が必要になる場合があります)

Agentをアンインストールする (Solaris 11)

次のコマンドを入力します。

```
pkg uninstall ds-agent
```

アンインストール後に再起動が必要になる場合があります。

Agentをアンインストールする (AIX)

次のコマンドを入力します。

```
installp -u ds_agent
```

Deep Security Notifierをアンインストールする

Windowsの [コントロール パネル] で、 [プログラムの追加と削除] を選択します。 [Trend Micro Deep Security Notifier] をダブルクリックして、 [削除] をクリックします。

コマンドラインからアンインストールするには、次のコマンドを入力します。

```
msiexec /x <package name including extension>
```

サイレントアンインストールを実行する場合は、 /quietを追加します。

Deep Security Managerをアンインストールする

Managerをアンインストールする (Windows)

Windowsの [スタート] メニューで、 [Trend Micro]→[Trend Micro Deep Security Managerアンインストーラ] の順に移動し、ウィザードの手順に従って、アンインストールを完了します。

コマンドラインから上記と同じWindowsのGUIを起動してアンインストールするには、次のコマンドを入力します。

```
<installation folder>\Uninstall.exe
```

WindowsのGUIを使用せず、コマンドラインからサイレントアンインストールするには、 -qオプションを追加します。

```
<installation folder>\Uninstall.exe -q
```

コマンドラインからのサイレントアンインストール中に設定ファイルが維持されるため、後で再インストールする場合、インストーラは既存の設定を使用して修復またはアップグレードします。設定を再度入力する必要はありません。

Managerをアンインストールする (Linux)

コマンドラインからアンインストールするには、インストールフォルダに移動して次のコマンドを入力します。

```
sudo ./uninstall
```

サイレントアンインストールを実行する場合は、`-q`を追加します。

初期設定では、コマンドラインからのサイレントアンインストール中に設定ファイルが維持されるため、後で再インストールする場合、インストーラは既存の設定を使用して修復またはアップグレードします。設定を再度入力する必要はありません。

アンインストール中に設定ファイルを維持しないように選択した場合、後でDeep Security Managerを再インストールする場合は、再インストール前に手動でクリーンアップを実行する必要があります。Deep Security Managerのインストールディレクトリを削除するには、次のコマンドを入力します。

```
sudo rm -rf <installation location>
```

初期設定のインストール場所は`/opt/dsm`です。

NSX環境からのDeep Securityのアンインストール

Deep SecurityをNSX環境からアンインストールすると、Deep Security Virtual ApplianceがNSX Data Center for vSphere (NSX-V) またはNSX-Tから削除され、関連するすべての履歴がDeep Security Managerから削除されます。

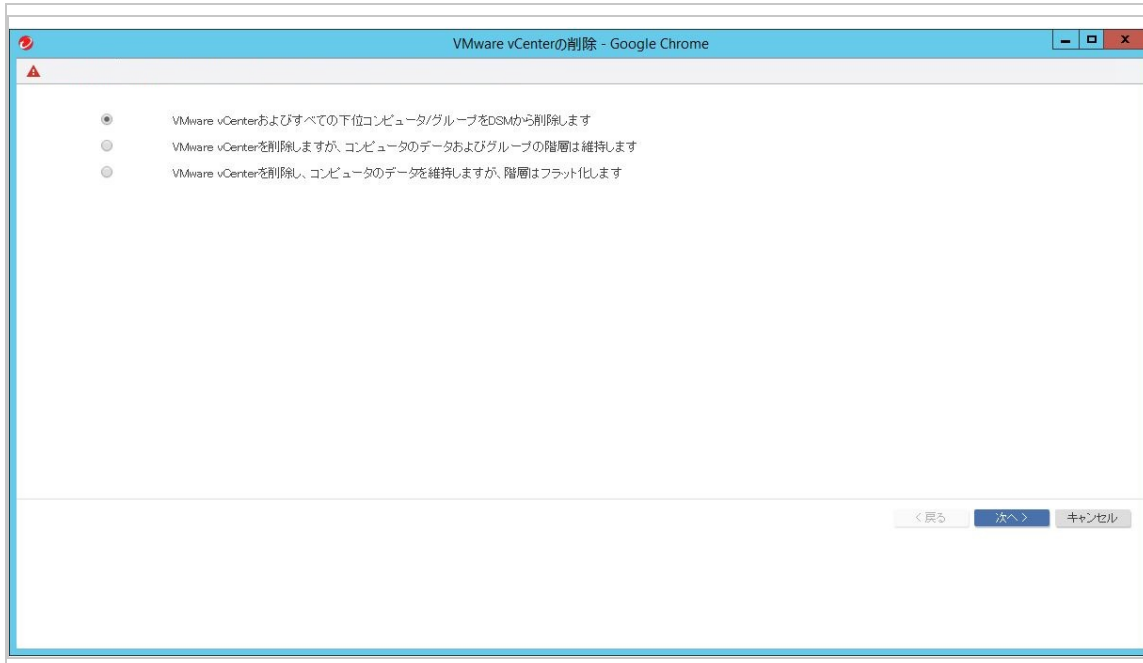
このページのトピック:

- ["NSX-V環境からのDeep Securityの自動アンインストール" on the next page](#)
- ["NSX-V環境からのDeep Securityの手動アンインストール" on page 1511](#)
- ["NSX-T環境からのDeep Securityの手動アンインストール" on page 1519](#)

NSX-V環境からのDeep Securityの自動アンインストール

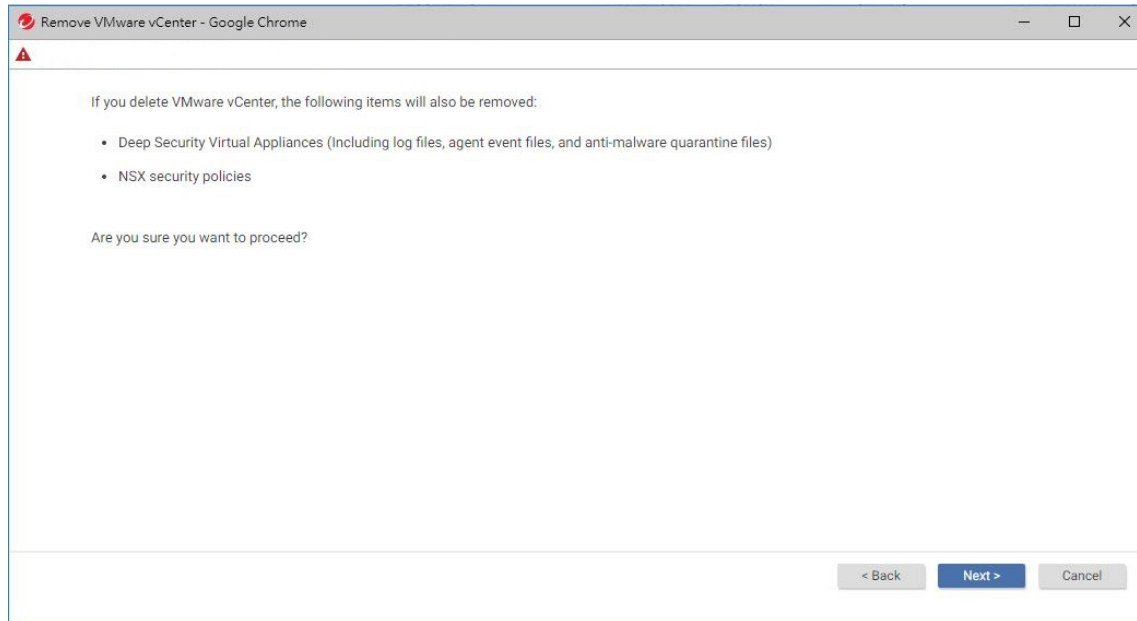
1. 開始する前に、NSX-V環境があることを確認します。NSX-T環境での自動アンインストールはサポートされていません。
2. Deep Security Managerで、[コンピュータ]に進みます。
3. 左側のナビゲーションツリーでvCenterを右クリックして、[VMware vCenterの削除]を選択します。
4. 次のいずれかのオプションを選択します。
 - VMware vCenterおよびすべての下位コンピュータ/グループをDSMから削除します: vCenterとすべての仮想マシンのレコード (割り当てられているDeep Securityのポリシーとルールを含む) を削除します。
 - VMware vCenterを削除しますが、コンピュータのデータおよびグループの階層は維持します: vCenterを削除しますが、階層構造と仮想マシンのレコード (割り当てられているDeep Securityのポリシーとルールを含む) は維持します。
 - VMware vCenterを削除し、コンピュータのデータを維持しますが、階層はフラット化します: vCenterを削除しますが、仮想マシンのレコード (割り当てられているDeep Securityのポリシーとルールを含む) は維持します。vCenterの階層構造は1つのグループにまとめられます。

Trend Micro Deep Security On-Premise 12.0



Trend Micro Deep Security On-Premise 12.0

5. いずれかのオプションを選択した後、[次へ]をクリックします。



6. もう一度 [次へ] をクリックして、削除を続行します。

たとえば1番目のオプションである [VMware vCenterおよびすべての下位コンピュータ/グループをDSMから削除します] を選択した場合は、NSX環境からDeep Security Virtual ApplianceおよびNSXのすべてのポリシーが自動的に削除されます。

「VMware vCenterが正常に削除されました」という処理の成功を通知するメッセージが表示されます。

注意: Deep Security ManagerとNSX Managerの接続が切断されている場合、「VMwareからDeep Securityを削除できません」というエラーが表示されることがあります。このエラーが発生した場合は、NSX ManagerからDeep Securityサービスを手動で削除する必要があります。詳細については、[次のセクション](#)を参照してください。

NSX-V環境からのDeep Securityの手動アンインストール

このセクションが該当するのは、NSX-V環境のみです。NSX-T環境の手順については、"[NSX-T環境からのDeep Securityの手動アンインストール](#)" on page 1519を参照してください。

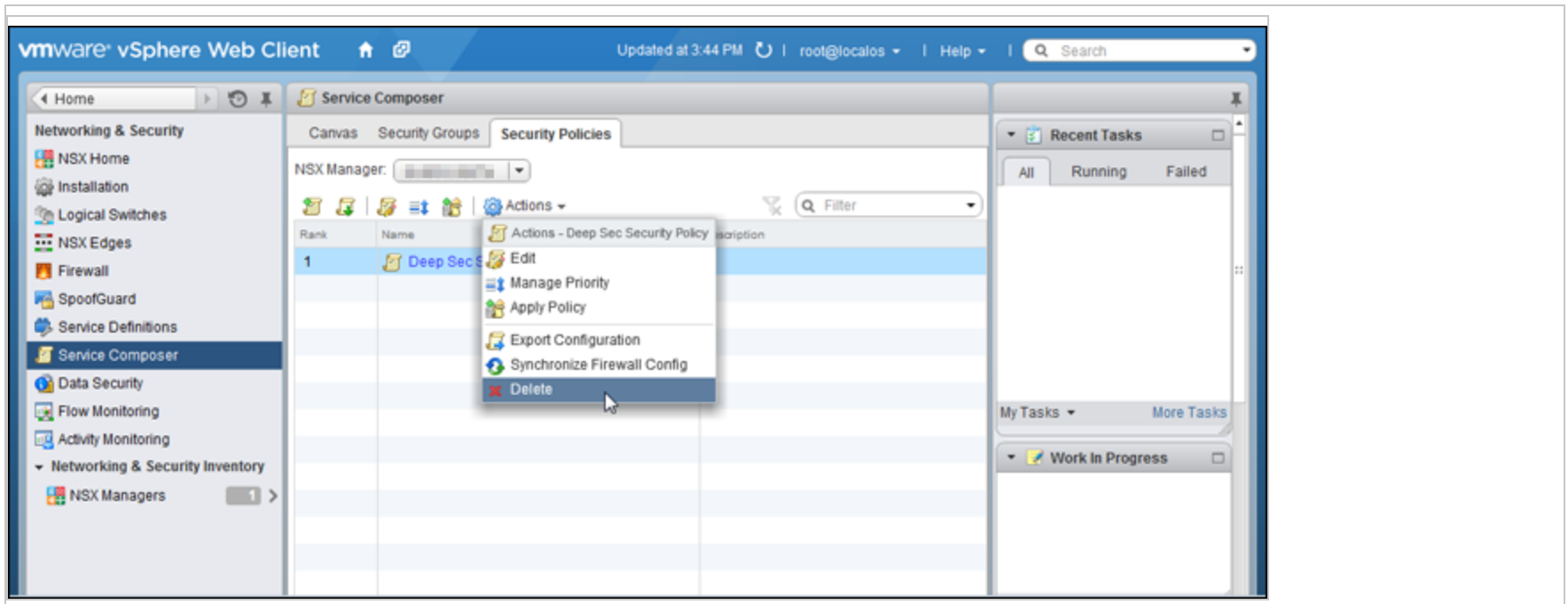
"[NSX-V環境からのDeep Securityの自動アンインストール](#)" on page 1508の手順に従ってvCenterをDeep Security Managerから削除する際に「VMwareからDeep Securityを削除できません」というエラーが表示された場合は、Deep Security ManagerとNSX Managerの接続が切断されている可能性があります。このエラーが発生した場合は、NSX ManagerからDeep Securityを手動で削除する必要があります。

最初に、Deep Security ManagerからNSX Managerを削除します

1. Deep Security Managerで、[コンピュータ]に進みます。
2. 左側のナビゲーションツリーでvCenterを右クリックして、[プロパティ]を選択します。
3. [NSX Manager] タブで、[NSX Managerの削除] をクリックします。
4. [OK] をクリックします。

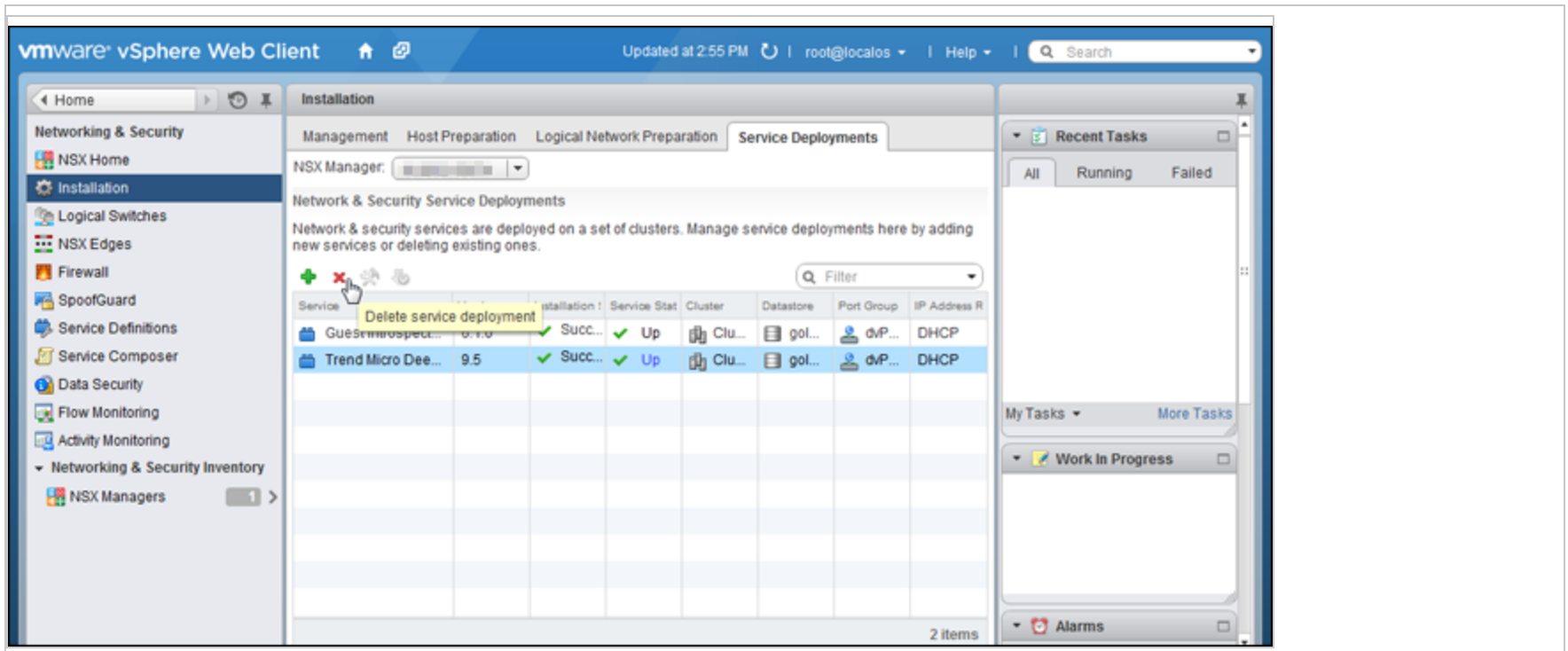
次に、NSX Managerでトレンドマイクロのサービスを削除します

1. vSphere Web Clientで、[Home]→[Networking and Security]→[Service Composer]→[Security Policies] の順に移動します。
- [Deep Security] セキュリティポリシーを削除します。

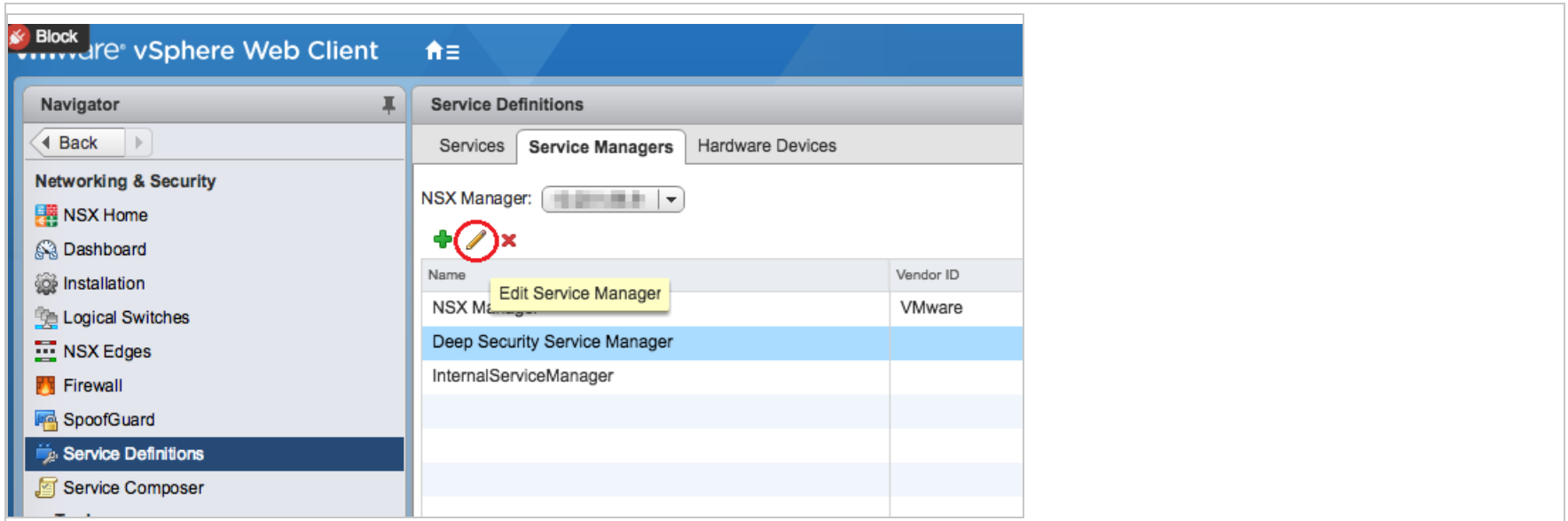


2. [Home]→[Networking and Security]→[Installation]→[Service Deployments] の順に移動します。

Trend Micro Deep Security サービスの配信を削除します。



3. [Home]→[Networking and Security]→[Service Definitions]→[Service Managers] の順に移動します。
[Deep Security Service Manager] を選択し、鉛筆アイコンをクリックします。[Operational State] を選択解除します。



Edit Service Manager

Name: * Deep Security Service Manager

Description: Service manager for DS services.

Administration URL:

Base API URL: https://[redacted]/rest

Credentials

Name: T0

Password:

Retype Password:

Thumbprint:

Vendor Details

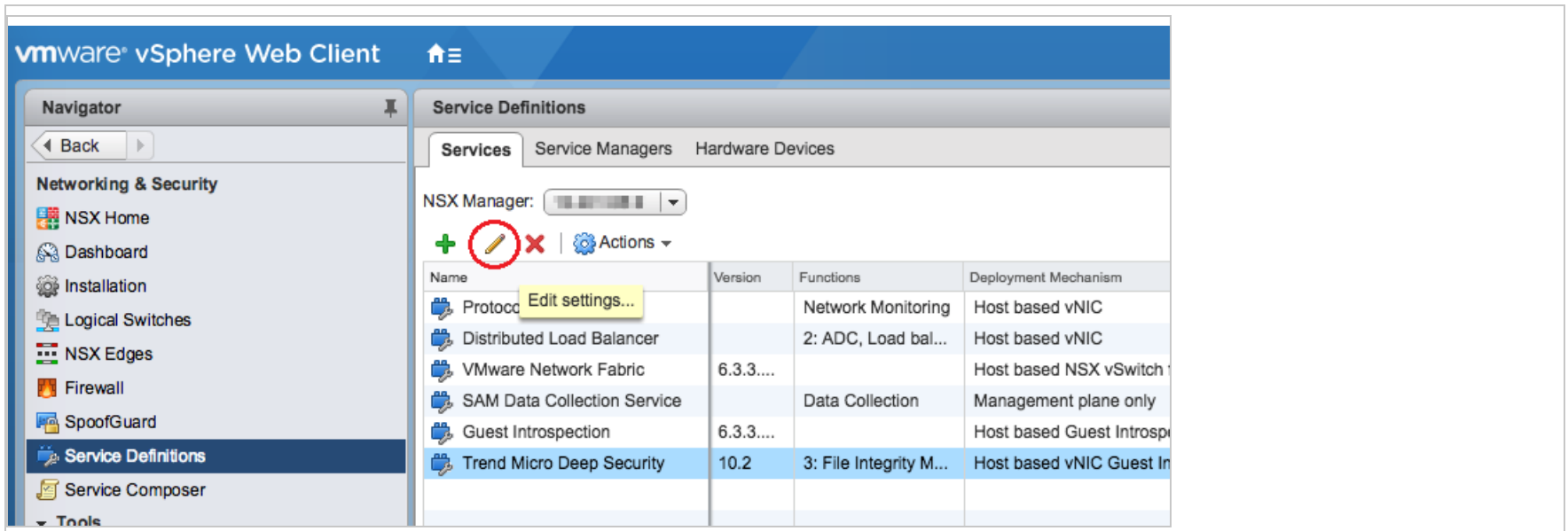
Vendor ID:

Vendor Name:

Operational State

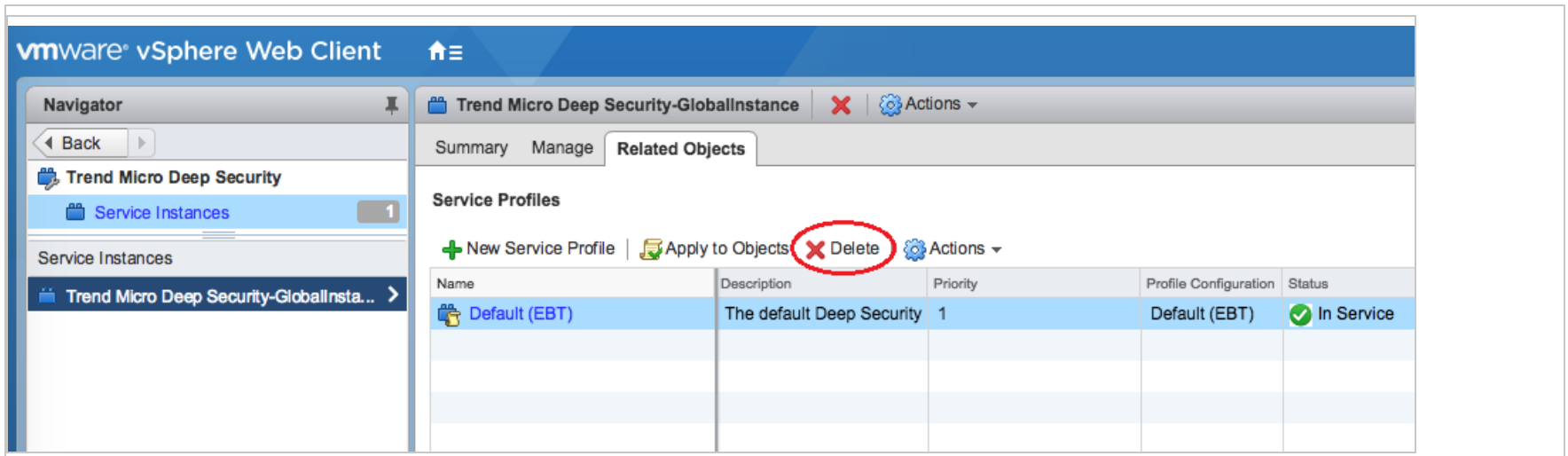
OK Cancel

4. [Home]→[Networking and Security]→[Service Definitions]→[Services] の順に移動します。
[Trend Micro Deep Security] をクリックし、鉛筆アイコンをクリックします。



5. 左側のナビゲーション画面で、[Service Instances] をクリックし、左側の [Trend Micro Deep Security-GlobalInstance] をクリックします。

メイン画面で、[Default (EBT)] を選択し、[Delete] をクリックしてサービスプロファイルを削除します。

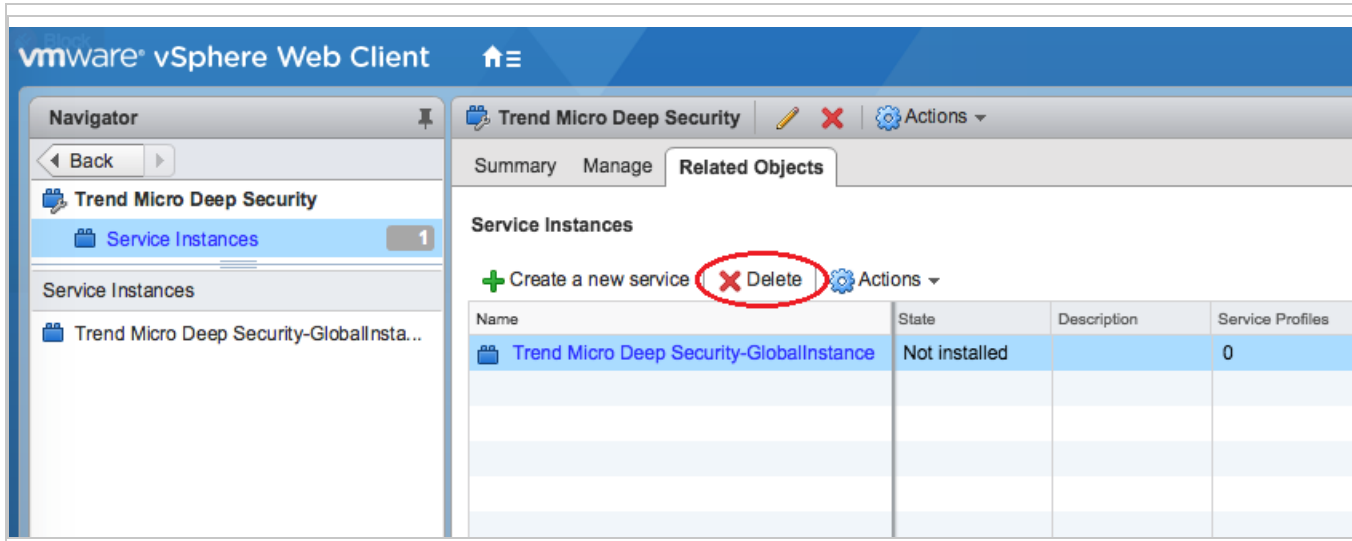


The screenshot shows the VMware vSphere Web Client interface for Trend Micro Deep Security. The left sidebar contains a 'Navigator' with 'Trend Micro Deep Security' and 'Service Instances' (1 instance). The main content area shows 'Trend Micro Deep Security-GlobalInstance' with tabs for 'Summary', 'Manage', and 'Related Objects'. Under 'Service Profiles', there are buttons for '+ New Service Profile', 'Apply to Objects', 'Delete' (circled in red), and 'Actions'. Below this is a table with the following data:

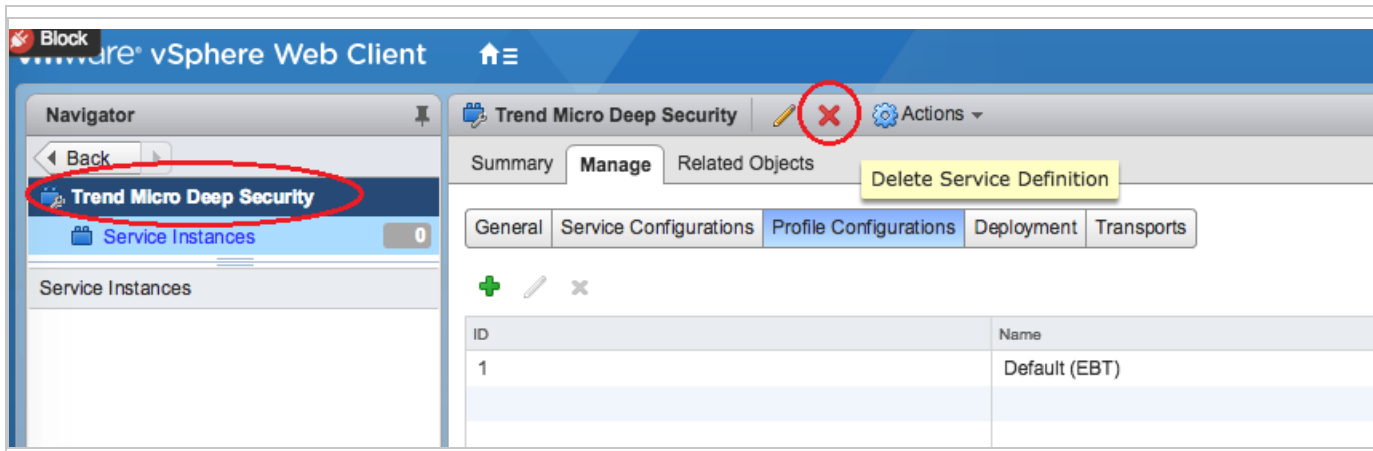
Name	Description	Priority	Profile Configuration	Status
Default (EBT)	The default Deep Security	1	Default (EBT)	In Service

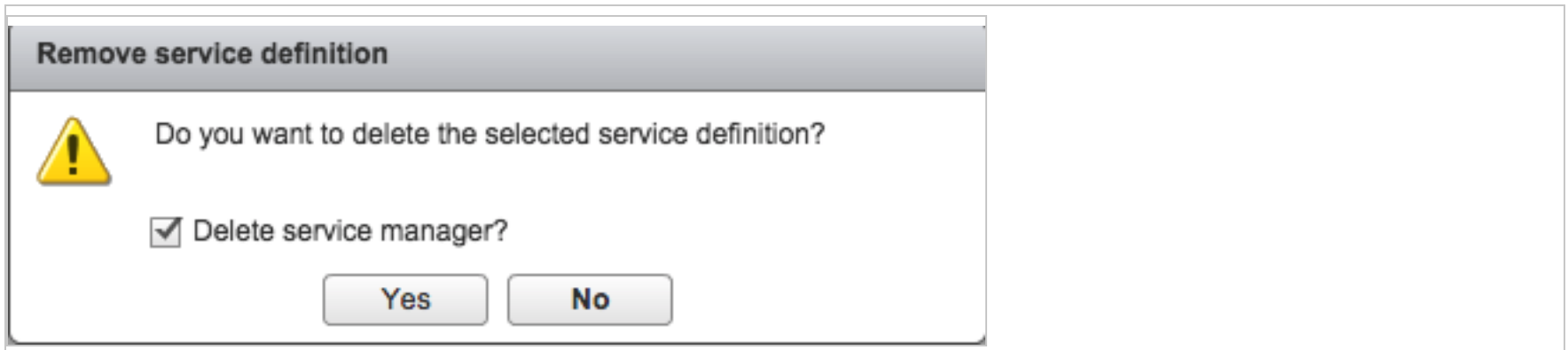
6. 左側のナビゲーション画面で、[Service Instances] をクリックします。

メイン画面で、[Trend Micro Deep Security-GlobalInstance] を選択し、[Delete] をクリックしてサービスインスタンスを削除します。



7. Trend Micro Deep Security のサービス定義を選択し、最上部の削除アイコンをクリックして削除します。





最後に、Deep Security ManagerからvCenterを削除します。

1. Deep Security Managerで、[コンピュータ]をクリックします。
2. 左側でvCenterを右クリックして [VMware vCenterの削除] をクリックします。

ウィザードが表示されます。このウィザードのオプションの説明については、"[NSX-V環境からのDeep Securityの自動アンインストール](#)" on page 1508を参照してください。

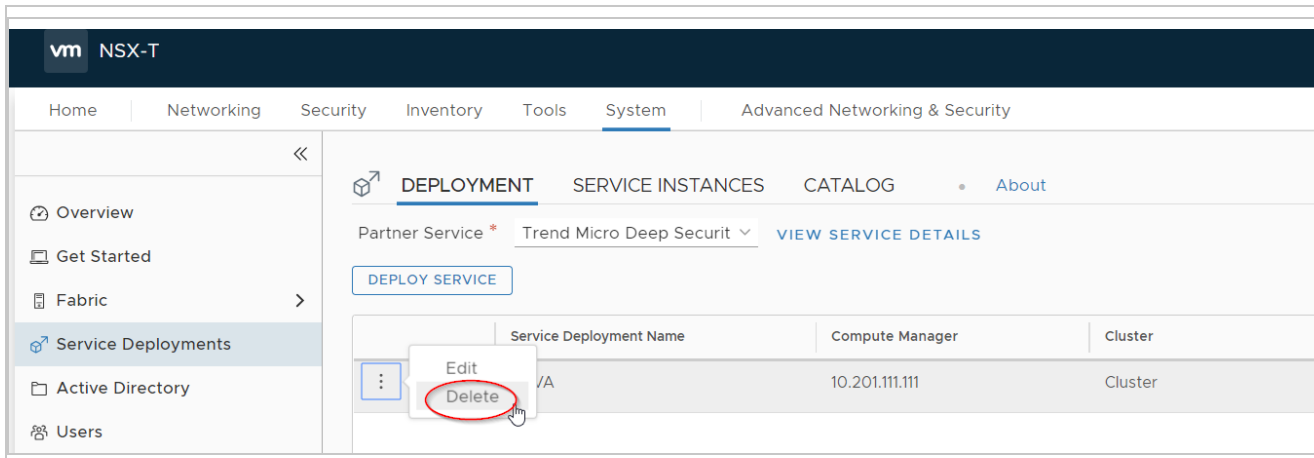
これで、NSX-V環境からDeep Securityを手動で削除することができました。

NSX-T環境からのDeep Securityの手動アンインストール

最初に、Deep Security Virtual Applianceサービスのインストールを削除します。

1. NSX-T Managerで、[System]→[Service Deployments]→[DEPLOYMENT] の順に進みます。
2. [Partner Service] ドロップダウンリストから、[Trend Micro Deep Security] を選択します。表示されていなかった場合、サービスのインストールが表示されます。

Trend Micro Deep Security On-Premise 12.0

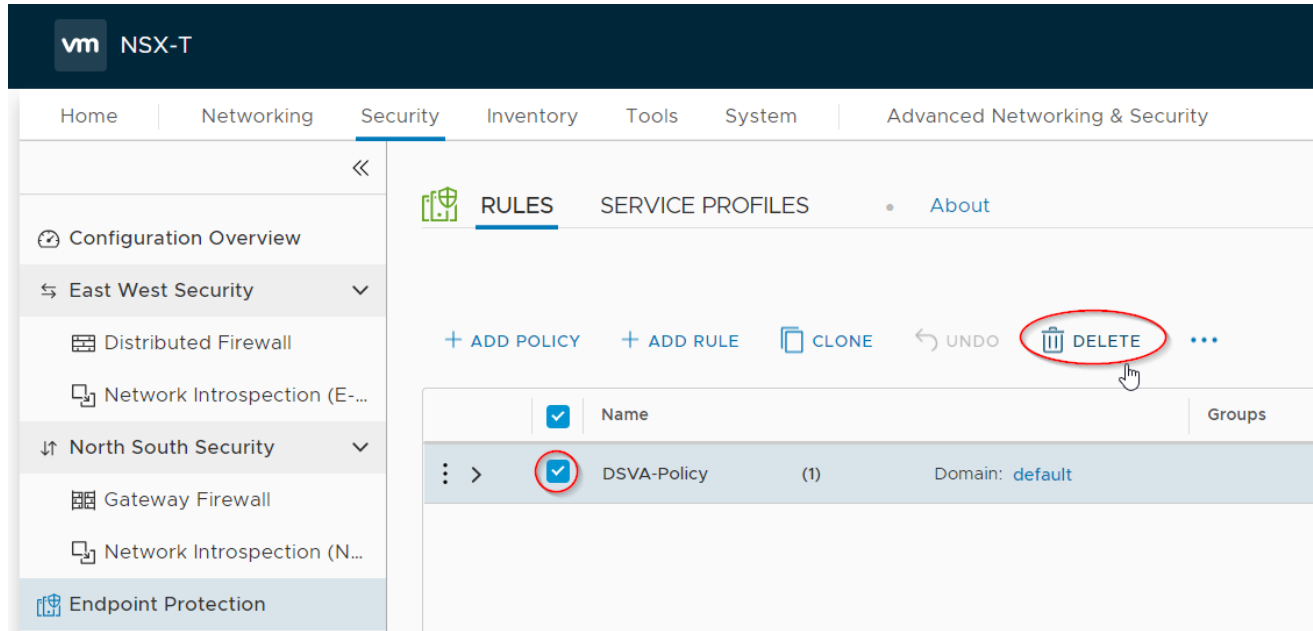


3. サービスのインストール名の横にある3つのドットをクリックして、[Delete] を選択します。

次に、Deep Security Virtual Applianceのポリシーと関連するルールを削除します。

Trend Micro Deep Security On-Premise 12.0

1. NSX-T Managerで、[Security]→[Endpoint Protection]→[RULES] の順にクリックします。

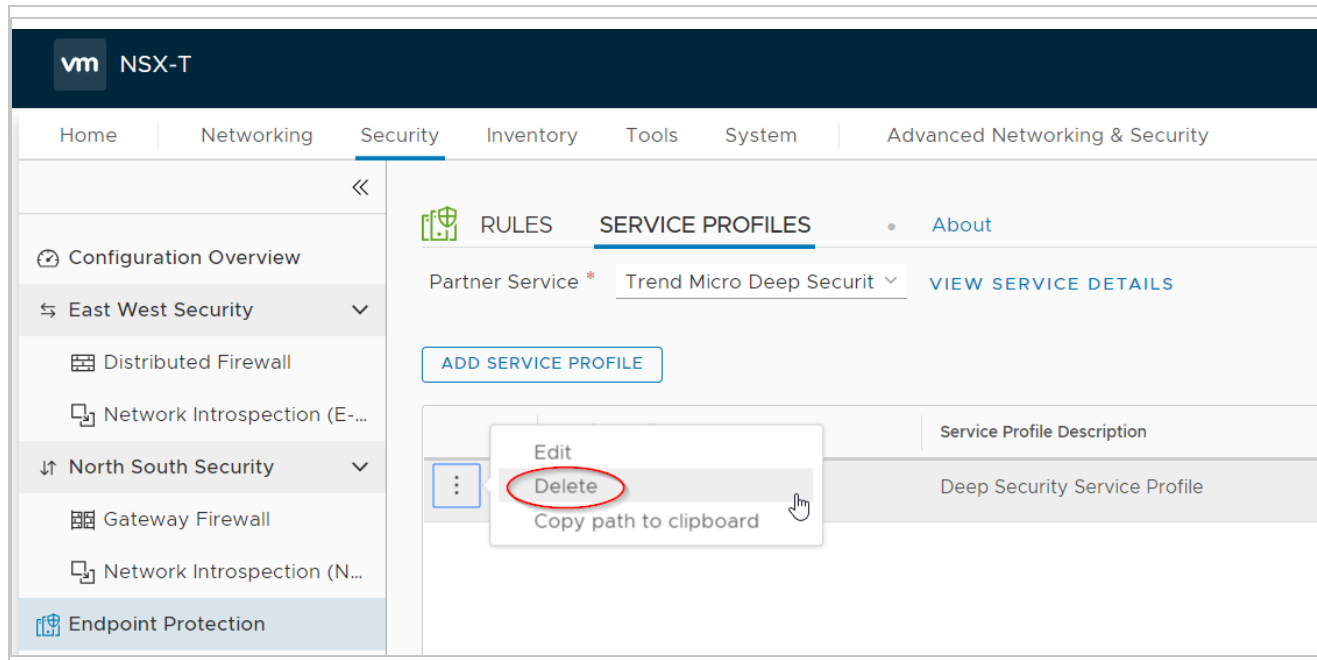


2. ポリシー選択して、[Delete] をクリックします。
3. 変更を反映するには、[Publish] をクリックします。ポリシーと関連するルールが削除されます。

次に、Deep Security Virtual Applianceサービスのプロファイルを削除します。

Trend Micro Deep Security On-Premise 12.0

1. NSX-T Managerで、[System]→[Endpoint Protection]→[SERVICE PROFILES] の順にクリックします。



2. サービスプロファイルの横にある3つのドットをクリックして、[Delete] を選択します。

最後に、Deep Security ManagerからvCenterを削除します。

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 左側でvCenterを右クリックして [VMware vCenterの削除] をクリックします。

ウィザードが表示されます。このウィザードのオプションの説明については、"[NSX-V環境からのDeep Securityの自動アンインストール](#)" on page 1508を参照してください。

これで、NSX-T環境からDeep Securityを手動で削除することができました。

非アクティブなAgentのクリーンアップによるオフラインコンピュータの削除の自動化

Deep Security Managerと通信していないオフラインコンピュータがDeep Security環境内に多数ある場合は、最初にコネクタを使用することをお勧めします ("[AWSクラウドアカウントの追加](#)" on page 516または"[Deep SecurityへのMicrosoft Azureアカウントの追加](#)" on page 539を参照)。コネクタを使用すると、コンピュータがライフサイクル全体を通して自動的に管理されるため、クラウドアカウントから削除されたコンピュータはDeep Securityからも自動的に削除されます。環境内でコネクタを使用できない場合は、[非アクティブなAgentのクリーンアップ]を使用して、非アクティブなコンピュータの削除を自動化できます。非アクティブなAgentのクリーンアップを有効にすると、指定された期間 (2週間~12か月) にわたってオフラインまたは非アクティブになっているコンピュータが1時間おきに確認され、このようなコンピュータが見つかった場合は削除されます。

注意: 非アクティブなAgentのクリーンアップを使用すると、1時間おきの確認時に最大で1000台のオフラインコンピュータが削除されます。これを上回る数のオフラインコンピュータがある場合は、確認時に1000台ずつ削除され、すべてのオフラインコンピュータが削除されるまでこの動作が繰り返されます。

非アクティブなAgentのクリーンアップを有効にした後には、次のことも行えます。

- "[長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護](#)" on the next page (任意ですが、有効にしておくことをお勧めします)
- "[オーバーライド設定による特定のコンピュータの削除の回避](#)" on the next page (任意)
- "[非アクティブなAgentのクリーンアップジョブによって削除されたコンピュータの監査証跡の確認](#)" on page 1525

注意: 非アクティブなAgentのクリーンアップでは、クラウドコネクタによって追加されたオフラインコンピュータは削除されません。

非アクティブなAgentのクリーンアップを有効にする

1. [管理] ページに移動します。
2. [システム設定]→[Agent]→[非アクティブなAgentのクリーンアップ] で、[次の期間を超過した非アクティブなAgentを削除する:] を選択します。
3. 非アクティブな期間がどのくらい続いているコンピュータを削除するかをリストから選択します。
4. アクティブではあるものの"[長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護](#)" [below](#) の設定をします (任意ですが、有効にしておくことをお勧めします)。
5. [保存] をクリックします。

長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護

アクティブではあるもののDeep Security Managerと不定期に通信しているオフラインコンピュータがある場合、定義した非アクティブ期間内に通信が行われなければ、それらのコンピュータは非アクティブなAgentのクリーンアップによって削除されます。それらのコンピュータがDeep Security Managerに再接続されるようにするには、[Agentからのリモート有効化] と [不明なAgentの再有効化] を両方とも有効にすることをお勧めします。これらを有効にするには、[システム設定]→[Agent]→[Agentからのリモート有効化] で、[Agentからのリモート有効化を許可] を選択した後、[不明なAgentの再有効化] を選択します。

注意: 削除されたコンピュータが再接続した場合、ポリシーは割り当てられず、新しいコンピュータとして追加されます。そのコンピュータへの直接リンクは、Deep Security Managerイベントデータからすべて削除されます。

ヒント: [イベントベースタスク](#)を使用すると、Agentからのリモート有効化の際に、コンピュータに割り当てられたポリシーを自動的に割り当てることができます。

オーバーライド設定による特定のコンピュータの削除の回避

コンピュータまたはポリシーレベルでオーバーライドを設定すると、非アクティブなAgentのクリーンアップによってコンピュータが削除されるのを明示的に回避できます。

オーバーライドを設定するには、次の手順に従います。

1. オーバーライドを設定するコンピュータやポリシーの**コンピュータエディタ**または**ポリシーエディタ**¹を開きます。
2. [設定]→[一般] に移動します。
3. [非アクティブなAgentのクリーンアップのオーバーライド] で、[はい] を選択します。
4. [保存] をクリックします。

非アクティブなAgentのクリーンアップジョブによって削除されたコンピュータの監査証跡の確認

非アクティブなAgentのクリーンアップジョブの実行時には、削除されたコンピュータの追跡に利用できるシステムイベントが生成されます。

次のシステムイベントを確認する必要があります。

- ["2953 - 非アクティブなAgentのクリーンアップが正常に完了しました" on the next page](#)
- ["251 - コンピュータの削除" on page 1527](#)
- ["716 - 不明なAgentの再有効化の試行" on page 1527](#) ([不明なAgentの再有効化] が有効になっている場合)

システムイベントを検索する

非アクティブなAgentのクリーンアップジョブによって生成されたシステムイベントを表示するには、次のように、それらのイベントを表示するためのフィルタ条件を追加した検索を作成する必要があります。

¹これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

1. [イベントとレポート] ページに移動します。
2. 右上にある検索フィールドのリストをクリックし、[詳細検索を開く] を選択します。



3. [期間] のリストから [カスタム範囲] を選択します。
4. [開始] に、非アクティブなAgentのクリーンアップジョブが最初に実行された時刻の直前にあたる日時を入力します。[終了] に、クリーンアップジョブが完了した時刻の直後にあたる日時を入力します。
5. [検索] で、[イベントID] と [次のリストに含まれる] を選択し、「2953, 251」と入力します。必要に応じて、「716」やコンピュータの再有効化に関連するイベントID (130, 790, 350, 250) を入力することもできます。

これにより、非アクティブなAgentのクリーンアップジョブによって生成されたすべてのシステムイベントが表示されます。時間、イベントID、またはイベント名の列をクリックすると、表示されているイベントをソートできます。その後、イベントをダブルクリックすると、以下で説明するイベントの詳細情報が表示されます。

システムイベントの詳細

2953 - 非アクティブなAgentのクリーンアップが正常に完了しました

このイベントは、非アクティブなAgentのクリーンアップジョブが実行され、コンピュータが正常に削除された場合に生成されます。このイベントの説明には、削除されたコンピュータの数が表示されます。

注意: すべてのコンピュータを削除するために複数回の確認が必要な場合は、確認が行われるたびにシステムイベントが生成されます。

251 - コンピュータの削除

「非アクティブなAgentのクリーンアップが正常に完了しました」イベントに加え、コンピュータが1台削除されるたびに「コンピュータの削除」イベントが生成されます。

716 - 不明なAgentの再有効化の試行

[不明なAgentの再有効化] が有効になっている場合は、削除済みの有効化されたコンピュータがDeep Security Managerへの再接続を試みると、このイベントが生成されます。再有効化されたコンピュータごとに、次のシステムイベントも生成されます。

- 130 - 資格情報の生成
- 790 - Agentからのリモート有効化の要求
- 350 - ポリシーの作成 (ポリシーを割り当てるイベントベースタスクが有効になっている場合)
- 250 - コンピュータの作成
または
252 - コンピュータのアップデート

Workload Securityへのポリシーの移行

現在Deep Securityを使用している場合は、この記事の手順に従ってDeep Security 12ポリシーを Trend Micro Cloud One - Workload Securityに移行できます。

への移行の詳細については、Workload Securityについては、[Deep Security 20のヘルプの移行に関する記事](#)を参照してください。

要件

1. ポリシーの移行をサポートするDeep Securityのバージョンを実行していることを確認します。
 - Deep Security Manager 12.0 LTS Update 17 (12.0.501) 以降
 - Deep Security Manager 12 FR 2020-04-29 (12.5.855) 以降
2. [をまだ契約していない場合は、Trend Micro Cloud One](#)にサインアップしてください。

その後、"ポリシーの移行" [below](#)を移行できます。

ポリシーの移行

1. ポリシーをXMLファイルにエクスポートします。Deep Security Managerのポリシーツリーで、ポリシーを選択し、[エクスポート]→[選択項目をXMLにエクスポート (インポート用)]の順に選択します。

注意: ポリシーをXMLにエクスポートすると、エクスポートされたパッケージに子ポリシーが含まれる場合があります。アプリケーションコントロール 設定は移行されません。ネットワークに依存するオブジェクトと設定 (プロキシ設定、Syslog設定など) は移行されないことがあります。

2. XMLファイルをgzipファイルに圧縮し、gzipファイルをBase64文字列にエンコードします。

Macの場合：

```
cat {Policy_File.xml} | gzip | base64 > {Policy_File.txt}
```

Linux (RedHat / CentOS / Ubuntu / Debian) の場合：

```
cat {Policy_File.xml} | gzip | base64 -w 0 > {Policy_File.txt}
```

Windowsの場合：

Windowsでのgzipコマンドの公式サポートはありません。

[7-Zip](#) for gzip圧縮をインストールし、次のコマンドを使用してgzipファイルをBase64文字列に転送できます。

```
certutil -encodehex -f {Policy_File.xml.gz} {Policy_File.txt} 0x40000001
```

3. [APIドキュメントに従って、ポリシーインポートタスク](#)を作成します。このタスクによって、ポリシーが Workload Security アカウントに移行されます。

注意: Workload Security コンソールを使用したポリシーのインポートは、現在サポートされていません。

4. ポリシーのインポートタスクでは、Deep Security Managerからエクスポートしたポリシーとその子ポリシーをインポートします。他のポリシーを移行する場合は、ポリシーをエクスポートして、複数のポリシーインポートタスクを作成します。

移行状態を確認する

[APIドキュメント](#) に従って、ポリシーインポートタスクの状態を確認します。

Status	Description
要求されました	Workload Security へのポリシー移行タスクが要求されました。 ポリシーの移行タスクがDeep Security Managerで受け入れられましたが、ポリシーの移行が開始されていません。
実行中	ポリシーを Workload Securityに移行しています。
完了	ポリシーが Workload Securityに正常に移行されました。
失敗	何らかの理由でポリシーを Workload Security に移行できませんでした。 のトラブルシューティングのセクションを確認してください。

トラブルシューティング

ステータスが「失敗」の場合：

- エラーコードが100の場合、Deep Security Managerのバージョンはサポートされていません。
- エラーコードが20xの場合は、ポリシーXMLファイルを確認し、ポリシーを再度エンコードします。
- その他のエラーについては、トレンドマイクロのテクニカルサポートにお問い合わせください。

よくある質問

保護をオンにするとWindowsマシンのネットワーク接続が失われる理由

Deep Security Agentがトラフィックの検査用にネットワークドライバをインストールする際、Windowsマシンは短時間ネットワークから接続されます。この状況は、次のいずれかを含むポリシーを初めて適用する場合にのみ発生します。

- Webレピュテーション
- ファイアウォール
- 侵入防御

Windowsマシンでは、上記3つの保護モジュールすべてに同じドライバを使用します。Webレピュテーション、ファイアウォールまたは侵入防御のいずれかがすでにオンの状態であれば、これらの機能の1つをオンにしても、ネットワークの切断は発生しません。Agentのアップグレード時にも、同様にネットワーク接続が一時的に途切れることがあります(ドライバもアップグレードする必要があるため)。

Deep Securityに関するニュースの取得方法

Deep Securityのニュースフィードは廃止されました。代わりに、["新機能" on page 85](#)

トレンドマイクロでは、毎週火曜日に新しいルールのアップデートをリリースし、新しい脅威が検出された場合には更なるアップデートを行います。各ルールのアップデートに関する詳細は、[トレンドマイクロの脅威百科事典](#)に掲載されています。

Solarisゾーンでのエージェント保護はどのように機能しますか？

Deep Security エージェントは、Solarisグローバルゾーンにのみ配置できます。お使いのSolaris環境で非グローバルゾーンを使用している場合、グローバルゾーンと非グローバルゾーンに対してAgentが提供可能な保護は、各保護モジュールによって異なります。

- [侵入防御](#)
- [ファイアウォール](#)
- [Webレピュテーション](#)
- [不正プログラム対策](#)
- [変更監視](#)
- [セキュリティログ監視](#)

SolarisへのDeep Security Agentのインストールについては、"[SolarisにAgentをインストールする](#)" on page 379を参照してください。

Solarisのドメインを保護する方法については、[を参照してください](#)のようにSolarisの管理ドメインと論理ドメインのエージェント保護の仕事は？。

侵入防御 (IPS)、ファイアウォール、およびWebレピュテーション

お使いのSolaris環境で非グローバルゾーンを使用している場合、侵入防御、ファイアウォール、およびWebレピュテーションのモジュールによって保護できるのは、グローバルゾーン、非グローバルゾーン、および外部IPアドレスの間でやり取りされる特

定のトラフィックフローのみです。Agentが保護できるトラフィックフローは、非グローバルゾーンで[共有IPネットワークインタフェース](#)と[専用IPネットワークインタフェース](#)のどちらを使用しているかで決まります。

カーネルゾーンでは[専用IPネットワークインタフェース](#)が使用され、トラフィックフローに対するAgentの保護はそのネットワーク設定に制限されます。

共有IPネットワークインタフェースを使用する非グローバルゾーン

共有IPの設定でAgentの保護対象となるトラフィックフローは次のとおりです。

トラフィックフロー	Agentによる保護
外部アドレス <-> 非グローバルゾーン	○
外部アドレス <-> グローバルゾーン	○
グローバルゾーン <-> 非グローバルゾーン	×
非グローバルゾーン <-> 非グローバルゾーン	×

専用IPネットワークインタフェースを使用する非グローバルゾーン

専用IPの設定でAgentの保護対象となるトラフィックフローは次のとおりです。

トラフィックフロー	Agentによる保護
外部アドレス <-> 非グローバルゾーン	×
外部アドレス <-> グローバルゾーン	○

トラフィックフロー	Agentによる保護
グローバルゾーン <-> 非グローバルゾーン	○
非グローバルゾーン <-> 非グローバルゾーン	×

不正プログラム対策、変更監視、およびセキュリティログ監視

不正プログラム対策、変更監視、およびセキュリティログ監視のモジュールは、グローバルゾーンを保護します。非グローバルゾーンについては、グローバルゾーンでも参照可能なファイルまたはディレクトリは保護されます。非グローバルゾーン固有のファイルは保護されません。

Solaris Control ドメインとLogical Domainsのエージェント保護はどのように機能しますか？

Deep Security Agentは、Solaris Control Domain (CDOM) およびLogical Domains (LDOM) をサポートしています。これには、同じ環境で実行されているCDOMとLDOMのサポートが含まれます。ただし、次の制限があります。

- コントロールドメイン上のエージェントは、同じサーバ上のLDOM間を流れるパケットに対してファイアウォール または 侵入防御 保護を適用できません。
- コントロールドメイン上のエージェントは、不正プログラム対策, 変更監視、またはセキュリティログ監視 検索を実行できません。サーバ上のLDOM内のファイルを検索します。

ヒント: 保護のため、すべてのCDOMおよびLDOMに Deep Security Agentをインストールすることをお勧めします。

Solaris CDOMとLDOMの詳細については、[Oracle VMサーバ管理ガイドの「Control Domain](#) および [Hypervisorの設定方法](#)」および [「Logical Domains](#) の設定方法」のセクションを参照してください。

エージェントのインストール手順については、[Deep Security Agent](#)の手動インストールを参照してください。

Solarisゾーンの詳細については、[を参照してくださいどのようにSolarisゾーンのエージェント保護の仕事は？](#)

Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか

AWSのEC2インスタンスで実行している場合、Deep Security AgentはAmazonインスタンスメタデータサービス (IMDS) を使用してEC2インスタンスに関する情報をクエリします。

注意: IMDS v2のDeep SecurityのサポートがDeep Security 12.0 update 10に追加されました。以前のバージョンのDeep Securityを使用している場合は、IMDS v1のみがサポートされているため、IMDS v1を使用してDeep Security AgentがメタデータをホストするためのAWS設定を行う必要があります。

Deep Security Agentによって取得された情報は、適切なAWSの下でエージェントが作動をDeep Security内占め、右のインスタンスのサイズは、計量された課金のために使用されていることを確認する必要があります。

Deep Security Agentがメタデータサービスバージョン1 (IMDSv1) または2 (IMDSv2,) を使用してインスタンスからデータを正常に取得できない場合は、次の問題が発生することがあります。

問題	根本原因	解決方法	その他の注意事項
重複したコンピュータが表示されます。1つはAWSアカウントの下、もう1つはAWSアカウントの外部に表示されます。	Deep Security AgentがInstance Metadata Service Version 1 (IMDSv1) または2 (IMDSv2), Deep Securityは、このアクティベーションを目的のクラウドアカウントに適切に関連付けることができません。	Deep SecurityがIMDS v1またはIMDS v2にアクセスで	あなたが重複したコンピュータの作成が発生したと判断した場合は、自動的にこれらのコンピュータを削除するには 非アクティブなエージェントのクリーンアップ を使用することができます。

問題	根本原因	解決方法	その他の注意事項
ワークロードのサイズに関連付けられているレートではなく、1時間あたりの\$00.06の初期設定レートでのインスタンス時間の請求が正しくありません。	Deep Security AgentがInstance Metadata Service Version 1 (IMDSv1) または2 (IMDSv2), Deep Securityはmetered課金のインスタンスサイズを適切に判断できません。その結果、コンピュータはクラウドアカウントの下に表示されず、データセンターの料金で課金されます。	<p>きることを確認してください。</p> <p>詳細については、インスタンスメタデータサービスの設定を参照してください。</p>	<p>過払いが発生したと思われる場合は、次の点を確認してください。</p> <ol style="list-style-type: none"> 1. Deep Security AgentはIMDS v1またはIMDS v2にアクセスできます。 2. Deep SecurityにAWSクラウドアカウントを追加しています。 <p>詳細については、テクニカルサポートにお問い合わせください。</p>
スマートフォルダまたはAWSメタデータに基づくイベントベースのタスクが失敗します。	Deep Security Agentがインスタンスメタデータサービスバージョン1 (IMDSv1) または2 (IMDSv2), Deep Securityはこれらの操作に必要なAWSメタデータにアクセスできません) へのアクセス権を持っていない場合。	<p>してください。</p>	N/A

AWS GovCloud (US) インスタンスを保護するにはどうすればいいですか？

Deep Security が [AWS GovCloud \(US\)](#) のサポートを提供する方法は2つあります。

- AWS GovCloudのAWS Marketplaceから入手可能な Trend MicroDeep Security AMI (Protected Instance HourまたはBYOLライセンスタイプ) を使用できます (US).AWS GovCloud (米国) リージョンのインストール手順は、その他のリージョンと同じです。 [「Deep Security AMI from AWS Marketplaceの使用開始」](#) を参照してください。

- AWS GovCloud (米国) リージョンで実行されているAWSインスタンスにDeep Securityソフトウェアのエンタープライズバージョンをインストールできます。

AWS GovCloud (US) のAWSインスタンスの管理者によるインスタンスの保護

警告: Deep Security ManagerがAWS GovCloudの外部にある場合、AWS GovCloudのコンピュータを管理するためにこのサービスを使用すると、ITARのコンプライアンスが損なわれる可能性があることに注意してください。

Deep Security Managerが商用AWSインスタンスにあり、AWS GovCloudインスタンスを保護するためにこのインスタンスを使用する場合は、Deep Security Managerコンソールにあるクラウドコネクタを使用してインスタンスを追加することはできません。Deep Security ManagerがAWS GovCloud) などの特定の地域で実行されている場合、その地域に接続したり、商用AWS地域のインスタンスに接続したりできます。しかし、Deep Security Managerが商業地域にいる場合、AWS GovCloudなどの特別な地域ではなく、すべての商用AWS地域に接続できます。

特定の地域コネクタ (AWS GovCloudなど) を商用AWSで実行されている Deep Security Managerに追加する場合は、Deep Security レガシREST APIを使用して `seedRegion` 引数を指定して、外部に接続していることを Deep Security Managerに通知する必要があります。商用AWSのAPIの詳細については、"[Deep Security APIを使用したタスクの自動化](#)" on page 478を参照してください。

Azure Governmentのインスタンスを保護するにはどうすればいいですか？

[Azure Government](#) インスタンスを保護するには、Azure GovernmentのMarketplace (下の画像を参照) 内に表示されている「Deep Security Manager (BYOL)」仮想マシンを使用してDeep Security Managerをインストールする必要があります。[グローバル Azure](#)のMarketplaceからインストールした場合やAzure Governmentの内外にあるAzureインスタンスにインストールした場合は、Deep Security ManagerでGovernmentインスタンスを保護できません。

Azure Government内でのDeep Security Manager (BYOL) のインストールの詳細については、このページの上部にあるバージョンセレクタを使用して [Deep Security 12.0 Azure Marketplace] オプションを選択した後、「Deep Security Manager


Trend Micro Deep Security On-Premise 12.0

「VM for Azure Marketplace」を検索して、インストールに関するトピックを見つけてください。Deep Security Manager (BYOL) は、インストールすると、通常のインスタンスと同じようにAzure Governmentインスタンスの保護に使用できます。

警告: Deep Security ManagerがAzure Governmentの外部にある場合、ManagerでAzure Government内のコンピュータを管理すると、[ITARコンプライアンス](#)に違反することになるので注意してください。

Make sure you deploy from Azure Government, and use the Deep Security Manager (BYOL) VM

The screenshot shows the Microsoft Azure Government Marketplace interface. The left sidebar contains navigation options: 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function Apps', and 'SQL databases'. The main content area is titled 'Marketplace' and shows a search for 'Deep Security Manager (BYOL)'. The search results are displayed under the heading 'Results' and include a table with the following entry:

NAME
 Deep Security Manager (BYOL)

The search bar and the search results are highlighted with a red box. A red arrow points from the text 'Make sure you deploy from Azure Government, and use the Deep Security Manager (BYOL) VM' to the search results.

AWS Elastic Beanstalk環境でオフライン環境に対するハートビートアラートを最小限に抑える方法

AWS Elastic Beanstalkを使用すると、複数の環境を作成して異なるバージョンのアプリケーションを同時に実行することができます。複数の環境には一般に実稼働環境と開発環境が含まれ、多くの場合、夜間は開発環境の電源が停止されます。翌日になって開発環境をオンラインに戻すと、オフラインだった時間帯について、Deep Securityから通信の問題に関するアラートが生成されます。これらのアラートは実際には不要なものですが、Deep Securityでは指定の数のハートビートが失われると常にアラートを生成するため誤検出というわけではありません。

これらのハートビート関連のアラートを最小限に抑え、毎日同じ時間帯にオフラインになることがわかっている環境についてアラートが生成されないようにするには、ハートビート設定を含むポリシーを作成し、そのポリシーを時間帯によってオフラインになる環境のサーバに適用します。

1. Deep Security Managerのメイン画面の [ポリシー] タブに移動します。
2. 新しいポリシーを作成するか、既存のポリシーを編集します。
3. **ポリシーエディタ**¹で [設定] タブをクリックし、[コンピュータ] タブに移動します。
4. Elastic Beanstalk環境がオフラインになる時間を考慮して、[ハートビート間隔] 設定または [次の数を超えるハートビートが失われた場合にアラートを発令] 設定、あるいはその両方を変更します。
たとえば、サーバが1日のうち12時間はオフラインになることがわかっていて、[ハートビート間隔] が10分に設定されている場合は、[次の数を超えるハートビートが失われた場合にアラートを発令] 設定を「無制限」に設定してアラートが発令されないようにしたり、[ハートビート間隔] を10分よりも長くしてアラートの数を抑えたりできます。
5. [保存] をクリックし、関連するすべてのサーバにポリシーを適用します。

AWS Elastic Beanstalk環境でのDeep Securityの使用の詳細については、トレンドマイクロのウェビナー「[Deploying Scalable and Secure Web Apps with AWS Elastic Beanstalk and Deep Security](#)」をご覧ください。

¹ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

Azureクラウドコネクタを使用してAzureサーバを追加できない

AzureサーバとAzureメタデータサービスとの接続が失われた場合、Deep Security ManagerはそのサーバをAzureサーバとして識別できなくなり、Azureクラウドコネクタを使用してAzureサーバを追加することはできません。

この状況は、Azureコンソールの外部でサーバのパブリックIPアドレスまたはプライベートIPアドレスが変更された場合に発生することがあります。AzureサーバはDHCPを使用してメタデータサービスと通信しますが、コンソールの外部でIPを変更するとDHCPが無効になります。

Microsoftでは、Windows仮想マシンに複数のIPアドレスを割り当てるなどの必要がない限り、Azure仮想マシンのオペレーティングシステム内からIPアドレスを変更しないことを推奨しています。詳細については、[こちらのAzureの記事](#)を参照してください。

AzureサーバがAzureメタデータサービスに接続できるかどうかを確認するには、[Windows Azure仮想マシンを検出する](#)ためのPowerShellスクリプトをMicrosoftスクリプトセンターからダウンロードして実行します。

Deep SecurityでAzureサブスクリプションの一部の仮想マシンが表示されない

Azureサブスクリプションの一部の仮想マシンリソースがDeep Security Managerの [コンピュータ] 画面に表示されない場合、それらのリソースがAzureのデプロイモデルであるResource Managerを使用してデプロイされているためと考えられます。[Select a deployment model] リストから [Classic] を選択しないかぎり、このモデルを使用してすべてのリソースがデプロイされます。

Deep Security Managerの古いバージョンでは、Azure仮想マシンへの接続にAzureのクラシックデプロイモデル (Service Managementモデル) で提供される[サービス管理API](#)を使用しているため、クラシックモデルでデプロイされた仮想マシンしか列挙できず、一部の仮想マシンが表示されません。

クラシック仮想マシンとResource Manager仮想マシンの両方を表示するには、クラウドコネクタをアップグレードします。詳細については、"[新しいAzure Resource Manager接続機能へのアップグレードについて](#)" on page 545を参照してください。

注意: 上記のトピックのようにResource Managerサーバをアップグレードできない場合でも、仮想マシン上でインストールスクリプトを使用して、有効化によりコネクタ外に新しいコンピュータオブジェクトが作成されるようにすることで、保護できます。

トラブルシューティング

「オフライン」のAgent

コンピュータの[ステータス](#)が [オフライン] または [管理対象 (オフライン)] の場合、Deep Security ManagerはDeep Security Agentのインスタンスとしばらく通信していない状態で、失われたハートビートのしきい値を超過しています。 ("[ハートビートを設定する](#)" on page 400を参照してください)。このステータスの変化はアラートおよびイベントにも示されます。

原因

ハートビート接続が失敗する原因としては次のことが考えられます。

- Agentは、シャットダウンしたワークステーションまたは他のコンピュータにインストールされます。Deep Securityを使用してシャットダウンされることがあるコンピュータを保護している場合、これらのコンピュータに割り当てられたポリシーは、ハートビートが失われたときにアラートを発令しません。ポリシーエディタで、[設定]→[一般]→[次の数を超えるハートビートが失われた場合にアラートを発令] に移動し、設定を [無制限] に変更します。
- ファイアウォール、IPSルール、またはセキュリティグループが、ハートビート[ポート番号](#)をブロックしている。

- 送信 (エフェメラル) ポートが誤ってブロックされた。トラブルシューティングのヒントについては、"[ポートのブロック](#)" [on page 1349](#)を参照してください。
- 双方向通信が有効になっているが、許可されている、または安定しているのが一方向のみである ("[通信方向を設定する](#)" [on page 401](#)を参照)。
- コンピュータの電源がオフになった。
- コンピュータがプライベートネットワークの[コンテキスト](#)外に移動した。
この状況は、ローミングを使用しているエンドポイント (ノートパソコンなど) が現在の場所でManagerに接続できない場合に発生します。たとえば、ゲストWi-Fiではオープンポートを制限することが多く、トラフィックがインターネットを通過するときにNATを使用します。
- Amazon WorkSpaceのコンピュータの電源をオフにしようとしていて、ハートビート間隔が短い (1分など)。この場合、WorkSpaceの電源がオフになるまで待ちます。オフになった時点でステータスは「オフライン」から「仮想マシン停止」になります。
- DNSが停止したか、Managerのホスト名を解決できなかった。
- Manager、Agent、またはその両方で、システムリソースの負荷が非常に高い。
- Agentプロセスが稼働していない可能性がある。
- SSLまたはTLS接続の[相互認証](#)用証明書が無効になったか失効した ("[Deep Security Manager TLS証明書の置き換え](#)" [on page 1057](#)を参照)。
- AgentまたはManagerのシステム時間が正しくない (SSL/TLS接続で必要)。
- Deep Security Deep Security の[ルールアップデート](#)中で、接続が一時的に中断している。
- AWS EC2で、ICMPトラフィックが必要だが、ブロックされている。

ヒント: Managerからの通信または双方向の通信で問題が発生した場合は、Agentからのリモート有効化に変更することを強く推奨します ("[Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する](#)" [on page 408](#)を参照)。

エラーをトラブルシューティングするには、Agentが実行されていること、およびManagerと通信できることを確認します。

Agentが実行されていることを確認する

Agentがインストールされたコンピュータで、Trend Micro Deep Security Agentサービスが実行されていることを確認します。方法はOSによって異なります。

- Windowsの場合は、Microsoft Windowsサービスコンソール (services.msc) またはタスクマネージャーを開きます。ds_agentという名前のサービスを探します。
- Linuxの場合は、ターミナルを開き、プロセスをリストするコマンドを入力します。次のコマンドを実行して、ds_agentまたはds-agentという名前のサービスを検索します。

```
sudo ps -aux | grep ds_agent  
sudo service ds_agent status
```

DNSを検証する

AgentがIPアドレスではなくドメイン名またはホスト名でManagerに接続する場合は、DNS解決をテストします。

```
nslookup [manager domain name]
```

DNSサービスは信頼できるものでなければなりません。

テストが失敗した場合は、Agentが正しいDNSプロキシまたはDNSサーバを使用していることを確認します (GoogleやISPなどのパブリックDNSサーバでは内部ドメイン名を解決できません)。IPアドレスに正しいルートとファイアウォールポリシーが設定されていても、dsm.example.comなどの名前をIPアドレスに解決できないと、通信は失敗します。

[ネットワークエンジンの詳細] 領域のコンピュータまたはポリシー設定で、コンピュータがDHCPを使用している場合は、[DHCP DNSを強制的に許可] の有効化が必要になる場合があります ("[ネットワークエンジン設定](#)" on page 612を参照)。

送信ポートを許可する (Agentからのハートビート)

Managerの[必要なポート番号](#)にtelnetで接続して、ルートが存在し、ポートが開いていることを確認します。

```
telnet [manager IP]:4120
```

ヒント: telnetの成功はpingの成功とほぼ同意味を持ち、ルートと正しいファイアウォールポリシーが存在すること、およびEthernetフレームサイズが正しいことを示しています(Managerの初期設定のセキュリティポリシーを使用するコンピュータでは、pingが無効になっています。攻撃者による予兆検索を阻止するためにネットワークがICMP pingとtracerouteをブロックすることがあるため、通常はManagerへpingを実行してテストすることはできません)。

telnetが失敗した場合は、ルートをトレースして、ネットワークのどのポイントで接続が中断されているかを特定します。

- Linuxの場合は次のコマンドを入力します。

```
traceroute [agent IP]
```

- Windowsの場合は次のコマンドを入力します。

```
tracert [agent IP]
```

ファイアウォールポリシー、ルート、NATポート転送、またはこれら3つすべてを調整して、問題を解決します。WindowsファイアウォールやLinuxのiptablesなど、ネットワークおよびホストベースのファイアウォールの両方を確認します。AWS EC2インスタンスの場合は、Amazonのドキュメントの[「Linux インスタンスの Amazon EC2 セキュリティグループ」](#)または[「Windows インスタンスの Amazon EC2 セキュリティグループ」](#)を参照してください。Azure VMインスタンスについては、[Network Security Groupの変更](#)に関するMicrosoftのAzureドキュメントを参照してください。

AgentからManagerへの接続テストが成功したら、次に逆方向の接続をテストする必要があります(ファイアウォールおよびルータでは、1組のポリシー/ルートがないと接続が許可されないことがよくあります。2つ必要なポリシーまたはルートのうち1つしか存在しない場合は、一方向のパケットだけが許可され、逆方向は許可されません)。

受信ポートを許可する (Managerからのハートビート)

ManagerからAgentにpingを実行し、ハートビートポート番号にtelnetで接続して、ハートビートと設定のトラフィックがAgentに到達できることを確認します。

```
ping [agent IP]
```

```
telnet [agent IP]:4118
```

pingとtelnetが失敗した場合は、次のコマンドを実行します。

```
tracert [agent IP]
```

これによって、ネットワークのどのポイントで接続が中断されているかを検出します。ファイアウォールポリシー、ルート、NATポート転送、またはこれら3つすべてを調整して、問題を解決します。

IPSルールまたはファイアウォールルールがAgentとManagerの間の接続をブロックしている場合は、Managerが接続して問題の原因であるポリシーを割り当て解除することができません。解決するには、コンピュータで次のコマンドを実行してAgentのポリシーをリセットします。

```
dsa_control -r
```

注意: このコマンドを実行した後に、Agentを再び有効化する必要があります。

Amazon AWS EC2インスタンスでICMPを許可する

AWSクラウドでは、ルータにICMP type3 code4が必要です。このトラフィックがブロックされていると、AgentとManager間の接続が中断される場合があります。

Deep Securityで強制的にこのトラフィックを許可できます。強制的に許可するファイアウォールポリシーを作成するか、コンピュータまたはポリシーの [ネットワークエンジンの詳細オプション] で、[ICMP type3 code4を強制的に許可] を有効にします ("[ネットワークエンジン設定](#)" on page 612を参照)。

Solaris 11でのアップグレードの問題を解決する

Solaris 11にDeep Security Agent 9.0がインストールされている場合、先に9.0.0-5616以降の9.0 AgentをインストールせずにAgentソフトウェアを11.0へ直接アップグレードすると、問題が発生することがあります。このようなシナリオでは、アップグレード後にAgentが起動しなくなり、Deep Security Managerでオフラインと表示されることがあります。この問題を解決するには、次の手順に従います。

1. サーバからAgentをアンインストールします。"[Deep Security Agentをアンインストールする](#)" on page 1503を参照してください。
2. Deep Security Agent 11.0をインストールします。"[SolarisにAgentをインストールする](#)" on page 379を参照してください。
3. ManagerでAgentを再有効化します。"[Agentの有効化](#)" on page 430を参照してください。

CPU使用率が高い

Deep Security Agentで保護されているコンピュータでは、次の手順を実行することで、CPU使用率が高い原因を特定して問題を解決することができます。

1. Trend Micro Deep Security Agentのプロセス (Windowsではds_agent.exe) のCPU使用率が異常に高いことを確認します。方法はOSによって異なります。

Windows:タスクマネージャー

Linux:top

Solaris:prstat

AIX:topas

2. Agentが最新バージョンにアップデートされていることを確認します。
3. ["不正プログラム対策のパフォーマンスのヒント" on page 750](#)および["侵入防御のパフォーマンスに関するヒント" on page 832](#)の推奨設定を適用します。
4. アプリケーションコントロールを有効にしたばかりの場合は、初期ベースラインルールセットの作成が完了するまで待機します。必要な時間は、ファイルシステム上のファイル数によって異なります。CPU使用率が低下するはずですが。
5. 推奨設定の検索を実行している場合は、コンピュータの負荷が低いときに検索を実行するようにします。仮想マシンの場合は、vCPUをさらに割り当てます。
6. 一時的に不正プログラム対策などの各保護機能を1つずつ無効にします。無効にするたびにCPU使用率を確認し、特定のモジュールが原因かどうかを確認します。
7. CPU使用率が依然として高い場合は、Agentを一時的に停止します。Agentが停止されているときに問題が解決するかどうかを確認します。問題が解決した場合、[診断情報を収集](#)し、サポート担当者に提出してください。

VMwareの「不正プログラム対策ドライバがオフライン」ステータス

[「不正プログラム対策エンジンがオフライン」](#)を参照してください。

Windowsプラットフォーム用不正プログラム対策のアップデート失敗

エラーメッセージをダブルクリックして、詳細情報を表示します。エラーイベントの「メッセージ」には、次のような内容が含まれます。

- ["互換性のない他のトレンドマイクロ製品の不正プログラム対策コンポーネント" on the next page](#)
- ["互換性のないサードパーティ製品の不正プログラム対策コンポーネント" on the next page](#)
- ["その他のエラー/不明なエラー" on the next page](#)

互換性のない他のトレンドマイクロ製品の不正プログラム対策コンポーネント

このエラーを解決する方法を以下に示します。

1. 互換性のないトレンドマイクロ製品 (ウイルスバスター コーポレートエディション、Endpoint Sensorなど) をアンインストールします。
2. Deep Security Agentを再インストールします。

互換性のないサードパーティ製品の不正プログラム対策コンポーネント

このエラーを解決する方法を以下に示します。

1. サードパーティ製品をアンインストールします。
2. Deep Security Agentを再インストールします。
3. サードパーティソフトウェアの例外リストにDeep Securityを追加します。不明点がある場合は、トレンドマイクロのサポートにお問い合わせください。

その他のエラー/不明なエラー

このエラーを解決する方法を以下に示します。

1. Deep Security Agentを一度アンインストールして再インストールします。
2. この方法でエラーが解決しない場合は、トレンドマイクロのサポートにお問い合わせください。

Agentレスによる仮想マシンのパフォーマンスの問題

原因:限られたリソース

1. Deep Security Virtual Agentリソースが確保されていることを設定から確認します。
2. インストール手順に指定されている要件を環境が満たしていることを確認します。

原因:不正プログラム対策

1. Deep Security Managerで、[コンピュータ]に進みます。
2. 保護されているコンピュータをダブルクリックします。
3. [不正プログラム対策]で[オフ]を選択します。

原因:ネットワークトラフィック

- パフォーマンスの低下を招くだけでセキュリティの強化には寄与しないことがわかっている場所を検索から除外します。

注意: ドライブレベルの検索除外では大文字と小文字が区別されます。

原因:ポリシー

- 仮想マシンのポリシー設定を[なし]に変更します。

原因:CPU使用率が高い

1. CPU使用率が高いDeep Security Virtual Agentを特定します。
 - vCenterコンソールに移動して、各Deep Security Virtual Agentをクリックし、[Performance] を選択してCPU使用率が高いマシンを特定します。
2. topコマンドを実行して、最もCPUを消費しているプロセスを確認します。
3. CPU使用率が高いプロセスのメモリ消費量を特定します。
 - a. 次のコマンドを実行して、プロセスメモリのステータスを確認します。#cat /proc/\$PID/status (\$PIDは実際のPIDに置き換えます。)
 - b. 仮想マシンのサイズが妥当であることを確認します。
 - c. 次のコマンドを使用して、コンテンツをログファイルにエクスポートします。

```
#cat /proc/$PID/status > /tmp/HighCPUProcessMemeory.txt
```

```
#sudo lsof -p $PID > /tmp/HighCPUProcessOpenedFile.t
```

4. Deep Security Virtual Agentに十分な空きメモリがあることを確認します。
 - a. cat /proc/meminfo コマンドを実行して、Deep Security Virtual Agentシステムの空きメモリを特定します。
 - b. cat /proc/meminfo > /tmp/DSVAMemory.txt コマンドを実行して、コンテンツをログファイルにエクスポートします。

原因:セキュリティアップデート

1. Relayとそのアップデート元またはプロキシサーバ間の接続を確認します。
 - a. プロキシサーバを使用する必要があるかどうかを確認します。
 - b. Deep Securityにログインし、[管理]→[システム設定]→[プロキシ] に移動して、設定が正しいことを確認します。
2. AgentとRelay有効化済みAgent間のpingテストを実行します。
3. telnet [RelayのIP] [ポート番号] を実行して、[Relayのポート番号](#)が開いていることを確認します。
4. DNSをテストして、Relayのホスト名を解決できるかどうかを確認します。

5. 通信がファイアウォールによってブロックされているかどうかを確認し、ブロックされている場合はファイアウォールを無効にします。
6. 現在のポリシーの割り当てを解除して、問題が解決されたかどうかを確認します。

セキュリティアップデートの接続

Relayサーバとそのアップデート元またはプロキシサーバとの間の接続を確認します。

1. ルートが存在すること、および[Relayのポート番号](#)が開いていることを確認するために、次のコマンドを入力します。

```
telnet [relay IP] [port number]
```

telnetが失敗した場合は、pingまたはtracertを実行して、ルートが存在すること、およびファイアウォールポリシー(存在する場合)がトラフィックを許可していることを確認します。また、ポート番号が開いていて、ポートの競合が発生していないことも確認します。

2. DNSサーバがRelayのドメイン名を解決できることを確認するために、次のコマンドを入力します。

```
nslookup [relay domain name]
```

テストが失敗した場合は、Agentが正しいDNSプロキシまたはDNSサーバを使用していることを確認します (GoogleやISPなどのパブリックDNSサーバでは内部ドメイン名を解決できません)。

3. プロキシサーバを使用する場合は、Deep Securityで[プロキシの設定](#)が正しいことを確認します。
4. Deep Securityの設定によって接続がブロックされているかどうかを確認するには、現在のポリシーの割り当てを解除します。

SQL Serverドメイン認証の問題

Deep Security Managerのインストール時にSQL Serverデータベースへの接続の問題が発生した場合は、以下の手順に従って問題をトラブルシューティングしてください。

注意: このトピックで扱う範囲は、Windowsドメイン認証の問題に限定されています。SQL Server認証を使用している場合は、「["Deep Security Managerで使用するデータベースの準備" on page 206](#)」を参照し、そのトピックに記載されている設定手順を確認して問題をトラブルシューティングします。

ヒント: 「Windowsドメイン認証」は、さまざまな名前と呼ばれます。Kerberos認証、ドメイン認証、Windows認証、統合認証などです。このトピックでは、「Kerberos」および「Windowsドメイン認証」という用語を使用しています。

"手順1: ホスト名とドメインを確認する" [below](#)

"手順2: servicePrincipalName (SPN) を確認する" [on page 1554](#)

"手順3: krb5.confファイルを確認する (Linuxのみ)" [on page 1568](#)

"手順4: システム時計を確認する" [on page 1570](#)

"手順5: ファイアウォールを確認する" [on page 1570](#)

手順1: ホスト名とドメインを確認する

[ホスト名] フィールドがFQDN形式であり、DNSサーバによって解決可能であることを確認する必要があります。

1. Deep Security Managerのインストーラを実行して、データベースの手順まで来たら、必ずSQLサーバのFQDNを指定してください。IPアドレスやNetBIOSホスト名を入力しないでください。

有効なホスト名の例: `sqlserver.example.com`

2. FQDNが登録されていて、DNSサーバによって解決可能であることを確認してください。DNSエントリに正しいホスト名が設定されているかどうかを確認するには、`nslookup` コマンドラインユーティリティを使用します。このユーティリティは、ドメイン上の任意のコンピュータから呼び出すことができます。次のコマンドを入力します。

```
nslookup <SQL Server FQDN>
```

ここで、`<SQL_Server_FQDN>` は、SQLサーバのFQDNに置き換えます。指定したFQDNをユーティリティが正常に解決できる場合、DNSエントリは正しく設定されています。FQDNを解決できない場合は、DNS Aレコードと、FQDNを含むリバースレコードを設定します。

3. さらに、インストーラのデータベースページで [詳細] をクリックし、[ドメイン] フィールドにSQLサーバの完全ドメイン名を指定します。ドメインには1つ以上のドット (「.」) を含める必要があります。短縮ドメイン名やNetBIOS名を入力しないでください。

有効なドメイン名の例: `example.com`

4. `nslookup` コマンドラインユーティリティを使用して、ドメイン名がFQDN形式であることを確認します。次のコマンドを入力します。

```
nslookup <Domain_Name>
```

ここで、`<Domain_Name>` は、SQLサーバの完全ドメイン名に置き換えます。指定したドメイン名をユーティリティが解決できる場合、それは完全なドメイン名です。

注意: Microsoftワークグループを使用したデータベース認証は、Deep Security Manager 10.2以降ではサポートされていません。Windowsドメイン認証の場合は、Active Directoryドメインコントローラをインストールし、ドメインを設定して、このドメインにSQLサーバを追加する必要があります。環境にActive Directoryドメインインフラストラクチャがない場合は、代わりにSQL Server認証を使用する必要があります。Windowsドメイン認証の代わりにSQL Server認証を使用するには、Managerのインストーラの [データベース] ページにある [ユーザ名] フィールドと [パスワード] フィールドに、Deep Security Managerデータベースの所有者のユーザ名とパスワードを入力します。ドメインを入力しないでください。

さい。ドメイン名を省略すると、SQL Server認証が使用されます。詳細については、「["Microsoft SQL Server" on page 208](#)」を参照してください。

手順2: servicePrincipalName (SPN) を確認する

servicePrincipalName (SPN) がActive Directoryで正しく構成されていることを確認する必要があります。

Microsoft SQL Serverの場合、SPNは次の形式です。

```
MSSQLSvc/<SQL_Server_Endpoint_FQDN>
```

```
MSSQLSvc/<SQL_Server_Endpoint_FQDN>:<PORT>
```

SPNが正しいことを確認するには、以下のタスクを実行します。最後に、特定の使用例での詳細な手順、他のドキュメントへの参照、およびデバッグのヒントがあります。

["手順2a: SQL Serverサービスを実行しているアカウント \(SID\) を特定する" on the next page](#)

["手順2b: Active Directoryでアカウントを確認する" on page 1557](#)

["手順2c: SPNで使用するFQDNを特定する" on page 1558](#)

["手順2d: 初期設定のインスタンスを使用しているのか、名前付きインスタンスを使用しているのかを特定する" on page 1558](#)

["ケース1: ローカル仮想アカウントでSPNを設定する" on page 1559](#)

["ケース2: ドメインアカウントでSPNを設定する" on page 1561](#)

["ケース3: 管理されたサービスアカウントでSPNを設定する" on page 1563](#)

["ケース4: フェールオーバークラスターのSPNを設定する" on page 1565](#)

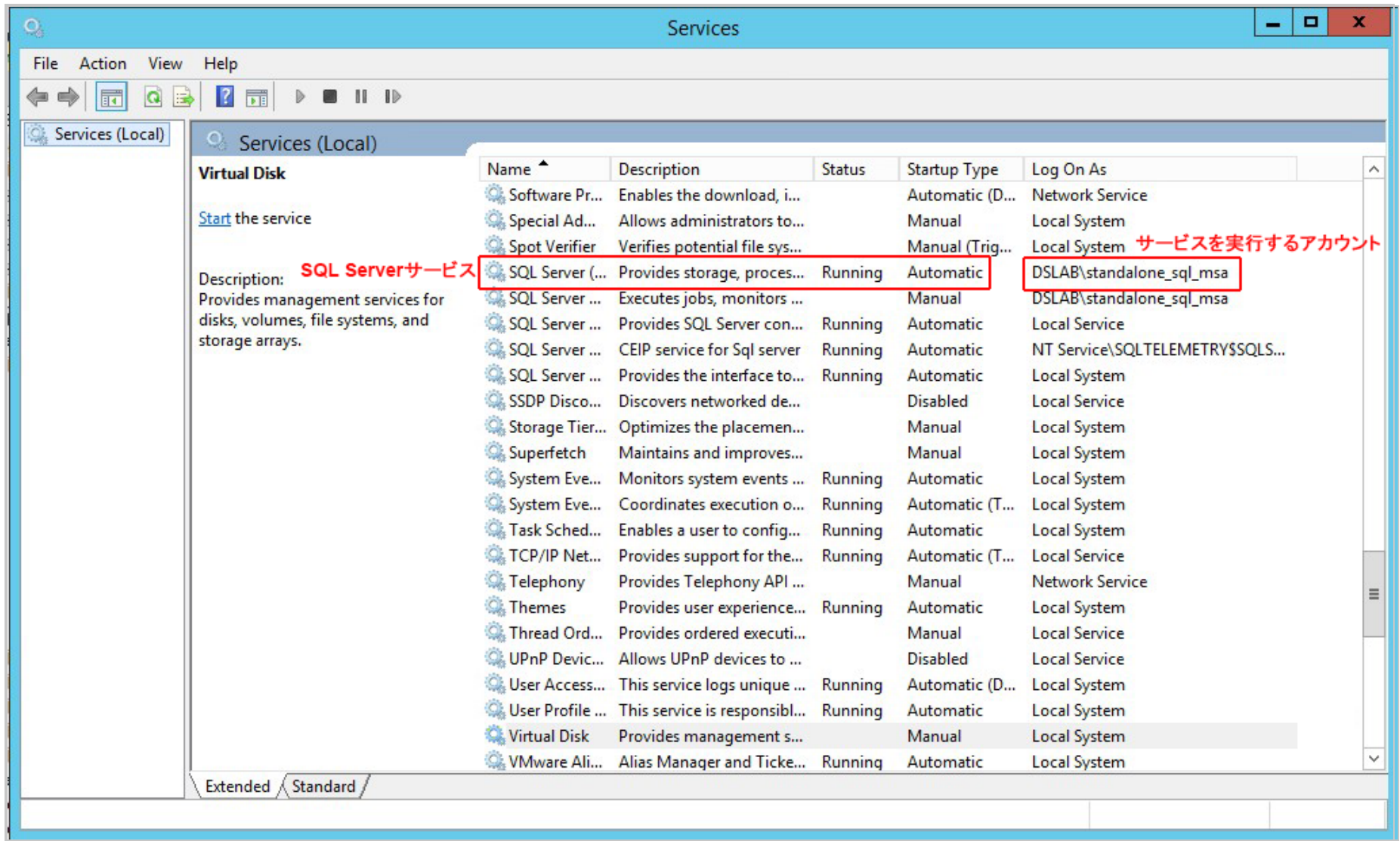
["SPNリファレンス" on page 1567](#)

["SPNのデバッグのヒント" on page 1567](#)

手順2a: SQL Serverサービスを実行しているアカウント (SID) を特定する

SPNは、SQL Serverサービスを実行しているアカウント内で設定されます。

どのアカウントがSQL Serverサービスを実行しているかを特定するには、`services.msc`ユーティリティを使用します。SQL Serverサービスが、関連付けられているアカウントと共に表示されます。



手順2b: Active Directoryでアカウントを確認する

SQL Serverサービスを実行しているアカウントの名前がわかったら、それをActive Directory内で見つける必要があります。アカウントが存在する可能性のある場所は、ローカル仮想アカウントであるか、ドメインアカウントであるか、管理されたサービスアカウントであるかに応じて決まります。以下の表は、それらの可能性のある場所をまとめたものです。Active DirectoryコンピュータでADSIエディター (adsiedit.msc) を使用して、Active Directory内のさまざまなフォルダを探し、アカウントを見つけることができます。

アカウントの種類	アカウントの名前	Active Directory内のアカウントの場所	説明
ローカル仮想アカウント	NT SERVICE\MSSQLSERVER (初期設定のインスタンス) NT SERVICE\MSSQL\$InstanceName (名前付きインスタンス)	CN=Computer CN=<コンピュータ名>	仮想アカウントで実行されるサービスは、コンピュータアカウントの資格情報を使用してネットワークリソースにアクセスします。初期設定のスタンドアロンSQL Serverサービスは、このアカウントを使用して起動されます。
ドメインアカウント	ドメインユーザ名 (例: SQLServerServiceUser)	CN=Users CN=<ユーザ名>	このアカウントを使用して開始されたサービスは、ドメインユーザの資格情報を使用してネットワークリソースにアクセスします。SQL Serverフェールオーバークラスターでは、サービスを実行するためにドメインアカウントが必要です。スタンドアロンSQL Serverサービスは、起動にドメインアカウントを使用するように設定することもできます。
管理されたサービスアカウント	管理されたサービスアカウント (MSA) 名 (例: SQLServerMSA)	CN=Managed Service Account CN=<アカウント名>	Windows Server 2008 R2で導入された、管理されたサービスアカウントは、ドメインアカウントに似ていますが、対話形式のログオンを実行するために使用できません。スタンドアロンのSQL ServerサービスとSQL Serverクラスターサービスの両方を、管理されたサービスアカウントを使用して起動するように設定できません。

手順2c: SPNで使用するFQDNを特定する

命名の一貫性を保つために、SPNをエンドポイントのFQDNに設定することをお勧めします。エンドポイントは、SQL Serverクライアント (Deep Security Manager) の接続先であり、個々のSQL Serverまたはクラスタである場合があります。使用するFQDNの詳細については、以下の表を参照してください。

SQL Serverのインストールの種類	SPNの設定
スタンドアロンSQL Server	SQL ServerがインストールされているホストのFQDN
フェールオーバーSQL Serverクラスタ	SQL ServerクラスタのFQDN (個々のSQL Serverノードはエンドポイントではないため、FQDNで使用しないでください)

手順2d: 初期設定のインスタンスを使用しているのか、名前付きインスタンスを使用しているのかを特定する

ポート番号とインスタンス名 (指定した場合) をSPNに含める必要があるため、SQL Serverが初期設定のインスタンスと名前付きインスタンスのどちらとしてインストールされたかを知っておく必要があります。

- 初期設定のインスタンスは、通常、ポート1433を使用します。
- 名前付きインスタンスは、別のポートを使用します。このポートを判断するには、[このWebページ](#)を参照してください。

例1: SQL ServerサービスのFQDNエンドポイントが`sqlserver.example.com`であり、それが初期設定のインスタンスである場合、SPNは次の形式になります。

```
MSSQLSvc/sqlserver.example.com
```

```
MSSQLSvc/sqlserver.example.com:1433
```

例2: SQL ServerサービスのFQDNエンドポイントが`sqlserver.example.com`であり、それがポート51635を使用するDEEPSECURITYというインスタンス名の名前付きインスタンスである場合、SPNは次の形式になります。

```
MSSQLSvc/sqlserver.example.com:DEEPSECURITY
```

```
MSSQLSvc/sqlserver.example.com:51635
```

ケース1:ローカル仮想アカウントでSPNを設定する

ローカル仮想アカウントで実行されるスタンドアロンSQL ServerのSPNを設定するには:

1. Active Directoryコンピュータで`ADSIEdit.msc`を開きます。ADSI エディターが開きます。
2. `[CN=Computers]` でSQL Serverホストを見つけます。
3. SQL Serverホストを右クリックし、`[プロパティ]` を選択します。
4. `[属性エディター]` タブで、`[servicePrincipalName]` までスクロールし、`[編集]` ボタンをクリックします。
5. 属性値が存在しない場合は、`[追加]` ボタンを使用して個別に追加します。`[OK]` をクリックします。

ADSI Edit

File Action View Help

← → ↻ ↵ ❌ 📄 🔄 📄 ? 📄

ADSI Edit

- Default naming context [Dio-SQL2014.ad.dsl:
 - DC=ad,DC=dslab
 - CN=Builtin
 - CN=Computers
 - CN=DIOWIN2016
 - CN=MSSQLSRV** SQL Serverホスト
 - OU=Domain Controllers
 - CN=ForeignSecurityPrincipals
 - CN=LostAndFound
 - CN=Managed Service Accounts
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users

Attributes:

Attribute	Value
sAMAccountName	MSSQLSRV\$
sAMAccountType	805306369 = (MACHINE_ACCOUNT)
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	TERMSRV/MSSQLSRV; TERMSRV/MSSG
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>
shadowMin	<not set>

Buttons: Edit, Filter, OK, Cancel, Apply, Help

ケース2:ドメインアカウントでSPNを設定する

SQL Serverサービスを実行しているドメインアカウント (CN=Users) でSPNが設定されることを除き、SPN設定はローカル仮想アカウント設定と似ています。

The screenshot shows the ADSI Edit console with the following structure:

- Default naming context [DIO-ADC.dslab.com]
 - DC=dslab,DC=com
 - CN=Builtin
 - CN=Computers
 - OU=Domain Controllers
 - CN=ForeignSecurityPrincipals
 - CN=LostAndFound
 - CN=Managed Service Accounts
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users** (highlighted with a red box)
 - CN=ADFS ServiceAccount
 - CN=Administrator
 - CN=Allowed RODC Password Replicat
 - CN=Cert Publishers
 - CN=Cloneable Domain Controllers
 - CN=Denied RODC Password Replicat
 - CN=DnsAdmins
 - CN=DnsUpdateProxy
 - CN=Domain Admins
 - CN=Domain Computers
 - CN=Domain Controllers
 - CN=Domain Guests

The right pane shows the 'CN=SQLServerServiceUser Properties' dialog box with the 'Security' tab selected. The 'Attributes' table is as follows:

Attribute	Value
sAMAccountName	sqlserver
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	MSSQLSvc/SQL2012.dslab.com:1433; MSS
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>
shadowMin	<not set>

Buttons at the bottom of the dialog include 'Edit', 'Filter', 'OK', 'Cancel', 'Apply', and 'Help'.

ケース3:管理されたサービスアカウントでSPNを設定する

SPNは、SQL Serverサービスを実行している管理されたサービスアカウント (CN=Managed Service Account) で設定されます。

The screenshot shows the ADSI Edit console with the following structure:

- Default naming context [DIO-ADC.dslab.com]
 - DC=dslab,DC=com
 - CN=Builtin
 - CN=Computers
 - OU=Domain Controllers
 - CN=ForeignSecurityPrincipals
 - CN=LostAndFound
 - CN=Managed Service Accounts** (highlighted with a red box)
 - CN=SQLServerMSA** (highlighted with a red box)
 - CN=StandaloneSQL StandaloneSC
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users
 - CN=ADFS ServiceAccount
 - CN=Administrator
 - CN=Allowed RODC Password Rep...
 - CN=Cert Publishers
 - CN=Cloneable Domain Controller
 - CN=Denied RODC Password Repli
 - CN=DnsAdmins
 - CN=DnsUpdateProxy
 - CN=Domain Admins
 - CN=Domain Computers

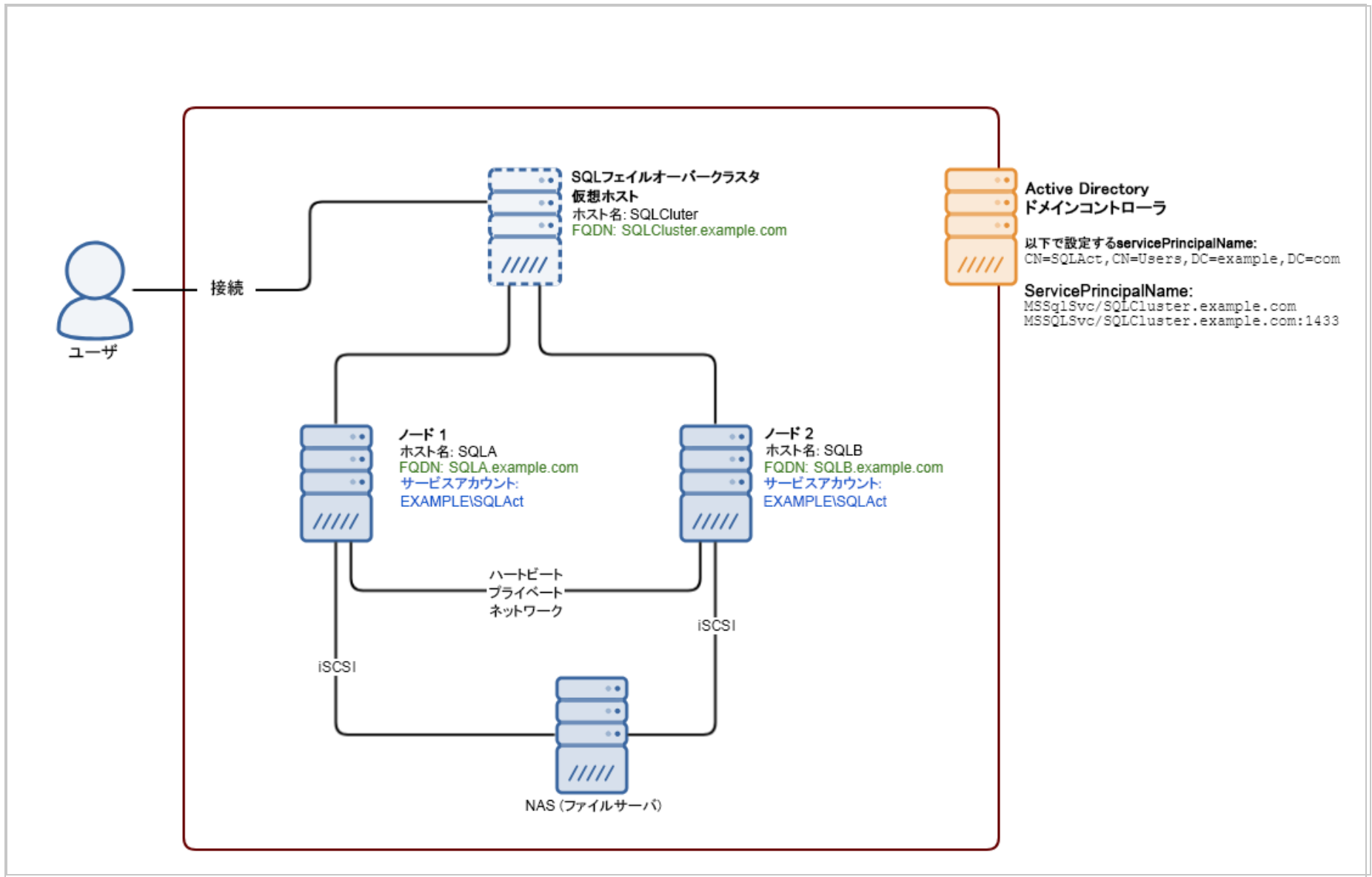
Red handwritten text in the center reads: "SQL Serverサービスを実行している管理されたサービスアカウント" (Managed service account for SQL Server service).

The right pane shows the "CN=SQLServerMSA Properties" dialog box, with the "Security" tab selected. The "Attributes" table is as follows:

Attribute	Value
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	MSSQLSvc/SQLServer.dslab.com; MSSQLS
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>
shadowMin	<not set>
shadowWarning	<not set>
showInAddressBook	<not set>
showInAdvancedVie...	<not set>

ケース4:フェールオーバークラスタのSPNを設定する

SQL Serverフェールオーバークラスタは、ドメインアカウントまたは管理されたサービスアカウントで実行できます。手順については、"[ケース2:ドメインアカウントでSPNを設定する](#)" on page 1561または"[ケース3:管理されたサービスアカウントでSPNを設定する](#)" on page 1563を参照してください。SPNは、個々のSQLノードではなく、必ずSQL「クラスタ」エンドポイントのFQDNに設定してください。



SPNリファレンス

以下は、SPN設定に関するMicrosoftの公式文書へのリンクです。

[Kerberos接続用のサービスプリンシパル名の登録](#)

[SQL Server フェールオーバークラスタでKerberos認証を有効にする方法](#)

SPNのデバッグのヒント

SPNが正しく設定されていることを確認するには、コマンドラインツール`setspn`を使用して、登録済みのSPNエントリを検索します。コマンド構文は次のとおりです。

```
setspn -T <Full_Domain_Name> -F -Q MSSQLSvc/<SQL_Server_Endpoint_FQDN>*
```

指定する項目は次のとおりです。

- `<Full_Domain_Name>`は、お使いの環境のドメイン名に置き換えます。
- `<SQL_Server_Endpoint_FQDN>`は、SQL ServerのFQDNに置き換えます。

次に例を示します。スタンドアロンのSQL Serverが`SQL2012.dslab.com`にあり、ドメイン`dslab.com`のローカル仮想アカウントで実行されているとします。次のコマンドを使用して、`MSSQLSvc/SQL2012.dslab.com`というプレフィックスを持つすべての登録済みSPNを検索し、それが正しく設定されているかどうかを確認できます。

```

Administrator: Command Prompt

C:\Users\Administrator>setspn -T DSLAB.com -F -Q MSSQLSvc/SQL2012.dslab.com*
Checking forest DC=dslab,DC=com
CN= SQL2012, CN=Computers, DC=dslab, DC=com
MSSQLSvc/SQL2012.dslab.com:1433
MSSQLSvc/SQL2012.dslab.com

Existing SPN found!

```

コマンドの結果から、SPNが、正しいLDAPパスおよびSQL Serverサービスを実行しているアカウントに、設定および登録されていることを確認できます。

手順3: krb5.confファイルを確認する (Linuxのみ)

LinuxにManagerをインストールする場合は、`/etc/krb5.conf`が存在していることと、それに正しいドメインとレルムの情報が含まれていることを確認する必要があります。

1. Kerberosを設定するには、テキストエディタで`/etc/krb5.conf`ファイルを開くか作成します。
2. 以下の情報を指定します。

```

[libdefaults]
...
default_realm = <DOMAIN>
...

[realms]
<DOMAIN> = {
    kdc = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>

```



```
admin_server = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>
}
```

```
[domain_realm]
```

```
.<DOMAIN_FQDN> = <DOMAIN>
```

```
<DOMAIN_FQDN> = <DOMAIN>
```

ここで、<DOMAIN>、<ACTIVE_DIRECTORY_CONTROLLER_FQDN>、および<DOMAIN_FQDN>は、独自の値に置き換えます。

サンプルファイル:

```
[libdefaults]
```

```
default_realm = EXAMPLE.COM
```

```
default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
```

```
default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
```

```
dns_lookup_kdc = true
```

```
dns_lookup_realm = false
```

```
[realms]
```

```
EXAMPLE.COM = {
```

```
    kdc = kerberos.example.com
```

```
    kdc = kerberos-1.example.com
```

```
    admin_server = kerberos.example.com
```

```
}  
  
[domain_realm]  
    .example.com = EXAMPLE.COM  
    example.com = EXAMPLE.COM  
  
[logging]  
    kdc = SYSLOG:INFO  
    admin_server = FILE=/var/kadm5.log
```

3. ファイルを保存して、閉じます。

手順4: システム時計を確認する

ドメインコントローラ、SQL Server、およびDeep Security Managerコンピュータのシステム時計が同期していることを確認する必要があります。Kerberosでは、最大許容クロックスキューは、初期設定で5分です。

手順5: ファイアウォールを確認する

ファイアウォールがSQL接続をブロックしていないことを確認する必要があります。初期設定のSQL Serverインスタンスでは、ポート1433を介した接続が許可されますが、名前付きSQL Serverインスタンスでは、ランダムに選択されたポートが使用されます。接続先のポートを見つけるために、SQLクライアント (この場合はDeep Security Manager) は利用可能な名前付きインスタンスを検索し、SQL Serverブラウザサービスにルックアップ要求を発行して、マッピングポートを見つけます。SQL Serverブラウザサービスは、ポート1434 (UDP) で実行されます。ファイアウォール設定で、ポート1433 (初期設定インスタンスを使用している場合)、または1434 (名前付きインスタンスを使用している場合) が許可されていることを確認してください。

複数のAmazon Virtual Private Cloud (VPC) からのAgent通信でMTUが原因で発生する問題の回避

異なるVPCにある複数のAgentがDeep Security Managerに通信しようとしたときに、問題が発生することがあります。これは、Amazon Web Servicesでサポートされるネットワーク[最大送信単位 \(MTU\)](#) が1500であるのに対し、Deep Security Agentではそれを超える通信トラフィックを送信できるため、パケットがフラグメント化および破棄されることが原因で発生します。

このようなMTUに起因する通信の問題が発生しないようにするには、すべてのファイアウォールポリシーに新しいファイアウォールルールを追加します。この新しいファイアウォールルールの重要な設定を次の図に示します。

一般	オプション	割り当て対象
一般情報		
名前:	新規ファイアウォールルール	
説明:	<div style="border: 1px solid #ccc; height: 100px;"></div>	
処理:	強制的に許可	
優先度:	0 - 最低	
パケット方向:	受信	
フレームの種類:	IP	<input type="checkbox"/> 選択以外
プロトコル:	ICMP	<input type="checkbox"/> 選択以外
パケット送信元		
IP:	任意	<input type="checkbox"/> 選択以外
MAC:	任意	<input type="checkbox"/> 選択以外
ポート:	任意	<input type="checkbox"/> 選択以外
パケット送信先		
IP:	任意	<input type="checkbox"/> 選択以外
MAC:	任意	<input type="checkbox"/> 選択以外
ポート:	任意	<input type="checkbox"/> 選択以外
指定フラグ		
<input type="checkbox"/> 任意のフラグ		

診断パッケージとログの作成

問題を診断するには、サポートプロバイダから、次のいずれかまたは両方のデバッグ情報を含む診断パッケージを送信するように要求されることがあります。

- [Deep Security Manager](#)
- [Deep Security Agent](#)

Deep Security Managerの診断

Deep Security Managerの診断パッケージを作成する

1. [管理]→[システム情報] の順に選択します。
2. [診断パッケージの作成] をクリックします。

パッケージの作成には数分かかります。パッケージが生成されると、概要が表示され、診断パッケージを含むzipファイルがダウンロードされます。

Deep Security Managerのデバッグログを有効にする

診断パッケージに加えて、サポート担当者から診断ログを有効にするように求められることがあります。

警告: サポート担当者から推奨されない限り、診断ログを有効にしないでください。診断ログは、大量のディスク容量を消費する可能性があり、CPU使用率が增大する場合があります。

1. 管理→[システム情報] の順に選択します。
2. [診断ログ] をクリックします。

3. 表示されるウィザードで、サポート担当者から求められたオプションを選択します。

マルチテナントのDeep Security Managerを使用していて、診断の対象とする問題が特定のテナントのみで発生する場合は、表示されるオプションでそのテナントの名前を選択してください。これにより、デバッグログの対象が絞り込まれ、デバッグログが有効になっている間のパフォーマンスへの影響を最小限に抑えることができます。

一部の機能については、十分なデバッグログを収集するために、ログ収集の期間とディスク容量を増やすことが必要になる可能性があります。たとえば、[データベース関連の問題] や [クラウドアカウント同期 - AWS] については、[ログファイルの最大サイズ] を25MBに増やし、期間を24時間に延長することが必要になる場合があります。

注意: [ログファイルの最大数] を減らした場合、既存のログファイルの数が指定した値を超えていても、Deep Security Managerによって既存のログが自動的に削除されることはありません。たとえば、ログファイルの最大数を10から5に変更しても、server5.logからserver9.logまでのログファイルを含め、すべてのログファイルがそのまま維持されます。ディスク容量を解放するには、それらのファイルをファイルシステムから手動で削除します。

診断ログの実行中は、Deep Security Managerのステータスバーに [診断ログが有効] というメッセージが表示されます。初期設定のオプションを変更した場合は、診断ログの完了時に [初期設定以外のログが有効] というメッセージがステータスバーに表示されます。

4. 診断ログファイルを見つけるには、Deep Security Managerのルートディレクトリに移動し、`server#.log`というパターンのファイル名 (`server0.log`など) を探します。

Deep Security Agentの診断

Agentの診断パッケージは次のいずれかの方法で作成できます。

- Deep Security Managerを使用
- 保護されているコンピュータでCLIを使用 (Deep Security ManagerがリモートからAgentにアクセスできない場合)

診断パッケージに使用する不正プログラム対策のデバッグログレベルの調整に関するLinux固有の情報については、"[保護対象のLinuxインスタンスにおける不正プログラム対策のデバッグログレベルの引き上げ](#)" on page 788を参照してください。

また、サポート担当者から次のものを収集するよう求められることがあります。

- タスクマネージャのスクリーンショット (Windows) または `top`からの出力 (Linux) , `topas` (AIX), または `prstat` (Solaris))
- [デバッグログ](#)
- [Perfmonログ](#) (Windows) またはSyslog
- [メモリダンプ](#) (Windows) またはコアダンプ (Linux、[Solaris](#)、AIX)

Deep Security Managerを使用してAgentの診断パッケージを作成する

注意: Agentの診断パッケージを作成するには、Deep Security ManagerとAgentがリモートで通信できる必要があります。Deep Security ManagerがリモートからAgentにアクセスできない場合や、AgentがAgentからのリモート有効化を使用している場合は、Agentから直接診断パッケージを作成する必要があります。

1. [コンピュータ] に移動します。
2. 診断パッケージを生成するコンピュータの名前をダブルクリックします。
3. [処理] タブを選択します。
4. [サポート情報] の [診断パッケージの作成] をクリックします。
5. [次へ] をクリックします。

パッケージの作成には数分かかります。パッケージが生成されると、概要が表示され、診断パッケージを含むzipファイルがダウンロードされます。

注意: System Information チェックボックスがオンの場合、パフォーマンスに悪影響を及ぼす巨大な診断パッケージが作成さ

れる可能性があります。このチェックボックスは、プライマリテナントでないか、適切な表示権限がない場合はグレー表示になります。

保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する

Linux、AIX、またはSolaris

1. 診断パッケージを生成するサーバに接続します。
2. 次のコマンドを入力します。

```
sudo /opt/ds_agent/dsa_control -d
```

診断パッケージのファイル名と場所が出力されます。 `/var/opt/ds_agent/diag`

Windows

1. 診断パッケージを生成するコンピュータに接続します。
2. コマンドプロンプトを管理者として開き、コマンドを入力します。

PowerShellの場合:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -d
```

Cmd.exeの場合:

```
cd C:\Program Files\Trend Micro\Deep Security Agent
```

```
dsa_control.cmd -d
```

診断パッケージのファイル名と場所が出力されます。 `C:\ProgramData\Trend Micro\Deep Security Agent\diag`

DebugViewを使用してデバッグログを収集する

Windowsコンピュータでは、DebugViewソフトウェアを使用してデバッグログを収集できます。

警告: デバッグログは、サポート担当者から求められた場合にのみ収集してください。デバッグログ収集中はCPU使用率が増大します。これにより、CPU使用率が高いという問題はさらに悪化します。

1. [DebugViewユーティリティ](#)をダウンロードします。
2. セルフプロテクションが有効になっている場合は、無効にします。
3. Trend Micro Deep Security Agentサービスを停止します。
4. C:\Windowsディレクトリにds_agent.iniという名前のプレーンテキストファイルを作成します。
5. ds_agent.iniファイルに次の行を追加します。

```
trace=*
```

6. DebugView.exeを起動します。
7. メニューの [Capture] を選択します。
8. 次の設定を有効にします。
 - Capture Win32
 - Capture Kernel
 - Capture Events
9. Trend Micro Deep Security Agentサービスを開始します。
10. DebugViewの情報をCSVファイルにエクスポートします。
11. この手順の最初にセルフプロテクションを無効にした場合は再び有効にします。

詳細な診断パッケージのプロセスメモリを増やす

多数のホスト (たとえば10,000以上) が存在する環境では、診断パッケージの作成中に、詳細な診断パッケージのプロセス (`dsm_c.exe`) でメモリが不足する場合があります。これを回避するために、詳細な診断パッケージのJVMプロセスに割り当てられたメモリを2GBまで増やすことができます。

1. Deep Security Managerのインストールディレクトリに移動します。
2. 「`dsm_c.vmoptions`」という名前の新しいファイルを作成します。
3. 作成したファイルを開き、`-Xmx2g`という行を追加します。

注意: メモリが2GBでも足りない場合は、上記の行の値を変更して、割り当てられているメモリをさらに増やすこともできます。たとえば、4GBを増やす場合は`-Xmx4g`、6GBの場合は`-Xmx6g`とします。

4. ファイルを保存し、`dsm_c.exe`を実行します。