注意事項
トレンドマイクロ（トレンドマイクロ株式会社およびその子会社を含みます）へのお客さま情報の送信について
(1) 「Webレピュテーションサービス」、「フィッシング詐欺対策」、「ベアレンタルコントロールURLフィルタリング」および「Trendツールバー」等について
①トレンドマイクロでは、お客さまがアクセスしたWebページの安全性の確認のため、お客さまより受領した情報に基づき、お客さまがアクセスするWebページのセキュリティーチェックを実施します。なお、お客さまがアクセスしたWebの情報(ドメイン、IPアドレス等)を含む、暗号化してトレンドマイクロのサーバに送信されます。サーバに送信されたURL情報は、Webサイトの安全性の確認、および当該機能の改良の目的にのみ利用されます。
②当該機能を有効にしたうえで、Webページにアクセスした場合、以下の事象がおこることがありますのでご注意ください。
(a)お客さまがアクセスしたWebページのWebサーバ側の仕様が、お客さまが入力した情報等をURLのオプション情報として付加し、Webサーバへ送信する仕様の場合、URLのオプション情報にお客さまが入力した情報(ID、パスワード等)などを含んだURLがトレンドマイクロのサーバに送信され、当該Webページのセキュリティーチェックが実施されます。
(b)お客さまがアクセスするWebページのセキュリティーチェックを実施する仕様になっていることから、お客さまがアクセスするWebサーバ側の仕様によっては、URLのオプション情報に含まれる情報(例えば、お客さまの個人情報など)が含まれる可能性がありますが、トレンドマイクロがファイルに含まれる個人情報や機密情報等を取得することはありません。お客さまから送信された情報の取り扱いについての詳細は、http://www.trendmicro.co.jp/jp/terms-use/privacy-policy/spn/index.htmlをご覧ください。
③Webサイトのセキュリティなどの対策、およびお客さま情報の保護のため、お客さまに送信される情報の匿名化が行われます。
(2) Trend Micro Smart Protection Network（「スマートフィードバック」、「ファイルレピュテーションサービス」、「脅威情報の送信」および「ウイルストラッキング」等を含みます）について
脅威に関する情報収集、分析し、保護を強化するために、お客さまのコンピュータに攻撃を試みる脅威に関連すると思われる情報を収集して、トレンドマイクロに送信することがあります。送信された情報はプログラムの安全性の判断に役立つために利用されます。また、お客さまの個人情報や機密情報等が含まれる可能性がありますが、トレンドマイクロがファイルに含まれる個人情報や機密情報等を取得することはありません。お客さまから送信された情報の取り扱いについての詳細は、http://www.trendmicro.co.jp/jp/terms-use/privacy-policy/spn/index.htmlをご覧ください。
(3) 「迷惑メール対策ツール」について
迷惑メールに関する情報を収集し、分析し、保護を強化するために、お客さまのコンピュータに攻撃を試みる脅威に関連すると思われる情報を収集して、トレンドマイクロに送信することがあります。あなたのコンピュータに迷惑メール情報が送信される可能性があります。
(4) 「E-mailレピュテーションサービス」について
スパムメールの特定のため、迷惑メールの情報等をトレンドマイクロのサーバに送信します。
(5) 「ユーザーハイパーセキュリティ」について
トレンドマイクロ製品の改良目的のために、お客さまがトレンドマイクロ製品をどのような設定にして利用しているのかがわかる設定情報およびお客さまがトレンドマイクロ製品をどのように操作したのかがわかる操作履歴情報を、匿名でトレンドマイクロのサーバに送信します。
(6) 「製品利用情報の送信」について
お客さまへのサポートサービスの提供、製品の改良および統計的処理のため、ご利用製品のライセンス情報および製品の使用環境情報を、トレンドマイクロのサーバに送信されることがあります。輸出規制について
お客さまは、本製品およびそれにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出管理規制、外国為替規制および省令、ならびに、米国輸出管理規定に基づく輸出規制の対象となる可能性があることを認識の上、本ソフトウェア等を輸出するものとします。
輸出規制について
お客さまは、本製品およびそれにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出管理規制、外国為替規制および省令、ならびに、米国輸出管理規定に基づく輸出規制の対象となる可能性があることを認識の上、本ソフトウェア等を輸出するものとします。
輸出規制について
お客さまは、本製品およびそれにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出管理規制、外国為替規制および省令、ならびに、米国輸出管理規定に基づく輸出規制の対象となる可能性があることを認識の上、本ソフトウェア等を輸出するものとします。
輸出規制について
お客さまは、本製品およびそれにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出管理規制、外国為替規制および省令、ならびに、米国輸出管理規定に基づく輸出規制の対象となる可能性があることを認識の上、本ソフトウェア等を輸出するものとします。
輸出規制について
お客さまは、本製品およびそれにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出管理規制、外国為替規制および省令、ならびに、米国輸出管理規定に基づく輸出規制の対象となる可能性があることを認識の上、本ソフトウェア等を輸出するものとします。
輸出規制について
お客さまは、本製品およびそれにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出管理規制、外国為替規制および省令、ならびに、米国輸出管理規定に基づく輸出規制の対象となる可能性があることを認識の上、本ソフトウェア等を輸出するものとします。
管理者ガイド


本書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。

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

P/N: APEM97215_150921_JP (2016/1)
目次

はじめに ................................................................................................................................................................................................. 8

概要 ........................................................................................................................................................................................................... 9

製品の機能 .................................................................................................................................................................................................. 10

設定と管理 .................................................................................................................................................................................................. 13

クイックスタート: システム設定 .................................................................................................................................................. 14

クイックスタート: コンピュータの保護 ........................................................................................................................................... 20

システム ................................................................................................................................................................................................ 28

Deep Security Managerを保護する .................................................................................................................................................. 29

通信 .................................................................................................................................................................................................. 30

ダッシュボードをカスタマイズする .................................................................................................................................................. 32

イベントログとデータ収集 ............................................................................................................................................................ 35

メール通知 ................................................................................................................................................................................................ 36

アラート .................................................................................................................................................................................................. 37

ポート検索の設定 ................................................................................................................................................................. 39

Syslogの統合 (SIEM) ................................................................................................................................................................. 40

Relayグループ ................................................................................................................................................................................................ 53

セキュリティアップデート ............................................................................................................................................................ 57

ソフトウェアアップデート ............................................................................................................................................................ 61

Virtual Applianceの検索キャッシュ ............................................................................................................................................ 63

ユーザ管理 ................................................................................................................................................................................................ 65

データベースのバックアップと復元 ................................................................................................................................................. 71

コンピュータを追加する ................................................................................................................................................................. 74

ローカルネットワーク ................................................................................................................................................................. 75

Active Directory .................................................................................................................................................................................................. 77

VMware vCenter ................................................................................................................................................................................................ 81

クラウドアカウント ................................................................................................................................................................. 82

インストールスクリプト ................................................................................................................................................................. 88

保護を実施する ................................................................................................................................................................................................. 90

Agentベースの保護 .............................................................................................................................................................................. 91

Agentレスによる保護 .............................................................................................................................................................................. 92

保護モジュール .................................................................................................................................................................................................. 93

不正プログラム対策 .............................................................................................................................................................................. 94

Webレピュテーション .............................................................................................................................................................................. 99

ファイアウォール ................................................................................................................................................................................................. 101

バイパスルール .................................................................................................................................................................................................. 111
はじめに
概要

Deep Securityは、物理、仮想、およびクラウドコンピュータにAgentベースまたはAgentレスによる保護を提供します。

次のような保護機能があります。

- 不正プログラム対策
- Webレビュテーション
- ファイアウォール
- 侵入検知および侵入防御
- 変更監視
- セキュリティログ監視
製品の機能

Deep Securityは、物理、仮想、およびクラウドサーバーに高度なサーバセキュリティを提供します。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洩やビジネスの中断を防ぎます。この包括的な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、規制に準拠し、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。緊密に統合された各モジュールを使用することによって、プラットフォームを簡単に拡張し、物理、仮想、クラウドサーバおよび仮想デスクトップ全体のサーバ、アプリケーション、データのセキュリティを確保できます。

保護モジュール

不正プログラム対策

VMware環境と連携してAgentレスによる保護を提供します。また、物理サーバや仮想デスクトップを保護するためのAgentも提供します。

VMware vShield EndpointのAPIを統合して、ゲスト内の領域を占有することなく、VMwareの仮想マシンにAgentレスによる不正プログラム対策保護を提供します。

Webレピュテーション

トレンドマイクロのWebレビューションサービスは、不正なWebサイトへのアクセスをブロックします。

トレンドマイクロでは、Webサイトの古さ、サイトの変更履歴、不正プログラムの挙動分析で検出された不審なアクティビティの兆候などの要素に基づいてレビューションスコアを割り当てています。

Webレビューションサービスには次の機能があります。

- 感染したサイトへのアクセスをブロックします。
- サイバー犯罪者が使用するコマンド&コントロール (C&C) サーバとの通信をブロックします。
- サイバー犯罪者がサイバー犯罪のために登録した不正ドメインへのアクセスをブロックします。

変更監視

ファイルやシステムのレジストリに対する不正な変更および予想外の変更をリアルタイムで検出してレポートします。

管理者は、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。

ファイアウォール

物理サーバと仮想サーバの攻撃の対象となる領域を削減します。

双方向のステートフルファイアウォールを使用して、サーバのファイアウォールポリシーを中央で管理します。仮想マシンのソーカリングをサポートし、DoS攻撃を防ぎます。IPベースのすべてのプロトコルおよびフレームの種類に幅広く対応し、ポート、IPアドレス、およびMACアドレスの詳細なフィルタを提供します。
侵入防御

パッチが適用されるまでの間、既知の脆弱性に対する様々な攻撃コードにさらされないようにします。

既知またはゼロデイの攻撃からの適切な保護を提供します。侵入防御ルールを使用して、既知の脆弱性 (たとえば、Microsoftが毎月開示する脆弱性) に対する様々な攻撃コードにさらされないようにすることができます。データベース、Web、メール、およびFTPサービスを含む100を超えるアプリケーション向けに、すぐに適用できる侵入防御ルールが用意されています。

Webアプリケーションの脆弱性を防ぎます。

PCI要件6.6に準拠して、Webアプリケーションやその処理データを保護できます。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を防ぎます。コードの修正が完了する前でも、脆弱性に対する攻撃にさらされないようにします。

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ます。

ネットワークにアクセスするアプリケーションを監視し、制御します。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、サーバの脆弱性のリスクを低減します。

セキュリティログ監視

ログファイルに含まれている重要なセキュリティイベントに対する可視性を提供します。

データセンター全体の複数のログエントリに含まれている重要なセキュリティイベントの特定が最適化されます。SIEMシステムまたは中央のログサーバに不審なイベントを転送して関連付け、レポート、およびアーカイブに使用します。OSSECで入手可能なオープンソースのソフトウェアを利用したり、拡張したりできます。

Deep Securityのコンポーネント

Deep Securityは次のコンポーネントの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 (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 (Appliance):** VMware vSphere環境用に構築されたセキュリティ仮想マシン。不正プログラム対策および変更監査を提供します。
- **Deep Security Agent (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。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による保護を提供します。

Deep Security Manager

Deep Security Manager (以下、「Manager」) はWebベースの強力な管理システムです。このシステムを使用すると、セキュリティ管理者は包括的な侵入防御セキュリティポリシーを作成および管理し、脅威および脅威に対する防御処理を記録できます。Managerは、データセンターのさまざまな要素 (VMware vCenter、Microsoft Active Directoryなど) と連携します。Managerには、データセンター自動化環境と連携するためのWebサービスAPIが用意されています。
ポリシー

ポリシーは、1台以上のコンピュータに適用されるセキュリティルールを設定し、指定できるポリシーテンプレートです。このコンパクトで管理可能なルールセットを使用すると、包括的なセキュリティの提供が容易になり、数千というルールを管理する必要がなくなります。初期設定のポリシーでは、一連の共通のコンピュータ設定に対して必要なルールが提供されます。

ダッシュボード

カスタマイズ可能なWebベースのコンソールにより、特定の情報を迅速に検索できます。次の機能が提供されます。

- ドリルダウン機能を使用した、システム、イベント、およびコンピュータに関するさまざまなレポート機能
- ドリルダウン機能を使用した、主要な測定内容のトレンドグラフ
- ドリルダウン機能を使用した、詳細イベントログ機能
- パーソナライズされたダッシュボードレイアウトを複数保存する機能

組み込みセキュリティ

役割ベースのアクセスを使用すると、アクセスと編集の権限が異なる複数の管理者（ユーザ）がシステムのさまざまな要素を編集および監視し、各ユーザに適した情報を取得できます。電子署名は、システムコンポーネントを認証してルールの整合性を検証するのに使用します。コンポーネント間の情報交換の機密性は、セッションの暗号化によって保護されています。

Deep Security Agent

Deep Security Agent（以下、「Agent」）は高パフォーマンスで省スペースのソフトウェアコンポーネントで、コンピュータにインストールされ、保護を提供します。

Deep Security Virtual Appliance

Deep Security Virtual Appliance（Appliance）はVMwareの仮想マシンとしてESXiサーバ上で動作し、同じESXiサーバ上の他の仮想マシンをそれぞれ固有のセキュリティポリシーで保護します。

Deep Security Relay

Deep Security Relay（Relay）は、トレンドマイクロのアップデートサーバからDeep Securityシステムに、Deep Securityのアップデートを配信するサーバです。Relayを使用して、Manager、Appliance、およびAgentにアップデートを配布するタスクを分散することによって、パフォーマンスを向上できます。

注意: Windows（64ビット）版およびLinux（64ビット）版のDeep Security 9.5以降のAgentにはRelay機能が搭載されており、コンピュータのエディタ画面から有効にできます。

Deep Security Notifier

設定と管理
クイックスタート: システム設定

このクイックスタートガイドでは、コンピュータリソースの保護を開始する前に必要な、Deep Securityの基本的な初期システム設定について説明します。

Deep Securityの基本的なシステム設定を完了するには、次の手順を実行する必要があります。

1. Relay有効化済みAgentが1つ以上インストールされていることを確認する
2. Deep Securityがトレンドマイクロからアップデートを取得できるように設定する
3. 定期的にアップデートを実行するための予約タスクが作成済みであることを確認する
4. 重要なイベントのメール通知を設定する

Relay有効化済みAgentが1つ以上インストールされていることを確認する

Relayは、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て、保護対象のコンピュータに配布します。そのため、Relayが1つ以上有効化済みである必要があります。Deep Security Relayがインストールされていない場合は、インストールガイドでインストール手順を参照してください。

注意: Windows (64ビット) およびLinux (64ビット) 版のDeep Security AgentにはRelay機能が搭載されており、コンピュータのエディタ画面から有効にできます。

Relayは必ずRelayグループにまとめられます。新しいRelayがすべて割り当てられる「初期設定のRelayグループ」1つしかグループがない場合も同様です。コンピュータが多数あるためにRelayの階層構造を作成する必要がある場合や、コンピュータが多くの地域に分散している場合は、複数のRelayグループを作成できます。Relayグループの詳細については、「Relayグループ (53ページ)」を参照してください。

Deep Security Relayを確認するには、[管理]→[アップデート]→[Relayグループ]に進みます。

現在のRelayグループが[Relayグループ]画面に表示されます。通常、初期設定のRelayグループのみが表示されます。

[初期設定のRelayグループ]をダブルクリックして、Relayグループのプロパティ画面を表示します。
 Relayグループのプロパティ 画面の [メンバー] エリアで、グループのメンバーであるRelayを確認できます。

注意: [メンバー] エリアにコンピュータが表示されない場合は、インストールガイドの『Relay有効化済みAgentのインストールおよび設定』を参照してください。

トレンドマイクロからアップデートを取得できるように設定する

Relayがインストールされていることを確認したので、Relayがトレンドマイクロからアップデートを取得できるかどうかを確認します。

[管理]→[アップデート]→[セキュリティ] の順に選択し、[パターンファイルアップデート] と [ルールアップデート] 両方にある [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。

パターンファイルのダウンロードまたはルールのダウンロードウィザードが表示されます。このウィザードからトレンドマイクロのアップデートサーバーに接続して、最新のセキュリティアップデートをダウンロードし、コンピュータに配布します。ウィザードの終了時に成功のメッセージが表示された場合は、Relayがインストールされているコンピュータがアップデートサーバと通信できます。
定期的にアップデートを実行するための予約タスクが作成済みであることを確認する

Relayがアップデートサーバと通信できることがわかったので、次に、セキュリティアップデートを定期的に取得して配布するための予約タスクを作成します。

[管理]→[予約タスク] の順に選択します。初期設定の予約タスク2つが表示されます（セキュリティアップデートを毎日確認およびソフトウェアアップデートを毎日確認）。

予約タスクをダブルクリックして、[プロパティ] 画面を表示します。

予約タスクのリストに[セキュリティアップデートの確認] がない場合は、[予約タスク] 画面のメニューの [新規] をクリックし、新規予約タスクウィザードの手順に従うと、予約タスクを作成できます。
重要なイベントのメール通知を設定する

Deep Securityのアラートは、特別な注意を必要とする状況で発令されます。セキュリティイベント（不正プログラムの検出や保護対象のコンピュータでの異常な再起動など）またはシステムイベント（ディスクの空き容量が少ない状態でDeep Security Managerが実行されている場合など）が発生した際に、アラートを発令できます。特定のアラートが発令された場合にメール通知を送信するようにDeep Securityを設定できます。

メール通知を生成するアラートを設定するには、[アラート]画面に移動し、[アラートの設定]をクリックして、Deep Securityのアラートのリストを表示します。

アラートをダブルクリックすると、[プロパティ]画面が表示されます。この画面で、アラートのメール通知のオプションを設定できます。

次に、Deep Securityから送信されるメール通知を受信するようにユーザアカウントを設定する必要があります。[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。[連絡先情報]タブに移動し、メールアドレスを入力して、[アラートメールを受信]オプションを選択します。
Deep Securityからのメール通知を送信するには、SMTPサーバと通信できるように設定する必要があります。Deep Security ManagerをSMTPサーバに接続するには、[管理]→[システム設定]→[SMTP]タブの順に選択します。

[SMTP]エリアの必要なフィールドに情報を入力し、完了したら、画面の下部の[SMTP設定のテスト]をクリックします。「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。

注意：SMTPサーバに接続できない場合は、Managerがポート25を使用してSMTPサーバに接続できることを確認してください。
基本的な設定の完了

これで、Deep Securityの基本的なシステム設定は完了です。トレンドマイクロから定期的にセキュリティアップデートを取得して配布し、アラートが発令された場合にメール通知を送信するようにDeep Securityが設定されました。次に、Deep Securityによる保護をコンピュータに適用する必要があります。2種類のコンピュータリソース（サーバとノートパソコン）を保護するための簡単なガイドについては、「クイックスタート: コンピュータの保護（20ページ）」または「データセンター外部のコンピュータの保護（167ページ）」を参照してください。
クイックスタート：コンピュータの保護

ここでは、Deep Securityを使用してWindows Server 2008コンピュータを保護する手順について説明します。

次の手順に従ってください。

1. Deep Security Managerにコンピュータを追加します。
2. 推奨設定の検索を実行します。
3. 検索の推奨設定を自動的に適用します。
4. 定期的に推奨設定の検索を実行するための予約タスクを作成します。
5. Deep Security Managerを使用してアクティビティを監視します。

ル済みであるものとします。また、Deep Security ManagerにAgentソフトウェアパッケージ(.zip)をインポート済
みであり、保護するコンピュータにDeep Security Agentがインストールされているものとします（有効化はされてい
ない）。最後に、最新のセキュリティアップデートをダウンロードするための、Relay有効化済みAgentがあるものとし
ます。いずれかの要件を満たしていない場合は、インストールガイドに記載されている手順を参照し、ここで説明した
状態にしてください。

Deep Security Managerにコンピュータを追加する

Deep Security Managerに追加するコンピュータは、ポート4120でDeep Security Managerにアクセスできれば、場所は問いません。

次のいずれかの手順を行ってください。

- IPアドレスまたはホスト名を指定してローカルネットワークから個々のコンピュータを追加する
- ネットワークを検索してローカルネットワーク上のコンピュータを検出する
- Microsoft Active Directoryに接続してコンピュータのリストをインポートする
- VMware vCenterに接続してコンピュータのリストをインポートする
- 次のクラウドプロバイダサービスからコンピューティングリソースに接続する
  - Amazon EC2
  - VMware vCloud
  - Microsoft Azure

ここではローカルネットワークからコンピュータを追加しますが、Managerにコンピュータが追加された後は、コンピュータの場所に
関係なく、同じ手順に従って保護を実行します。

ローカルネットワークからコンピュータを追加するには

メニューから[新規コンピュータ...]を選びます。
2. 新規コンピュータウィザードで、コンピュータのホスト名またはパスワードを入力し、適用する適切なセキュリティポリシーをポリシーツリーのドロップダウンメニューから選択します（ここでは、Windows Server 2008ポリシーを選択します）。[次へ] をクリックします。

3. ウィザードがコンピュータに接続し、そのコンピュータを [コンピュータ] 画面に追加します。さらに、有効化されていないAgentを検出して有効にし、選択したポリシーを適用します。[完了] をクリックします。

注意: インストール時に有効化を自動的に開始するようにAgentを設定できます。詳細については、「コマンドラインユーティリティ (184ページ)」を参照してください。

4. コンピュータが追加されると、ウィザードに確認メッセージが表示されます。
5. 「コンピュータの詳細」を開く] オプションの選択を解除して、「閉じる」をクリックします。

これで、「コンピュータ」画面のDeep Security Managerの管理対象コンピュータのリストにコンピュータが表示されます。

Deep Securityでは、有効化した後に、最新のセキュリティアップデートをコンピュータに自動的にダウンロードします。また、コンピュータに割り当てられたWindows Server 2008ポリシーで変更監視が有効になっているため、コンピュータ用の変更監視のベースラインの作成が開始されます。実行中のアクティビティは、Manager画面のステータスバーで確認できます。

Deep Security Managerによる有効化後の初期タスクが完了すると、コンピュータのステータスが「管理対象 (オンライン)」と表示されます。

| 注意: | メニューの [サポート] リンクをクリックすると、Deep Security Managerの各画面の詳しい説明を表示できます。 |

推奨設定の検索を実行する

コンピュータに割り当てられたセキュリティポリシーは、Windows Server 2008 OSを実行しているコンピュータ向けに設計された一連のルールと設定で構成されます。ただし、静的なポリシーはすぐに十分なものではなくなくなってしまう可能性があります。これは、新しいソフトウェアがコンピュータにインストールされる、トレンドマイクロが作成した新しい保護ルールによって新しいOSの脆弱性が検出される、または過去の脆弱性がOSやソフトウェアのサービスパックによって修正されたためです。コンピュータ上のセキュリティ要件は動的であるため、推奨設定の検索を定期的に実行する必要があります。この検索では、コンピュータの現在の状態を評価し、Deep Security保護モジュールの最新のアップデートと比較して、現在のセキュリティポリシーをアップデートする必要があるかどうかを確認します。

推奨設定の検索では、次の保護モジュールの推奨設定が作成されます。

- 侵入防御
- 変更監視
- セキュリティログ監視

コンピュータで推奨設定の検索を実行するには

2. 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。
推奨設定の検索の実行中は、コンピュータのステータスが「推奨設定の検索中」と表示されます。検索の完了後、Deep Securityからの推奨設定がある場合、[アラート]画面に【x台のコンピュータに対する推奨設定が作成されました】というアラートが表示されます。

推奨設定の検索の結果を確認するには

1. 【コンピュータ】画面のメニューまたは右クリックメニューの【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画面で、【侵入防御】モジュール画面に移動します。
   【一般】タブの【推奨設定】エリアで検索の結果を確認できます。
現在のステータスは、現在このコンピュータに割り当てられている侵入防御ルールが253個あることを示しています。

前回の推奨設定の検索は、前回の検索が2015年12月28日の16時14分に実行されたことを示します。

未解決の推奨設定は、検索の結果として、侵入防御ルールを追加で46個割り当てて、現在割り当てられている179個のルールの割り当てを解除するようDeep Securityが推奨していることを示します。

備考は、割り当てを解除するよう推奨されている179個すべてのルールが、コンピュータレベルで直接割り当てられているのではなくポリシーレベルで割り当てられていることを示します。ポリシーレベルの上位のレベルで割り当てられているルールは、そのルールが割り当てられたポリシー (この場合は、Windows Server 2008ポリシー) でのみ割り当てを解除できます (Windows Server 2008ポリシーのエディタを開いた場合にも同じ推奨設定が表示され、そのポリシーからの割り当てを解除することができます)。

通常これらのルールは、設定が必要なルールと、誤判定が発生しやすいため検出のみモードで動作を監視する必要のある (防衛モードで施行した) ルールのどちらかです。割り当てが推奨されているルールを確認するには、[割り当て/割り当て解除] をクリックして、ルールの割り当てのための [IPSルール] 画面を表示します。次に、2番目のドロップダウンフィルタリストから [割り当てを推奨] を選択します。
設定が必要なルールには、小さな設定アイコン（設定）が表示されます。ルールに設定可能なオプションを確認するには、ルールをダブルクリックして、ローカル編集モードで[プロパティ]画面を開き、[設定]タブに移動します。ルールを割り当てるには、ルール名の横にあるチェックボックスをオンにします。

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、同じリストから[割り当て解除を推奨]を選択してルールのリストをフィルタします。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フにします。

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、同じリストから[割り当て解除を推奨]を選択してルールのリストをフィルタします。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フにします。

注意: コンピュータで有効な、ポリシーツリーの上位のポリシーで割り当てられているルールの割り当てをローカルドで解除することはできません。このようなルールの割り当てを解除するには、ルールが割り当てられたポリシーを編集し、そのポリシーから割り当てを解除する必要があります。この種のルールの継承の詳細については、「ポリシー、継承、およびオーバライド(292ページ)」を参照してください。

検索の推奨設定を自動的に適用

推奨設定の検索の後にルールの割り当てと割り当ての解除を自動的に実行するようにDeep Securityを設定できます。そのためには、コンピュータまたはポリシーのエディタを開き、推奨設定の検索をサポートする個々の保護モジュール画面（侵入防御、変更監視、およびセキュリティログ監視）に移動します。[一般]タブの[推奨設定]エリアで、[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。

定期的に推奨設定の検索を実行するための予約タスクの作成

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。このタスクを自動的に実行するための予約タスクを作成できます。

予約タスクを作成するには

1. Deep Security Managerの管理コンソールで、[管理]→[予約タスク]の順に選択します。
2. メニューバーの[新規]をクリックして新規予約タスクウィザードを表示します。
3. 検索の種類として【コンピュータの推奨設定を検索】を選択し、検索の頻度として【週単位】を選択します。【次へ】をクリックします。
4. 開始時刻、スケジュール (1週間ごと)、および曜日を選択します。【次へ】をクリックします。
5. 検索するコンピュータを指定する場合は、最後のオプション (【コンピュータ】) を選択し、保護するWindows Server 2008 コンピュータを選択します。【次へ】をクリックします。
6. 新しい予約タスクの名前を入力します。【完了】でタスクを実行】の選択は解除したままにします (推奨設定の検索を実行したばかりであるため)。【完了】をクリックします。

これで、新しい予約タスクが予約タスクのリストに表示されます。この予約タスクにより、コンピュータの検索が週に1回実行され、コンピュータの推奨設定が作成されます。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する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。

注意：Agentベースの保護の予約タスクには、エンドポイントのOSと同じタイムゾーンが使用されます。Agentレスによる保護の予約タスクには、Deep Security Virtual Applianceと同じタイムゾーンが使用されます。

通常のセキュリティアップデートのスケジュールを作成する

「クイックスタート: システム設定 (14ページ)」に記載されている手順に従うと、トレンドマイクロが提供する最新の保護モジュールによってコンピュータが定期的にアップデートされます。

Deep Security Managerによるアクティビティの監視

ダッシュボード

コンピュータにポリシーを割り当て、一定時間開催した後で、そのコンピュータの処理を確認する場合があります。処理の確認で最初に閲覧するのは、ダッシュボードです。ダッシュボードには、Deep Security Managerと管理対象のコンピュータの状態に関わる、さまざまな種類の情報を表示する多数の情報パネル (「ウィジェット」) があります。

ダッシュボード画面の上端にある「ウィジェットの追加/削除」をクリックして、表示可能なウィジェットのリストを表示します。

ここでは、【ファイアウォール】セクションから次のウィジェットを追加します。

- ファイアウォールのアクティビティ (防御)
- ファイアウォールIPのアクティビティ (防御)
- ファイアウォールイベント履歴 [2x1]
3つのウィジェットの横にあるチェックボックスをそれぞれ選択して、[OK]をクリックします。ダッシュボードにウィジェットが表示されます。データが生成されるまで、しばらく時間がかかります。

- [ファイアウォールのアクティビティ (防御)] ウィジェットは、拒否されたパケットの数とともに、パケットが拒否される最も一般的な理由、つまりそのコンピュータ上のAgentによってコンピュータへの接続がブロックされた理由のリストを表示します。このリストの項目は、パケット拒否またはファイアウォールルールのいずれかの種類になります。それぞれの「理由」は、その拒否パケットに対応するログへリンクされています。

- [ファイアウォールIPのアクティビティ (防御)] ウィジェットは、拒否パケットの最も一般的なソースIPのリストを表示します。[ファイアウォールのアクティビティ (防御)] ウィジェットと同様に、各ソースIPは、対応するログへリンクされています。

- [ファイアウォールイベント履歴 [2x1]] ウィジェットは、選択されたビューに応じて、過去24時間以内または7日間以内にブロックされたパケットの数を棒グラフで表示します。棒グラフをクリックすると、その棒が表す期間に対応したログが表示されます。

| 注意: | [ファイアウォールのアクティビティ (防御)] および [ファイアウォールIPのアクティビティ (防御)] ウィジェットの数値の横には、推移を表すインジケータがあります。上向きまたは下向きの三角形は指定期間における全体の増減を示し、横線は大きな変更がなかったことを示します。 |

ファイアウォールおよび侵入防御イベントのログ

次に、拒否されたパケットの数値が多いために対応するログをドリルダウンします。[ファイアウォールのアクティビティ (防御)] ウィジェットで、拒否されたパケットの数値が多い理由をクリックします。クリックすると、[ファイアウォールイベント] 画面に移動します。

[ファイアウォールイベント] 画面には、ファイアウォールイベントがすべて表示されます。[ファイアウォールのアクティビティ (防御)] ウィジェットでは、ある一つの理由（「ポリシーで未許可」）は、『理由』列エントリに対応します。ログは、過去24時間または7日間のダッシュボードの表示期間中に発生したイベントの数を表示するようフィルタされています。[ファイアウォールイベント] と [侵入防御イベント] 画面の詳細は、これらの画面のヘルプページを参照してください。

その他のパケット拒否の理由の意味については、以下を参照してください。

- ファイアウォールイベント (246ページ)
- 侵入防御イベント (244ページ)

レポート

ログデータの表示には、通常、より高度で要約された情報を単純に理解できるようにすることが求められます。レポートはこうした役割を担い、コンピュータ、ファイアウォールおよび侵入防御イベントログ、イベント、アラートなどの詳細な概要を表示します。[レポートの生成] 画面では、生成するレポートのさまざまなオプションを選択できます。

ここでは、指定した期間のファイアウォールルールやファイアウォールステートフル設定処理の記録を表示するファイアウォールレポートを生成します。[レポート] ドロップダウンから [ファイアウォールレポート] を選択します。[生成] をクリックして、新しい画面でレポートを開きます。

Deep Security Managerからユーザにメール送信された定期レポートを確認する、システムにログインしてダッシュボードを調べ、特定のログをドリルダウンして詳細な調査を実行する、重要イベントを通知するアラートを設定するなどの操作を行うことで、ネットワークの最新の状態やステータスを把握することができます。
システム

- **Deep Security Managerを保護する (29ページ)**: Agentを使用してDeep Security Managerを保護する方法について説明します。
- **通信 (30ページ)**: Deep Securityのコンポーネントが相互に通信する方法について説明します。
- **ダッシュボードをカスタマイズする (32ページ)**: 自分用または他のユーザ用のカスタムダッシュボードレイアウトを作成する方法について説明します。
- **メール通知 (36ページ)**: Deep Securityの重要なイベントに関するメール通知をさまざまなユーザに送信するようにDeep Securityを設定する方法について説明します。
- **アラート (37ページ)**: アラートを発令するイベント、アラートの重要度、およびアラートの通知をメールで送信するかどうかを設定する方法について説明します。
- **ポート検索の設定 (39ページ)**: Deep Securityの各ポート検索の対象となるポートを設定する方法について説明します。
- **Syslogの統合 (SIEM) (40ページ)**: イベントをSyslog経由でSIEMに送信するようにDeep Securityを設定する方法について説明します。
- **Relayグループ (53ページ)**: トレンドマイクロから最新のセキュリティおよびソフトウェアのアップデートを取得してDeep Securityシステムを最新の状態に保つプロセスを自動化するようにRelayグループを設定し、使用する方法について説明します。
- **セキュリティアップデート (57ページ)**: Deep Securityのセキュリティアップデートを管理する方法について説明します。
- **ソフトウェアアップデート (61ページ)**: Deep Securityのソフトウェアアップデートを管理する方法について説明します。
- **Virtual Applianceの検索のキャッシュ (63ページ)**: Deep Security Virtual Applianceの検索キャッシュ機能を使用して、仮想マシンでの不正プログラム検索と変更の検索のパフォーマンスを大幅に向上させる方法について説明します。
- **ユーザ管理 (65ページ)**: 役割に基づいたアクセス制御を使用してDeep Securityとネットワークの特定領域に対するユーザのアクセスを制限する方法など、Deep Securityのユーザを管理する方法について説明します。
- **データベースのバックアップと復元 (71ページ)**: Deep Securityのデータのバックアップを実行 (および自動化) する方法について説明します。
Deep Security Managerを保護する

Agentを使用してDeep Security Managerを保護する


Deep Security Managerのコンピュータ上のAgentを設定する

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]画面で、Managerのコンピュータを追加します。この時点でポリシーの適用を選択しないでください。
3. [コンピュータ]画面で、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]へ進みます。
4. 選択したコンピュータのSSL設定リストが表示されます。[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。
5. 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. 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)。
8. 次に、[Deep Security Manager内蔵のSSL資格情報]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。
9. ウィザードを終了して、[SSL設定]画面を閉じます。

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ます。これにより、Managerコンポーネント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。そのため、Managerでブラウザセッションを再起動して、Managerコンポーネントから新しい証明書を取得する必要があります。

[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。


SSLデータインスペクションの詳細については、「SSLデータストリーム (136ページ)」を参照してください。
通信

通信方向の決定

初期設定（双方向）では、Agent/Applianceによってハートビートが開始されますが、Managerの接続をAgentのポートで待機するため、Managerは必要に応じてAgent/Applianceに自由に接続できます。

注意: Deep Security Virtual Applianceは双方向モードでのみ動作します。この設定を変更すると、機能が中断します。


注意: Deep Security ManagerとAgent/Applianceとの通信は、FIPSに準拠した対称暗号化アルゴリズムAES-256とハッシュ関数SHA-256を使用して、SSL/TLS経由で行われます。

注意: ハートビート処理では、Managerによって次の情報が収集されます。
• ドライバのステータス（オンラインまたはオフライン）
• Agent/Applianceのステータス（時刻を含む）
• 前回のハートビート後後のAgent/Applianceのログ
• カウンタをアップデートするデータ
• Agent/Applianceのセキュリティ設定のフィンガープリント（設定が最新のものかどうか判断するために使用）

ハートビートの実行間隔（Agent/ApplianceまたはManagerによる開始）およびアラートが生成されるまでに失われるハートビートの許容数を変更できます。

この設定は（他の多くの設定と同様に）、複数のレベルで設定できます。ベースポリシー（すべてのポリシーの親ポリシー）で設定すると、ポリシーが割り当てられているすべてのコンピュータに適用されます。また、下位ポリシーやコンピュータごとに設定することもできます。

ポリシーで通信方向を設定するには

1. 通信を設定するポリシーのポリシーエディタ ([詳細]画面) を開きます。
2. [設定]→[コンピュータ]→[通信方向]に移動します。
4. [保存]をクリックして変更を適用します。

特定のコンピュータの通信方向を設定するには

1. 通信を設定するコンピュータのコンピュータエディタ ([詳細]画面) を開きます。
2. [設定]→[コンピュータ]→[通信方向]に移動します。
4. [保存] をクリックして変更を適用します。

注意: Agent/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/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。

関連項目:

- ポリシー、継承、およびオーバーライド (292ページ)
ダッシュボードをカスタマイズする

ダッシュボードは、Deep Security Managerにログオンしたときに最初に表示される画面です。ダッシュボードの機能を設定したりカスタマイズしたりできます。またレイアウトを保存してログオン時に表示することもできます(ダッシュボードは、前回ログアウトしたときのまま表示されます。別のユーザがログオンし、レイアウトを変更した場合でも、影響されません)。

ダッシュボードの表示で設定可能な要素は、取得するデータの期間、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、表示する「ウィジェット」、およびそのウィジェットの画面上のレイアウトです。

日時の範囲

ダッシュボードには、過去24時間または7日間のデータが表示されます。

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:] ドロップダウンメニューを使用して、特定のコンピュータから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め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。

タグの詳細については、「イベントのタグ付け (145ページ)」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] リンクをクリックし、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。

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交換されます(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、それぞれ別個のタブとして保存できます。ログオン後、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。
イベントログとデータ収集

初期設定で、Deep Security Managerでは、ハートビートごとにAgent/Applianceからイベントが収集されます。収集されるデータの量は、保護されているコンピュータの台数、コンピュータの使用状況、およびイベント記録の設定によって異なります。

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。

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。

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。


セキュリティログ監視モジュールは、指定の重要度を超える条件が含まれるセキュリティログ監視ルールがトリガされた場合にのみイベントを記録するように設定できます。セキュリティログ監視イベントが記録される重要度を設定するには、ポリシーまたはコンピュータエディタの [セキュリティログ監視]→[詳細]→[重要度のクリッピング] に移動します。

イベント収集の効率性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。
- 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していると、ログエントリーが多くなる場合があります。
- 侵入防御ルールの場合、攻撃元の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)。それ以外のときにパケットデータの追加をオフのままにしておくと、ログサイズが非常に大きくなってしまいいます。
メール通知

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。このメールシステムを有効にするには、Deep Security ManagerにSMTPサーバへのアクセス権を与える必要があります。また、SMTPを設定し、ユーザに対してメールをトリガするアラートを選択します。

SMTPを設定する

SMTP設定パネルには、[管理]→[システム設定]→[SMTP] タブからアクセスできます。

SMTPサーバのアドレスを入力します（必要に応じてポート番号も入力します）。メールの送信元とする「送信元」メールアドレスを入力します。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の、配信不能通知を送信先となる「バウンス」メールアドレスを入力します。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。必要な情報を入力したら、[SMTP設定のテスト] を使用して設定をテストします。

メールを送信するアラートを設定する

アラートをトリガさせる条件の数は30を超えるが、そのすべてでメール送信をトリガしない設定にすることもできます。メール送信をトリガするアラートを設定するには、[管理]→[システム設定]→[アラート] に進みます。[アラート設定の表示] をクリックして、すべてのアラートのリストを表示します。アラートの横のチェックマークは、アラートが「オン」になっているかどうかを示します。アラートがオンの場合、該当する状況になった場合にそのアラートがトリガされますが、メールが送信されるというわけではありません。アラートをダブルクリックすると、その[アラート設定] 画面が表示されます。

アラートメールを受信するユーザを設定する

最後に、アラートメールを受信するユーザを設定する必要があります。[管理]→[ユーザ管理]→[ユーザ] に進みます。ユーザをダブルクリックし、[連絡先情報] タブを選択します。

[アラートメールを受信] チェックボックスをオンにして、このユーザがアラートのメール通知を受信できるようにします。

SIEM、Syslog、およびSNMP

Agent/ApplianceとManagerの両方が、SIEMシステムにイベントを送信するように設定できます。Agent/Applianceからは保護モジュール関連のセキュリティイベント情報、Managerからはシステムイベントが送信されます。

システムイベントは、SyslogまたはSNMP経由で、Managerから転送されます。システムイベントのSyslogまたはSNMPの設定を行うには、Deep Security Managerで [管理]→[システム設定]→[SIEM] タブまたは[管理]→[システム設定]→[SNMP] タブに進みます。

保護モジュールのセキュリティイベントは、Syslog経由でAgent/Applianceから転送できます。保護モジュールのセキュリティイベントのSyslog設定を行うには、ポリシーまたはコンピュータエディタの[設定]→[SIEM] タブに進みます。

Syslogの設定の詳細については、「Syslogの統合 (SIEM) (40ページ)」を参照してください。
アラート

通常、アラートは、コンピュータがオフラインになったり、ルールが期限切れになるなどシステムステータスの異常を警告することが目的ですが、フィンガープリント検索やその他のセキュリティ関連イベントの検出を通知するアラートもあります（個々の侵入防御イベントおよびファイアウォールイベントに関する通知については、Syslogサーバの設定を検討してください）。

定義済みのアラートリストを確認するには、[アラート]画面を開き、画面の上部にある[アラートの設定]をクリックするか、[管理]→[システム設定]→[アラート]に進み、[アラート設定の表示]をクリックします。

アラートに関連する処理は、各アラートの[プロパティ]画面を開いて設定できます。アラートはオンとオフを切り替えたり、重要度の警告と重大を切り替えられます。メールアラートを受信するユーザを設定することもできます。[管理]→[ユーザ管理]→[ユーザ]に進み、個々のユーザをダブルクリックして、[連絡先情報]タブをクリックし、[アラートメールを受信]オプションを選択するか、または選択を解除します。

注意：アラートは、ポリシーとコンピュータごとに異なる設定にはできません。1つのアラートに関するプロパティに加えた設定変更は、全体に適用されます。
アラート通知を受信するユーザの設定に加えて、すべてのアラート通知が送信される初期設定のメールアドレスを指定するオプションもあります。このオプションは、[管理]→[システム設定]→[アラート]タブにあります。

注意： [管理]→[システム設定]→[SMTP]タブで、SMTPが設定されていることを確認してください。

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。
ポート検索の設定

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画面にある [ファイアウォール]→[一般]タブの [ポート検索]エリアで [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: ポート範囲の設定に関係なく、ポート4118は常に検索されます。このポートは、Managerによって開始された通信が送信先であるAgent/Appliance上のポートです。コンピュータに対して通信方向が [Agent/Applianceから開始] (ポリシーまたはコンピュータエディタの [設定]→[コンピュータ]) に設定されると、ポート4118は閉じられます。

検索する新しいポート範囲を定義するには

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、メニューーパーの [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」入力します)。[OK] をクリックします。
3. ポリシーまたはコンピュータエディタの [設定]→[検索] に進み、[検索するポート] ドロップダウン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。
Syslogの統合 (SIEM)

Deep Securityでは、syslogサーバに次の形式でイベントを転送できます。

- **Common Event Format 1.0**: ArcSight (www.arcsight.com) が提供している形式。
- **Log Event Extended Format (LEEF) 2.0**: IBM QRadarとの統合に使用される形式。
- **Basic Syslog形式**: 一部のモジュールではBasic Syslog形式がサポートされますが、これはあくまで旧環境用の対応であり、新しいSyslog統合プロジェクトには使用しないでください。

Syslogメッセージは、[システムイベント] タブで選択したイベントについてのみ送信されます。それ以外のイベントタイプのsyslog通知については、ポリシーエディタまたはコンピュータエディタで設定できます。

| 注意: | Deep Security ManagerでSyslog転送を有効にしても初期設定のイベントログ処理には影響を与えません。つまり、Syslogを有効にしても、通常のイベント記録メカニズムが無効になることはありません。 |

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。
   ```bash
touch /var/log/DSM.log
   ```
3. 末尾に、次の2行を追加します。
   ```bash
   # 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. rsyslog.confの末尾に、次の2行を追加します。
   ```bash
   #ModLoad imudp
   #UDPServerRun 514
   
   #ModLoad imtcp
   #InputTCPServerRun 514
   ```
   変更後のコードは、次のとおりです。

   ```bash
   #ModLoad imudp
   #UDPServerRun 514
   
   #ModLoad imtcp
   #InputTCPServerRun 514
   ```

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、/var/log/DSM.log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。

```bash
service rsyslog restart
```

Red Hat Enterprise Linux 7で次のコマンドを実行します。

```bash
systemctl restart rsyslog
```

Syslogが機能すると、/var/log/DSM.log にログが記録されます。

### 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。
   ```bash
   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. クリを保存して、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、/var/log/DSM.logログに権限を設定します。
7. 次のコマンドを実行します。
   ```bash
   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。
    ```bash
        /etc/init.d/syslog restart
    ```

Syslogが機能すると、/var/log/DSM.log にログが記録されます。

### Manager設定

すべての管理下のコンピュータからSyslogコンピュータにログが送信されるようにDeep Security Managerを設定したり、個々のコンピュータを別々に設定したりできます。

すべての管理下のコンピュータでSyslogが使用されるようにManagerを設定するには、次の手順を実行します。

1. [管理]→[システム設定]→[SIEM]タブに進みます。
2. [システムイベント通知 (Managerから)]エリアで、[リモートコンピュータにシステムイベントを転送する (Syslog経由)]オプションを設定します。
3. Syslogコンピュータのホスト名またはIPアドレスを入力します。
4. 使用するUDPポートを入力します (通常は514)。
5. 使用するSyslogファシリティを選択します (前述のRed Hatの例ではLocal4)。
6. 使用するSyslog形式を選択します。

   **注意:** Common Event Format 1.0は、Arcsight (www.arcsight.com) が提供している形式です。この仕様は、ArcsightのWebサイトから入手できます。
これで、すべての既存および新規のコンピュータが初期設定でリモートSyslogを使用するようにDeep Security Managerを設定しました。

Syslogメッセージの送信元には、2つのオプションがあります。1つ目のオプション ([直接転送する]) は、AgentまたはVirtual Applianceからメッセージをリアルタイムで直接送信します。2つ目のオプション ([Manager経由でリレーする]) は、ハートビートでイベントを収集した後、ManagerからSyslogメッセージを送信します。送信元の数に基づいて送信先がライセンス許可する場合は、Managerから送信するオプションを選択することが望ましいです。

SyslogメッセージがManagerから送信される場合は、いくつかの違いがあります。元のホスト名(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』) が使用されます。「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。また、イベントがタグ付けされている場合は、拡張「TrendMicroDsTags」が使用されます(これは、自動タグ付けが実行されている場合のみ適用されます。Managerによって収集された場合のみイベントがsyslog経由で転送されるためです)。Managerを通じてリレーされるログには、製品名が「Deep Security Agent」と表示されますが、バージョンはManagerのバージョンになっています。

すべてのCEFイベントには、イベントの元のソースを判断するためのdvc=IPv4アドレスまたはdvchost=ホスト名 (またはIPv6アドレス) が含まれています。この拡張はVirtual ApplianceやManagerから送信されるイベントに重要なものです。ここでは、Syslogメッセージの送信先はイベントの発信元ではないためです。

この初期設定は、特定のポリシーに対して、および個々のコンピュータでオーバーライドできます。個々のコンピュータで初期設定をオーバーライドするには、設定するコンピュータを見つけ、[詳細]→[設定] に進んで [SIEM] タブをクリックします。この設定は、コンピュータ上の他の多くの設定と同様に、初期設定を継承するように設定することも、オーバーライドすることもできます。このコンピュータで継承可能の初期設定をオーバーライドするように設定するには、[イベントの転送先] オプションを選択して別のsyslogサーバの詳細を入力するか、ログを一切転送しないようにします。ポリシーの設定のオーバーライドする場合も、同じ手順に従います。


Syslogメッセージを解析する (CEF)

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 chrisds7 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。  

<table>
<thead>
<tr>
<th>署名ID</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>カスタム侵入防衛ルール</td>
</tr>
<tr>
<td>20</td>
<td>ログのみのファイアウォールルール</td>
</tr>
<tr>
<td>21</td>
<td>拒否のファイアウォールルール</td>
</tr>
<tr>
<td>30</td>
<td>カスタム変更監視ルール</td>
</tr>
<tr>
<td>40</td>
<td>カスタムセキュリティリック監視ルール</td>
</tr>
<tr>
<td>100-7499</td>
<td>システムイベント</td>
</tr>
<tr>
<td>100-199</td>
<td>ポリシーで未許可のファイアウォールルール</td>
</tr>
<tr>
<td>200-299</td>
<td>侵入防衛システム (IPS) の内部エラー</td>
</tr>
</tbody>
</table>
### 管理者ガイド

#### Syslogの統合 (SIEM)

<table>
<thead>
<tr>
<th>記号ID</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>300-399</td>
<td>SSLイベント</td>
</tr>
<tr>
<td>500-899</td>
<td>僞侵入の規範化イベント</td>
</tr>
<tr>
<td>1,000,000-1,999,999</td>
<td>Trend Microが提供する侵入防御ルール。署名ID (Signature ID) は、侵入防御ルールIDと同一です。</td>
</tr>
<tr>
<td>2,000,000-2,999,999</td>
<td>Trend Microが提供する変更監視ルール。署名ID (Signature ID) は、変更監視ルールID + 1,000,000です。</td>
</tr>
<tr>
<td>3,000,000-3,999,999</td>
<td>Trend Microが提供するセキュリティログ監視ルール。署名ID (Signature ID) は、セキュリティログ監視ルールID + 2,000,000です。</td>
</tr>
<tr>
<td>4,000,000-4,999,999</td>
<td>Trend Microの不正プログラム対策イベント用に予約済み。現在は、以下の署名IDのみが使用されています。</td>
</tr>
</tbody>
</table>
- 4,000,000
- 4,000,001
- 4,000,002
- 4,000,003
- 4,000,010
- 4,000,011
- 4,000,012
- 4,000,013
| 5,000,000-5,999,999 | Trend MicroのWebレピュテーションイベント用に予約済み。現在は、以下の署名IDのみが使用されています。 |
- 5,000,000
- 5,000,001

#### 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ないかもしれません。同様に、これらの拡張が表示される順序も、表に示す順序とは異なる場合があります。正規表現を使用してエントリを解析する場合は、表に示す各キーと値のペアの位置や順番に依存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。まれに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。

#### Syslogメッセージを解析する (LEEF 2.0)

**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 (DSMシステムイベントログのサンプル):**

#### Managerで発生するイベント

**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 fe80:0:0:0:2d02:9870:beaa:fd41

**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:

```
Subject: 10.201.114.164
Severity: Warning
sev=3
src=10.201.114.164

usrName=System msg=Alert: CPU Warning Threshold Exceeded
Subject: 10.201.114.164

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。

<table>
<thead>
<tr>
<th>CEF拡張フィールド</th>
<th>LEEF拡張フィールド</th>
<th>名前</th>
<th>説明</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>src</td>
<td>src</td>
<td>Source IP Address</td>
<td>送信元のDeep Security ManagerのIPアドレス。</td>
<td>src=10.52.116.23</td>
</tr>
<tr>
<td>suser</td>
<td>suserName</td>
<td>Source User</td>
<td>送信元のDeep Security Managerのユーザアカウント。</td>
<td>suser=MasterAdmin</td>
</tr>
<tr>
<td>target</td>
<td>target</td>
<td>Target Entity</td>
<td>イベントの対象のエンティティ。イベントの対象は、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。</td>
<td>target=MasterAdmin target=server01</td>
</tr>
<tr>
<td>targetType</td>
<td>targetType</td>
<td>Target Entity Type</td>
<td>イベントの対象のエンティティの種類。</td>
<td>targetType=Host</td>
</tr>
<tr>
<td>msg</td>
<td>msg</td>
<td>Details</td>
<td>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。</td>
<td>msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1</td>
</tr>
<tr>
<td>TrendMicroDsTags</td>
<td>TrendMicroDsTags</td>
<td>Event Tags</td>
<td>イベントに割り当てられたDeep Securityのイベントタグ</td>
<td>TrendMicroDsTags=suspicious</td>
</tr>
<tr>
<td>TrendMicroDsTenant</td>
<td>TrendMicroDsTenant</td>
<td>Tenant Name</td>
<td>Deep Securityのテナント</td>
<td>TrendMicroDsTenant=Primary</td>
</tr>
<tr>
<td>TrendMicroDsTenantId</td>
<td>TrendMicroDsTenantId</td>
<td>Tenant ID</td>
<td>Deep SecurityのテナントID</td>
<td>TrendMicroDsTenantId=0</td>
</tr>
<tr>
<td>なし</td>
<td>sev</td>
<td>Severity</td>
<td>イベントの重要度。最も低い重要度は1、高い重要度は10です。</td>
<td>sev=3</td>
</tr>
<tr>
<td>なし</td>
<td>cat</td>
<td>Category</td>
<td>イベントのカテゴリ</td>
<td>cat=System</td>
</tr>
<tr>
<td>なし</td>
<td>name</td>
<td>Name</td>
<td>イベント名</td>
<td>name=Alert Ended</td>
</tr>
<tr>
<td>なし</td>
<td>desc</td>
<td>Description</td>
<td>イベントの説明</td>
<td>desc=Alert: CPU Warning Threshold Exceeded</td>
</tr>
</tbody>
</table>

### Agentで発生するイベント

#### 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 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 Manager|9.6.2007|21|cat=Firewall name=Remote Domain Enforcement (Split Tunnel) desc=Remote Domain Enforcement (Split Tunnel) sev=5 cn1=37 cn1Label=Host ID dvchost=laptop_adaggs 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
```
<table>
<thead>
<tr>
<th>CEF拡張フィールド</th>
<th>LEEF拡張フィールド</th>
<th>名前</th>
<th>説明</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>act</td>
<td>act</td>
<td>Action</td>
<td>ファイアウォールルールによる処理。値は、LogまたはDenyです。ルールまたは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、処理の値の前に「IDS:」が付きます。</td>
<td>act=Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>act=Deny</td>
</tr>
<tr>
<td>cn1</td>
<td>cn1</td>
<td>Host Identifier</td>
<td>特定のSyslogイベントからAgentコンピュータを一意に識別するために使用できる。Agentコンピュータの内部識別子。</td>
<td>cn1=113</td>
</tr>
<tr>
<td>cn1Label</td>
<td>cn1Label</td>
<td>Host ID</td>
<td>フィールドcn1のフレンドリ名のラベル。</td>
<td>cn1Label=ID</td>
</tr>
<tr>
<td>cnt</td>
<td>cnt</td>
<td>Repeat Count</td>
<td>このイベントが連続して繰り返された回数。</td>
<td>cnt=8</td>
</tr>
<tr>
<td>cs2</td>
<td>cs2</td>
<td>TCP Flags</td>
<td>(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あります。[Manager経由でリレーする]を選択した場合は、この拡張の出力にはフラグ名のみが含まれます。</td>
<td>cs2=0x10 ACK cs2=0x14 ACK RST</td>
</tr>
<tr>
<td>cs2Label</td>
<td>cs2Label</td>
<td>TCP Flags</td>
<td>フィールドcs2のフレンドリ名のラベル。</td>
<td>cs2Label=TCP Flags</td>
</tr>
<tr>
<td>cs3</td>
<td>cs3</td>
<td>Packet Fragmentation Information</td>
<td>(IP送信側の場合のみ)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。</td>
<td>cs3=DF cs3=MF cs3=DF MF</td>
</tr>
<tr>
<td>cs3Label</td>
<td>cs3Label</td>
<td>Fragmentation Bits</td>
<td>フィールドcs3のフレンドリ名のラベル。</td>
<td>cs3Label=Fragmentation Bits</td>
</tr>
<tr>
<td>cs4</td>
<td>cs4</td>
<td>ICMP Type and Code</td>
<td>(ICMPプロトコルの場合のみ)送信元コンピュータのIP アドレス。</td>
<td>cs4=11 cs4=80</td>
</tr>
<tr>
<td>cs4Label</td>
<td>cs4Label</td>
<td>ICMP Type and Code</td>
<td>フィールドcs4のフレンドリ名のラベル。</td>
<td>cs4Label=ICMP Type and Code</td>
</tr>
<tr>
<td>dmac</td>
<td>dstMAC</td>
<td>Destination MAC Address</td>
<td>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。</td>
<td>dmac= 00:0C:29:2F:09:83</td>
</tr>
<tr>
<td>dpt</td>
<td>dstPort</td>
<td>Destination Port</td>
<td>送信元コンピュータのIPアドレス。</td>
<td>dpt=80 dpt=135</td>
</tr>
<tr>
<td>dst</td>
<td>dst</td>
<td>Destination IP Address</td>
<td>送信元コンピュータのIPアドレス。</td>
<td>dst=192.168.1.102 dst=10.30.128.2</td>
</tr>
<tr>
<td>in</td>
<td>in</td>
<td>Inbound Bytes Read</td>
<td>読み取られた送信バイト数。</td>
<td>in=137 in=21</td>
</tr>
<tr>
<td>out</td>
<td>out</td>
<td>Outbound Bytes Read</td>
<td>読み取られた送信バイト数。</td>
<td>out=216 out=13</td>
</tr>
<tr>
<td>proto</td>
<td>proto</td>
<td>Transport protocol</td>
<td>使用する接続転送プロトコルの名前。</td>
<td>proto=tcp proto=udp proto=icmp</td>
</tr>
<tr>
<td>smac</td>
<td>srcMAC</td>
<td>Source MAC Address</td>
<td>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。</td>
<td>smac= 00:0E:04:2C:02:B3</td>
</tr>
<tr>
<td>spt</td>
<td>srcPort</td>
<td>Source Port</td>
<td>送信元コンピュータのIPアドレス。</td>
<td>spt=1032 spt=443</td>
</tr>
<tr>
<td>src</td>
<td>src</td>
<td>Source IP Address</td>
<td>送信元コンピュータのIPアドレス。</td>
<td>src=192.168.1.105 src=10.10.251.231</td>
</tr>
<tr>
<td>TrendMicroDsFrameType</td>
<td>TrendMicroDsFrameType</td>
<td>Ethernet frame type</td>
<td>拡張のイーサネットフレームの種類。</td>
<td>TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI</td>
</tr>
<tr>
<td>TrendMicroDsPacketData</td>
<td>TrendMicroDsPacketData</td>
<td>Packet data</td>
<td>(パケットデータを含めるように設定されている場合)パケットデータのBase64でエンコード。</td>
<td>TrendMicroDsPacketData=AA...BA=</td>
</tr>
</tbody>
</table>
### CEF拡張フィールド

<table>
<thead>
<tr>
<th>名前</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>act</td>
<td>侵入防御ルールによる処理。値は、Block、Reset、またはLogのいずれかです。ルールまたはネットワークエンジンが検出のモードで動作している場合、処理の前に「IDS:」が付きます (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。)</td>
</tr>
<tr>
<td>CEF拡張フィールド</td>
<td>LEEF拡張フィールド</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>cn1</td>
<td>cn1</td>
</tr>
<tr>
<td>cn1Label</td>
<td>cn1Label</td>
</tr>
<tr>
<td>cn3</td>
<td>cn3</td>
</tr>
<tr>
<td>cn3Label</td>
<td>cn3Label</td>
</tr>
<tr>
<td>cnt</td>
<td>cnt</td>
</tr>
<tr>
<td>cs1</td>
<td>cs1</td>
</tr>
<tr>
<td>cs1Label</td>
<td>cs1Label</td>
</tr>
</tbody>
</table>
| 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あります。
<p>| cs2Label        | cs2Label        | TCP Flags       | フィールドcs2のフレンドリ名のラベル。                                                                                                                                                      | cs2Label=TCP Flags |
| cs3             | cs3             | Packet Fragmentation Information | [DF]フィールドは、「IP Don't Fragment」ビットが設定されている場合に存在します。「MF」フィールドは、「IP More Fragments」ビットが設定されている場合に存在します。                                           | cs3=DF    |
| cs3Label        | cs3Label        | Fragmentation Bits | フィールドcs3のフレンドリ名のラベル。                                                                                                                                                        | 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    |
| cs4Label        | cs4Label        | ICMP            | フィールドcs4のフレンドリ名のラベル。                                                                                                                                                        | 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    |
| cs5Label        | cs5Label        | Intrusion Prevention Stream Position | フィールドcs5のフレンドリ名のラベル。                                                                                                                                                        | cs5Label=Intrusion Prevention Stream Position |</p>
<table>
<thead>
<tr>
<th>CEF拡張フィールド</th>
<th>LEEF拡張フィールド</th>
<th>名前</th>
<th>説明</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs6</td>
<td>cs6</td>
<td>Intrusion Prevention Filter Flags</td>
<td>次のフラグの値の合計値。</td>
<td>例: cs6=9 (Data truncated) と 8 (Have Data) の組み合わせの例</td>
</tr>
<tr>
<td>cs6Label</td>
<td>cs6Label</td>
<td>Intrusion Prevention Flags</td>
<td>フィールドcs6のフレンドリ名のラベル。</td>
<td></td>
</tr>
<tr>
<td>dmac</td>
<td>dstMAC</td>
<td>Destination MAC Address</td>
<td>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。</td>
<td>dmac= 00:0C:29:2F:09:B3</td>
</tr>
<tr>
<td>dpt</td>
<td>dstPort</td>
<td>Destination Port</td>
<td>(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。</td>
<td>dpt=80</td>
</tr>
<tr>
<td>dst</td>
<td>dst</td>
<td>Destination IP Address</td>
<td>送信元コンピュータのIPアドレス。</td>
<td>dst=192.168.1.102 dst=10.30.128.2</td>
</tr>
<tr>
<td>in</td>
<td>in</td>
<td>Inbound Bytes Read</td>
<td>(受信接続の場合のみ) 読み取られた受信バイト数。</td>
<td>in=137 in=21</td>
</tr>
<tr>
<td>out</td>
<td>out</td>
<td>Outbound Bytes Read</td>
<td>(送信接続の場合のみ) 読み取られた送信バイト数。</td>
<td>out=216 out=13</td>
</tr>
<tr>
<td>proto</td>
<td>proto</td>
<td>Transport protocol</td>
<td>使用する接続転送プロトコルの名前。</td>
<td>proto(tcp) proto(udp) proto(icmp)</td>
</tr>
<tr>
<td>smac</td>
<td>srcMAC</td>
<td>Source MAC Address</td>
<td>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。</td>
<td>smac= 00:0E:04:2C:02:B3</td>
</tr>
<tr>
<td>spt</td>
<td>srcPort</td>
<td>Source Port</td>
<td>(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。</td>
<td>spt=1032 spt=443</td>
</tr>
<tr>
<td>src</td>
<td>src</td>
<td>Source IP Address</td>
<td>送信元コンピュータのIPアドレス。</td>
<td>src=192.168.1.105 src=10.10.251.231</td>
</tr>
<tr>
<td>TrendMicroDsFrameType</td>
<td>TrendMicroDsFrameType</td>
<td>Ethernet frame type</td>
<td>接続のイーサネットフレームの種類。</td>
<td>TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI</td>
</tr>
<tr>
<td>TrendMicroDsPacketData</td>
<td>TrendMicroDsPacketData</td>
<td>Packet data</td>
<td>パケットデータを含めるように設定されている場合、パケットデータのBase64でエンコードされたコピー。等号はエスケープされます。たとえば、「='」のようになります。この設定は [Manager経由でリレーする] オプションを選択したときには含まれません。</td>
<td>TrendMicroDsPacketData=AA...BA=</td>
</tr>
<tr>
<td>dvc</td>
<td>dvc</td>
<td>Device address</td>
<td>cn1のIPv4アドレス。アドレスがIPv4の場合、dvcを使用します。アドレスがIPv6またはホスト名の場合は、dvchostを使用します。</td>
<td>dvc=10.1.144.199</td>
</tr>
<tr>
<td>dvchost</td>
<td>dvchost</td>
<td>Device host name</td>
<td>cn1のIPv6アドレスまたはホスト名。アドレスがIPv6またはホスト名の場合は、dvchostを使用します。</td>
<td>dvchost=exch01</td>
</tr>
<tr>
<td>TrendMicroDsTags</td>
<td>TrendMicroDsTags</td>
<td>Event tags</td>
<td>イベントに割り当てられたDeep Securityのイベントタグ</td>
<td>TrendMicroDsTags=Suspicious</td>
</tr>
<tr>
<td>TrendMicroDsTenant</td>
<td>TrendMicroDsTenant</td>
<td>Tenant name</td>
<td>Deep Securityのテナント名</td>
<td>TrendMicroDsTenant=Primary</td>
</tr>
<tr>
<td>CEF拡張フィールド</td>
<td>LEEF拡張フィールド</td>
<td>名前</td>
<td>説明</td>
<td>例</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>------</td>
<td>------</td>
<td>----</td>
</tr>
<tr>
<td>TrendMicroDsTenantId</td>
<td>TrendMicroDsTenantId</td>
<td>Tenant ID</td>
<td>Deep SecurityのテナントID</td>
<td>TrendMicroDsTenantId=0</td>
</tr>
<tr>
<td>なし</td>
<td>sev</td>
<td>Severity</td>
<td>イベントの重要度。最も低い重要度は1、高い重要度は10です。</td>
<td>sev=10</td>
</tr>
<tr>
<td>なし</td>
<td>cat</td>
<td>Category</td>
<td>カテゴリ</td>
<td>cat=Intrusion Prevention</td>
</tr>
<tr>
<td>なし</td>
<td>name</td>
<td>Name</td>
<td>イベント名</td>
<td>name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities</td>
</tr>
<tr>
<td>なし</td>
<td>desc</td>
<td>Description</td>
<td>イベントの説明。侵入防御イベントにはイベントの説明がないため、イベント名を使用します。</td>
<td>desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities</td>
</tr>
</tbody>
</table>

セキュリティログ監視イベントの形式

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-RM6HMG42G65V msg=WinEvtLog Security:AUDIT_FAILURE(4625): Microsoft-Windows-Security-Auditing; (no user): no domain: WIN-RM6HMG42G65V: 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)|| | | | | |

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Manager|9.6.2007|3003486|cat=Log Inspection name=Mail Server - MDaemon desc=Server Shutdown. sev=3 cn1=37 cn1Label=Host ID dvchost=laptop_adaggs TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cs1=Server Shutdown. cs1Label=LI Description fname=| shost= |

msg=

<table>
<thead>
<tr>
<th>CEF拡張フィールド</th>
<th>LEEF拡張フィールド</th>
<th>名前</th>
<th>説明</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn1</td>
<td>cn1</td>
<td>Host Identifier</td>
<td>特定のSyslogイベントからAgentコンピュータを一意に識別するのに使用できる、Agentコンピュータの内部識別子。</td>
<td>cn1=113</td>
</tr>
<tr>
<td>cn1Label</td>
<td>cn1Label</td>
<td>Host ID</td>
<td>フィールドcn1のフレンドリ名のラベル。</td>
<td>cn1Label=Host ID</td>
</tr>
<tr>
<td>cs1</td>
<td>cs1</td>
<td>Specific Sub-Rule</td>
<td>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。</td>
<td>cs1=Multiple Windows audit failure events</td>
</tr>
<tr>
<td>cs1Label</td>
<td>cs1Label</td>
<td>LI Description</td>
<td>フィールドcs1のフレンドリ名のラベル。</td>
<td>cs1Label=LI Description</td>
</tr>
<tr>
<td>duser</td>
<td>duser</td>
<td>User Information</td>
<td>(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。</td>
<td>duser=(no user) duser=NETWORK SERVICE</td>
</tr>
<tr>
<td>fname</td>
<td>fname</td>
<td>Target entity</td>
<td>セキュリティログ監視ルールの対象のエンティティ。監視対象のログファイルが含まれます。</td>
<td>fname=Application fname=C:\Program Files\CMS\logs\server0.log</td>
</tr>
<tr>
<td>msg</td>
<td>msg</td>
<td>Details</td>
<td>セキュリティログ監視イベントの詳細。検出したログイベントの詳細で記載される。</td>
<td>msg=WinEvtLog:Application:AUDIT_FAILURE(20187): pgEvent:(no user): no domain: SERVER01:Remote login failure for user ‘xyz’</td>
</tr>
<tr>
<td>shost</td>
<td>shost</td>
<td>Source Hostname</td>
<td>送信元コンピュータのホスト名。</td>
<td>shost=webserver01.corp.com</td>
</tr>
<tr>
<td>src</td>
<td>src</td>
<td>Source IP Address</td>
<td>送信元コンピュータのIPアドレス。</td>
<td>src=192.168.1.105 src=10.10.251.231</td>
</tr>
<tr>
<td>dvc</td>
<td>dvc</td>
<td>Device address</td>
<td>cn1のIPv4アドレス。アドレスがIPv4の場合、dvcを使用します。</td>
<td>dvc=10.1.144.199</td>
</tr>
</tbody>
</table>
### 変更監視ログイベントの形式

#### 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>|30|New Integrity Monitoring Rule|6|cn1=1 cn1Label=Host ID dvchost=hostname act=updated filePath=c:\windows\message.dll 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)|拡張 (Extension)

#### LEEFログエントリのサンプル
LEEF:2.0|Trend Micro|Deep Security Manager|9.6.2007|2002779|cat=Integrity Monitor name=Microsoft Windows - System file modified desc=Microsoft Windows - System file modified sev=8 cn1=37 cn1Label=Host ID dvchost=customHost

### CEF拡張フィールド

<table>
<thead>
<tr>
<th>名前</th>
<th>説明</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>act</td>
<td>Action</td>
<td>act=created, act=updated, act=deleted, act=renamed</td>
</tr>
<tr>
<td>cn1</td>
<td>cn1 Host Identifier</td>
<td>cn1=113</td>
</tr>
<tr>
<td>cn1Label</td>
<td>cn1Label Host ID</td>
<td>cn1Label=Host ID</td>
</tr>
<tr>
<td>filePath</td>
<td>filePath Target Entity</td>
<td>filePath=C:\WINOWDS\system32\drivers\etc\hosts</td>
</tr>
<tr>
<td>msg</td>
<td>Attribute changes</td>
<td>msg=lastModified,sha1, size</td>
</tr>
<tr>
<td>oldfilePath</td>
<td>Old target entity</td>
<td>oldFilePath=C:\WINOWDS\system32\logs\files\ds_agent.log</td>
</tr>
<tr>
<td>dvc</td>
<td>Device address</td>
<td>dvc=10.1.144.199</td>
</tr>
<tr>
<td>dvchost</td>
<td>dvchost Device host name</td>
<td>dvchost=laptop_adaggs</td>
</tr>
</tbody>
</table>

### LEEF拡張フィールド

<table>
<thead>
<tr>
<th>名前</th>
<th>説明</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrendMicroDsTags</td>
<td>TrendMicroDsTags Events tags</td>
<td>TrendMicroDsTags=suspicious</td>
</tr>
<tr>
<td>TrendMicroDsTenant</td>
<td>TrendMicroDsTenant Tenant name</td>
<td>TrendMicroDsTenant=Primary</td>
</tr>
<tr>
<td>TrendMicroDsTenantId</td>
<td>TrendMicroDsTenantId Tenant ID</td>
<td>TrendMicroDsTenantId=0</td>
</tr>
<tr>
<td>sev</td>
<td>Severity</td>
<td>sev=3</td>
</tr>
<tr>
<td>cat</td>
<td>Category</td>
<td>cat=Log Inspection</td>
</tr>
<tr>
<td>name</td>
<td>Name</td>
<td>name=Mail Server - MDaemon</td>
</tr>
<tr>
<td>desc</td>
<td>Description</td>
<td>desc=Server Shutdown</td>
</tr>
</tbody>
</table>
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 filepath=C:\Users\trend\Desktop\Eicar.txt act=Delete msg=Realtime

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)|拡張 (Extension)

LEEFログエントリのサンプル：LEEF:2.0|Trend Micro|Deep Security Manager|9.6.2007|4000010|cat=Anti-Malware name=SPYWARE_KEYL_ACTIVE desc=SPYWARE_KEYL_ACTIVE sev=6 cn1=45 cn1Label=Host ID dvchost=laptop_mneil TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cs3=C:\Windows\System32\certreq.exe cs3Label=Infected Resource cs4=10 cs4Label=Resource Type cs5=50 cs5Label=Risk Level act=Clean msg=Realtime

CEF拡張フィールド | LEEF拡張フィールド | 名前 | 説明 | 例
--- | --- | --- | --- | ---
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
なし | sev | Severity | イベントの重要度。最も低い重要度は1、高い重要度は10です。 | sev=8
なし | cat | Category | カテゴリ | cat=Integrity Monitor
なし | name | Name | イベント名 | name=Microsoft Windows - System file modified
なし | desc | Description | イベントの説明。変更監視イベントにはイベントの説明がないため、イベント名を使用します。 | desc=Microsoft Windows - System file modified

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
なし | sev | Severity | イベントの重要度。最も低い重要度は1、高い重要度は10です。 | sev=6
Webレビュート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=site.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 Manager|9.6.2007|5000000|cat=Web Reputation name=WebReputation desc=WebReputation sev=6 cn1=3 cn1Label=Host ID dvchost=hr_data2 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 request=http://yw.olx5x9ny.org.it/HvuauRH/eighgSS.htm msg=Suspicious

関連項目:
- ポリシー、継承、およびオーバーライド (292ページ)
Relayグループ

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。ManagerはRelayに最新アップデートを取得するように指示します。新しいアップデートが入手可能になると、AgentおよびApplianceはRelayからアップデートを取得するように自動的に指示されます。Relayモジュールは64ビットWindowsおよびLinux Agentでのみ利用でき、初期設定では無効になっています。AgentでRelayモジュールを有効にするには、有効化されている64ビットWindowsまたはLinux版Agentを実行しているコンピュータの詳細画面を開き、概要→処理→ソフトウェアに進んで、[Relayの有効化]をクリックします。

RelayはRelayグループにまとめられます。新しく有効にしたRelayは、初期設定のRelayグループに割り当てられます。Agent/Applianceは、設定を変えないかぎり、初期設定のRelayグループからアップデートを取得します。特定の地域またはオフィスでは、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ように、コンピュータ上のAgentを設定することを推奨します。

Relayグループには、Relayメンバーを1つだけ含めることもできます。パフォーマンスおよび冗長性を高めるためには、複数のRelayメンバーを含むようにRelayグループを設定します。負荷や障害時の影響を分散させるため、グループ内のRelayに優先順位は付けられていません。Relayグループに割り当てられたAgent/Applianceは、それぞれ接続先のRelayメンバーをランダムに自動選択します。Agent/Applianceがアップデートをダウンロードしようとしたときに、最初のRelayが応答しなかった場合、Agent/Applianceはアップデートの送信元となる他のRelayメンバーからランダムに選択します。リストの順番はAgent/Applianceごとに変更されるため、それぞれが異なる順番でRelayと通信します。

注意: Relayは、別のRelayグループからセキュリティアップデートを取得することができますが、(同じRelayグループに属しているRelayであっても)別のRelayから取得することはできません。上位のRelayグループまたは設定済みの別のアップデート元から取得する必要があります。

RelayがあるAgent/Applianceのアップデート処理でビジー状態にある場合、別のAgent/Applianceからの新規接続は拒否されます。

帯域幅を最適化し、冗長性を高めるために、Relayグループを階層構造にすることができます。環境には、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するRelayグループが常に1つ以上存在しなければなりませんが、Relayグループ内のRelayは他のRelayグループからのアップデートをダウンロードすることもできます。割り当てられたRelayグループとの通信がすべて失敗した場合、Agent/Applianceは親のRelayグループに切り替えます。その後、Agent/Applianceは親RelayグループのRelayメンバーと通信して、アップデートを取得しようとします。

注意: Relayは、常に、Relayグループ階層の1つ上のグループから、またはトレンドマイクロのアップデートサーバから、アップデートを取得します。同じRelayグループ内のRelayからは取ることはできません。

Relay有効化済みAgentに接続できない場合には、セキュリティアップデート元からパターンファイルアンダーデートを直接ダウンロードするようにAgent/Applianceに許可するかどうかを指定できます。この設定を変更するには、[システム設定]→[アップデート]に移動し、セキュリティアップデートエリアにあるパターンファイルの設定を変更します。
Relayグループを作成する

1. Relayをインストールして有効化した後、 [管理]→[アップデート]→[Relayグループ] に進みます。
2. [新規] をクリックすると、 Relayグループウィザードが表示されます。 Relayグループを作成して名前を付け、このグループのメンバーになる Relayを選択します。
3. ブライマリ Relayグループには、 [セキュリティアップデート] セクションで [セキュリティアップデート元] を選択します。このように設定すると、 [管理]→[システム設定]→[アップデート] タブの [セキュリティアップデート] エリアで設定されたアップデートサーバーのURLからアップデートがダウンロードされます。
4. 手順2を繰り返し、さらにRelayグループを作成します。階層を作成するには、 [アップデートのダウンロード元] で、既存のRelayグループに含める新しいRelayグループの送信元を選択します。

Agent/ApplianceをRelayグループに割り当てる

1. [コンピュータ] 画面でコンピュータを選択し、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。 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。
2. 複数のコンピュータを割り当てるには、 [コンピュータ] 画面で、 <Shift> または <Ctrl> キーを押しながらリスト内のコンピュータをクリックして選択します。 [処理]→[Relayグループの割り当て] を選択します。 選択したすべてのコンピュータで使用するRelayグループを、リストから選択します。

注意： 複数のコンピュータを選択する場合、 [Relayグループの割り当て] が有効になるのは、選択したすべてのコンピュータでこの処理を使用できる場合のみになります。

3. すべてのRelayグループの割り当てを確認するには、 [管理]→[システム設定]→[アップデート] で [Relayグループの表示] ボタンをクリックします。リスト内の各Relayグループを右クリックして、 [プロパティ] を選択します。 [割り当て対象] タブに移動して、Relayグループに割り当てられたAgent/Applianceのリストを確認します。Agent/Applianceの割り当てをすばやく変更するには、 [割り当て対象] リストのリンクをクリックして、該当するAgent/Applianceの [コンピュータの詳細] 画面を開いて、そこから別のRelayグループ割り当てを選択します。

注意： Agent/Applianceが特定のRelayグループに割り当てられていない場合は、「初期設定のRelayグループ」に自動的に割り当てられます。

Relayグループを変更すると、このRelayグループ (子Relayグループを含む) に割り当てられているコンピュータの設定が自動的にアップデートされます。

イベントベースのタスクを作成し、コンピュータがManagerの [コンピュータ] 画面に追加された場合に、コンピュータにRelayグループが自動的に割り当てられるようにすることもできます。詳細については、ユーザインタフェースガイドまたはオンラインヘルプの「イベントベースタスク」を参照してください。

不正プログラム対策パターンのみをアップデートする

注意： このオプションは、 Relayグループに9.5よりも前のバージョンのDeep Security Relayのみが含まれる場合に使用できます。
セキュリティアップデートを開始する

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/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] 画面のコンピュータのリストからAgent/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。

セキュリティアップデートの確認タスクを定期的に予約するには、[管理]→[予約タスク] の順に選択し、[セキュリティアップデートの確認] タイプの新しい予約タスクを作成します。

アップデート元

Relayグループ階層の最上位グループに属するRelayは、セキュリティアップデート元に接続します。セキュリティアップデート元は、Deep Security Managerの [管理]→[システム設定]→[アップデート] タブで設定します。

Relayグループは、セキュリティアップデート元または別の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できます。Relayグループのダウンロード元を設定するには、[管理]→[アップデート]→[Relayグループ] ページに進み、Relayグループの [プロパティ] ヴィンテュウを開きます。
プロキシ

各Relayグループ（初期設定のRelayグループを除く）は、それぞれ別のプロキシサーバを使用してトレンドマイクロに接続し、セキュリティアップデートを取得するように設定できます。初期設定のRelayグループは、Deep Securityと同じプロキシを使用してインターネットに接続します。

プロキシサーバを使用するようにRelayグループを設定するには

1. Deep Security Managerで、[管理]→[アップデート]→[Relayグループ] に進み、Relayグループをダブルクリックして [プロパティ] ウィンドウを表示します。
2. [プロキシ] タブで、[プライマリセキュリティアップデートプロキシ] ドロップダウンリストからプロキシサーバを選択します。
3. [OK] をクリックします。

注意： 使用可能なプロキシサーバのリストは、[管理]→[システム設定]→[プロキシ] タブで管理します。
セキュリティアップデート

Deep Securityは、最新の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で定期的に更新する必要があります。アップデートパッケージはトレンドマイクロからセキュリティアップデートの形式で取得します。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、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もDeep Security Managerで行います。

セキュリティアップデート

注意：セキュリティアップデートを設定する前に、AgentとAppliance、およびアップデートを配信するRelay有効化済みAgentをインストールして、有効化する必要があります。すべてのDeep Securityコンポーネントのインストール手順は、『Deep Securityインストールガイド』に記載されています。

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のアップデート元の設定
2. Relay有効化済みAgentおよびRelayグループの編成
3. Agent/ApplianceへのRelayグループの割り当て
4. 特殊な場合：オフライン環境内のRelay有効化済みAgentに関するアップデートの設定
セキュリティアップデートのアップデート元の設定

現在のアップデート元の設定を表示するには、[管理]→[システム設定]→[アップデート] の順に選択します。

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

[セキュリティアップデート] エリアで、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。


新しいルールアップデートを自動的にポリシーに適用: トレンドマイクロでは、定期的にDeep Securityルールのアップデートを配信しています。この設定により、セキュリティアップデートの際にアップデートされたルールが自動的にManagerに適用され、利用可能になります。

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: 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。
プロキシサーバ

Relayがプロキシ経由でインターネットおよびトレンドマイクロのアップデートサーバに接続しなければならない場合は、[管理]→[システム設定]→[プロキシ] タブの [プロキシサーバ] エリアでプロキシを設定できます。

セキュリティアップデートを開始する

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/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] 画面のコンピュータのリストからAgent/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。

セキュリティアップデートの確認タスクを定期的に予約するには、[管理]→[予約タスク] の順に選択し、[セキュリティアップデートの確認] タイプの新しい予約タスクを作成します。

RelayグループへのRelay有効化済みAgentのグループ化

Deep Securityのインストール環境には、Relay有効化済みAgentが少なくとも1つ必要です。グループ内にRelay有効化済みAgentが1つしかない場合も含めて、Relay有効化済みAgentはRelayグループに編成されます。Managerを使用してRelay有効化済みAgentを有効化するとすぐに、初期設定のRelayグループというグループにRelay有効化済みAgentが追加されます。このRelayグループは、新規作成したすべてのRelay有効化済みAgentの受け皿となります。Relay有効化済みAgentを有効化すると、別のRelayグループに移動できるようになります。

現在のRelayグループを表示する、または新しいRelayグループを作成するには、[管理]→[アップデート]→[Relayグループ] の順に選択します。

Relay有効化済みAgentのアップデート元がRelayグループ単位で割り当てられます。初期設定では、Relayグループは[管理]→[システム設定]→[アップデート] タブで指定したアップデート元からアップデートを取得するように設定されています。ただし、別のRelayグループからアップデートを取得するように設定して、Relayグループの階層を作成することもできます。

注意: Relay有効化済みAgentは、別のRelayグループからセキュリティアップデートを取得することができますが、（同じRelayグループに属しているRelay有効化済みAgentであっても）別のRelay有効化済みAgentから取得することはできません。上位のRelayグループまたは設定済みの別のアップデート元から取得する必要があります。

Relayグループの詳細については、「Relayグループ (53ページ)」を参照してください。

Agent/ApplianceへのRelayグループの割り当て

Relayグループを確立し、アップデート元と通信するように設定すると、RelayグループをAgentおよびApplianceに割り当てることができるようになります。

RelayグループをAgent/Applianceに割り当てるには、[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]→[Relayグループの割り当て] の順に選択します。使用可能なRelayグループのリストが表示され、そこから選択できます。
特殊な場合: オフライン環境におけるRelay有効化済みAgentでのアップデートの設定

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から上位のRelayグループ内のRelay有効化済みAgentまたはアップデートサーバにインターネット経由で接続できない環境の場合は、代わりにRelay有効化済みAgentにアップデートパッケージをインポートして、別のDeep Securityソフトウェアコンポーネントに配布することができます。

Relay有効化済みAgentを使用したアップデートパッケージの生成

トレンドマイクロのアップデートサーバから最新アップデートをダウンロードできるRelay有効化済みAgentを使用して、セキュリティアップデートのエクスポートパッケージを生成し、オフラインの別のRelay有効化済みAgentにインポートすることができます。

セキュリティアップデートのパッケージを作成するには、Relay有効化済みAgentのコマンドラインで次のように入力します。

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。

オフライン環境内のRelay有効化済みAgentへのアップデートのインポート

オフライン環境内のRelay有効化済みAgentのインストールディレクトリに、コマンドラインで生成した.zipファイルをコピーします。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。

Deep Security Managerからセキュリティアップデートの予約ダウンロードまたは手動ダウンロードを開始したにもかかわらず、Relay有効化済みAgentが設定済みのアップデート元からアップデートを取得できない場合は、インストールディレクトリ内でRelayのアップデート用の.zipファイルが自動的に検索されます。zip形式のアップデートパッケージが見つかったら、Relay有効化済みAgentによってファイルが展開され、インポートされます。

注意: アップデート用.zipファイルの名前は変更しないでください。

注意: アップデートがRelay有効化済みAgentに正常にインポートされると、アップデート用.zipファイルを削除してください。

オフライン環境内のRelay有効化済みAgentのアップデート元の設定

オフライン環境内のRelay有効化済みAgentは引き続きアップデートサーバと通信して、アップデートを検索しようとします。アップデート失敗アラートが表示されないようにするには、アップデート元として自分自身を使用するようにRelay有効化済み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] 画面に進みます。
3. [保存] をクリックします。
ソフトウェアアップデート


新しいソフトウェアが入手可能になったというアラートを受信したら、ソフトウェアをDeep Security Managerにインポートする必要があります。

ソフトウェアをDeep Security Managerにインポートするには、次の手順に従います。

1. [管理]→[アップデート]→[ソフトウェア] に進みます。
2. [トレンドマイクロのダウンロードセンター] セクションで、利用可能な新しいソフトウェアアップデートの有無を確認します。利用できる新しいアップデートがない場合は、「インポートされたソフトウェアはすべて最新です」と表示されます。アップデートがある場合は、希望するパッケージを選択して[インポート]をクリックします。複数のパッケージを選択するには、<Shift> または <Ctrl> キーを押しながらパッケージをクリックします。
3. パッケージがDeep Security Managerにダウンロードされると、[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。インポートしたパッケージは、[管理]→[アップデート]→[ソフトウェア]→[ローカル] にも表示されます。
4. しばらくすると、Relay有効化済みAgentによってパッケージが複製されます。

ソフトウェアをDeep Security Managerにインポートすると、Deep Security Agent/Applianceをアップグレードできるようになります。
特定のAgent/Applianceのみをアップグレードするには、[コンピュータ]画面でそのAgent/Appliance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...]または[Applianceのアップグレード...]を選択します。

すべてのAgentを一度にアップグレードするには、[管理]→[アップデート]→[ソフトウェア]を選択して、[Agent/Applianceソフトウェアのアップグレード...]をクリックします。
Virtual Applianceの検索キャッシュ

概要

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排除されるため、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]ボタンをクリックします。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時間です。

[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つの式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いことがあるわけではないからです。
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、ポリシー/エディタまたはコンピュータエディタを開き、[不正プログラム対策]→[詳細]→[仮想マシンの検索キャッシュ]の順に進めます。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、ポリシー/エディタまたはコンピュータエディタを開き、[変更監視]→[詳細]→[仮想マシンの検索キャッシュ]の順に進めます。

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/エディタを開き、[設定]→[検索]→[Virtual Appliance]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で処理待ちになり、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10万件の場合、使用されるメモリは約100MB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10万件の場合、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2万個の場合、使用されるメモリは約100MBです。

初期設定を変更する場合

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を使用することもありますが、これによってパフォーマンスの向上が低下したり、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正在です（データがある場合は、自動的にこのような状態になります。

VDI環境など、ホストあたりの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。検索に時間がかかる場合は、キャッシュのサイズを増やすか、必要なパフォーマンスが得られるように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、それに伴い、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。
ユーザ管理

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]で確認できます。


注意: 連絡先はDeep Security Managerにログオンすることはできませんが、役割は割り当てられます。この役割によって、連絡先に送信される情報の範囲が決まります。たとえば、3名の連絡先を週次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役割に付与されている「表示」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。

役割に基づいたアクセス権限と編集権限

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。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。

コンピュータとポリシーに対する役割に基づいたアクセス

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。これは、かなり詳細なレベルで制御することができます。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権限が許可されるが、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。役割を編集するには、[管理]→[ユーザ管理]→[役割]で役割をダブルクリックするか、または[新規]ボタンをクリックして、[役割のプロパティ]ウィンドウを表示します。
役割に基づいた編集権限

このようなアクセス制限内では、役割は編集権限に制限を設定することができます。

ユーザ権限

役割を使用すると、別のユーザから委任された権限をユーザに付与することができます。つまり、その役割を持つユーザは、自分自身と同等またはそれ以下のアクセス権限を持つユーザのプロパティのみを作成および編集することができます。
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。

<table>
<thead>
<tr>
<th>権限</th>
<th>ロール別の設定</th>
<th>Full Accessの役割</th>
<th>Auditorの役割</th>
<th>新規役割の初期設定</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Security Managerユーザインタフェースへのアクセス</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>許可</td>
</tr>
<tr>
<td>WebサービスAPIへのアクセス</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>不許可</td>
</tr>
<tr>
<td>コンピュータの権限</td>
<td></td>
<td>Full Accessの役割</td>
<td>Auditorの役割</td>
<td>新規役割の初期設定</td>
</tr>
<tr>
<td>表示</td>
<td>許可、すべてのコンピュータ</td>
<td>許可、すべてのコンピュータ</td>
<td>許可、すべてのコンピュータ</td>
<td></td>
</tr>
<tr>
<td>編集</td>
<td>許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td></td>
</tr>
<tr>
<td>刪除</td>
<td>許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td></td>
</tr>
<tr>
<td>アラートの消去</td>
<td>許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td></td>
</tr>
<tr>
<td>アイテムのタグ付け</td>
<td>許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td>不許可、すべてのコンピュータ</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>許可、すべてのコンピュータ</td>
</tr>
<tr>
<td>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</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>許可、すべてのコンピュータ</td>
</tr>
<tr>
<td>選択したグループ内に新しいコンピュータを作成</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>不許可</td>
</tr>
<tr>
<td>選択したグループ内にサブグループを追加または削除</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>コンピュータファイルをインポート</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>ディレクトリーを追加、削除、および同期</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>VMware vCenterを追加、削除、および同期</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>ユーザーアカウントの追加、削除、および同期を許可</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>ポリシーの権限</td>
<td></td>
<td>Full Accessの役割</td>
<td>Auditorの役割</td>
<td>新規役割の初期設定</td>
</tr>
<tr>
<td>表示</td>
<td></td>
<td>許可、すべてのポリシー</td>
<td>許可、すべてのポリシー</td>
<td>許可、すべてのポリシー</td>
</tr>
<tr>
<td>編集</td>
<td></td>
<td>許可、すべてのポリシー</td>
<td>不許可、すべてのポリシー</td>
<td>不許可、すべてのポリシー</td>
</tr>
<tr>
<td>削除</td>
<td></td>
<td>許可、すべてのポリシー</td>
<td>不許可、すべてのポリシー</td>
<td>不許可、すべてのポリシー</td>
</tr>
<tr>
<td>選択されていないポリシーの表示</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>許可</td>
</tr>
<tr>
<td>新規ポリシーの作成</td>
<td></td>
<td>許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>ポリシーのインポート</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>ユーザ権限（この後の「ユーザ権限に関する注意」を参照）</td>
<td></td>
<td>Full Accessの役割</td>
<td>Auditorの役割</td>
<td>新規役割の初期設定</td>
</tr>
<tr>
<td>ユーザの表示</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>許可</td>
</tr>
<tr>
<td>ユーザの作成</td>
<td></td>
<td>許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>ユーザプロパティの編集</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>ユーザの削除</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>役割の表示</td>
<td></td>
<td>許可</td>
<td>許可</td>
<td>許可</td>
</tr>
<tr>
<td>役割の作成</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>役割のプロパティの編集</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>役割の削除</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>権限の委任</td>
<td></td>
<td>不許可</td>
<td>不許可</td>
<td>不許可</td>
</tr>
<tr>
<td>その他の権限</td>
<td></td>
<td>Full Accessの役割</td>
<td>Auditorの役割</td>
<td>新規役割の初期設定</td>
</tr>
<tr>
<td>アラート</td>
<td></td>
<td>表示のみ</td>
<td>表示のみ</td>
<td>表示のみ</td>
</tr>
<tr>
<td>アラート設定</td>
<td></td>
<td>表示のみ</td>
<td>表示のみ</td>
<td>表示のみ</td>
</tr>
<tr>
<td>IPリスト</td>
<td></td>
<td>表示のみ</td>
<td>表示のみ</td>
<td>表示のみ</td>
</tr>
<tr>
<td>ポートリスト</td>
<td></td>
<td>表示のみ</td>
<td>表示のみ</td>
<td>表示のみ</td>
</tr>
<tr>
<td>スケジュール</td>
<td></td>
<td>表示のみ</td>
<td>表示のみ</td>
<td>表示のみ</td>
</tr>
<tr>
<td>権限</td>
<td>役割別の設定</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>システム設定 (グローバル)</td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>システム情報</td>
<td>完全 (システム情報を表示、Managerノードを編集および使用停止、およびシステムの拡張機能を管理可能) 表示のみ 非表示</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>診断</td>
<td>完全 (診断パッケージを作成可能) 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>タグ付け</td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>タスク</td>
<td>完全 (タスクを表示、追加、編集、および削除可能) 表示のみ 非表示</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>マルチテナントの管理</td>
<td>完全 非表示 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>検索キャッシュ設定の管理</td>
<td>完全 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>連絡先</td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ライセンス</td>
<td>完全 (ライセンスの表示および変更可能) 表示のみ 非表示</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>アップデート</td>
<td>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ルールアッデータを削除可能) 表示のみ 非表示</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>資産評価</td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>証明書</td>
<td>完全 (SSL証明書を作成および削除可能) 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relayグループ</td>
<td>完全 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>プロキシ</td>
<td>完全 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>不正プログラム検索設定</td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>隔離ファイル</td>
<td>完全 (隔離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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webレピュテーション設定</td>
<td>完全 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ディレクトリリスト</td>
<td>完全 (作成、編集、および削除可能) 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ファイルリスト</td>
<td>完全 (作成、編集、および削除可能) 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ファイル拡張子リスト</td>
<td>完全 (作成、編集、および削除可能) 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ファイアウォールルール</td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ファイアウォールステートフル設定</td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>侵入防御ルール</td>
<td>完全 (作成、編集、および削除可能) 表示のみ 表示のみ</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
権限

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

役割別の設定

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

ユーザ権限に関する注意


[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
<table>
<thead>
<tr>
<th>[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</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ユーザを表示できます</td>
<td>許可</td>
</tr>
<tr>
<td>新規ユーザを作成できます</td>
<td>許可</td>
</tr>
<tr>
<td>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）</td>
<td>許可</td>
</tr>
<tr>
<td>ユーザを削除できます</td>
<td>許可</td>
</tr>
<tr>
<td>役割</td>
<td></td>
</tr>
<tr>
<td>役割を表示できます</td>
<td>許可</td>
</tr>
<tr>
<td>新規の役割を作成できます</td>
<td>許可</td>
</tr>
<tr>
<td>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）</td>
<td>許可</td>
</tr>
<tr>
<td>役割を削除できます</td>
<td>許可</td>
</tr>
<tr>
<td>権限の委任</td>
<td></td>
</tr>
<tr>
<td>同等以下の権限を持つユーザのみを操作</td>
<td>なし</td>
</tr>
</tbody>
</table>
データベースのバックアップと復元

バックアップ

データベースのバックアップは、大规模な障害の発生時にDeep Securityシステムを復元するため、またはDeep Security Managerを別のコンピュータに転送するため行います。

内部データベースまたはMicrosoft SQL Serverデータベース

データベースのバックアップは、予約タスクのインタフェースを使用して実行できます。[管理]→[予約タスク]画面に進みます。[新規]をクリックして「予約タスク」を選択し、新規予約タスクウィザードを表示します。[種類]ドロップダウンリストから「バックアップ」を選択します。次の画面では、このタスクをいつどのくらいの頻度で実行するかを指定するよう求められます。バックアップを1回だけ行うには、[1回のみ]を選択し、時間（たとえば、今から5分後）を入力します。次の画面では、バックアップファイルを格納する場所を指定するよう求められます。ウィザードの最後までクリックして、ウィザードを終了します。完全バックアップは1分ほどで完了します。


SQL Serverデータベースを使用している場合は、{タイムスタンプ}.dsmbackupというSQL Serverデータベースバックアップファイルが、予約タスクで指定したバックアップフォルダに作成されます (SQL Serverデータベースを復元する方法については、SQL Serverのドキュメントを参照してください)。

復元

データベースのみ

1. Deep Security Manager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Managerのデータベースである必要があります)。
3. Deep Security Manager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

1. 失われた/破損したManagerおよびデータベースの不要なデータを削除します。
2. 新規/空のデータベースを使用してDeep Security Managerを新規でインストールします。
3. Deep Security Managerサービスを停止します。
4. 新規インストールされた同じ名前のデータベースの上にデータベースを復元します (同じビルド番号のManagerのデータベースである必要があります)。
5. Deep Security Managerサービスを開始します。
6. データベースが復元されたことを確認します。
7. 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。

エクスポート

Deep SecurityのさまざまなオブジェクトをXML形式またはCSV形式でエクスポートできます。


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/強調表示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 (ファイアウォールルール、ステートフル設定)、侵入防御ルール、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**: ポリシーは、[ポリシー] 画面からXML形式でエクスポートできます。

注意: 選択したポリシーをXMLにエクスポートすると、子ポリシーもエクスポートパッケージに含まれる場合があります。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。

- **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/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/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/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/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/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、データは画面とは順序が異なる場合があります。

インポート

各オブジェクトをDeep Securityにインポートするには、オブジェクトのそれぞれの画面のツールバーの [ 新規 ] ボタンの横にあるリストから [ ファイルからインポート ] を選択します。
コンピュータを追加する

Deep Securityでコンピュータを保護するには、Deep Security Managerのコンピュータリストにコンピュータを追加する必要があります。次の方法で、コンピュータリストに新しいコンピュータを追加できます。

- **ローカルネットワークからコンピュータをインポートする (75ページ)**: ローカルから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。
- **ディレクトリをインポートする (77ページ)**: 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をインポートできます。
- **VMware vCenterからコンピュータをインポートする (81ページ)**: VMware vCenterをインポートして、ホストされている仮想マシンにAgentベースまたはAgentレスによる保護を提供できます。
- **クラウドプロバイダーからコンピュータをインポートする (82ページ)**: VMware vCloud、Amazon EC2、またはMicrosoft Azureインフラストラクチャでホストされている仮想マシンをインポートできます。
- **インストールスクリプトを使用する (88ページ)**: 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。
ローカルネットワーク

Agentからのリモート有効化


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、「コマンドラインユーティリティ (184ページ)」を参照してください。

IPアドレスまたはホスト名を直接入力する

個々のコンピュータを手動で追加できます。

コンピュータを手動で追加するには

1. [コンピュータ] 画面に移動し、ツールバーの[新規]→[新規コンピュータ]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アドレスと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。

注意: 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のインストールを進めません。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たら、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。
検出操作を実行する

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]画面にあるツールバーの[新規]→[検出]をクリックします。[コンピュータの検出]画面が表示されます。

検出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。多数のコンピュータを検出/検索する場合は非常に時間がかかるため、このオプションを使用する際には注意が必要です。

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、「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なことがあります。その後、検出されたコンピュータを、プロバ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、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場合、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。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。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を無効にして再度検出する必要があります。

- **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が一時的に他の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、これらが該当する可能性があります。このコンピュータでAgentの管理を開始する時には、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を無効にしたManagerを使用して行う必要があります。または、コンピュータでAgentを直接リセットすることもできます。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。

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や、ディレクトリ/Active Directoryのコンピュータは検出されません。
Active Directory

Deep Security Managerでは、Microsoft Active Directoryによるコンピュータの検出をサポートします。検出されたコンピュータはDeep Security Managerにインポートされ、Active Directoryの構造に従ってグループ化および表示されます。

Microsoft Active Directoryをインポートするには

1. ナビゲーションパネルで「コンピュータ」を右クリックし、「ディレクトリの追加」を選択します。
2. インポートするディレクトリの名前と説明 (Active Directoryのものと一致していないてもかまいません)、Active DirectoryサーバのIPとポート、および最後にアクセス方法と資格情報を入力します。

注意: [ユーザ名] フィールドのユーザ名には、ドメイン名を含める必要があります。

[次へ] をクリックして続行します。
3. ディレクトリの追加ウィザードの2番目の画面で、スキーマの詳細を入力するよう求められます (初期設定値のままにすることができます)。


Deep Security Managerのこの構造と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その同期をとる予約タスクの作成] チェックボックスをオンにします。このチェックボックスをオンにすると、ディレクトリの追加が完了したときに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)。[次へ] をクリックして続行します。
4. 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リストが表示されます。[完了] をクリックします。

これで、[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、[コンピュータ]の下に一覧表示されている通常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破棄します: 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と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のディレクトリ構造をActive Directoryサーバと同期します。

この処理は、予約タスクとして自動化できます。

Deep Securityでは、Active Directoryの情報を利用してコンピュータを検出したり、ユーザアカウントや連絡先を作成したりできます。

ポートの要件

Active Directoryとの統合の性質に応じて、次のポートが必要になることがあります。

- ポート389: 非SSLベースのアクセス方式に使用
- ポート636: SSLベースのアクセス方式に使用

注意: SSLベースのアクセス方式を使用するには、Active DirectoryサーバでSSLを有効にする必要があります。SSLは初期設定で無効になっていることがあります。

サーバ証明書を使用する

コンピュータの検出にはSSLベース方式とクリアテキスト方式どちらも使用できますが、ユーザおよび連絡先に使用できるのは非匿名SSL方式のみです。この制限により、ユーザアカウントおよびその使用は保護されます。SSLベースのアクセス方法はSSL対応のActive Directoryサーバを使用する場合のみ有効です。したがって、ユーザおよび連絡先は適切に設定されたサーバからインポートする必要があります。

SSL対応のActive Directoryサーバには、サーバ証明書をインストールする必要があります。サーバ証明書には、自己署名証明書またはサードパーティの認証局が発行した証明書を使用できます。

証明書の有無を確認するには、Active DirectoryサーバでInternet Information Services (IIS) Managerを開いて、「[サーバ証明書]」を選択します。

Active Directoryオブジェクトをフィルタする

Active Directoryオブジェクトをインポートする場合は、検索フィルタを使用して、返されるオブジェクトを管理することができま

注意: 管理者ガイド

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からアカウントを一元的に無効にすることができる。
- 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の通知のみ受け信すことができます。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に正常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）。

ユーザまたは連絡先をインポートするには

1. Managerで、[管理]→[ユーザ管理]→[ユーザ] または [連絡先] 画面に進みます。
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。この画面のオプションの設定方法については、前に出たコンピュータのインポートに関するセクションを参照してください。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ます。[次へ] をクリックします。
5. [新しいユーザ/連絡先のオプションの選択] 画面で、インポートしたアカウントをディレクトリに設定する初期設定をユーザ役割を定義します。誤って各ユーザに不適切な権限を設定しないように、最小限のアクセス権限が付与された役割を選択します。[次へ] をクリックします。
6. 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。[完了] をクリックします。

インポートしたアカウントは、Deep Securityアカウントと異なり、アカウントの一般情報を変更できません。

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オプションを設定することが必要です。ホスト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、ホストの場合は [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/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が確認されます。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。

ManagerからActive Directoryを削除する

コンピュータの検出およびユーザと連絡先に関するDeep Security ManagerとActive Directoryの統合を解除できます。

コンピュータリストからのActive Directoryの削除

コンピュータリストからActive Directoryを削除する場合は、次のオプションが表示されます。

- 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: 既存のActive Directory構造は維持されますが、Active Directoryと同期しなくなります。構造は影響を受けないため、フォルダまたはホストに対するユーザおよび役割のアクセス権限は維持されます。
- 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: ホストレコードは元の階層から削除されます。既存のActive Directoryに基づく名前の付いたグループにすべて格納されます。Active Directory
ユーザーおよび役割のアクセス権限はこのグループに転送されるため、すべてのホストに対するアクセス権限は維持されます。

Active Directoryを削除するには、次の手順を実行します。

1. [コンピュータ] 画面でActive Directoryを右クリックし、[ディレクトリの削除]を選択します。
2. [ディレクトリの削除] ダイアログボックスで削除オプションを選択します。
3. この後に表示されるダイアログボックスで処理について確認します。Active Directoryの削除が完了します。

Active Directoryのユーザおよび連絡先の削除

Active Directoryを削除する場合は特定のタイプの情報を維持することもできますが、ユーザおよび連絡先を削除する場合はこれらのレコードがすべて削除されます。したがって、インポートされたユーザアカウントを使用してDeep Security Managerコンソールにログオンしている場合は、この処理を実行できません。この処理を実行すると、エラーが表示されます。

ユーザおよび連絡先を削除するには、次の手順を実行します。

2. [同期を中止する] を選択して、[OK] をクリックします。ウィザードに、変更の概要を示す画面が表示されます。
3. [完了] をクリックします。

管理者ガイド

Active Directory
VMware vCenter

Deep Securityでは、Virtual Applianceのみを使用して仮想マシンを保護することも、Virtual ApplianceとAgentの両方を使用してコンピュータを保護することもできます。Virtual Applianceでは使用できない保護モジュールもあります。インストールと設定のすべての手順を含む詳細については、『Deep Securityインストールガイド (vShield)』または『Deep Securityインストールガイド (NSX)』を参照してください。
クラウドアカウント

Deep Securityでは、次のクラウドプロバイダーサービスのコンピューティングリソースをAgentベースで保護できます。

- Amazon EC2
- VMware vCloud
- Microsoft Azure

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すると、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Amazon Web Servicesアカウントを作成する

1. AWS Management Consoleにログインします。
2. IAM (Identity and Access Management) に移動します。
3. 左側のナビゲーションペインで [Users] をクリックします。
4. [Create New Users] をクリックして、[Create User] 画面を開きます。
5. ユーザ名を入力し、[Generate an access key for each User] オプションを選択します。
6. 生成されたユーザのセキュリティ資格情報 (アクセスキーと秘密鍵) を書き留め、画面を閉じます。
7. [Users] 画面に戻り、ユーザを選択して、画面の下部にある [Permissions] タブをクリックします。
9. [Policy Generator] オプションを選択します。
10. 新しいユーザに付与する権限を編集するには、[Select] ボタンをクリックします。
11. [Effect: Allow] を選択します。
12. [AWS Service: Amazon EC2] を選択します。
13. [Actions] として次を選択します。
   - DescribeImages
DescribeInstances
DescribeTags

14. [Amazon Resource Name] を「'」を設定します。
15. [Add Statement] をクリックします。
16. [Continue] をクリックして権限のポリシーを生成します。
17. [Apply Policy] をクリックして、ポリシーをユーザアカウントに適用します。

これで、Deep Security ManagerからAmazon Web Servicesアカウントにアクセスする準備は完了です。

注意：Amazon AWSのリソースをDeep Security Managerにインポートする際、リソースがホストされているリージョン、アクセスキーID、および秘密アクセスキーの入力を求められます。リソースが複数のリージョンにホストされている場合、リージョンごとに個別にリソースを追加する必要があります。

Amazon Web Servicesアカウントからコンピュータをインポートする

Amazon Web Servicesのクラウドリソースからインポートするには

2. クラウドプロバイダの種類に [Amazon]を選択します。
3. クラウドリソースがホストされているリージョンを選択します (リソースが複数のリージョンにホストされている場合、リージョンごとに個別にリソースを追加する必要があります)。
4. 追加するリソースの名前と説明を入力します (これらの情報は、Deep Security Managerでの表示に使用されます)。
5. AWSの管理者から提供されたアクセスキーIDと秘密アクセスキーを入力します。[次へ]をクリックします。
7. クラウドプロバイダのリソースのインポート終了後、ウィザードに処理結果が表示されます。

Amazon AWS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。

注意：クラウドリソースをホストしているAmazonリージョンがリストに表示されない場合は、Deep Security Managerにリージョンを追加する必要があります。詳細については、「Amazon Web Servicesのリージョンを管理する (304ページ)」を参照してください。

Manager用のVMware vCloud Organizationアカウントを作成する

Deep Security Manager用のVMware vCloud Organizationアカウントを作成するには

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選択します。
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. 新しいユーザを作成するには、「プラス」記号 (+) をクリックします。
8. ユーザの資格情報などの必要な情報を入力し、ユーザの [Role]で [Organization Administrator]を選択します。
注: [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、インストールガイド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: VMware vCloudのリソースをDeep Security Managerにインポートする際、vCloudのアドレス、ユーザ名、およびパスワードの入力を求められます。

ユーザ名には「@orgName」を含める必要があります。たとえば、vCloudアカウントのユーザ名がkevin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「kevin@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）。

VMware vCloud Organizationアカウントからコンピュータをインポートする

VMware vCloud Organizationのリソースをインポートするには

2. クラウドプロバイダの種類に [vCloud] を選択します。
3. 追加するリソースの名前と説明を入力します（これらの情報は、Deep Security Managerでの表示に使用されます）。
4. 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）。
5. 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。

6. [次へ] 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] 画面に、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

VMware vCloud Airデータセンターをインポートするには

2. クラウドプロバイダの種類に [vCloud] を選択します。
3. 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（これらの情報は、Deep Security Managerでの表示に使用されます）。
4. vCloud Airデータセンターのアドレスを入力します。

注意: 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。
1. vCloud Airポータルにログインします。
2. [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。

3. [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。

4. 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、(完全なURLではなく) ホスト名のみを使用します。

5. 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。

6. [次へ] 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] 画面に、それぞれ別個の項目として表示されます。

Agent起動通信を有効にする (Microsoft Azure用)


Agent起動通信を有効にするには

1. Deep Security Managerコンソールで、[管理]→[システム設定]→[Agent]→[Agentからのリモート有効化] に進みます。
2. [Agentからのリモート有効化を許可] が選択されていることを確認します。
3. [保存] をクリックします。

Microsoft Azureで使用する証明書とキーペアを生成する

Microsoft AzureリソースをDeep Security Managerに追加する前に、証明書とキーペアを生成する必要があります。必要なファイルを生成したら、Azure Webサービスコンソールに証明書 (.cerファイル) をインポートします。キーペア (.pemファイル) は、Microsoft Azureリソースを追加する際にDeep Security Managerにアップロードします。

証明書とキーペアを作成するには

1. Deep Security Managerで、[管理]→[システム設定]→[セキュリティ] に進みます。
2. [キーペアの生成] の下で、[キーペアの生成] をクリックします。
3. [キーペアのパスワード] ボックスと [パスワードの確認入力] ボックスにパスワードを入力します。
4. [キーペアの作成] をクリックします。
5. .pemファイルをローカルに保存します。
6. [証明書のエクスポート] をクリックします。
7. .cerファイルをローカルに保存します。
8. [閉じる] をクリックします。
Manager用Microsoft Azureアカウントを作成する

Deep Security ManagerがアクセスするためのMicrosoft Azureアカウントを作成するには

1. Azure Webサービスコンソールにログインします。
2. 左側のナビゲーションペインで [Settings] をクリックします。
3. 該当するサブスクリプションIDをクリックします。
4. [Management Certificates] をクリックします。
5. ページの一番下にある [Upload] をクリックし、前の手順で生成した.cerファイルを選択します。

Microsoft Azureアカウントからコンピュータをインポートする

Microsoft Azureのクラウドリソースをインポートするには

2. クラウドプロバイダの種類に [Azure] を選択します。
3. 追加するリソースの名前と説明を入力します (これらの情報は、Deep Security Managerでの表示に使用されます)。
4. サブスクリプションIDを入力し、[参照] をクリックして前の手順で生成した.pemファイルを選択します。


5. [次へ] をクリックします。

Azureのリソースが、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。

クラウドアカウントを管理する

クラウドコンピュータでDeep Securityの保護を実装するには、ネットワーク上の他のコンピュータと同じように、Agentをインストールしてポリシーを割り当てることが必要です。コンピュータにDeep Security Agentをインストールする方法については、インストールガイドを参照してください。クラウドプロバイダインフラストラクチャで実行されているコンピュータは、他のコンピュータと同じように、Agentベースの保護を管理してDeep Securityによって管理されます。

同期が有効になっている場合、クラウドプロバイダアカウントのインスタンスのリストが10分間隔で更新されます。定期的な同期を有効または無効にするには、ナビゲーションペインでクラウドプロバイダアカウントを右クリックして [プロパティ] 画面を開き、[一般] タブに進みます ([管理] セクションでこの処理を予約タスクとして自動化することで、独自の同期スケジュールを指定できます)。

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。

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


Deep Security Managerからクラウドプロバイダアカウントを削除するには

1. [コンピュータ] 画面を開き、ナビゲーションパネルでクラウドプロバイダ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。
インストールスクリプト

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、Managerの[サポート]メニューからアクセスできます。

インストールスクリプトを生成するには

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(ドロップダウンメニューには、トレンドマイクロのダウンロードセンターからDeep Security Managerにインポートしたソフトウェアに対応するプラットフォームが表示されます。Deep Securityソフトウェアのインポートの詳細については、ユーザインタフェースガイドまたはオンラインヘルプの[管理]→[アップデート]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(保護ポリシーを実装する前に、Deep Security ManagerによってAgentが有効化されている必要があります)。
4. コンピュータで実装するポリシーを選択します(オプション)。
5. コンピュータグループを選択します(オプション)。
6. Relayグループを選択します(オプション)。

上記の選択を行うと、インストールスクリプトジェネレータによって、任意のインストールツールにインポートできるスクリプトが生成されます。

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 2.0以降が必要です。

Amazon Web Servicesを使用していて、新しいEC2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[User Data]フィールドにコピーします。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にアクセスできる必要があります。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]フィールドに入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。詳細については次のURLを参照してください。
注意: Windows Agentでコンピュータで不正プログラム対策保護を使用しない場合は、不正プログラム対策エンジンをインストールしないように指定できます。指定するには、インストールスクリプト内の文字列「ADDLOCAL=ALL」を削除します。
保護を実施する

• **Agentベースの保護:** (91ページ) Deep Security Agentでは、物理コンピュータまたは仮想マシンを保護できます。Agentコンポーネントをコンピュータにインストールすると、適用したセキュリティポリシーが実装されます。

• **Agentレスによる保護:** (92ページ) Deep Security Virtual Applianceでは、Deep Security AgentをインストールしなくてもVMware vSphere仮想マシンを保護できます。Virtual Applianceは、仮想マシンと同じESXiにインストールします。

• **ポリシーの適用:** コンピュータの保護にAgentとVirtual Applianceのどちらを使用する場合でも、セキュリティポリシーを割り当てます。セキュリティポリシーは、一連のルール、設定、権限、およびスケジュールの定義です。ポリシーを作成し、保存したら、複数のマシンで使用できます。ポリシーは階層構造で作成し、親ポリシーを、子ポリシー作成時のテンプレートとして使用できます。このとき、特定の要件がある個々のマシン用にポリシーをカスタマイズできます。
Agentベースの保護

手動インストール

Deep Security Agentをコンピュータに手動でインストールするには、適切なインストールパッケージをコンピュータで実行します。Agentのインストールパッケージは、トレンドマイクロのダウンロードセンターhttp://www.trendmicro.co.jp/download/からダウンロードできます。各Agentパッケージのインストール手順については、インストールガイドを参照してください。

Agentのインストールが完了したら、そのコンピュータを管理対象コンピュータのリストに追加し、Agentを手動で有効にする必要があります。コンピュータの追加方法については、「コンピュータを追加する (74ページ)」を参照してください。

インストールスクリプト

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、Managerの [サポート] メニューからアクセスできます。手順については、「インストールスクリプト (88ページ)」を参照してください。
Agentレスによる保護

Deep Security Virtual Applianceは、ゲストOS (仮想マシン) 内にDeep Security Agentがなくても、VMware vSphere環境の仮想マシンに保護を提供します。仮想マシンは、Agentがインストールされているかのように管理されます。

- Virtual Applianceを使用すると、各仮想マシンにAgentをインストールする必要がないため、各仮想マシンは、最低限必要なソフトウェアのみをインストールして、操作できます。
- 使用期間が短いコンピュータや繰り返し初期化を行うようなコンピュータについては、管理者がセキュリティソフトウェアのインストール時間を十分に確保できない場合があります。その場合も、Virtual Applianceを使用すると、簡単にかつ迅速にコンピュータを保護できます。
- 管理者権限がないために、OSにアクセスできない仮想マシンでもVirtual Applianceを使用する事で保護が可能です。
- Deep Security Virtual Applianceは簡単に配置できます。仮想マシンにAgentソフトウェアをリモートでインストールする必要はありません。仮想マシンへの接続も必要ありません。

インストールと設定のすべての手順の詳細については、『Deep Securityインストールガイド (vShield)』または『Deep Securityインストールガイド (NSX)』を参照してください。
保護モジュール

Deep Securityの保護モジュールの設定について説明します。

- 不正プログラム対策 (94ページ) モジュールは、ウイルス、トロイの木馬、スパイウェア、およびコンピュータに損害を与えるり、ユーザの同意なしに処理を実行したりすることを目的とするその他のソフトウェアからコンピュータを保護します。

- Webレピュテーション (99ページ) 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Webレピュテーションの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。

- ファイアウォール (101ページ) モジュールは、双方向のステートフルファイアウォールであり、許可されていない送信元からのパケットがホスト上のアプリケーションに到達しないようにします。

- 働入防御 (112ページ) モジュールは、既知またはゼロデイの脆弱性に対する攻撃、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コンピュータを保護します。ポードの修正が完了する前でも、脆弱性に対する攻撃にさらされないようにします。また、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。

- 変更監視 (115ページ) モジュールは、コンピュータ上の特定の領域に関する変更を監視します。Deep Securityで監視できるのは、インストール済みのソフトウェア、実行中のサービス、プロセス、ファイル、ディレクトリ、待機中のポート、レジストリキー、およびレジストリ値です。変更監視モジュールは、割り当てられているルールで指定されたコンピュータ上の領域に対し、ベースライン検索を定期的に実行することで、変更点を検出します。Deep Security Managerに、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。

- セキュリティログ監視 (116ページ) モジュールは、コンピュータで実行中のOS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監視します。セキュリティログ監視ルールは、コンピュータに直接割り当てることも、セキュリティプロファイルの一部にすることもできます。変更監視イベントと同様に、セキュリティログ監視イベントについてもアラートを生成するためにDeep Security Managerで設定できます。

- SAP統合モジュールは、Deep SecurityをSAP NetWeaverと統合します。
不正プログラム対策

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。脅威を特定するために、サーバにホストされている、またはアップデート可能なパターンとしてローカルに保管されている包括的な脅威データベースに対して、ファイルを照合します。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。

不正プログラム対策では、システムへの影響を最小限に抑えつつ、脅威を阻止して取り除く処理が実行されます。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。


不正プログラムの種類

不正プログラム対策は、次のものを含むすべての種類のファイルベースの脅威から保護します。

ウイルス (ファイル感染型)

ウイルスは、正常な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を起動させの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。

トロイの木馬などの非感染型ウイルス

非感染型ウイルスは、他のファイルを感染させることを目的とする不正ファイルのことを指します。これには次のタイプの不正プログラムを含む、さまざまなものがあります。

・ トロイの木馬: パックドアやワーム機能を持たない、非感染型の実行可能な不正プログラムファイル。
・ パックドア: 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。パックドアは、開いているポートを利用してサーバと通信します。
・ ワーム: システム間で伝播することがある不正プログラムは、一般に「ワーム」と言います。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適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のコアポーテ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
スパイウェア/グレーウェア

スパイウェア/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することがあります。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ネルを通じて配布されるものなど、もともと不正性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/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、ユーザー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 (広告サポートソフトウェア)**: 广告を自動的に再生、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もあります。

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ーが自ら、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。

パッカー

パッカーは圧縮または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。<不正プログラムからの保護> 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査します。

不正プログラムの可能性があるファイル

不正プログラムの可能性があるとして検出されるファイルは、通常、未知の不正プログラムコンポーネントです。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。

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。このカテゴリーには、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。
不正プログラム検索の種類

Deep Securityには、次の3種類の不正プログラム検索があります。

- フル検索
- クイック検索
- リアルタイム検索

フル検索では、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システム検索が実行されます。フル検索は、予約タスクを作成することで決まった日時に実行するか、必要に応じて手動で実行できます。

クイック検索では、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出されが、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、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。

リアルタイム検索は、実行中のプロセスやI/Oイベントの継続的な監視です。

基本的な設定

コンピュータで不正プログラム対策機能を有効にするには、次の手順に従います。

1. ポリシーまたはコンピュータエディタで、【不正プログラム対策】→【一般】に移動します。
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。
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。

詳細設定

不正プログラム検索設定を変更する

不正プログラム検索の範囲は、【不正プログラム検索設定】で編集できます。【不正プログラム検索設定】では、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、または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）を設定します。不正プログラム検索には、次の2種類の設定があります。

- 手動/予約検査の設定
- リアルタイム検索の設定

手動検査の設定と予約検査の設定は、フル検査が対象です。リアルタイム検査の設定は、リアルタイム検査が対象です。

Deep Securityでは、不正プログラム検査の初期設定が検査の種類ごとに事前に設定されています。不正プログラム検査の初期設定は、Deep Securityの事前に設定されたセキュリティポリシーで使用されます。

不正プログラム検査設定を変更するには、次の手順に従います。

1. 【ポリシー】画面で、【共通オプジェクト】→【その他】→【不正プログラム検査設定】に移動します。
2. 既存の不正プログラム検査設定を編集するか、新規に作成します。詳細については、Deep Security Managerのヘルプで「不正プログラム検査設定」を参照してください。

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。
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ネチャが参照されます。スマートスキャンを使用するとき、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。

スマートスキャンには、次の機能と利点があります。

• 脅威からの保護にかかる合計時間を削減
• パターン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に関連する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
• クラウドで、高速でリアルタイムのセキュリティステータス検索機能を実現

スマートスキャンのオンとオフを切り替えるには、ポリシーやまたはコンピュータエディタで、[不正プログラム対策]→[Smart Protection]に進みます。

NSXセキュリティタグ

Deep Securityでは、不正プログラムによる脅威の検出時に、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。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セキュリティタグと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 NSXのドキュメントを参照してください。

注意：NSXセキュリティタグはVMware NSX環境に属しています。Deep Securityのイベントタグと混同しないようにしてください。Deep Securityでのイベントのタグ付けの詳細については、(145ページ)「イベントのタグ付け」を参照してください。

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および侵入防御システム保護モジュールを設定できます。

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、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]→[詳細]→[NSXセキュリティのタグ付け]に移動します。
不正プログラム対策エンジンが試行した修復処理が失敗した場合に、NSXセキュリティタグの適用のみを行うように選択できます（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）。

後続の不正プログラム検索で不正プログラムが検出されない場合にセキュリティタグを削除するように選択することもできます。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のみ使用してください。
Webレピュテーション

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Webレピュテーションの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。

基本的な設定

コンピュータでWebレピュテーション機能を有効にするには、次の手順に従います。

1. ポリシーまたはコンピュータエディタで、[Webレピュテーション]→[一般]の順に選択します。
2. [オン]を選択し、[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

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。

- インラインモード: 実際の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。したがって、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: 実際のパケットストリームが複製され、メインストリームを迂回して流れます。

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、ポリシーまたはコンピュータエディタを開き、[設定]→[ネットワークエンジン]の順に選択してください。

Smart Protection Server

Webレピュテーションモジュールは、Trend Micro Smart Protection Networkで管理されるデータベースを使用します。Deep Securityは、ローカルにインストールされたSmart Protection ServerまたはGlobal Smart Protectionサービスに接続します。Trend Micro Smart Protection Networkへの接続を設定するには、ポリシーまたはコンピュータエディタで、[Webレピュテーション]→[Smart Protection]タブの順に選択します。

セキュリティレベル

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。

- 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Webアドレス
- 非常に不審：不正または脅威の発信元である可能性が疑われたWebアドレス
- 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

次のいずれかのセキュリティレベルを適用できます。

- 高：次のリスクレベルのサイトをブロックします。
  - 危険
非常に不審
不審

中: 次のリスクレベルのサイトのみブロックします。
危険
非常に不審

低: 次のリスクレベルのサイトのみブロックします。
危険

注意: セキュリティレベルによって、Deep SecurityがURLへのアクセスを許可するかブロックするかが決定されます。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。

トレンドマイクロでテストしていないURLをブロックするように選択することもできます。

セキュリティレベルを適用するには、ポリシーまたはコンピュータエディタで、[Webレビュー]→[一般] タブの順に選択します。

除外

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。ブロック/許可の除外リストを作成するには、ポリシーまたはコンピュータエディタで、[Webレビュートー]→[除外] タブの順に選択します。
ファイアウォール

Deep Securityのファイアウォールは、双方向のステートフルファイアウォールであり、許可されていない送信元からのパケットがホスト上のアプリケーションに到達しないようにします。

基本的な設定

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. ポリシーまたはコンピュータエディタで、[ファイアウォール]→[一般]の順に選択します。
2. [オン]を選択し、[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

ファイアウォールモジュールは、次の2つのモードで動作するDeep Securityネットワークエンジンを使用します。

- **インラインモード**: 実際の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。したがって、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**: 実際のパケットストリームが複製され、メインストリームを迂回して流れます。

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、ポリシーまたはコンピュータエディタを開き、[設定]→[ネットワークエンジン]→[ネットワークエンジンモード]の順に選択してください。

ファイアウォールルールのプロパティ

パケットの送信元と送信先

ファイアウォールでは、次の条件を使用して、トラフィックの送信元と送信先を判断できます。

- **IPアドレス**
- **MACアドレス**
- **ポート**

IPアドレス

IPアドレスの定義には、次のオプションを使用できます。

- **任意**: アドレスの指定がないので、送信元または送信先として任意のホストが対象
- **単一IP**: IPアドレスを使用してコンピュータを特定
- **マスクされているIP**: 同じサブネットマスクを使用するすべてのコンピュータにルールを適用
- **範囲**: IPアドレスが特定の範囲内にあるすべてのコンピュータにルールを適用
- **IP**: IPアドレスが連続しない複数のコンピュータにルールを適用する場合に使用
- **IPリスト**: IPアドレスのコンポーネントリストを使用してホストを定義
MACアドレス

MACアドレスの定義には、次のオプションを使用できます。

- 任意: MACアドレスの指定がないので、すべてのアドレスにルールを適用
- 単一MAC: 特定のMACアドレスにルールを適用
- MAC: ここで指定された複数のMACアドレスにルールを適用
- MACリスト: MACリスト内のMACアドレスにルールを適用

ポート

ポートの定義には、次のオプションを使用できます。

- 任意: すべてのポートにルールを適用
- ポート: ここで指定された複数のポートにルールを適用
- ポートリスト: ポートリストにルールを適用

トランスポートプロトコル

ルールがインターネットプロトコル (IP) のフレームの種類を対象としている場合、プロトコルフィールドが有効になり、管理者は分析するトランスポートプロトコルの指定を求められます。使用できるプロトコルオプションは次のとおりです。

- 任意 (ファイアウォールはプロトコルで区別しない)
- ICMP
- ICMPV6
- IGMP
- GGP
- TCP
- PUP
- UDP
- IDP
- ND
- RAW
- TCP+UDP
- その他 (プロトコル番号の指定が必要)

方向

Deep Securityのファイアウォールは双方向のファイアウォールです。したがって、ネットワークからDeep Securityホストへのトラフィック (受信) とホストからネットワークへのトラフィック (送信) の両方にルールを適用できます。

注意: 1つのファイアウォールルールは一方向にのみ適用されます。このため、特定の種類のトラフィックを対象とするファイアウォールルールはペアにしてください。
TCPヘッダフラグ

TCPトラフィックについては、ルールを適用するTCPフラグを選択できます。すべてのフラグにルールを適用するのでない場合、次のいずれかを選択できます。

- 任意のフラグ
- URG
- ACK
- PSH
- RST
- SYM
- FIN

これらのフラグは、複数の攻撃に対してさまざまな方法で使用できます。ここでは、一部についてのみ説明します。

URGフラグは、パケットの緊急性が高く、他のパケットよりも先に処理する必要があることを示します。PSHフラグは、パッファを消去し、すべての情報をアプリケーションに送信するためにTCPスタックを設定します。どちらのフラグも、Xmas検索と呼ばれるポート検索に使用できます。これは通常、URGフラグとPSHフラグが有効になっているFINパケットです。この検索の名前は、フラグのバイト (00101001) で、各ビットがクリスマスツリーのように交互にオンとオフになっていることに由来します。

保護されていないコンピュータがXmas検索に関連するパケットを受信すると、次の処理が実行されます。

<table>
<thead>
<tr>
<th>条件</th>
<th>応答</th>
</tr>
</thead>
<tbody>
<tr>
<td>ポートが閉じている</td>
<td>RSTパケットを返す</td>
</tr>
<tr>
<td>ポートが開いている</td>
<td>応答なし、開いているポートの存在を公開</td>
</tr>
</tbody>
</table>

RST (RESET) フラグは、TCP接続を即座に終了します。上記のように、正常な使用方法の1つに、接続できない、または接続が許可されていない閉じているポートへの接続の終了があります。ただし、RSTフラグは、実行中のセッションを中断することを目的としたRESET攻撃に使用されることもあります。次の図は、ホストBからのパケットに含まれるとホストAが予測していたTCPシーケンス番号を、ホストCが計算し、RSTパケットがホストBから送信されたようにホストAに対して偽装した状況を示しています。最終的な結果は、DoS攻撃になります。

フレームの種類

「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。

インターネットプロトコル (IP)、アドレス解決プロトコル (ARP)、および逆アドレス解決プロトコル (REVARP) が、現在のイーサネットワークで使用されている最も一般的なプロトコルですが、リストから [その他] を選択することで、その他の任意のフレームの種類を「フレーム番号」で指定できます。
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通信にのみ使用します。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: ホストコンピュータが、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: ホストコンピュータが、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を対象に設計されています。ネットワーク負荷の高いプロトコルでは、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、望まされていないためです。

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ので、一方向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はバイパスされません。したがって、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します。

| 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。 |

す。これは、ルール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からデータベースホスト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るリスクがあります。通信のファーマンスが支障を来すリスクを評価し、通信のファ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、Deep Security Agentを実行しているコンピュータが受信TCPトラフィック用にポート4118を許可する優先度4のバイパスルールを自動的に作成します。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。このポートでAgentを強化するには、このポートを、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: 4118

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じ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ために便利です。「強制的に許可」ルールのうち、通常有効に設定される初期設定は次の通りです。

注意: 複数ノード構成で複数のManagerコンピュータを使用する場合は、これらのコンピュータのIPリストを定義し、このリストをManagerトラフィックのカスタムルールに使用すると便利です。

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
   1. バイパス
   2. ログのみ (ログのみルールは優先度4 (最高) にのみ割り当て可能)
   3. 強制的に許可
   4. 拒否
2. 優先度3 (高) のファイアウォールルール
1. バイパス
2. 強制的に許可
3. 拒否

3. 優先度2（標準）のファイアウォールルール
   1. バイパス
   2. 強制的に許可
   3. 拒否

4. 優先度1（低）のファイアウォールルール
   1. バイパス
   2. 強制的に許可
   3. 拒否

5. 優先度0（最低）のファイアウォールルール
   1. バイパス
   2. 強制的に許可
   3. 拒否
   4. 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（有効な許可ルールがない場合、拒否）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つ作成しても、許可ルールの条件を満たしていないかぎり、その他の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、拒否ルールでブロックされていないかぎり、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TCP/UDPポート53の受信DNSクエリをすべて許可するDNSサーバのポリシーの例について考えてみます。この場合、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することによって、特定範囲のIPアドレスを指定して、同一の公開サーバへのアクセスを禁止する必要があります。

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。それ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. ログのみ: パケットがログ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/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るため、柔軟性に優れた処理を実現できます。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す。 |

ステートフルフィルタ

コンピュータでステートフル設定が有効になっている場合は、トラフィック履歴のコンテキスト、TCPおよびIPヘッダ値の正当性、およびTCP接続状態の変化の範囲内でパケットが分析されます。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機能が実装されます。

| 注意 | ステートフル設定は、Deep Security Managerの[ポリシー]→[共通オブジェクト]→[ファイアウォールステートフル設定]に保存されています。ステートフル設定をコンピュータに適用するには、ポリシーエディタまたはコンピュータエディタで[ファイアウォール]→[一般]→[ファイアウォールステートフル設定]に移動します。 |

静的ルールで明確に許可されている場合、パケットはステートフルルーチンを通過します。

- パケットが調査され、既存の接続に属しているかどうかが接続テーブルで確認されます。
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。

ステートフルエンジンが有効になると、インタフェースを横断するすべてのトラフィックに適用されます。

UDPの擬似ステートフルインスペクションは、初期設定で「未承諾」のUDPパケットの受信を拒否します。コンピュータでUDPサーバを実行している場合は、強制的に許可ルールをポリシーに設定してサーバへのアクセスを許可する必要があります。たとえば、UDPの擬似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は、53番ポートに対するUDPトラフィックを許可する強制的に許可ルールが必要です。

ICMPの擬似ステートフルインスペクションは、初期設定で、未承諾のICMP要求/応答およびエラーパケットの受信を拒否します。未承諾のICMP/パケットを許可するには、強制的に許可ルールを明確に設定する必要があります。静的ルールで明確に許可されていなければ、要求/応答やエラータイプではない別のすべてのICMPパケットは破棄されます。

ファイアウォールポリシーをまとめて設計する

一般的に、コンピュータのファイアウォールポリシーを定義するには次の2つの方法があります。

• 禁止: 明確に許可されていないトラフィックを禁止します。許可するトラフィックを記述した許可ルールと許可するトラフィックをさらに制限した拒否ルールの組み合わせを使用することによって、禁止ポリシーを作成できます。

• 許可: 明確に禁止されていないトラフィックを許可します。破棄する必要のあるトラフィックを記述した拒否ルールを制限的に使用することによって許可ポリシーを作成できます。

通常、禁止ポリシーを優先して許可ポリシーを使用しないようにします。

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サブセットを許可するには、許可および拒否ルールを連動して強制的に許可ルールを使用する必要があります。また、ICMPおよびUDPステートフルが有効になっている際に、未承認の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。

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. まず、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。そのためにには、受信許可ルールを作成し、プロトコルセレクトを「TCP+UDP」に設定し、[指定フラグ] の下にある [選択以外] チェックボックスと [SYN] チェックボックスをオンにします。この時点で、ワークステーションのユーザからの要求に応答する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で有効化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. ウェブ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他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、承認された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. 次に、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内の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. そのためには、送信元IPアドレス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（マッチングルール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認の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、強制的に許可を使用して未承認の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要求を受け入れる場合は、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は、まずAgent/Appliance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しく設定できます。
バイパスルール

バイパスルールという特別な種類のファイアウォールルールがあります。これは、フィルタリングを望まないメディア集約プロトコルのために設計されたものです。バイパスルールを作成するには、新しいファイアウォールルールを作成するときにルールの「処理」として「バイパス」を選択します。

ファイアウォールルールの「バイパス」処理は、次の点で「強制的に許可」ルールとは異なります。

- バイパスルールと一致するパケットは、侵入防御ルールによって処理されません。
- 「強制的に許可」ルールとは異なり、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場合、バイパスルールはTCP接続での応答を自動的に許可しません（詳細については、下記を参照してください）。
- バイパスルールの中には最適化されているものもあり、Agent/Applianceプラグインが存在しないかのように効率的にトラフィックが流れます（詳細については、下記を参照してください）。

ファイアウォールステートフル設定の有効時にバイパスを使用する

バイパスルールを使用してTCP送信先ポートに対する受信トラフィックで侵入防御ルールをスキップし、ファイアウォールステートフル設定を設定してTCPステートフルインスペクションを実行する場合は、対応する送信元ポートに対する送信フィルタを必ず作成してTCP応答を許可する必要があります（これは「強制的に許可」ルールには必要はありません。強制的に許可されたトラフィックはステートフルエンジンによって処理されるためです）。

すべての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。

最適化

一致するトラフィックを可能な限り早く通過させるには、バイパスルールを作成します。次の設定により、最大スループットを実現できます。

- 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ます。送信元ポートを「任意」にすると必要があります。
  - 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

バイパスルールに一致するパケットはログに記録されません。このオプションは設定できません。
侵入防御

侵入防御モジュールは、既知またはゼロデイの脆弱性に対する攻撃、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コンピュータを保護します。コードの修正が完了する前でも、脆弱性に対する攻撃にさらされないようにします。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。

侵入防御は、ネットワークトラフィック内の不正な命令を検出し、該当するパケットを破棄することで、攻撃を防御します。

次の機能で使用されます。

- **仮想パッチ**: 侵入防御ルールで、特定のアプリケーションやOS自体のパッチが適用されていないという脆弱性を利用してトラフィックを破棄できます。これにより、アプリケーションに各パッチが適用されるのを待つ間もホストを保護できます。
- **プロトコルの正常性確認**: 不正な命令が含まれるトラフィックを検出し、ブロックします。
- **アプリケーション制御**: Skypeやファイル共有ユーティリティなど、特定のアプリケーションに関連するトラフィックをロックできます。

基本的な設定

コンピュータで侵入防御機能を有効にするには、次の手順に従います。

1. ポリシーまたはコンピュータエディタで、[侵入防御]→[一般]に移動します。
2. [オン]を選択し、[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

侵入防御モジュールは、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。

- **インラインモード**: 実際の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。したがって、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**: 実際のパケットストリームが複製され、メインストリームを迂回して流れます。

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、ポリシーまたはコンピュータエディタを開き、[設定]→[ネットワークエンジン]→[ネットワークエンジンモード]の順に選択してください。

防御と検出

Deep Securityのネットワークエンジンがインラインモードの場合は、次の2つの追加オプションを使用できます。

- **防御**: 侵入防御ルールがトラフィックに適用され、関連するログイベントが生成されます。
- **検出**: 侵入防御ルールがトリガされ、イベントが生成されますが、トラフィックに影響はありません。侵入防御の新しい設定やルールは必ず検出モードでテストし、誤判定によってコンピュータ上のサービスが中断しないことを確認する必要があります。侵入防御イベントを一定期間監視して、誤判定がトリガされないことを確認できたなら、防御モードに切り替えます。
個々の侵入防御ルールを、検出のみモードまたは防御モードで適用することもできます。新しい侵入防御ルールを適用するときは、検出のみモードで一定期間実行し、正常なトラフィックを妨害しないことを確認するようお勧めします。トレンドマイクロが用意している一部のルールは、初期設定で検出のみモードになっています。たとえば、メールクライアントの侵入防御ルールは、後続するメールのダウンロードがブロックされないように、一般に検出のみモードになっています。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トリガするので、個々の状況は防止されませんが、状況が再度発生した場合はアラートが発令されます。また、一部のルールは、誤判定が発生しやすくなっています。これらのルールは、初期設定で検出のみモードになっているので、誤判定がトリガされないことを確認できてから、防御モードに切り替えるかどうかを判断してください。

NSXセキュリティタグ

Deep Securityでは、不正プログラムによる脅威の検出時に、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。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、NSXセキュリティタグと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 NSXのドキュメントを参照してください。

注意：NSXセキュリティタグはVMware NSX環境に属しています。Deep Securityのイベントタグと混同しないようにしてください。Deep Securityでのイベントのタグ付けの詳細については、(145ページ)「イベントのタグ付け」を参照してください。

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および侵入防御システム保護モジュールを設定できます。

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、コンピュータまたはポリシーエディタで、[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。

注意：侵入防御ルールの重要度は、[ルールのプロパティ]→[一般]タブで設定できます。

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。

<table>
<thead>
<tr>
<th>侵入防御ルールの重要度</th>
<th>NSXセキュリティタグ</th>
</tr>
</thead>
<tbody>
<tr>
<td>重大</td>
<td>IDS_IPS.threat=high</td>
</tr>
<tr>
<td>高</td>
<td>IDS_IPS.threat=high</td>
</tr>
<tr>
<td>中</td>
<td>IDS_IPS.threat=medium</td>
</tr>
<tr>
<td>低</td>
<td>IDS_IPS.threat=low</td>
</tr>
</tbody>
</table>

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。
- 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。

防御モードで動作しているルールと検出のみモードで動作しているルールでは、別々の設定が適用されます。

注意: 侵入防御ルールが防御モードと検出のみモードのどちらで動作しているかは、侵入防御モジュール設定 (ポリシーまたはコンピュータのエディタの [侵入防御]→[一般] タブ) だけでなく、個々のルール設定 ([ルールのプロパティ]→[一般]→[詳細]) で判断されます。
変更監視

変更監視は、コンピュータ上の特定の領域に関する変更を監視します。Deep Securityで監視できるのは、インストール済みのソフトウェア、実行中のサービス、プロセス、ファイル、ディレクトリ、待機中のポート、レジストリキー、およびレジストリ値です。変更監視モジュールは、割り当てられているルールで指定されたコンピュータ上の領域に対し、ベースライン検査を定期的に実行することで、変更点を検出します。Deep Security Manager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。

推奨設定の検索では、変更監視ルールをコンピュータに推奨します。

コンピュータで変更監視を有効にする一般的な手順は次のとおりです。

1. 変更監視をグローバルに、または特定のコンピュータでオンにします。
2. コンピュータで推奨設定の検索を実行します。
3. 推奨される変更監視ルールを適用します。
4. オプションで、コンピュータ用に作成した固有の変更監視ルールを適用します。
5. コンピュータ用のベースラインを作成します。そのためには、コンピュータの [詳細] 画面を開き、[変更監視] 画面に進み、[ベースラインの再構築] をクリックします。
6. 手動で、または予約タスクを作成して、定期的に変更を検索します。

基本的な設定

変更監視機能をコンピュータで有効にするには、次の手順に従います。

1. 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。
2. [オン] を選択し、[保存] をクリックします。

変更監視のオン/オフを切り替えて、推奨設定の検索の後に、推奨される変更監視ルールを自動的に適用するかどうかを設定するには、メインの [変更監視] 画面を使用します。

・ オン: 変更監視の検索を予約できます。Deep Securityの他の操作と同様に、変更監視の検索は予約することができます。前回の検索後に監視対象のエンティティに変更があった場合、その変更が特定され、イベントが記録されます。

・ オフ: 变更監視の検索を必要に応じて行います。変更監視による変更の検索を管理者が開始することもできます。処理内容は、変更監視の検索の予約と同様です。

・ リアルタイム: リアルタイムの変更監視を実施します。リアルタイムの変更監視では、エンティティの変更をリアルタイムで監視し、変更が検出されると変更監視イベントを発生させることができます。イベントは、リアルタイムでSyslog経由でSIEMに、または次回のDeep Security Managerとのハートビート通信時 (設定可能) に転送されます。

コンピュータの [詳細] 画面の [変更監視] 画面には、特定のコンピュータにのみ適用する追加のオプションが用意されています。この画面では、変更の検索を開始したり、コンピュータ用のベースラインデータを再作成したりできます。また、推奨設定の検索を開始したり、既存の推奨設定をクリアしたりすることもできます。

カスタムの変更監視ルールを作成する方法については、変更監視ルール画面のドキュメントおよび「参照」セクションの「変更監視ルールの言語 (252ページ)」を参照してください。
セキュリティログ監視

OSSECのセキュリティログ監視エンジンがDeep Securityに統合されました。このエンジンにより、コンピュータで実行されているOSおよびアプリケーションで生成されたログとイベントを検査できるようになりました。セキュリティログ監視ルールは、コンピュータに直接割り当てることも、セキュリティプロファイルの一部にすることもできます。変更監視イベントと同様に、セキュリティログ監視イベントについてもアラートを生成するようにDeep Security Managerで設定できます。

| 注意： | 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、ローカルでの設定が必要となります。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。 |

基本的な設定

コンピュータでセキュリティログ監視機能を有効にするには、次の手順に従います。

1. ポリシーまたはコンピュータエディタで、[セキュリティログ監視]→[一般]に移動します。
2. [オン]を選択し、[保存]をクリックします。

推奨設定の検索

Agentでは、定期的に推奨設定の検索を実行するよう設定できます。これは、コンピュータを検索してさまざまなセキュリティルールの適用を推奨するものです。チェックボックスをオンにすると、推奨されるセキュリティログ監視ルールがコンピュータに自動で割り当てられ、不要なルールは自動的に外されます。

推奨設定エンジンのオンとオフを切り替えるには、ポリシーまたはコンピュータエディタで、[設定]→[検索]に進みます。

詳細トピック

セキュリティログ監視の詳細については、「セキュリティログ監視ルールの確認 (117ページ)」を参照してください。
セキュリティログ監視ルールの確認

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は、Deep Security Managerの[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]にあります。

セキュリティログ監視ルールの構造とイベント照合プロセス

次のスクリーンショットは、「Mail Server - Microsoft Exchange」というセキュリティログ監視ルールのプロパティ画面にある[設定]タブの内容を示します。

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 - 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
セキュリティログ監視エンジンは、この構造にログイベントを適用し、一致が存在するかどうかを確認します。Exchangeイベントが存在し、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とします。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の行の重要度は「無視」であるため、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。一致がここを停止する場合、重要度が「Medium(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、重要度が「High(9)」である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みなされると、重要度が「High(9)」である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】タブを調べると、重要度が「中 (4)」のサブルールが一致していても、Deep Security Managerによってアラートが発令されることがあります。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では、サブルールが重複している場合があります。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。
セキュリティログ監視ルールを作成する

Deep Securityのセキュリティログ監視モジュールでは、OSとアプリケーションのログを収集して分析し、何千ものログエントリに含まれている重要なセキュリティイベントを識別できます。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でまとめて安全に収集されます。

Deep Securityのセキュリティログ監視モジュールでは、次の処理が可能です。

- 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/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/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。

Deep Securityのセキュリティログ監視では、次に示すさまざまな方法で、重要なセキュリティイベントの収集が自動的に行われます。

- 推奨設定の検索：推奨設定の検索では、検索対象のサーバに対して、セキュリティログ監視ルール（Windowsのセキュリティログ監視ルールやUNIXのセキュリティログ監視ルールなど）を推奨します。
- 初期設定のセキュリティログ監視ルール：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。
- 自動タグ付け：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。

注意：セキュリティログ監視モジュールは、指定されたログファイルをリアルタイムで監視し、そのファイルに対する変更が発生した場合に処理します。一定の期間無効にしていたAgentが有効に戻った場合、セキュリティログ監視モジュールはログファイルに対する変更を検出しません（ベースラインを作成し、指定されたファイルとシステムコンポーネントを定期的に検索して、それらをベースラインと比較する変更監視モジュールとは異なります）。

セキュリティログ監視プロセス

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およびトリガするルール用の条件のセットで構成されています。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: プログラム名。イベントのSyslogヘッダから取得されます。
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]→[SIEM]タブの[システムイベント通知]エリアで設定できます）
- イベントのDeep Security Managerへの送信（ポリシーまたはコンピュータエディタの[設定]→[SIEM]タブの[セキュリティログ監視イベントの転送 (Agent/Applianceから)]エリアで設定できます）

セキュリティログ監視ルール

セキュリティログ監視エンジンは、コンピュータのログエントリにセキュリティログ監視ルールを適用して、それらのエントリでセキュリティログ監視イベントを生成する必要があるかどうかを判断します。

1つのセキュリティログ監視ルールには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。

アトミックルール

グループ

各ルールまたはルールのグループは、<group></group>エレメント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Agentに送信されると、そのAgent上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1つ以上の長いセキュリティログ監視ルールにアセンブルします。
一部のグループ定義は、トレンドマイクロによるすべてのセキュリティログ監視ルールで共通です。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、他のトレンドマイクロによるルールを割り当てずにそのルールをコンピュータに割り当てる場合は、作成した新しいルールに「Default Rules Configuration」ルールの内容をコピーするか、コンピュータに対する「Default Rules Configuration」ルールの割り当ても選択する必要があります。

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。

```xml
<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。

<table>
<thead>
<tr>
<th>グループの種類</th>
<th>グループ名</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>攻撃の予兆</td>
<td>connection_attempt</td>
<td>接続の試行</td>
</tr>
<tr>
<td></td>
<td>web_scan</td>
<td>Web検索</td>
</tr>
<tr>
<td></td>
<td>recon</td>
<td>一般的な検索</td>
</tr>
<tr>
<td></td>
<td>authentication_success</td>
<td>成功</td>
</tr>
<tr>
<td></td>
<td>authentication_failed</td>
<td>失敗</td>
</tr>
<tr>
<td></td>
<td>invalid_login</td>
<td>無効</td>
</tr>
<tr>
<td></td>
<td>login_denied</td>
<td>ログイン拒否</td>
</tr>
<tr>
<td></td>
<td>authentication_failures</td>
<td>損失の失敗</td>
</tr>
<tr>
<td></td>
<td>adduser</td>
<td>ユーザアカウントの追加</td>
</tr>
<tr>
<td></td>
<td>account_changed</td>
<td>ユーザアカウントの変更または削除</td>
</tr>
<tr>
<td>攻撃/悪用</td>
<td>automatic_attack</td>
<td>ワーム (対象を指定しない攻撃)</td>
</tr>
<tr>
<td></td>
<td>exploit_attempt</td>
<td>攻撃コードのパターン</td>
</tr>
<tr>
<td></td>
<td>invalid_access</td>
<td>無効なアクセス</td>
</tr>
<tr>
<td></td>
<td>spam</td>
<td>スパム</td>
</tr>
<tr>
<td></td>
<td>multiple_spam</td>
<td>損失のスパムメッセージ</td>
</tr>
<tr>
<td></td>
<td>sql_injection</td>
<td>SQLインジェクション</td>
</tr>
<tr>
<td></td>
<td>attack</td>
<td>一般的な攻撃</td>
</tr>
<tr>
<td></td>
<td>virus</td>
<td>ウイルスの検出</td>
</tr>
<tr>
<td>アクセス管理</td>
<td>access_denied</td>
<td>アクセス拒否</td>
</tr>
<tr>
<td></td>
<td>access_allowed</td>
<td>アクセス許可</td>
</tr>
<tr>
<td></td>
<td>unknown_resource</td>
<td>存在しないリソースへのアクセス</td>
</tr>
<tr>
<td></td>
<td>firewall_drop</td>
<td>ファイアウォールによるドロップ</td>
</tr>
<tr>
<td></td>
<td>multiple_drops</td>
<td>無効なファイアウォールによるドロップ</td>
</tr>
<tr>
<td></td>
<td>client_misconfig</td>
<td>クライアントの誤った設定</td>
</tr>
<tr>
<td></td>
<td>client_error</td>
<td>クライアントエラー</td>
</tr>
<tr>
<td>ネットワーク制御</td>
<td>new_host</td>
<td>新しいホストの検出</td>
</tr>
<tr>
<td></td>
<td>ip_spoof</td>
<td>可能性のあるARPスプーフィング</td>
</tr>
<tr>
<td>システム監視</td>
<td>service_start</td>
<td>サービスの開始</td>
</tr>
<tr>
<td></td>
<td>system_error</td>
<td>システムエラー</td>
</tr>
<tr>
<td></td>
<td>system_shutdown</td>
<td>停止</td>
</tr>
</tbody>
</table>
### 説明

<description/>

タグを含めます。ルールがトリガーされると、説明のテキストがイベントに表示されます。

```xml
<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/>

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。

```xml
<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]→[セキュリティログ監視デコーダ] に進みます。[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/> 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。

```plaintext
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/> タグを使用します。

```xml
<rule id="100124" level="5">
  <decoded_as>sshd</decoded_as>
  <match>^Failed password</match>
  <description>Failed SSHD password attempt</description>
</rule>
```
次の表は、サポートされている正規表現の構文を一覧表示しています。

<table>
<thead>
<tr>
<th>正規表現の構文</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>\w</td>
<td>A<del>Z、a</del>z、0~9の英数字1文字</td>
</tr>
<tr>
<td>\d</td>
<td>0~9の数字1文字</td>
</tr>
<tr>
<td>\s</td>
<td>単一のスペース (空白文字)</td>
</tr>
<tr>
<td>\t</td>
<td>単一のタブ</td>
</tr>
<tr>
<td>\p</td>
<td>()*+,-.:;&lt;=&gt;?[]</td>
</tr>
<tr>
<td>\W</td>
<td>\w以外</td>
</tr>
<tr>
<td>\D</td>
<td>\d以外</td>
</tr>
<tr>
<td>\S</td>
<td>\s以外</td>
</tr>
<tr>
<td>.</td>
<td>任意の文字</td>
</tr>
<tr>
<td>+</td>
<td>上記のいずれかの1つ以上に一致 (たとえば、\w+、\d+)</td>
</tr>
<tr>
<td>*</td>
<td>上記のいずれかの0個以上に一致 (たとえば、\w*、\d*)</td>
</tr>
<tr>
<td>^</td>
<td>文字列の先頭 (^&lt;任意の文字列&gt;)</td>
</tr>
<tr>
<td>$</td>
<td>文字列の末尾 (&lt;任意の文字列&gt;$)</td>
</tr>
<tr>
<td></td>
<td>複数の文字列間の「OR」</td>
</tr>
</tbody>
</table>

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。ログにルールを適用する前に、セキュリティログ監視エンジンは <if_sid></if_sid>タグを評価して親子ルールの階層を作成します。
注意:  ルールを使用すると、まったく別の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、後からルールを確認するのが非常に難しくなるため、この指定はお勧めしません。

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。

<table>
<thead>
<tr>
<th>タグ</th>
<th>説明</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>match</td>
<td>パターン</td>
<td>イベント（ログ）に対して照合される任意の文字列。</td>
</tr>
<tr>
<td>regex</td>
<td>正規表現</td>
<td>イベント（ログ）に対して照合される任意の正規表現。</td>
</tr>
<tr>
<td>decoded_as</td>
<td>文字列</td>
<td>事前一致する任意の文字列。</td>
</tr>
<tr>
<td>srcip</td>
<td>送信元のIPアドレス</td>
<td>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アドレスを無効にするには、「!」を使用します。</td>
</tr>
<tr>
<td>dstip</td>
<td>送信先のIPアドレス</td>
<td>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アドレスを無効にするには、「!」を使用します。</td>
</tr>
<tr>
<td>srcport</td>
<td>送信元のポート</td>
<td>任意の送信元のポート（形式の一致）。</td>
</tr>
<tr>
<td>dstport</td>
<td>送信先のポート</td>
<td>任意の送信先のポート（形式の一致）。</td>
</tr>
<tr>
<td>user</td>
<td>ユーザ名</td>
<td>ユーザ名としてデコードされる任意のユーザ名。</td>
</tr>
<tr>
<td>program_name</td>
<td>プログラム名</td>
<td>Syslogプロセス名からデコードされる任意のプログラム名。</td>
</tr>
<tr>
<td>hostname</td>
<td>システムのホスト名</td>
<td>Syslogのホスト名としてデコードされる任意のホスト名。</td>
</tr>
<tr>
<td>time</td>
<td>次の形式の時刻の範囲</td>
<td>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。</td>
</tr>
<tr>
<td>weekday</td>
<td>曜日（日曜、月曜、火曜など）</td>
<td>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。</td>
</tr>
<tr>
<td>id</td>
<td>ID</td>
<td>イベントからデコードされる任意のID。</td>
</tr>
<tr>
<td>url</td>
<td>URL</td>
<td>イベントからデコードされる任意のURL。</td>
</tr>
</tbody>
</table>

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。

```xml
<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。

```xml
<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ベースのオプションを一覧表示しています。

<table>
<thead>
<tr>
<th>タグ</th>
<th>説明</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_sid</td>
<td>ルールID</td>
<td>指定された署名IDに一致するルールのデルタルとしてこのルールを追加します。</td>
</tr>
<tr>
<td>if_group</td>
<td>グループID</td>
<td>指定されたグループに一致するルールのデルタルとしてこのルールを追加します。</td>
</tr>
<tr>
<td>if_level</td>
<td>ルールレベル</td>
<td>指定された重要度レベルに一致するルールのデルタルとしてこのルールを追加します。</td>
</tr>
<tr>
<td>description</td>
<td>文字列</td>
<td>ルールの説明。</td>
</tr>
<tr>
<td>info</td>
<td>文字列</td>
<td>ルールの追加情報。</td>
</tr>
<tr>
<td>cve</td>
<td>CVE番号</td>
<td>ルールに関連付ける任意のCommon Vulnerabilities and Exposures (CVE)番号。</td>
</tr>
</tbody>
</table>
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するのに、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。コンポジットルールには、2つの追加オプションが必要です。frequencyオプションでは、ルールによってアラートが生成されるまでのイベントパターンの発生回数を指定します。timeframeオプションでは、セキュリティログ監視エンジンがどのくらい前までをかきのうってログを検索する必要があるか（秒単位）をエンジンに通知します。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">
<description>5 Failed passwords within 10 minutes</description>
</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>
<description>5 Failed passwords within 10 minutes</description>
</if_matched_sid>
```

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。

<table>
<thead>
<tr>
<th>タグ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>same_source_ip</td>
<td>送信元のIPアドレスが同じになるように指定します。</td>
</tr>
<tr>
<td>same_dest_ip</td>
<td>送信先のIPアドレスが同じになるように指定します。</td>
</tr>
<tr>
<td>same_dst_port</td>
<td>送信元のポートが同じになるように指定します。</td>
</tr>
<tr>
<td>same_location</td>
<td>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。</td>
</tr>
<tr>
<td>same_user</td>
<td>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。</td>
</tr>
<tr>
<td>same_id</td>
<td>デコードされるIDが同じになるように指定します。</td>
</tr>
</tbody>
</table>

認証が失敗するたびにアラートを生成するため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、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>
<description>5 Failed passwords within 10 minutes</description>
</rule>
```

```
<if_matched_sid><if_matched_group>authentication_failure</if_matched_group>
<description>5 Failed passwords within 10 minutes</description>
</if_matched_sid>
```

```
<if_matched_group>authentication_failure</if_matched_group>
<same_source_ip />
<description>5 Failed passwords within 10 minutes</description>
</if_matched_group>
```

```
<if_matched_sid><if_matched_group>authentication_failure</if_matched_group>
<description>5 Failed passwords within 10 minutes</description>
</if_matched_sid>
```

管理者ガイド
実稼働環境での使用例

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 .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ありません。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自然分類を調べることによる逆の方法で実行できます。

たとえば、CMSアプリケーションは、セキュリティログ監視ルールの作成対象である次の機能をサポートします。

- 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
      - 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）

これにより、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]→[新しいセキュリティログ監視ルール…]をクリックして[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。

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。

9. 次に、[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。
注意：eventlogは、Deep Security固有的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>
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。

```xml
<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。

ポリシーまたはコンピュータにルールが割り当てられると、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監視をすぐに開始します。

完成したカスタムCMSセキュリティログ監視ルール:

```xml
<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>
</group>
```
<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>
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

<table>
<thead>
<tr>
<th>レベル</th>
<th>説明</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>無視され、処理は行われない</td>
<td>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前に検索され、セキュリティとは無関係のイベントが含まれます。</td>
</tr>
<tr>
<td>1</td>
<td>事前定義された使用法はなし</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2</td>
<td>システムの優先度の低い通知</td>
<td>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。</td>
</tr>
<tr>
<td>3</td>
<td>成功した/承認されたイベント</td>
<td>成功したログイン試行、ファイルファイアオーバーで許可されたイベントなど。</td>
</tr>
<tr>
<td>4</td>
<td>システムの優先度の低いエラー</td>
<td>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。</td>
</tr>
<tr>
<td>5</td>
<td>ユーザによって生成されたエラー</td>
<td>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。</td>
</tr>
<tr>
<td>6</td>
<td>関連性の低い攻撃</td>
<td>システムに脅威を及ぼさないウイルスまたはウィルスを示します (Linuxサーバを攻撃するWindowsウイルスなど)。また、频繁にトリガされる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。</td>
</tr>
<tr>
<td>7</td>
<td>事前定義された使用法はなし</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>8</td>
<td>事前定義された使用法はなし</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9</td>
<td>無効なソースからのエラー</td>
<td>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。</td>
</tr>
<tr>
<td>10</td>
<td>ユーザによって生成された複数のエラー</td>
<td>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。</td>
</tr>
<tr>
<td>11</td>
<td>事前定義された使用法はなし</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>12</td>
<td>重要度の高いイベント</td>
<td>システムやハーネス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。</td>
</tr>
</tbody>
</table>
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。

重要度の高いセキュリティイベント
通常は、複数の攻撃ルールと攻撃の兆候の相関関係の結果。

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

<table>
<thead>
<tr>
<th>指定子</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>%a</td>
<td>曜日の省略名 (例: Thu)</td>
</tr>
<tr>
<td>%A</td>
<td>曜日の正式名 (例: Thursday)</td>
</tr>
<tr>
<td>%b</td>
<td>月の省略名 (例: Aug)</td>
</tr>
<tr>
<td>%B</td>
<td>月の正式名 (例: August)</td>
</tr>
<tr>
<td>%c</td>
<td>日時形式 (例: Thu Sep 22 12:23:45 2007)</td>
</tr>
<tr>
<td>%d</td>
<td>月初から数えた日 (01~31) (例: 20)</td>
</tr>
<tr>
<td>%H</td>
<td>24時間形式の時刻 (00~23) (例: 13)</td>
</tr>
<tr>
<td>%I</td>
<td>12時間形式の時刻 (00~12) (例: 02)</td>
</tr>
<tr>
<td>%j</td>
<td>年初から数えた日 (001~366) (例: 235)</td>
</tr>
<tr>
<td>%m</td>
<td>10進表記の月 (01~12) (例: 02)</td>
</tr>
<tr>
<td>%M</td>
<td>分 (00~59) (例: 12)</td>
</tr>
<tr>
<td>%p</td>
<td>AMまたはPMの指定 (例: AM)</td>
</tr>
<tr>
<td>%S</td>
<td>秒 (00~61) (例: 55)</td>
</tr>
<tr>
<td>%U</td>
<td>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)</td>
</tr>
<tr>
<td>%W</td>
<td>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)</td>
</tr>
<tr>
<td>%x</td>
<td>日付形式 (例: 02/24/79)</td>
</tr>
<tr>
<td>%X</td>
<td>時時形式 (例: 04:12:51)</td>
</tr>
<tr>
<td>%y</td>
<td>年の末尾2桁 (00~99) (例: 76)</td>
</tr>
<tr>
<td>%Y</td>
<td>年 (例: 2008)</td>
</tr>
<tr>
<td>%Z</td>
<td>タイムゾーン名または省略形 (例: EST)</td>
</tr>
<tr>
<td>%%</td>
<td>%記号 (例: %)</td>
</tr>
</tbody>
</table>

詳細については、次のWebサイトを参照してください。

www.php.net/strftime
www.cplusplus.com/reference/clibrary/cstdio/strftime.html
推奨設定の検索

Deep Securityでは、コンピュータで推奨設定の検索を実行して既知の脆弱性を特定できます。この処理では、OSだけでなくインストール済みのアプリケーションも検索します。検出結果に基づいて、Deep Securityは、適用する必要のあるセキュリティルールを推奨します。

推奨設定の検索時に、Deep Security Agentは次の項目を検索します。

- OS
- 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
- ユーザ

注意: 大規模な環境の場合、トレンドマイクロでは、ポリシーレベルで推奨設定を管理することを推奨します。つまり、検索対象のすべてのコンピュータに、ポリシーを割り当てておく必要があります。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。

推奨設定の検索は手動で開始できます。または、指定したコンピュータで検索を定期的に実行する、予約タスクを作成することもできます。

制限事項

Linuxでは、アプリケーションと一緒にインストールされたカーネルライブラリまたはソフトウェアライブラリがそのアプリケーションでサポートされていない場合、推奨設定の検索エンジンでアプリケーション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。

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、検索できる項目は次のものに限定されます。

- OS
- 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

推奨設定の検索の実行

推奨設定の検索を手動で起動するには

2. 検索対象のコンピュータ(複数台も可)を選択します。
3. 選択したコンピュータを右クリックして、[処理]→[推奨設定の検索]を選択します。

推奨設定の検索の予約タスクを作成するには

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] をクリックして「新規予約タスク」を選択し、新規予約タスクウィザードを表示します。
4. 次に表示される画面では、手順3で選択した内容に応じて、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:
通常、大規模な環境の場合は、ポリシーを通じてすべての処理を実行することを推奨します。

6. 最後に、新しい予約タスクの名前を指定して、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、[完了] をクリックします。

## 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。

### 推奨設定の検索をキャンセルするには

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。

## 推奨設定の検索の結果を管理する

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。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。
- 以前の推奨設定の検索に基づいて自動的に割り当てられたが、割り当てが解除されたが、ユーザが優先させたルール。たとえば、Deep Securityによって自動的にルールが割り当てられ、その後でユーザがそのルールの割り当てを解除した場合、次回の推奨設定の検索の後に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消できません。ポリシーのレベルでコンピュータに割り当てられたルールは、ポリシーのレベルで割り当てを解消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、誤判定の可能性があるルール(ルールの説明を参照してください)。

最新の推奨設定の検索の結果は、ポリシーまたはコンピュータ編集画面の [侵入防御]→[一般] タブの [推奨設定] エリアに表示されます。

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。[侵入防御]→[一般] の順に選択します。[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。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 [割り当てに推奨される設定の表示] を選択します。
ポリシーに含まれるすべてのコンピュータに対する推奨設定がすべて一覧表示されます。

**注意:**
緑色のフラグには2つの種類があります。完全フラグ（□）と部分フラグ（△）です。推奨ルールには常に完全フラグが指定されます。アプリケーションの種類には、どちらかのフラグが指定されます。完全フラグの場合は、このアプリケーションの種類に属するすべてのルールの割り当てが推奨されていることを示します。部分フラグの場合は、この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ことを示します。

また、上記のスクリーンショット内の「このポリシーが割り当てられている1台のコンピュータのうち1台に対し、この侵入防御ルールの使用をお勧めします」というヒントにも注目してください。トレンドマイクロでは、ポリシーの対象となるすべてのコンピュータにすべての推奨ルールを割り当てることを推奨します。これにより、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。

推奨設定の検索では、侵入防御ルール、セキュリティログ監視ルール、および変更監視ルールの推奨設定が作成されます。

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にアラートが発令されます。

**注意:**
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。

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。
SSLデータストリーム

侵入防御モジュールは、SSLトラフィックのフィルタをサポートしています。ユーザは、[SSL]画面を使用して、1つ以上のインタフェース上で指定された資格情報とポートが対になっているSSL設定を作成できます。資格情報はPKCS#12またはPEM形式でインポートでき、Windowsのコンピュータでは直接CryptoAPIを使用するオプションが用意されています。

注意: SSLトラフィックのフィルタは、Deep Security Agentでのみサポートされます。Deep Security Virtual Applianceではサポートされません。Agentは、SSL圧縮が実装されているSSL接続のフィルタをサポートしません。

コンピュータにSSLデータストリームのフィルタを設定する

SSL設定ウィザードを開始する

設定するコンピュータの[詳細]画面を開き、[侵入防御]→[詳細]→[SSL設定]に進み、[SSL設定の表示]をクリックして[SSL設定]画面を表示します。[新規...]をクリックして、SSL設定ウィザードの最初の画面を開きます。

1. インタフェースを選択する

この設定をコンピュータ上のすべてのインタフェースに適用するのか、それとも1つのインタフェースのみに適用するのかを指定します。

2. ポートを選択する

この設定の適用先のポートをカンマで区切って入力するか、ポートリストを選択します。

注意: コンピュータの[詳細]画面でポート設定を変更する必要もあります(下記参照)。

3. IP選択

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)。

4. 資格情報の入手元を指定する

資格情報ファイルを自分で用意するのか、それともコンピュータにすでに資格情報があるのかを指定します。

5. 資格情報の種類を指定する

今自分が資格情報を用意することを選択した場合、資格情報の種類、格納場所、および必要に応じてパスフレーズを入力します。

資格情報がすでにコンピュータにあると指定した場合は、検索する資格情報の種類を指定します。

6. 資格情報の詳細を入力する

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フレーズを入力します。
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。

以下は、サポートされる暗号の一覧です。

<table>
<thead>
<tr>
<th>16進値</th>
<th>OpenSSL名</th>
<th>IANA名</th>
<th>NSS名</th>
<th>Deep Security Agentバージョン</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00,0x04</td>
<td>RC4-MDS</td>
<td>TLS_RSA_WITH_RC4_128_MDS</td>
<td>SSL_RSA_WITH_RC4_128_MDS</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x05</td>
<td>RC4-SHA</td>
<td>TLS_RSA_WITH_RC4_128_SHA</td>
<td>SSL_RSA_WITH_RC4_128_SHA</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x09</td>
<td>DES-CBC-SHA</td>
<td>TLS_RSA_WITH_DES_CBC_SHA</td>
<td>SSL_RSA_WITH_DES_CBC_SHA</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x0A</td>
<td>DES-CBC3-SHA</td>
<td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>SSL_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x2F</td>
<td>AES128-SHA</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x35</td>
<td>AES256-SHA</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x3C</td>
<td>AES128-SHA256</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256</td>
<td>9.5 SP1以上</td>
</tr>
<tr>
<td>0x00,0x3D</td>
<td>AES256-SHA256</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256</td>
<td>9.5 SP1以上</td>
</tr>
<tr>
<td>0x00,0x41</td>
<td>CAMELLIA128-SHA</td>
<td>TLS_RSA_WITH_CAMELLIA_128_CBC_SHA</td>
<td>TLS_RSA_WITH_CAMELLIA_128_CBC_SHA</td>
<td>9.5 SP1以上</td>
</tr>
<tr>
<td>0x00,0x84</td>
<td>CAMELLIA256-SHA</td>
<td>TLS_RSA_WITH_CAMELLIA_256_CBC_SHA</td>
<td>TLS_RSA_WITH_CAMELLIA_256_CBC_SHA</td>
<td>9.5 SP1以上</td>
</tr>
<tr>
<td>0x00,0xBA</td>
<td>なし</td>
<td>TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256</td>
<td>なし</td>
<td>9.5 SP1以上</td>
</tr>
<tr>
<td>0x00,0xC0</td>
<td>DES-CBC3-MDS</td>
<td>TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256</td>
<td>なし</td>
<td>9.5 SP1以上</td>
</tr>
<tr>
<td>0x00,0x7C</td>
<td>なし</td>
<td>TLS_RSA_WITH_3DES_EDE_CBC_RMD160</td>
<td>なし</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x7D</td>
<td>なし</td>
<td>TLS_RSA_WITH_AES_128_CBC_RMD160</td>
<td>なし</td>
<td>4.5以上</td>
</tr>
<tr>
<td>0x00,0x7E</td>
<td>なし</td>
<td>TLS_RSA_WITH_AES_256_CBC_RMD160</td>
<td>なし</td>
<td>4.5以上</td>
</tr>
</tbody>
</table>

以下は、サポートされるプロトコルの一覧です。

<table>
<thead>
<tr>
<th>プロトコル</th>
<th>Deep Security Agentバージョン</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL 3.0</td>
<td>4.5以上</td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>4.5以上</td>
</tr>
<tr>
<td>TLS 1.1</td>
<td>9.5 SP1以上</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>9.5 SP1以上</td>
</tr>
</tbody>
</table>

7. この設定に名前を付けて説明を追加する

このSSL設定の名前と説明を入力します。

8. 概要を確認して、SSL設定ウィザードを閉じる

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。

コンピュータの [詳細] 画面で、SSLポートを監視するようにポート設定を変更する

最後に、Agent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する必要があります。コンピュータの [詳細] 画面の [侵入防御ルール] へ進み、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参照します。ルールをアプリケーションの種類別にソートします。リストをスクロールダウンして、このコンピュータで実行されているアプリケーションの種類を見つけます (この例では、[Web Server Common])。
アプリケーションの種類「Web Server Common」のヘッダを右クリックし、「アプリケーションの種類プロパティ」を選択します（「アプリケーションの種類プロパティ（グローバル）」ではありません）。これにより、「アプリケーションの種類のプロパティ」画面が（ローカル編集モードで）表示されます。

継承した「HTTP」ポートリストを使用するのではなく、オーバーライドしてSSLの設定時に定義したポート（ここではポート9090）およびポート80をこのポートリストに追加します。ポート9090と80をカンマ区切り値として入力し、[OK]をクリックして画面を閉じます（「アプリケーションの種類プロパティ」を選択したので、加えた変更はこのコンピュータにのみ適用されます。他のコンピュータの[Web Server Common]アプリケーションの種類は変更されません）。

このコンピュータは、SSL暗号化データストリームをフィルタするよう設定されました。

追加メモ

**注意:** Deep Security Agentは、Apacheサーバでディフィー・ヘルマン暗号をサポートしていません。Apache Webサーバでディフィー・ヘルマン暗号を無効化する方法は、「Apacheにおけるディフィー・ヘルマン暗号を無効にする（198ページ）」を参照してください。
イベント、アラート、およびレポート

イベント

Deep Security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、管理またはシステム関連のイベント（ユーザのログオン、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。イベントは日常的に多数発生し、必ずしも個別に対処が必要であるとは限りません。

コンピュータで発生するほとんどのイベントは、次回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(30ページ)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（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]で、設定が有効になっている場合）

初期設定で、Deep Security Managerでは、ハートビートごとにAgent/Applianceからイベントを収集します。イベントのデータを使用して、Deep Security Managerの各種レポート、グラフ、およびチャートが作成されます。

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]画面の[ストレージ]タブで設定された一定の期間保持されます。

メイン画面から、次のことを実行できます。

• 個々のイベントのプロパティを表示する
• リストをフィルタする。イベントのリストをフィルタするには、[期間]および[コンピュータ]ツールバーを使用します。
• イベントリストのデータをCSVファイルにエクスポートする
• 既存の自動タグ付けルールを表示する
• 特定のイベントを検索する

さらに、イベントを右クリックすると、次のオプションが表示されます。

• タグの追加：このイベントにタグを追加します（「イベントのタグ付け (145ページ)」を参照)。
• タグを削除：このイベントからタグを削除します。
• コンピュータの詳細：ログエントリを生成したコンピュータの[コンピュータの詳細]画面を表示します。
イベントプロパティを表示する

イベントをダブルクリック（またはコンテキストメニューから [表示] を選択）すると、そのエントリの [プロパティ] 画面が表示され、そのイベントに関するすべての情報が1つの画面に表示されます。[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「イベントのタグ付け (145ページ)」を参照してください。

リストをフィルタし、イベントを検索する

[検索] ドロップダウンメニューから [詳細検索を開く] を選択すると、詳細検索オプションが表示されます。

[期間] ツールバーでリストをフィルタし、特定の期間中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。

詳細検索機能 (大文字/小文字の区別なし):

- 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
- 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
- 等しくない: 選択した列の入力内容と検索文字列が一致しない
- 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

検索バーの右側にある「プラス」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。

エクスポート

[エクスポート] をクリックして、すべてのイベントまたは選択されたイベントをCSVファイルへエクスポートします。

自動でタグを付ける

[自動タグ付け] をクリックして、既存の自動タグ付けルールリストを表示します(「イベントのタグ付け (145ページ)」を参照)。

アラート

アラートは、ユーザに注意を促す必要がある異常な状況が発生したときに作成されます (ユーザ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)。定義済みのアラートリストがあります。また、トリガ時にアラートを生成するように保護モジュールのルールを設定できます。

Deep SecurityをSMTPサーバに接続すると、特定のアラートが発令されたときにユーザにメール通知を送信できます。
画面には、有効な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」の横にあるドロップダウンメニューを使用します。

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拡大すると、その特定のアラートを生成したコンピュータ（場合によりユーザを含む）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）。

概要ビューでは、コンピュータのリストが5項目を超える場合、5つ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、「選択対象を消去」リンクをクリックして、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。

アラートには、システムアラートとセキュリティアラートの2種類があります。システムアラートは、Agentのオフライン化やコンピュータの時計の変更などのシステムイベントでトリガされます。セキュリティアラートは、侵入防御、ファイアウォール、変更監視、およびセキュリティログ監視の各ルールによってトリガされます。アラートは、「アラートの設定」をクリックして設定できます。

注意:  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。

レポート

Deep Security Managerは、PDFまたはRTFの形式でレポートを生成します。「レポートの生成」画面で生成された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。

単独レポート

各種レポートはPDFまたはRTF形式で出力することができます。ただし、「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CSV形式で出力されます。

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の概要表 (モード別)
- コンピュータレポート: コンピュータのタブに表示される各コンピュータの概要
- DPIルールの推奨レポート: 侵入防御ルールの推奨。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ホストのベースライン（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
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

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。

タグ

イベントデータを含むレポートを選択する場合、イベントタグでレポートをフィルタするオプションを使用できます。【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。

期間

期間を設定して、ログの記録期間を任意で設定できます。これにより、セキュリティ監視に役立ちます。

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。
- 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日の午前0時から11月1日の午前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時までに設定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、この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日よりも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日間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となります。
コンピュータ

コンピュータに対して、どのデータをレポートに含めるかを設定します。

- すべてのコンピュータ: Deep Security Manager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閲覧権限があるユーザを生成し、「すべてのコンピュータ」レポートを定期的に生成するよう予約タスクを作成するか、生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。

暗号化

レポートは、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は、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

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。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、次のようにになります。

<table>
<thead>
<tr>
<th>頻度</th>
<th>過去</th>
<th>1</th>
<th>日間</th>
<th>週間</th>
<th>か月間</th>
</tr>
</thead>
<tbody>
<tr>
<td>頻度</td>
<td>過去</td>
<td>1</td>
<td>日間</td>
<td>週間</td>
<td>か月間</td>
</tr>
</tbody>
</table>

- 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刻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。
- 過去 [N] か月間: 過去 [N] か月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。

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
日よりも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、[管理]→[予約タスク]でオンラインヘルプを参照してください。
イベントのタグ付け

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。

タグ付けの方法は次のとおりです。

- 手動によるタグ付け: 一時的に手動でタグを付けることができます。
- 自動タグ付け: 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: 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: 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にすぎません。

手動によるタグ付け

イベントに手動でタグを付けるには

1. [イベント]リストで、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、入力された名前に一致する既存のタグの候補が表示されます)。
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]リストで、イベントにタグが付けられたことを確認できます。

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。

自動タグ付けルールを作成するには

1. [イベント]リストで、ベースにするイベントを右クリックし、[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、入力された名前に一致する既存のタグの候補が表示されます)。
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。
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（「送信元IP」、「理由」、「重要度」など）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。


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/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、すべてのユーザログオンイベントに『suspicious』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。そうすると、優先度が『1』のルールが先に実行されて、すべてのユーザログオンイベントに『suspicious』タグが適用されます。その後、優先度が『2』のルールが実行され、ユーザが自分自身であるすべてのユーザログオンイベントから『suspicious』タグが削除されます。この結果、将来発生するすべてのユーザログオンイベントの中うち、ユーザが自分以外のものに『suspicious』タグが適用されます。

自動タグ付けルールに優先度を設定するには

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、[表示]をクリックします。
3. ルールの[優先度]を選択します。

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のみ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、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]で検出し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、Deep Securityの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。また、変更監視ルールを実行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に信頼済みソースのコンピュータを使用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には

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、信頼済みのソース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。
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の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. 信頼済みの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. 信頼済みの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。

ソフトウェア安全性評価サービス

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保持している、信頼できる既知のファイル署名の許可リストです。このタイプの信頼済みのソースタグ付けでは、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を監視します。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。一致が見つかると、イベントにタグが付けられます。

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には

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

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。

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には

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。


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指定します。[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。
Deep Security Notifier


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。

<table>
<thead>
<tr>
<th>注意</th>
<th>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/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。</th>
</tr>
</thead>
</table>

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することもできます。インストール手順については、インストールガイドを参照してください。

<table>
<thead>
<tr>
<th>注意</th>
<th>Deep Security Notifierに情報を表示されるためには、Virtual Applianceで保護されている仮想マシンで不正プログラム対策モジュールがライセンス許可され、有効になっている必要があります。</th>
</tr>
</thead>
</table>

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た、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レビュー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。

注意：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。
マルチテナント

目的と要件

マルチテナントとは、Deep Security Managerとデータベースサーバの単一のインストールを使用して、複数の異なる管理環境を作成する機能です。マルチテナント環境では、各テナントの設定、ポリシー、およびイベントが完全に分離され、インフラストラクチャの追加拡張オプションがいくつか使用されます。

マルチテナント機能は、組織内で各事業単位を区分けし、実稼働環境への展開前に準備環境でテストしやすいように設計されています。サービスモデル内で顧客にDeep Securityをプロビジョニングすることもできます。

注意: MSSP (Managed Security Service Provider) には、マルチテナントよりも、役割に基づいたアクセス制御の方が、一括管理とレポートの機能があるため、適している場合があります。

Deep Securityのマルチテナント機能を使用するための要件:

- Deep Security Manager 9.0以上
- Oracle DatabaseまたはMicrosoft SQL Server
- データベースを作成/削除するために必要なデータベースアカウント権限（「マルチテナント (詳細) (161ページ)」を参照）
- マルチテナント機能のアクティベーションコード

任意の要件（推奨）:

- 複数ノードのManager (スケーラビリティのため複数のDeep Security Managerノードが同じデータベースを参照)
- SMTPサーバ

アーキテクチャー

Deep Security Managerのマルチテナント機能は、ハイパーバイザと同じように動作します。Deep Security Managerの同じインストール環境内に複数のテナントが存在しても、それぞれのデータは分離されます。すべてのManagerノードで、任意のテナントのGUI、ハートビート、またはジョブの要求が処理されます。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。Managerノードが追加されるか、オフラインになると、割り当てられたManagerノードが自動的に再調整されます。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ーに共存させることもできます。専用のデータベースサーバー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と同時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ーが利用可能な場合、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。

<table>
<thead>
<tr>
<th></th>
<th>單一テナント</th>
<th>マルチテナント</th>
</tr>
</thead>
<tbody>
<tr>
<td>管理対象コンピュータ</td>
<td>100,000</td>
<td>1,000,000以上</td>
</tr>
<tr>
<td>Deep Security Managerのノード</td>
<td>1-5</td>
<td>1-50</td>
</tr>
<tr>
<td>データベース</td>
<td>1</td>
<td>1-10,000</td>
</tr>
<tr>
<td>データベースサーバー</td>
<td>1 (複製あり、またはなし)</td>
<td>1-100</td>
</tr>
</tbody>
</table>

マルチテナントを有効にして、プライマリテナントには、Deep Security Managerの通常のインストール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。

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。
マルチテナントの有効化

マルチテナントを有効にするには、次の手順に従います。

2. 販売店から受け取った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. 実装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。準備環境のテストにマルチテナントを使用する場合や、同じ企業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: Deep Securityをサービスとして提供する場合はこのモードが推奨されます。この設定を使用する場合、テナントアカウントの作成時 (APIを使用) にライセンスを指定するか、テナント自身がはじめてログオンするときにライセンスを入力します。
4. [次へ] をクリックして、Deep Security Managerでのマルチテナントの有効化を終了します。
5. [管理]→[システム設定]→[テナント] 画面が表示されます。マルチテナントのオプションを設定します。設定の詳細については、[管理]→[システム設定]→[テナント] 画面に進み、そのページのオンラインヘルプを参照してください。

テナントの管理

マルチテナントモードを有効にしたら、[管理]→[テナント] 画面からテナントを管理できます。

テナントを作成する

新しいテナントを作成するには、次の手順に従います。

1. [管理]→[テナント] 画面に移動し、[新規] をクリックして新規テナントウィザードを開きます。
2. 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「Primary」以外の任意の名前を使用できます。
3. メールアドレスを入力します。メールアドレスは各テナントの連絡先として必要です。また、以降の手順に示す、3つのユーザアカウントの生成方法のうち2つで使用されます。

4. ロケールを選択します。ロケールによって、Deep Security Managerコンソールの言語が決まります。

5. タイムゾーンを選択します。テナント関連のイベントは、テナントアカウントのタイムゾーンでテナントのユーザに表示されます。

6. 複数のデータベースを使用している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ようにするか([自動 - 設定なし])、特定のサーバを指定できます。

| 注意: | 新しいテナントの受け入れを停止しているデータベースサーバは、このリストには含まれません。また、データベースが1つだけの場合、このオプションは表示されません。 |

選択したら、[次へ]をクリックして続けます。

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ここで定義します。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ここで設定します。ただし、ユーザがメールで受け取る確認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。
   ◦ 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。このオプションは、管理者がアクセスする必要のないアカウントをユーザ用に手動で作成する場合に適しています。

| 注意: | 確認オプションは、一般ユーザが登録する場合に適した方法を提供します。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は、CAPTCHAが推奨です。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。 |

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。新しいテナントデータベースを作成されてデータとサンプルポリシーが登録されるまで、30秒～4分程度かかる場合があります。

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

Deep Securityへようこそ。アカウントの使用を開始するには、次の確認用URLをクリックしてください。パスワードを入力するとコンソールにアクセスできます。
アカウント名: AnyCo
ユーザ名: admin
アカウントを有効にするには次のURLをクリック:
https://managername:4119/SignIn.screen?confirmation=1A16EC7A-D84F-D451-05F6-706095B6F646&tenantAccount=AnyCo&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

Deep Securityへようこそ。新しいアカウントが作成されました。パスワードは別のメールでお知らせします。

アカウント名: AnyCo
ユーザ名: admin
Deep Securityの管理コンソールは次のURLからアクセスできます:
https://managername:4119/SignIn.screen?tenantAccount=AnyCo&username=admin
2通目のメール: パスワード通知

Deep Securityアカウント用に自動生成されたパスワードをお知らせします。アカウント名とユーザ名、Deep Securityの管理コンソールにアクセスするためのリンクを別のメールでお知らせします。

パスワード: z3IgRUQ0jaFi

テナントの管理

[テナント] 画面 ([管理]→[テナント]) に、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: 作成されましたが、まだ有効ではありません。
- 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まだ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: テナントは削除されましたが、処理はまだ実行されていません。「削除の保留中」状態になってから約7日後にデータベースが削除されます。
- 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。
テナントのロケール、タイムゾーン、および状態を変更できます。タイムゾーンとロケールを変更しても、既存のテナントユーザには反映されません。テナント内の新規ユーザ、イベント、およびユーザ固有ではないUIのその他の部分にだけ反映されます。

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。ハイパーリンクから、データベースが実行されているサーバーにアクセスできます。

モジュール

テナントのロケール、タイムゾーン、および状態を変更できます。タイムゾーンとロケールを変更しても、既存のテナントユーザには反映されません。テナント内の新規ユーザ、イベント、およびユーザ固有ではないUIのその他の部分にだけ反映されます。

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。ハイパーリンクから、データベースが実行されているサーバーにアクセスできます。

モジュール

一般

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。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。

[プライマリテナントからライセンスを継承] を選択した場合、プライマリテナントにライセンス許可されているすべての機能がすべてのテナントに表示されます。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。

テナント単位のライセンスを使用している場合、初期設定では各テナントにライセンス許可されているモジュールだけが表示されます。

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。
デモモードは、実稼働環境での使用を目的としたものではありません。

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。

Agentの有効化

[Agentの有効化] タブには、このテナントのコンピュータでAgentを有効にするためのコマンドが表示されます。このコマンドは、Agentのインストールディレクトリから実行できます。Agentが有効になると、テナントはDeep Security Managerを使用して、ポリシーの割り当てやその他の設定を実行できます。

主担当者の連絡先
テナントアカウントユーザのDeep Security使用環境

テナントのユーザ環境

マルチテナントが有効になっている場合、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）。

注意: プライマリテナントが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、「Primary」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。次の画面は、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 (後述)
- 一部のアラートタイプも非表示:
  - 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（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、ユーザインタフェースガイドまたはオンラインヘルプの[管理]→[システム設定]→[テナント]を参照してください。

テナントは、複数のユーザアカウントに役割に基づいたアクセス制御を使用して、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。

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]をクリックし、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]ボタンをクリックします。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://manageraddress:4120/ "tenantID:7156CF5A-D130-29F4-5FE1-8AFD12E0EC02"
"tenantPassword:98785384-3966-B729-1418-3E2A7197D0D5"
```

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]画面の[処理]タブで[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。この情報は、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、およびチャージバックレポートに表示されます。

このチャージバック（またはショーバック）情報をカスタマイズして、レコードに含める属性を指定できます。この設定は、サービスプロバイダ環境で必要な、さまざまな課金モデルに対応するように設計されています。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。

マルチテナントのダッシュボード/レポート

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ダッシュボードウィジェットが追加されます。
テナント関連のウィジェットの例

同じ情報を、「管理」→「テナント」画面（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、攻撃を受けている可能性があります。

チャージバックレポートには、さらに詳細な情報が含まれます（[イベントとレポート]セクション）。このレポートは、保護時間、現在のデータベースサイズ、コンピュータの台数（有効および無効）をテナントごとに示します。
マルチテナント (詳細)

データベースのユーザアカウントの設定

<table>
<thead>
<tr>
<th>注意:</th>
<th>SQL ServerとOracleとでは、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。</th>
</tr>
</thead>
<tbody>
<tr>
<td>複数のテナントが実行されるプロセス</td>
<td>データベースサーバ</td>
</tr>
<tr>
<td>單一のテナントのデータ</td>
<td>データベース</td>
</tr>
</tbody>
</table>

次のセクションでは、SQL ServerとOracleの両方にSQL Serverの用語を使用します。

SQL Server

マルチテナントを使用するには、ソフトウェアでデータベースを作成できる必要があるので、SQL Serverの`dbcreator`の役割が必要です。次に例を示します。

プライマリテナントのユーザの役割については、メインデータベースのDB所有者を割り当てることが重要です。
必要な場合は、権限を詳細に設定し、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。

$dbcreator$の役割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`サーバ役割のみが必要です。ユーザマッピングを定義する必要はありません。

**Oracle**

Oracleにおけるマルチテナントは、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与えられます。

Oracleでは、引用符で囲まれた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。OracleのWebサイトにある次のページで、引用符を使わない名前で使用可能な文字について説明しています。[http://docs.oracle.com/cd/B28359_01/server.111/b28286/sql_elements008.htm#SQLRF00223](http://docs.oracle.com/cd/B28359_01/server.111/b28286/sql_elements008.htm#SQLRF00223)

注意:  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）データベースから派生します。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）。メインデータベース名を短くすると、テナントのデータベース名が読み取りやすくなります。

マルチテナントを有効にする場合、Oracleの次の権限を割り当てる必要があります。
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。

---

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、テーブルスペースが基本的に空になります。設定は、プライマリユーザアカウントと同じです。

API

Deep Security Managerには、次の処理を実行するためのREST 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ーの管理

また、従来のSOAP APIに、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。

REST APIの詳細については、REST APIのドキュメントを参照してください。
アップグレード

アップグレードは、これまでのバージョンと変わりません。インストーラが実行され、既存のインストールが検出されます。次に、アップグレードオプションが表示されます。アップグレードが選択された場合、他のノードにシャットダウンするように通知してから、アップグレードの処理が開始されます。

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、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、残りのManagerノードで同じインストーラパッケージを実行します。

テナントのアップグレード中に問題が発生した場合は、テナントの状態 ([管理]→[テナント] 画面) が「データベースアップグレード失敗 (オフライン)」になります。テナントのインタ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。

テナントのサポート

プライマリテナントがテナントのユーザインタフェースにアクセスする必要がある場合があります。テナントリストとテナントプロパティの画面に、特定のテナントとして認証するオプションがあり、このオプションを使用すると、すぐに管理者アクセスが可能です。

ユーザは、接頭辞「support_」を使用する特殊なアカウントとしてログオンします。たとえば、プライマリテナントのユーザ「jdoe」が、テナントとしてログオンした場合、「Full Access」役割を持つ「support_jdoe」というアカウントが作成されます。サポートユーザがタイムアウトになるか、アカウントからログアウトすると、ユーザは削除されます。

テナントは、このユーザアカウントの作成、ログオン、ログアウト、および削除と、その他の操作をシステムイベントで確認できます。

プライマリテナントのユーザは、他にも次の診断ツールを使用できます。

1. [管理]→[システム情報] 画面には、テナントのメモリ使用量とスレッドの状態に関する追加情報が表示されます。この情報は、直接使用する以外に、トレンドマイクロのサポートに提供することもできます。

2. Managerノードのディスクにある`server0.log`には、ログの原因となったテナント (該当する場合はユーザ) の名前に関する追加情報が含まれます。この情報は、問題の原因特定に役立つ場合があります。

テナントが、GUIにないカスタム調整を行う必要がある場合があります。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。このような設定を変更するコマンドラインユーティリティは、次の引数を受けます。

`-Tenantname "account name"`

この引数を使用して、設定の変更や、その他のコマンドライン処理の対象として特定のテナントを指定できます。引数を省略した場合は、プライマリテナントに対して処理が実行されます。

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Manager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、このアドレスのリストを使用して、アクセスするノードをランダムに選択し、接続できるノードがなくなるまで (またはノードがすべてビジー状態になるまで) リスト内の残りのノードへのアクセスを続けると、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。これは、Managerノードの数が固定されている環境に適しており、可用性とスケーラビリティのためにManagerノードの前にロードバランサを設定する必要をなくします。

マルチテナント環境では、クラウド環境のオートスケーリング機能などを使用して、必要に応じてManagerノードを追加または削除する場合があります。このような場合、Managerを追加または削除すると、環境内のすべてのAgentとVirtual Applianceのアップデートが発生します。このアップデートを回避するために、ロードバランサの設定を使用できます。

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。

管理者ガイド マルチテナント (詳細)
いずれの場合も、ロードバランサは、セッションを維持するTCPのロードバランサとして設定します（SSL終端ではない）。この方法で、Agent/Virtual ApplianceとManagerの間で通信が最初から最後まで直接実行されます。次の接続は、別のノードに分散される可能性があります。

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vShieldコネクタをプライマリテナントに構成し、vCloud Connectorをテナントに構成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コンポーネントを確認でき、テナントでは、vCloud環境でテナントが所有する仮想マシンのみを確認できます。テナントでは、Agentを導入しなくてもこれらの仮想マシンを有効化できます。

このような環境を設定するには、[管理]→[システム設定]→[Agent]に進み、[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の統合の詳細については、インストールガイドを参照してください。

詳細な技術情報

各テナントデータベースには約100MB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、30秒〜4分程度かかります。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。
データセンター外部のコンピュータの保護

ここでは、Deep Securityを使用してモバイルノートパソコンなどのリモートコンピュータを保護する手順について説明します。次の手順に従ってください。

1. Managerにコンピュータを追加します。
   1. 個々のコンピュータを追加します。
   2. ネットワークに対する検出操作を実行します。
   3. Microsoft Active Directoryからコンピュータをインポートします。

2. Windowsノートパソコン用の新しいポリシーを作成します。
   1. 新規にポリシーを作成し、名前を付ける
   2. 監視対象のインタフェースを設定する
   3. ネットワークエンジンをインラインモードに設定する
   4. ファイアウォールルールにロケーション識別などを割り当て、ファイアウォールステートフル設定を有効にします。
   5. 侵入防御ルールを割り当てる
   6. セキュリティログ監視ルールを割り当てる
   7. 変更監視ルールを割り当てる

3. コンピュータにポリシーを適用します。

4. Managerを使用してアクティビティを監視します。

ここでは、ネットワーク全体のDeep Security Agentを管理するコンピュータにManagerがインストール済みであるものとします。また、保護するリモートコンピュータにもDeep Security Agentがインストールされている(有効化はされていない)ものとします。インストールが済んでいない場合は、インストール手順を参照して、ここで説明した状態にしてください。

Managerにコンピュータを追加する

Deep Securityの【コンピュータ】画面で、次のいずれかの方法でコンピュータを追加します。

1. IPアドレスまたはホスト名を指定して個々のコンピュータを追加する
2. ネットワークを検索してコンピュータを検出する
3. Microsoft Active Directoryに接続してコンピュータのリストをインポートする
4. VMware vCenterに接続してコンピュータのリストをインポートする（このセクションでは物理コンピュータを対象としているため、ここでは説明しません）

IPアドレスまたはホスト名を指定して個々のコンピュータを追加する

IPアドレスまたはホスト名を指定して個々のコンピュータを追加するには、【コンピュータ】画面に進み、ツールバーの【新規】をクリックします。

【ホスト名】テキストボックスに、追加するコンピュータのホスト名またはIPアドレスを入力します。追加したコンピュータが検出され、有効化されていないAgentが存在すると判断された場合、新規コンピュータウィザードで、そのコンピュータに適用するポリシーを指定することができます（ここではまだポリシーを選択しないでください）。【次へ】をクリックすると、ウィザードによってコンピュータが検出され、Agentが有効化されます。Agentの有効化が完了すると、ウィザードからコンピュータエディタ画面（詳細画面）を開くことができます。この画面でAgentのさまざまな設定ができます。ここでは【詳細】画面の説明は省略します。
ネットワークを検索してコンピュータを追加する（検出）

ネットワークを検索してコンピュータを検出するには

1. [コンピュータ] 画面に移動します。
2. [新規] → [検出] をクリックして、[コンピュータの検出] 画面を表示します。
3. コンピュータを検索するIPアドレスの範囲を入力します。マスクされているIPアドレスを入力しても、同じことがわかります。
4. [IPをホスト名に自動的に解決します] を選択して、Managerに検出の実行時にホスト名を自動的に解決するように指示します。
5. 検出されたコンピュータは、作成したコンピュータグループに追加することもできます。ここでは、[検出されたコンピュータをグループに追加] リストで [コンピュータ] が選択されている状態のままにします。
6. 最後に、[検出されたコンピュータにポート検索を自動実行します] チェックボックスをオフにします（ポート検索により、検出されたコンピュータ上で開いているポートが検出されます）。
7. [OK] をクリックします。画面が閉じ、ブラウザの下部のManagerのステータスバーに「検索実行中」と表示されます（検出プロセスをキャンセルするには、[X] をクリックします）。

数分後に、ネットワーク上のアクセス可能なすべてのコンピュータが検出され、そのうちDeep Security AgentがインストールされているコンピュータがManagerによって特定されます。これらのAgentはここで有効にする必要があります。

Microsoft Active Directoryからコンピュータをインポートする

Active Directoryからインポートされたコンピュータは、[コンピュータ] 画面内の他のコンピュータと同等に扱われます。

Microsoft Active Directoryからコンピュータをインポートするには

1. [コンピュータ] → [新規] → [ディレクトリの追加] をクリックし、ディレクトリの追加ウィザードを開始します。
2. Active Directoryサーバ名、Managerに表示されるインポートしたディレクトリの名前と説明（Active Directoryのものと同じでなくても可）、Active DirectoryサーバのIPとポート、アクセス方法と資格情報を入力します。[次へ] をクリックします。
   注意: [ユーザ名] フィールドのユーザ名には、ドメイン名を含める必要があります。
4. ディレクトリの追加ウィザードの2番目の画面で、スキーマの詳細を入力するよう求められます（初期設定値のままにします）。[完了] をクリックします。
5. 次の画面で、エラーが発生しなかったかどうかが通知されます。[次へ] をクリックします。
6. 最後の画面では、Managerの [コンピュータ] 画面を定期的にActive Directoryと同期する予約タスクを作成できます。ここでは、このオプションはオフのままにします。[閉じる] をクリックします。

これで、[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、[コンピュータ]の下に一覧表示されている通常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: 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のディレクトリ構造をActive Directoryサーバと同期します (この処理は、予約タスクとして自動化できます)。

Agentが有効になったので、ファイアウォールルールと侵入防御ルールを割り当てることができます。個々のセキュリティオブジェクトは個別にAgentに割り当てることができますが、共通のセキュリティオブジェクトをポリシーにグループ化してから、そのポリシーを1つまたは複数のAgentに割り当てた方が便利です。

メニューバーの[サポート]リンクをクリックすると、Deep Security Managerの各画面の詳しい説明を表示できます。

注意: メニューバーの[サポート]リンクをクリックすると、Deep Security Managerの各画面の詳しい説明を表示できます。

コンピュータ上のAgentを有効化する

ポリシーとルールを割り当てた後には、AgentがManagerによって「有効化」される必要があります。有効化プロセスには、AgentとManager間での一意のフィンガープリントの交換が含まれます。その結果、このDeep Security Managerのみ、またはその1つのノードのみがAgentに指示を送信することができます。

インストール時に有効化を自動的に開始するようにAgentを設定できます。詳細については、「コンピュータ上のAgentを手動で有効にするには、選択した1つ以上の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。」

注意: インストール時に有効化を自動的に開始するようにAgentを設定できます。詳細については、「コマンドラインユーティリティ(184ページ)」を参照してください。

Windowsノートパソコン用のポリシーを作成する

Agentを有効にしたら、次のコンピュータを保護するためのルールを割り当てます。コンピュータへ直接ルールを割り当てることもできますが、これらのルールを含むポリシーを作成して、複数のコンピュータへ割り当てる方が便利です。

ポリシーは、次のとおりに作成します。

1. 新規にポリシーを作成し、名前を付ける
2. 監視対象のインタフェースを設定する
3. ネットワークエンジンをインラインモードに設定する
4. ファイアウォールルールにロケーション識別などを割り当て、ステートフル設定を有効にする
5. 侵入防御ルールを割り当てる
6. 変更監視ルールを割り当てる
7. セキュリティログ監視ルールを割り当てる
8. コンピュータにポリシーを割り当てる
新規にポリシーを作成して名前を付ける

新規にポリシーを作成して名前を付けるには
1. 【ポリシー】に移動し、左側にあるナビゲーションパネルの【ポリシー】をクリックして【ポリシー】画面に移動します。
2. ツールバーの【新規】→【新規ポリシー】をクリックして、新規ポリシーウィザードを表示します。
3. 新規ポリシーの名前として「My New Laptop Policy」と入力し、【継承元：】メニューから【Base Policy】を選択します。【次へ】をクリックします。
4. 次の画面で、既存コンピュータの現在の設定に基づいてポリシーを作成するかどうかの確認を求められます。【はい】を選択すると、管理下の既存のコンピュータを1台選択するよう指示されます。ウィザードはその設定情報を使って取得し、それに基づいて新規ポリシーを作成します。これは、継続して調整されてきた既存コンピュータのセキュリティ設定を基にしてポリシーを作成し、機能的に似た別のコンピュータへ適用する場合に有用です。ここでは【いいえ】を選択して【次へ】をクリックします。
5. 最後の画面は、新しいポリシーが作成されたことを確認する画面です。【閉じる】で【ポリシー詳細】を開く】オプションを選択し、【閉じる】をクリックします。

監視対象のインタフェースを設定する

監視対象のインタフェースを設定するには
1. 【閉じる】で【ポリシー詳細】を開く】オプションを選択することで、新規ポリシーのエディタ画面が表示されます。
2. このポリシーを割り当てるノートパソコンには、2つのネットワークインタフェース（ローカルエリア接続とワイヤレス接続）が搭載されています。使用するインタフェースを考慮して、セキュリティ設定を調整します。ナビゲーションパネルで【インタフェースの種類】をクリックし、【ルールを特定のインタフェースに適用】オプションを選択します。ノートパソコンのインタフェース名と一致するよう、Agentが使用するインタフェースと文字列の名前を、ワイルドカードを使用して入力します。インタフェースの種類の欄で最初の2つに「LAN Connection」および「ローカルエリア接続 *」、「Wireless」および「ワイヤレスネットワーク接続 *」と入力します。画面の右下にある【保存】をクリックします。

ネットワークエンジンをインラインモードに設定する

ネットワークエンジンをインラインモードに設定するには
Agentの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します。インラインモードで動作する場合、実際のパケットストリームはネットワークエンジンを通じます。ステートフルテーブルは維持され、ファイアウォールルールは適用され、侵入防御ルールがバイロードコンテンツに適用されるようトラフィックの規範化が実行されます。タップモードで動作する場合、実際のパケットストリームはクローン化され、メインストリームを迂回して流れます。タップモードでは、実際のパケットストリームは変更されません。すべての操作はクローン化されたストリーム上で行われます。
ここでは、インラインモードでファイアウォールエンジンが動作するようにポリシーを設定します。

ネットワークエンジンをインラインモードに設定するために
1. 引き続き、My New Laptop Policyのエディタで【設定】に移動し、【ネットワークエンジン】タブを選択します。
2. ネットワークエンジンモードを【インライン】に設定します。ベースポリシーの初期設定モードを【インライン】に設定しており、新規のポリシーは初期設定を継承することから、すでに初期設定は【継承 (インライン)】に設定されています。

ファイアウォールルールにロケーション識別などを割り当て、ステートフル設定を有効にする

ファイアウォールルールを割り当てるには
1. ナビゲーションパネルの【ファイアウォール】をクリックし、【ファイアウォールの設定エリア、】【ファイアウォールルール】リストから【オン】を選択します。
2. 次に、このポリシーにいくつかの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ルールを割り当てます。[ファイアウォールルール]をクリックして、使用可能な定義済みファイアウォールルールのリストを表示します。独自にファイアウォールルールを作成することもできますが、この手順では既存ルールのリストから選択します。次の一連のファイアウォールルールを選択して、基本通信を許可します。

- Allow Solicited ICMP replies
- Allow solicited TCP/UDP replies
- Domain Client (UDP)
- ARP
- Wireless Authentication
- Windows File Sharing (Windowsファイル共有トラフィックの受信を許可する強制的な許可ルール)

ファイアウォールルールのチェックボックスの横に、灰色の下矢印があります。これらは、前の手順で複数のインタフェースを定義した場合に表示されます。これにより、ファイアウォールルールをコンピュータ上の全インタフェースに対して適用するか、または指定したインタフェースのみに適用するかを特定できます。ここでは、初期設定のままにします。

[保存]ボタンをクリックします。

Windowsファイル共有を許可するファイアウォールルールを割り当てました。Windowsファイル共有は非常に便利なWindowsの機能の1つですが、セキュリティ上の問題があります。保護されているオフィス環境でノートパソコンを使用するときのみこの機能を利用し、オフィスから持ち出したときは利用しないよう、制限することを推奨します。このポリシーを実装するために、このポリシーともにファイアウォールルールを使用するときは、ロケーション識別を適用します。

ロケーション識別を実装するには


2. [プロパティ] 画面で [オプション] タブをクリックします。

3. コンテキストエリアで、リストから [新規] を選択します。この操作により、[新規コンテキスト] プロパティ画面が表示されます。ノートパソコンがドメインコントローラへローカルアクセスできる場合にのみファイアウォールルールを有効化するルールコンテキストを作成します(つまり、ノートパソコンがオフィス内にある場合です)。

4. 新規ルールコンテキストに「In the Office」と名前を付けます。[オプション] エリアで、[接続が次の場合にコンテキストを適用:] オプションを選択し、その下にある [ドメインとのローカル接続] を選択します。次に、[OK] をクリックします。


これで、ノートパソコンがWindowsドメインコントローラへローカルアクセスできる場合のみ、Windows File Sharingファイアウォールルールは有効になります。Windows File Sharingファイアウォールルールは、ポリシーの [詳細] 画面内に太字で表示されるようになりました。これは、ファイアウォールルールのプロパティがこのポリシーに対してのみ編集されたことを示しています。

注意: 侵入防御ルールでもロケーション識別を使用できます。

ファイアウォールセクションの最後の手順は、ステートフルインスペクションを有効にすることです。

ステートフルインスペクションを有効にするには

1. 引き続き、My New Laptop Policyポリシーのエディタ画面で、[ファイアウォール]→[一般]→[ファイアウォールステートフル設定]の順に選択します。

2. [グローバル (すべてのインタフェース)] 設定で [Enable Stateful Inspection] を選択します。

3. [保存] をクリックして終了します。
侵入防御ルールを割り当てる

ポリシーやに侵入防御ルールを割り当てるには

1. 引き続き、My New Laptop Policyのエディタ画面で、ナビゲーションパネルの[侵入防御]をクリックします。

注意：侵入防御ルールは、ネットワークエンジンがタップモードではなくインラインモードで動作しているときのみ、防衛モードまたは検出モードのいずれかに設定できます。検出モードは、新規侵入防御ルールが正常に動作するかどうかを確認するためにトラフィックを破棄されるのを回避する場合に便利です。検出モードでは、通常は破棄されるトラフィックもイベントを生成した上で通過することができます。侵入防御を[オン]に設定します。

注意：[推奨設定]エリアについて説明します。Deep Security Agentを推奨設定の検索を実行するよう指示できます。これには、Managerの[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]→[推奨設定の検索]を選択します。推奨設定エンジンは、コンピュータでアプリケーションを検索し、検索結果に対して侵入防御ルールの推奨を適用します。推奨設定の検索結果は、コンピュータエディタ画面で表示できます。表示するには、[推奨設定]→[現在割り当てられている侵入防御ルール]→[割り当て/割り当て解除]の順に選択し、2番目のドロップダウンフィルタメニューから[割り当てを推奨]を選択します。

3. ここでは、[推奨設定]→[推奨設定の推奨設定を自動的に適用 (可能な場合;)]オプションを[継承 (いいえ)]に設定します。
4. [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。
5. 侵入防御ルールは、アプリケーションの種類別に整理されます。アプリケーションの種類をプロパティは、通信方向、プロトコル、ポートの3つしかないため、侵入防御ルールをグループ化するのに便利です。ノートパソコンの新規ポリシーで、次のアプリケーションの種類を割り当てます。
   - Mail Client Outlook
   - Mail Client Windows
   - Malware
   - Malware Web
   - Microsoft Office
   - Web Client Common
   - Web Client Internet Explorer
   - Web Client Mozilla Firefox
   - Windows Services RPC Client
   - Windows Services RPC Server

注意：最初の2つのリストフィルタメニューが[すべて]に設定され、3番目のソートフィルタメニューが[アプリケーションの種類別]に設定されていることを確認してください。[ルール]リスト内を右クリックして[すべて折りたたむ]を選択すると、アプリケーションの種類を確認しやすくなります。アプリケーションの種類と侵入防御ルールは多数あるため、画面の右下にあるレイアウトコントロールを使用してすべてを確認するか、または画面の右上にある検索機能を使用します。アプリケーションの種類を選択するには、アプリケーションの種類の名前の横にあるチェックボックスをオンにします。

注意：侵入防御ルールの一部は、他のルールに依存します。別のルールとともに割り当てる必要があるルールを割り当てる場合、別ルールを割り当てていないと、必要なルールを割り当てるよう促すポップアップ画面が表示されます。

注意：さまざまなルールをコンピュータに割り当てるとき、使用可能なルールすべてを割り当て、「過度の保護状態」にしないように注意してください。ルールは、さまざまなOS、システム、アプリケーション、脆弱性に対応するよう設計されているため、使用中のコンピュータに対して適切であるとは限りません。トラフ...
イックフィルタリングエンジンは、発生する可能性のないパターンの検索を実行して、CPU時間を無駄に消費する可能性があります。コンピュータの保護に関しては、保護項目を十分に検討してください。

6. [OK] をクリックし、[保存] をクリックして、ポリシーにアプリケーションの種類を割り当てます。

変更監視ルールを割り当てる

ポリシーに変更監視ルールを割り当てるには

1. 引き続き、My New Laptop Policyのエディタ画面で、ナビゲーションパネルの [変更監視] をクリックします。
3. [変更監視ルールの推奨設定を自動的に適用 (可能な場合):] を [いいえ] に設定します。
4. 次に、[現在割り当てられている変更監視ルール] エリアの [割り当て/割り当て解除] をクリックします。
5. 画面の右上部にある [検索] ボックスに、「Windows」と入力して <Enter> キーを押します。Microsoft Windowsに適用されるすべてのルールがルールリストに表示されます。ルールのいずれかを右クリックして [すべて選択] を選択し、次にもう一度右クリックして [ルールの割り当て] を選択します。これにより、検索結果として検出されたすべてのルールがこのポリシーに割り当てられます。

セキュリティログ監視ルールを割り当てる

ポリシーにセキュリティログ監視ルールを割り当てるには

1. 引き続き、My New Laptop Policyのエディタ画面で、ナビゲーションパネルの [セキュリティログ監視] をクリックします。
2. [継承] オプションの選択を解除して、[セキュリティログ監視] を [オン] に設定します。
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):] を [いいえ] に設定します。
4. 次に、[現在割り当てられているセキュリティログ監視ルール] エリアの [割り当て/割り当て解除] をクリックします。
5. 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 [1002792 - Default Rules Configuration] ルールと、[1002795 - Microsoft Windows Events] ルールを選択します。この結果、Windowsの監査機能がノートパソコンにイベントを登録するたびに、イベントがログに記録されるようになります。
6. [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。

これで、新規ポリシーの編集が終了しました。My New Laptop Policyの [詳細] 画面を閉じてください。

ドメインコントローラのIPリストを編集する

最後に、新規ポリシーには「ドメインコントローラ」IPリストを使用する3つのファイアウォールルールが含まれているので、ローカルのWindowsドメインコントローラのIPアドレスをIPリストに含めるよう編集します。

ドメインコントローラIPリストを編集するには

1. Deep Security Managerコンソールのメイン画面で、[ポリシー]→[共通オプジェクト]→[IPリスト] の順に選択します。
2. [Domain Controller(s)] のIPリストをダブルクリックし、[プロパティ] 画面を表示します。
3. ドメインコントローラのIPを入力します。
4. [OK] をクリックします。
コンピュータにポリシーを適用する

コンピュータにポリシーを適用できるようになりました。

コンピュータにポリシーを適用するには
1. [コンピュータ]画面に移動します。
2. ポリシーを適用するコンピュータを右クリックして、[処理]→[ポリシーの割り当て]の順に選択します。
4. [OK]をクリックします。

[OK]をクリックすると、ManagerがそのポリシーをAgentに送信します。コンピュータの[ステータス]列とManagerのステータスバーに、Agentがアップデート中であるというメッセージが表示されます。

コンピュータ上のAgentがアップデートされると、[ステータス]列に「管理対象 (オンライン)」と表示されます。

SMTP設定を設定する

Deep Security ManagerのSMTP設定を設定すると、ユーザにアラートメールが送信されます。

SMTP設定の設定方法は、次のとおりです。
1. [管理]→[システム設定]へ進み、[SMTP]タブを選択します。
2. 設定情報を入力して[SMTP設定のテスト]をクリックし、Deep Security Managerがメールサーバと通信できるか確認します。
3. [アラート]タブに移動します。
4. [アラートイベント転送 (Managerから)]で、通知先として初期設定のメールアドレスを入力します。
5. [保存]をクリックします。

注意: ユーザがアラートメールを受け取るかどうかは、[管理]→[ユーザ管理]→[ユーザ]の順に選択して、ユーザの[プロパティ]画面で設定できます。特定のアラートでメール通知をする場合は、アラートの[プロパティ]画面で設定できます。

Managerを使用してアクティビティを監視する

ダッシュボード

コンピュータにポリシーを割り当てて、一定期間稼働した後で、そのコンピュータの処理を確認する場合があります。処理の確認で最初に開くのは、ダッシュボードです。ダッシュボードには、Deep Security Managerと管理対象のコンピュータの状態にかかわる、さまざまな種類の情報パネル（「ウィジェット」）があります。

ダッシュボード画面の右上にある[ウィジェットの追加/削除]をクリックして、表示可能なウィジェットのリストを表示します。

ここでは、[ファイアウォール]セクションから次のウィジェットを追加します。

- ファイアウォールコンピュータのアクティビティ (防御)
- ファイアウォールイベント履歴 [2x1]
- ファイアウォールIPのアクティビティ (防御)

3つのウィジェットの横にあるチェックボックスをそれぞれ選択して、[OK]をクリックします。ダッシュボードにウィジェットが表示されます。データが生成されるまで、しばらく時間がかかります。
ウィジェットは、拒否されたパケットの数とともに、パケットが拒否される最も一般的な理由、つまりそのコンピュータ上のAgentによってコンピュータへの接続がブロックされた理由のリストを表示します。このリストの項目は、パケット拒否またはファイアウォールルールのいずれかの種類になります。それぞれの「理由」は、その拒否パケットに対応するログへリンクされています。

ウィジェットは、選択されたビューに応じて、過去24時間以内または7日間以内にブロックされたパケットの数を棒グラフで表示します。棒グラフをクリックすると、その棒が表す期間に対応したログが表示されます。

ウィジェットは、拒否パケットの最も一般的なソースIPのリストを表示します。ウィジェットと同様に、各ソースIPは、対応するログへリンクされています。

ウィジェットの数値の横には、推移を表すインジケータがあります。上向きまたは下向きの三角形は指定期間における全体の増減を示し、横線は大きな変更がなかったことを示します。

パケット拒否のその他の理由については、以下を参照してください。

ファイアウォールおよび侵入防御イベントのログ

次に、拒否パケットの最も多い理由に対応するログへドリルダウンします。ウィジェットで、拒否されたパケットの最も多い理由をクリックします。クリックすると、ウィジェット画面に移動します。

ウィジェット画面には、ファイアウォールイベントがすべて表示されます。ウィジェットにある一番の理由（「ポリシーで未許可」）は、[理由]列エントリに対応します。ログは、過去24時間または7日間のダッシュボードの表示期間中に発生したイベントのみを表示するようフィルタされています。ウィジェットと[侵入防御イベント]画面の詳細は、これらの画面のヘルプページを参照してください。

レポート

ログデータの表示には、通常、より高度で要約された情報を簡単に理解できるようにすることが求められます。レポートはこうした役割を担い、コンピュータ、ファイアウォールおよび侵入防御イベントログ、イベント、アラートなどの詳細な概要を表示します。

ここでは、指定した期間のファイアウォールルールやファイアウォールステートフル設定処理の記録を表示するファイアウォールレポートを生成します。[レポート]ドロップダウンから[ファイアウォールレポート]を選択します。[生成]をクリックして、新しい画面でレポートを開きます。

Deep Security Managerからユーザにメール送信された定期レポートを確認する、システムログインしてダッシュボードを調べる、特定のログをドリルダウンして詳細な調査を実行する、重要イベントを通報するようなアラートを設定するなどの操作を行うことで、ネットワークの最新の状態やステータスを把握することができます。

関連項目:

- ポリシー、継承、およびオーバーライド (292ページ)
多要素認証 (MFA)

Deep Security Managerでは、多要素認証 (MFA) を使用することができます。MFAを有効にした場合、Deep Security Managerへのログオン時に次の情報を指定する必要があります。

- ユーザ名とパスワード
- MFAデバイス (携帯電話など) から発行された認証コード

多要素認証の有効化

MFAを有効にするには

1. Deep Security Managerで、画面右上のユーザ名をクリックし、【ユーザプロパティ】をクリックします。

2. 【多要素認証 (MFA)】で 【MFAの有効化】をクリックします。「多要素認証の有効化」ウィザードが開きます。ウィザードの指示に従って作業を進めてください。

3. ウィザードの最初の画面で、互換性のある仮想MFAアプリケーション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。お使いのスマートフォンに対応したMFAアプリケーションをスマートフォンのアプリケーションストアからインストールします。スマートフォン向けMFAアプリケーションは、それぞれの機種固有のアプリケーションストアからインストールできます。Deep Security Managerでは、次の組み合わせがサポートされます。
   - Android: Google Authenticator、Duo
   - iPhone: Google Authenticator、Duo
4. QRコードの読み取りに対応したデバイスの場合は、カメラで読み取ってMFAアプリケーションを設定します。QRコードを使用できない場合は、[QRコードの読み取りに対応していなかったため、手動設定用の秘密鍵を表示する]を選択すると、MFAアプリケーションに入力するコードが表示されます。[次へ]をクリックします。

5. デバイスの画面上部のDeep Securityと下部のユーザ名の間に、Deep Security用の認証コードが次のように表示されます。
6. ウィザードで、MFAアプリケーションから発行されたDeep Security用認証コードをスペースなしで入力し、[完了]をクリックします。

7. 認証コードが正しければアカウントでMFAが有効になり、Deep Security Managerへの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。

多要素認証の無効化

自分のアカウントのMFAを無効にするには


2. [多要素認証 (MFA)]で [MFAの無効化]をクリックします。確認画面で [OK]をクリックしてMFAを無効にします。
3. 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] をクリックします。

デバイスを紛失した他の管理者のMFAを無効にするには

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. 管理者の名前を選択し、[プロパティ] をクリックします。

dsm_c -unlockoutコマンドでも、自分または他のユーザのMFAを無効にすることができます。詳細については、「コマンドラインユーティリティ (184ページ)」を参照してください。

MFAを使用したDeep Security Managerへのログオン

MFAを使用してログオンするには

2. MFAデバイスで、有効な認証コードを取得します。

注意: Deep Security Managerではログオンの試行回数に上限があり、失敗した回数が上限を超えるとユーザはロックアウトされます。無効なMFAコードを入力した場合もログオンの失敗としてカウントされます。
参照
詳細なログ記録ポリシーモード

ログ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設定することができます。モードは、[設定]→[ネットワークエンジン]→[ネットワークエンジンの詳細設定]エリアの、ポリシーまたはコンピュータエディタで設定できます。

次の表は、より複雑である詳細なログ記録ポリシーモードのうちの4つで、どのイベントのタイプが無視されるかを一覧表示しています。

<table>
<thead>
<tr>
<th>モード</th>
<th>無視するイベント</th>
</tr>
</thead>
<tbody>
<tr>
<td>ステートフルおよび正規化の抑制</td>
<td>セッション情報なし、不正なフラグ、不正なシークエンス、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、再送の破棄</td>
</tr>
<tr>
<td>ステートフル、正規化、およびフラグメントの抑制</td>
<td>セッション情報なし、不正なフラグ、不正なシークエンス、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</td>
</tr>
<tr>
<td>ステートフル、フラグメント、および検証機能の抑制</td>
<td>セッション情報なし、不正なフラグ、不正なシークエンス、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</td>
</tr>
<tr>
<td>モード</td>
<td>無視するイベント</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6パケット</td>
<td>受信接続の上限                  各接続の上限                  SYN送信の上限</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>不正なデータオフセット              未定義                         未定義</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>読み取り不能なIPv4ヘッダ             不正なIPバージョン               ACK再送の上限</td>
</tr>
<tr>
<td></td>
<td>ACK再送の上限                      切断された接続上のパケット       再送の破棄</td>
</tr>
<tr>
<td>タップモード</td>
<td>セッション情報なし                  不正なフラグ                   不正なシーケンス</td>
</tr>
<tr>
<td></td>
<td>不正なACK                            未定義                         未定義</td>
</tr>
<tr>
<td></td>
<td>送信元および送信先IPが同一            切断された接続上のパケット       再送の破棄</td>
</tr>
</tbody>
</table>
コマンドラインユーティリティ

Deep Security Agent
dsa_control

使用方法


- **-a <str>, --activate=<str>**: 指定されたURLのManagerに対してAgentを有効化します。URLの形式は必ず「dsm://」ホストまたはIP:ポート/」にしてください。ポートはManagerのハートビートポート (初期設定では4120) です。
- **-b, --bundle**: アップデートバンドルを作成します。
- **-c <str>, --cert=<str>**: 証明書ファイルを特定します。
- **-d, --diag**: Agentの診断パッケージを生成します。
- **-g <str>, --agent=<str>**: AgentのURLです。初期設定は「https://localhost:4118/」です。
- **-m, --heartbeat**: Managerに今すぐ接続するようにAgentに指示します。
- **-p <str>, --passwd=<str>**: 認証パスワードです。パスワードの入力を求めるプロンプトを表示するには、「*」を指定します。「-p」パラメータに続けて、パスワードを入力します。「-p」パラメータの後に「*」を指定すると、Enterキーを押した後でパスワードの入力を求めるプロンプトが表示されます。パスワードは、1文字入力するごとに「*」で置き換えられ (隠され) ます。
- **-r, --reset**: Agentの設定をリセットします。
- **-R <str>, --restore=<str>**: 隔離ファイルを復元します。
- **-s <num>, --selfprotect=<num>**: 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、または制御を拒否することによって、Agentのセルフプロテクションを有効にします。セルフプロテクションが有効な場合、コマンドラインの命令に認証パスワードを含める必要があります (1: 有効、0: 無効)。この機能はWindows版でのみ使用できます。
- **--buildBaseline**: 変更監視のベースラインを構築します。
- **--scanForChanges**: 変更監視の変更を検索します。

注意：

[コンピュータ] 面でコンピュータを右クリックして、「処理」→「有効化/再有効化」の順に選択すると、Deep Security Managerから手動でAgentを有効化できます。
Deep Security Agentでは、ローカルで実行する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できます。これは、Deep Securityのインストール環境に多数のコンピュータを追加するため、有効化プロセスを自動化するスクリプトを記述する場合に便利です。

注意：Agentからのリモート有効化を実行するには、[管理]→[システム設定]→[Agent]タブの[Agentからのリモート有効化を許可]オプションを有効にする必要があります。

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。

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使用することもできます（以下の使用可能なパラメータの表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:値のペアの数制限はありませんが、キー:値のそれぞれのペアは空白文字で区切る必要があります。次に一部の例を示します。

dsa_control -a dsm://sec-op-john-doe-3:4120/ hostname:ABCwebserver12 "description:Long Description With Spaces" (引用符が必要なのは、空白文字または特殊文字が値に含まれる場合のみです)

プロキシサーバを経由した、プライベートネットワーク上でのAgentからのリモート有効化

プライベートネットワーク上のAgentは、AgentからのDeep Security Managerとの通信を、プロキシサーバ経由で実行できます。

プロキシサーバを経由したプライベートネットワーク上でのAgentからのリモート有効化を許可するには

1. Deep Security Managerで、[管理]→[システム設定]→[Agent]画面に進みます。
2. [Agentからのリモート有効化]エリアで次の手順を実行します。
   - [Agentからのリモート有効化を許可]を選択します。
   - [Agentによるホスト名指定を許可]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]のリストから、[同じ名前で新規コンピュータを有効化]を選択します。
3. [保存]をクリックします。
Agentがプロキシサーバ経由でDeep Security Managerと通信するように設定するには、次のコマンドラインオプションを使用します。

<table>
<thead>
<tr>
<th>コマンド</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsa_control -x &quot;dsm_proxy://&lt;プロキシサーバのURL&gt;&quot;</td>
<td>AgentがManagerとの通信に使用するプロキシサーバのアドレスを設定します。</td>
</tr>
<tr>
<td>dsa_control -x &quot;&quot;</td>
<td>プロキシサーバのアドレスをクリアします。</td>
</tr>
<tr>
<td>dsa_control -u &quot;&lt;ユーザ名:パスワード&gt;&quot;</td>
<td>プロキシサーバのユーザ名とパスワードを設定します。</td>
</tr>
<tr>
<td>dsa_control -u &quot;&quot;</td>
<td>プロキシサーバのユーザ名とパスワードをクリアします。</td>
</tr>
</tbody>
</table>

例

```
dsa_control -x "dsm_proxy://172.21.3.184:808/"
```

プロキシサーバのアドレスとしてIPv4を使用します。

```
dsa_control -x "dsm_proxy://winsrv2k3-0:808/"
```

プロキシサーバのアドレスとしてホスト名を使用します。

```
dsa_control -x "dsm_proxy://[fe80::340a:7671:64e7:14cc]:808/"
```

プロキシサーバのアドレスとしてIPv6を使用します。

```
dsa_control -u "root:Passw0rd!"
```

プロキシの認証に、「root」とパスワード「Passw0rd!」を使用します (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)。

Agentからのリモート有効化を行うには、最初にプロキシ設定コマンドを発行し、次にAgentからのリモート有効化のコマンドを発行する必要があります。プロキシサーバのアドレスと認証情報の設定、およびAgentの有効化を実行する一連のコマンドの例を次に示します。

```
dsa_control -x "dsm_proxy://172.21.3.184:808/"
dsa_control -u "root:Passw0rd!"
```

Deep Security Managerで必要な設定

Agentからのハートビート有効化コマンド（「dsa_control -m」）


次の表は、有効化コマンドとハートビートコマンドで使用できるパラメータを一覧表示しています。有効化でしか使用できないパラメータや、ハートビートでしか使用できないパラメータもあります。

<table>
<thead>
<tr>
<th>キー</th>
<th>説明</th>
<th>例</th>
<th>有効化中の実行</th>
<th>有効化後のハートビート中の実行</th>
<th>値の形式</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>「説明」の値を設定します。</td>
<td>&quot;description:ホストの追加情報&quot;</td>
<td>可</td>
<td>可</td>
<td>文字列</td>
<td>最大2000文字。</td>
</tr>
<tr>
<td>displayname</td>
<td>「表示名」の値を設定します(ホスト名の横にカッコで囲んで表示されます)</td>
<td>&quot;displayname:名前&quot;</td>
<td>可</td>
<td>可</td>
<td>文字列</td>
<td>最大2000文字。</td>
</tr>
<tr>
<td>externalid</td>
<td>externalid値を設定します</td>
<td>&quot;externalid:123&quot;</td>
<td>可</td>
<td>可</td>
<td>整数</td>
<td>この値を使用して、Agentを一意に識別できます。この値には、SOAP WebサービスAPIを使用してアクセスできます。</td>
</tr>
<tr>
<td>group</td>
<td>コンピュータの所属するコンピュータ画面のグ</td>
<td>&quot;group:Zone A/WebServers&quot;</td>
<td>可</td>
<td>可</td>
<td>文字列</td>
<td>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。スラッシュ（&quot;/&quot;）はグループの階層を示します。</td>
</tr>
<tr>
<td>キー</td>
<td>説明</td>
<td>例</td>
<td>有効化後のハートビット中の実行</td>
<td>備考</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>---</td>
<td>--------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>group</strong></td>
<td>ループを設定します。</td>
<td>groupid:33</td>
<td></td>
<td>(備考はありません)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **hostname** | | hostname:ABWebServer1 | | 最大254文字。
| | | | hostnameには、Deep Security Managerの【コンピュータ】リストに含まれるコンピュータへの接続に最も適したIPアドレス、ホスト名、またはFQDNを指定します。 |
| **policy** | | policy:ポリシー名 | | 最大254文字。
| | | | 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。 |
| | | | 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ライドします。 |
| **policyid** | | policyid:12 | | (備考はありません) |
| **relaygroup** | コンピュータを特定のRelayグループにリンクします。 | relaygroup:カスタムRelayグループ | | (備考はありません) 
<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す。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。 |
| | | | 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。 |
| <strong>relaygroupid</strong> | | relaygroupid:123 | | (備考はありません) |
| <strong>relayid</strong> | | relayid:123 | | (備考はありません) |
| <strong>tenantIDおよびtenantPassword</strong> | | tenantID:12651ADC-D4D5およびtenantPassword:8601626D-56EE | | 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tenantPasswordの両方が必要です。tenantIDとtenantPassword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。 |
| <strong>RecommendationScan</strong> | コンピュータに対する推奨設定の検索を開始します。 | RecommendationScan:true | | (備考はありません) |</p>
<table>
<thead>
<tr>
<th>キー</th>
<th>説明</th>
<th>例</th>
<th>有効化後のハートビット中の実行</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpdateComponent</td>
<td>セキュリティアップデート処理を実行するように Deep Security Managerに指示します。</td>
<td>&quot;UpdateComponent:true&quot;</td>
<td>不可</td>
<td>論理値（備考はありません）</td>
</tr>
<tr>
<td>RebuildBaseline</td>
<td>コンピュータに変更監視ベースラインを再構築します。</td>
<td>&quot;RebuildBaseline:true&quot;</td>
<td>不可</td>
<td>論理値（備考はありません）</td>
</tr>
<tr>
<td>UpdateConfiguration</td>
<td>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。</td>
<td>&quot;UpdateConfiguration:true&quot;</td>
<td>不可</td>
<td>論理値（備考はありません）</td>
</tr>
<tr>
<td>AntiMalwareManualScan</td>
<td>コンピュータで不正プログラムの手動検索を開始します。</td>
<td>&quot;AntiMalwareManualScan:true&quot;</td>
<td>不可</td>
<td>論理値（備考はありません）</td>
</tr>
<tr>
<td>AntiMalwareCancelManualScan</td>
<td>コンピュータで現在実行中の不正プログラムの手動検索をキャンセルします。</td>
<td>&quot;AntiMalwareCancelManualScan:true&quot;</td>
<td>不可</td>
<td>論理値（備考はありません）</td>
</tr>
<tr>
<td>IntegrityScan</td>
<td>コンピュータで変更の検索を開始します。</td>
<td>&quot;IntegrityScan:true&quot;</td>
<td>不可</td>
<td>論理値（備考はありません）</td>
</tr>
</tbody>
</table>

**dsa_query**

dsa_queryツールは次の情報を提供します。

- 各コンポーネントのライセンスのステータス
- 検索の進捗状況
- 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情報

**使用方法**

dsa_query [-c <str>] [-p <str>] [-r <str>]

管理者ガイド

コマンドラインユーティリティ
• -p, --passwd <文字列> 認証パスワードです。Agentのセルフプロテクションが有効な場合は必須です。

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。

• -c, --cmd <文字列> ds_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。
  ◦ "GetHostInfo": ハートビート中にDeep Securityに返されるIDを照会します。
  ◦ "GetAgentStatus"; 有効な保護モジュールと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。

• -r, --raw <文字列>: 「-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rawデータ形式で出力します。

pattern: 結果をフィルタするためのワイルドカードのパターン (オプション)。

例:
dsa_query -c "GetComponentInfo" -r "au" "AM*"

Deep Security Manager
dsm_c

使用方法
dsm_c -action 処理名

<table>
<thead>
<tr>
<th>処理名</th>
<th>説明</th>
<th>使用方法</th>
</tr>
</thead>
<tbody>
<tr>
<td>createinsertstatements</td>
<td>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</td>
<td>dsm_c -action createinsertstatements [-file ファイルパス] [-generateDDL] [-databaseType sqlserver</td>
</tr>
<tr>
<td>diagnostic</td>
<td>システム用の診断パッケージを作成します</td>
<td>dsm_c -action diagnostic</td>
</tr>
<tr>
<td>fullaccess</td>
<td>管理者にFull Accessの役割を与えます</td>
<td>dsm_c -action fullaccess -username ユーザ名 [-tenantname テナント名]</td>
</tr>
<tr>
<td>reindexhelp</td>
<td>ヘルプシステムのインデックスを再作成します</td>
<td>dsm_c -action reindexhelp</td>
</tr>
<tr>
<td>resetcounters</td>
<td>カウンタテーブルをリセットします (空の状態に戻します)</td>
<td>dsm_c -action resetcounters [-tenantname テナント名]</td>
</tr>
<tr>
<td>resetevents</td>
<td>イベントテーブルをリセットします (空の状態に戻します)</td>
<td>dsm_c -action resetevents -type all</td>
</tr>
<tr>
<td>setports</td>
<td>Deep Security Managerのポートを設定します</td>
<td>dsm_c -action setports [-managerPort ポート] [-heartbeatPort ポート]</td>
</tr>
<tr>
<td>trustdirectorycert</td>
<td>ディレクトリの証明書を信頼します</td>
<td>dsm_c -action trustdirectorycert -directoryaddress ディレクトリアドレス -directoryport ディレクトリポート [-username ユーザ名] [-password パスワード] [-tenantname テナント名]</td>
</tr>
<tr>
<td>unlockout</td>
<td>ユーザアカウントをロック解除します</td>
<td>dsm_c -action unlockout -username ユーザ名 [-newpassword 新規パスワード] [-disablemfa] [-tenantname テナント名]</td>
</tr>
<tr>
<td>addregion</td>
<td>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</td>
<td>dsm_c -action addregion -region リージョン -display 表示文字列 -endpoint エンドポイント</td>
</tr>
</tbody>
</table>

注意: 管理者ガイド コマンドラインユーティリティ

189
<table>
<thead>
<tr>
<th>コマンド</th>
<th>効果</th>
<th>コマンドの実行例</th>
</tr>
</thead>
<tbody>
<tr>
<td>listregions</td>
<td>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</td>
<td>dsm_c -action listregions</td>
</tr>
<tr>
<td>removeregion</td>
<td>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</td>
<td>dsm_c -action removeregion -region リージョン</td>
</tr>
<tr>
<td>addcert</td>
<td>信頼された証明書を追加します</td>
<td>dsm_c -action addcert -purpose 目的 -cert 証明書</td>
</tr>
<tr>
<td>listcerts</td>
<td>信頼された証明書を一覧表示します</td>
<td>dsm_c -action listcerts [-purpose 目的]</td>
</tr>
<tr>
<td>removecert</td>
<td>信頼された証明書を削除します</td>
<td>dsm_c -action removecert -id ID</td>
</tr>
</tbody>
</table>
コンピュータおよびAgentのステータス


コンピュータの状態

<table>
<thead>
<tr>
<th>コンピュータの状態</th>
<th>説明</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>検出済み</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>非管理対象</td>
<td>このDeep Security Managerによって管理されておらず、有効化されていないため、有効化されるまで通信できません。</td>
<td></td>
</tr>
<tr>
<td>管理対象</td>
<td>Agentが存在し、保護中または管理対象の保護を提供しています。</td>
<td></td>
</tr>
<tr>
<td>アップデート中</td>
<td>Agent/Applianceは、設定のアップデートまたはセキュリティアップデートを実行中です。</td>
<td></td>
</tr>
<tr>
<td>アップデートの保留中(スケジュール)</td>
<td>コンピュータのアクセススケジュールで可能となった時点で、設定のアップデートまたはセキュリティアップデートをAgent/Applianceで実行します。</td>
<td></td>
</tr>
<tr>
<td>アップデートの保留中(ハートビート)</td>
<td>次回のハートビート時にアップデートが実行されます。</td>
<td></td>
</tr>
<tr>
<td>アップデートの保留中(オフライン)</td>
<td>Managerは現在Agent/Applianceと通信できません。Agent/Applianceが再びオンラインになったときにアップデートを実行する準備ができています。</td>
<td></td>
</tr>
<tr>
<td>オープンポートの検索中</td>
<td>Managerがコンピュータのオープンポートを検索しています。</td>
<td></td>
</tr>
<tr>
<td>有効化中</td>
<td>ManagerがAgent/Applianceを有効化しています。</td>
<td></td>
</tr>
<tr>
<td>有効化中(遅延)</td>
<td>関連するイベントベースタスクで指定時間後に有効化される。</td>
<td></td>
</tr>
<tr>
<td>有効化済み</td>
<td>Agent/Applianceを有効化しました。</td>
<td></td>
</tr>
<tr>
<td>無効化の実行中</td>
<td>ManagerがAgent/Applianceを無効化しています。</td>
<td></td>
</tr>
<tr>
<td>無効化の保留中(ハートビート)</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>検出済み</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>検出済み(予測)</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>Agentのアップグレード中</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>推奨設定の検索中</td>
<td>推奨設定の検索が進行中です。</td>
<td></td>
</tr>
<tr>
<td>推奨設定の検索の保留中(スケジュール)</td>
<td>コンピュータのアクセススケジュールで可能となったときに推奨設定の検索が開始されます。</td>
<td></td>
</tr>
<tr>
<td>推奨設定の検索の保留中(ハートビート)</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>推奨設定の検索の保留中(オフライン)</td>
<td>Agent/Applianceが現在オンラインです。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。</td>
<td></td>
</tr>
<tr>
<td>変更の検索の保留中</td>
<td>Agent/Applianceが現在オンラインです。通信が再度確立されると、Managerが変更の検索を開始します。</td>
<td></td>
</tr>
<tr>
<td>変更の検索の保留中(オフライン)</td>
<td>Agent/Applianceが現在オンラインです。通信が再度確立されると、Managerが変更の検索を開始します。</td>
<td></td>
</tr>
<tr>
<td>変更の検査の保留中(オフライン)</td>
<td>Agent/Applianceが現在オンラインです。通信が再度確立されると、Managerが変更の検査を開始します。</td>
<td></td>
</tr>
<tr>
<td>ベースライン再構築の保留中</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>ベースライン再構築の実行中</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>ベースライン再構築の目的(オフライン)</td>
<td>Agent/Applianceが現在オンラインです。Managerとこのコンピュータ間の通信が再度確立されるとき、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。</td>
<td></td>
</tr>
<tr>
<td>ステータスの確認</td>
<td>Agent/Applianceの状態を確認しています。</td>
<td></td>
</tr>
<tr>
<td>イベントの取得</td>
<td>ManagerがAgent/Applianceからイベントを取得しています。</td>
<td></td>
</tr>
</tbody>
</table>
### コンピュータの状態

<table>
<thead>
<tr>
<th>状態</th>
<th>説明</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>準備完了</td>
<td>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）。</td>
<td>ESXi</td>
</tr>
<tr>
<td>準備が完了</td>
<td>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）。</td>
<td>ESXi</td>
</tr>
<tr>
<td>オフラインのFilter Driver</td>
<td>ESXiのFilter Driverがオフラインです。</td>
<td>ESXi</td>
</tr>
<tr>
<td>アップグレード推奨</td>
<td>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。</td>
<td>ESXi</td>
</tr>
<tr>
<td>不正プログラムの手動検索の保留中</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの手動検索の処理待ち</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの手動検索の実行中</td>
<td>手動で開始した不正プログラムの検索が処理中です。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの手動検索の一時停止</td>
<td>手動で開始した不正プログラムの検索が一時停止しています。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの手動検索キャンセルの保留中</td>
<td>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処理待ちでされています。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの手動検索キャンセルの実行中</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの予約検索の保留中</td>
<td>不正プログラムの予約検索をキャンセルする命令がまだ送信されていません。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの予約検索の処理待ち</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの予約検索の実行中</td>
<td>不正プログラムの予約検索が処理中です。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの予約検索の一時停止</td>
<td>不正プログラムの予約検索が一時停止になっています。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの予約検索キャンセルの保留中</td>
<td>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でされています。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの予約検索キャンセルの実行中</td>
<td>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。</td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>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、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。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの手動検索の保留中 (オフライン)</td>
<td>不正プログラムの手動検索をキャンセルする命令が送信され、Applianceがオフラインです。通信が再度確立されると、不正プログラムの手動検索をキャンセルする命令が送信されます。</td>
<td></td>
</tr>
<tr>
<td>不正プログラムの予約検索の保留中 (オフライン)</td>
<td>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、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。</td>
<td></td>
</tr>
<tr>
<td>不正プログラム対策コンポーネントのアップデートの保留中 (オンライン)</td>
<td>次回のハートビート時に、Agent/Applianceが最新の不正プログラム対策コンポーネントにアップデートされます。</td>
<td></td>
</tr>
<tr>
<td>不正プログラム対策コンポーネントのアップデートの保留中 (予約)</td>
<td>コンピュータのアクセススケジュールが許可されると、すぐに不正プログラム対策コンポーネントをアップデートされます。</td>
<td></td>
</tr>
<tr>
<td>不正プログラム対策コンポーヌンのアップデートの保留中</td>
<td>不正プログラム対策コンポーネントをアップデートする命令が送信処理待ちで、最新の不正プログラム対策コンポーネントで、Agent/Applianceをアップデート中です。</td>
<td></td>
</tr>
<tr>
<td>不正プログラム対策コンポーネントのアップデートの保留中 (オンライン)</td>
<td>不正プログラム対策コンポーネントをアップデートする命令が送信処理待ちで、最新の不正プログラム対策コンポーネントで、Agent/Applianceをアップデート中です。</td>
<td></td>
</tr>
</tbody>
</table>

### Agentの状態

<table>
<thead>
<tr>
<th>状態</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>有効化済み</td>
<td>Agent/Applianceが正常に有効化されました。Deep Security Managerで管理することができます。</td>
</tr>
<tr>
<td>有効化が必要</td>
<td>有効化されていないAgent/Applianceが対象のコンピュータで検出されました。Deep Security Managerで管理するには、有効化が必要があります。</td>
</tr>
<tr>
<td>仮想マシン停止</td>
<td>仮想マシンが「停止」状態です。</td>
</tr>
<tr>
<td>仮想マシン一時停止</td>
<td>仮想マシンが「一時停止」状態です。</td>
</tr>
<tr>
<td>Agent/Applianceなし</td>
<td>コンピュータでAgent/Applianceが検出されませんでした。</td>
</tr>
<tr>
<td>不明</td>
<td>Agent/Applianceが存在するかどうか判定されていません。</td>
</tr>
<tr>
<td>無効化が必要</td>
<td>他のDeep Security Managerによってすでに有効化されたAgent/Applianceを、Managerで有効化しようとしました。新しいManagerで有効化する前に、元のDeep Security ManagerでAgent/Applianceを無効にする必要があります。</td>
</tr>
<tr>
<td>再有効化が必要</td>
<td>Agent/Applianceが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。</td>
</tr>
<tr>
<td>オンライン</td>
<td>Agent/Applianceがオンラインで、予期したとおりに動作しています。</td>
</tr>
</tbody>
</table>
保護モジュールのステータス

コンピュータのエラー

<table>
<thead>
<tr>
<th>エラーの状態</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>通信エラー</td>
<td>一般的なネットワークエラーです。</td>
</tr>
<tr>
<td>コンピュータへのルートなし</td>
<td>通常は、ファイアウォールの干渉または中間ルータの停止が原因で、リモートホストにアクセスできません。</td>
</tr>
<tr>
<td>ホスト名解決不能</td>
<td>未解決のソケットアドレスです。</td>
</tr>
<tr>
<td>有効化が必要</td>
<td>有効化されていない場合、Agent/Applianceに命令が送信されます。</td>
</tr>
<tr>
<td>Agent/Applianceとの通信失敗</td>
<td>Agent/Applianceとの通信に失敗しました。</td>
</tr>
<tr>
<td>プロトコルエラー</td>
<td>HTTP層での通信エラーです。</td>
</tr>
<tr>
<td>無効化が必要</td>
<td>Agent/Applianceは、現在別のDeep Security Managerによって有効化されています。</td>
</tr>
<tr>
<td>Agent/Applianceなし</td>
<td>ダークトでAgent/Applianceが検出されていません。</td>
</tr>
<tr>
<td>有効なソフトウェアバージョンなし</td>
<td>要求したプラットフォーム/バージョンのインスタンスが見つからないことを示します。</td>
</tr>
<tr>
<td>ソフトウェアの送信失敗</td>
<td>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。</td>
</tr>
<tr>
<td>内部エラー</td>
<td>内部エラーです。</td>
</tr>
<tr>
<td>重複するコンピュータ</td>
<td>Managerのコンピュータリストにある2台のコンピュータが同じIPアドレスを共有しています。</td>
</tr>
<tr>
<td>VMware Toolsがインストールされていません</td>
<td>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のみ表示されます。</td>
</tr>
</tbody>
</table>

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/オフ状態:

<table>
<thead>
<tr>
<th>ステータス</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>オン</td>
<td>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。</td>
</tr>
<tr>
<td>オフ</td>
<td>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。</td>
</tr>
<tr>
<td>不明</td>
<td>保護モジュールでエラーが発生しています。</td>
</tr>
</tbody>
</table>

インストール状態:

<table>
<thead>
<tr>
<th>ステータス</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>インストール保留中</td>
<td>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。</td>
</tr>
<tr>
<td>インストール実行中</td>
<td>モジュールをAgentにインストール中です。</td>
</tr>
<tr>
<td>インストールされていません</td>
<td>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、モジュールのオン/オフ状態が「オフ」の場合のみ表示されます (オン/オフ状態が「オン」の場合、モジュールはAgentにインストール済みです)。</td>
</tr>
<tr>
<td>ステータス</td>
<td>説明</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>一致するモジュールプラグインが見つかりません</td>
<td>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。</td>
</tr>
<tr>
<td>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</td>
<td>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、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。</td>
</tr>
</tbody>
</table>
ソフトウェアアップデートサーバの設定


Webサーバがすでに配置されている場合は、配信用にRelayを配置する代わりに、それらのサーバでソフトウェアアップデートの配信タスクを実行することができます。そのためには、Deep Security 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。

新しいアップデート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を設定した場合も、セキュリティアップデートを配布するために少なくとも1つはDeep Security Relay有効化済みAgentが必要です。

以下に、ローカルWebサーバに専用のソフトウェアリポジトリをセットアップする方法を説明します。

Webサーバの要件

- ディスク容量: 8GB
- ポート
  - 4122: Agent/ApplianceからRelayへの通信 (TCP)
  - 4123: ローカルホストへの内部Relay通信 (TCP)

フォルダ構造

Deep Security Relayのソフトウェアリポジトリフォルダの構造をミラーしたフォルダを、ソフトウェアWebサーバに作成する必要があります。

Windows Relayのソフトウェアリポジトリ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\n
Linux Relayのソフトウェアリポジトリの初期設定の場所は次のとおりです。

/var/opt/ds_agent/relay/www/dsa/

フォルダの構造は次のとおりです。

```plaintext
|-- dsa
  |-- <プラットフォーム>.<アーキテクチャ>
  |   |-- <ファイル名>
  |   |-- <ファイル名>
  |   |-- ...
  |-- <プラットフォーム>.<アーキテクチャ>
  |   |-- <ファイル名>
  |   |-- <ファイル名>
  |   |-- ...
```

たとえば、次のとおりです。
Relay上のその他のファイルおよびフォルダ

Deep Security Relayのdsaフォルダには、上記以外にも多くのファイルやフォルダが含まれていますが、ソフトウェアリポジトリをホストするためにミラーする必要があるフォルダは、使用しているAgentのプラットフォームとアーキテクチャに関連するファイルを含むフォルダだけです（ただし、dsaフォルダ全体をミラーしても問題はなく、その方が簡単です）。

ソフトウェアリポジトリの使用

Webサーバでソフトウェアリポジトリをホストするための手順を完了したので、次に、そのWebサーバを使用するようにDeep Securityを設定します。

カスタマイズしたWebサーバをソフトウェアアップデートリポジトリとして使用するようにDeep Securityを設定するには、次の手順を実行します。

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. アップデートWebサーバのエリアで、ミラーしたソフトウェアリポジトリコンテンツを含むWebサーバ上のフォルダのURLを入力します。
3. [保存] をクリックします。

これで、今後Deep Security Agentは、指定したソフトウェアリポジトリの場所からソフトウェアアップデートを取得します。

Apacheにおけるディフィー・ヘルマン暗号を無効にする

Apache Webサーバでは、「鍵交換アルゴリズム」および「認証方法」としてディフィー・ヘルマン (DH) 公開鍵暗号化プロトコルを使用する場合があります。このプロトコルはDeep Security Agent/Applianceでサポートされていないので、SSLフィルタを動作させることなくApache Webサーバで無効にする必要があります。

httpd-ssl.confファイルの「SSLCipherSuite」変数で最初の2つのフィールドに、「鍵交換アルゴリズム」および「認証方法」のパラメータがあります。ディフィー・ヘルマンをApacheで使用しないようにするには、これらのフィールドに「!ADH」を追加します。

次の例は、ディフィー・ヘルマンでの鍵交換および認証方法をApache上で無効にするのに必要な構文を示したものです。

```
```

注意: ADHを無効にする際に問題となるのは、最初の2つのフィールドのみです。「!」は、ApacheでADHを「使用しない」ことを記述するものです。

Apacheのビルドによっては、設定ファイルが別の場所にある可能性があります。たとえば、次のとおりです。

- RHELの初期インストールの場合: /etc/httpd/conf.d/ssl.conf
- Apache 2.2.x: /apache2/conf/extra/httpd-ssl.conf

参照

詳細は、「http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite」にあるSSLCipherSuiteのApacheのドキュメントを参照してください。
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)

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環境は、RACノード間の通信チャネルが複雑なため、Deep Security Agentの初期設定のファイアウォール設定では一部のパケットがブロックされてしまうため機能しません。ファイアウォール自体を無効にするか、以下の手順に従ってファイアウォール設定をカスタマイズしてください。

ノード間の相互接続を許可するルールを追加する


2. Linux Serverポリシーを選択し、[詳細] をクリックします。

   注意： このドキュメントでは、初期設定の「Linux Server」ポリシーを編集します。実際に作業するときは、このポリシーのコピーを作成し、そのコピーをOracle RAC用にカスタマイズすることを推奨します。

3. [ファイアウォール] をクリックします。
4. [割り当て/割り当て解除] をクリックします。

5. [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。
6. [一般情報]で、次のように設定します。
   - 処理: 強制的に許可
   - プロトコル: 任意
7. [パケット送信元] で、次のように設定します。
   ◦ IP: すべてのノードのプライベートIPアドレスをカンマで区切って入力

8. [パケット送信先] で、次のように設定します。
   ◦ IP: すべてのノードのプライベートIPアドレスをカンマで区切って入力

9. [OK] 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。
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。

回避技術対策が「標準」に設定されていることを確認する

ネットワークエンジンの回避技術対策が初期設定の「標準」に設定されていることを確認します。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。
その他のRAC関連パケットを許可する (オプション)

ほとんどの環境では上記の手順を実行すれば十分ですが、Oracle RACデータベースに関する問題が発生し、一部のパケットがファイアウォールイベントから破棄される場合は、次のファイアウォールルールを追加してみてください。

- **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。
フレームの種類C0A8を許可する: [フレームの種類] を「その他」、[フレーム番号] を「C0A8」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。

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
ManagerとDB間の通信を暗号化する

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、両者間のチャネルがすでに保護されているということが前提にしているからです。


**注意:** 多数ノードモードで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。

Microsoft SQL Server (Linux)

Deep Security ManagerとMicrosoft SQL Serverデータベース間の通信を暗号化するには

1. Deep Security Manager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.ssl=require

3. /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サービスを開始します。

# service dsm_s start

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。

Microsoft SQL Server (Windows)

Deep Security ManagerとMicrosoft SQL Serverデータベースの間の通信を暗号化するには

1. Deep Security Manager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.ssl=require
3. \\Program Files\Trend Micro\Deep Security ManagerにDeep Security Manager.vmoptionsという名前のファイルを作成し、次の行を追加します。
-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。

![SQL Server配置管理画面](image1)

![SQL Server配置管理画面](image2)

5. Deep Security Managerサービスを開始します。

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。

Oracle Database

Deep Security ManagerとOracle Databaseの間の通信を暗号化するには

1. 次の行をdsm.propertiesに追加します（例）。
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。
## アラート

<table>
<thead>
<tr>
<th>アラート</th>
<th>初期設定の重要度</th>
<th>消去可能</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>异常な再起動の検出</td>
<td>警告</td>
<td>○</td>
<td>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] ダイアログボックスの [サポート] セクション) を起動する必要があります。</td>
</tr>
<tr>
<td>有効化の失敗</td>
<td>重大</td>
<td>×</td>
<td>有効化できない場合は、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。</td>
</tr>
<tr>
<td>Agentの設定パッケージが大きすぎる</td>
<td>警告</td>
<td>○</td>
<td>これは通常、割り当てられているファイアウォールおよびDPIルールが多すぎることが原因です。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。</td>
</tr>
<tr>
<td>Agentインストールの失敗</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>Agentのアップグレード推奨 (Applianceと非互換)</td>
<td>警告</td>
<td>×</td>
<td>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）</td>
</tr>
<tr>
<td>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)</td>
<td>警告</td>
<td>なし</td>
<td>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。/Applianceソフトウェアのアップグレードを推奨します。</td>
</tr>
<tr>
<td>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)</td>
<td>警告</td>
<td>なし</td>
<td>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。/Applianceソフトウェアのアップグレードを推奨します。</td>
</tr>
<tr>
<td>Agent/Applianceのアップグレードが必要</td>
<td>警告</td>
<td>なし</td>
<td>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。</td>
</tr>
<tr>
<td>ルールのアップデートが利用可能</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>不正プログラム対策アラート</td>
<td>警告</td>
<td>○</td>
<td>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。</td>
</tr>
<tr>
<td>不正プログラム対策コンポーネントの障害</td>
<td>重大</td>
<td>○</td>
<td>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。</td>
</tr>
<tr>
<td>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</td>
<td>警告</td>
<td>×</td>
<td>1台以上のAgent/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。</td>
</tr>
<tr>
<td>不正プログラム対策エンジンがオフライン</td>
<td>重大</td>
<td>×</td>
<td>Agent/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。</td>
</tr>
<tr>
<td>不正プログラム対策保護がないか、期限切れ</td>
<td>警告</td>
<td>×</td>
<td>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る。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。</td>
</tr>
<tr>
<td>不正プログラム対策の隔離ファイルがストレージ制限を超過</td>
<td>警告</td>
<td>○</td>
<td>ストレージの制限に達したため、不正プログラム対策でのファイルの隔離に失敗しました。</td>
</tr>
</tbody>
</table>
## アラート

<table>
<thead>
<tr>
<th>アラート</th>
<th>初期設定の重要度</th>
<th>消去可能</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>アプリケーションの種類の誤った設定</td>
<td>警告</td>
<td>x</td>
<td>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。</td>
</tr>
<tr>
<td>アプリケーションの種類の推奨設定</td>
<td>警告</td>
<td>○</td>
<td>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た。新しくコンピュータに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場合、新しいコンピュータのインストールを検出した。コンピュータにアプリケーションの種類を割り当てない場合、コンピュータの詳細ダイアログボックスをクリックし、アプリケーションの種類を割り当ててください。</td>
</tr>
<tr>
<td>ソフトウェア安全性評価サービスがオフライン</td>
<td>警告</td>
<td>x</td>
<td>Deep Security Managerノードはトレードマーケット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、保護実装モジュールのファイル名を変更できません。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を、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。</td>
</tr>
<tr>
<td>時計の変更の検出</td>
<td>警告</td>
<td>○</td>
<td>コンピュータで時計の変更が検出されました。時計が変更された場合は、コンピュータに問題がある可能性があり、アラートを消去する前に調査が必要があります。</td>
</tr>
<tr>
<td>通信の問題の検出</td>
<td>警告</td>
<td>○</td>
<td>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制限が原因で、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。</td>
</tr>
<tr>
<td>コンピュータがアップデートを受信していない</td>
<td>警告</td>
<td>x</td>
<td>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。</td>
</tr>
<tr>
<td>コンピュータの再起動が必要</td>
<td>警告</td>
<td>○</td>
<td>Agentフイルドのインストール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前に、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。</td>
</tr>
<tr>
<td>不正プログラム対策保護でコンピュータの再起動が必要</td>
<td>警告</td>
<td>x</td>
<td>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報告しました。コンピュータのシステムイベントを確認し、再起動の理由を特定してください。</td>
</tr>
<tr>
<td>設定が必要</td>
<td>警告</td>
<td>x</td>
<td>1台以上のコンピュータで、複数のインタ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フェースがあります。</td>
</tr>
<tr>
<td>Filter Driverとの接続失敗</td>
<td>警告</td>
<td>警告</td>
<td>Filter Driverへの接続に失敗したことがApplianceから報告されました。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。詳細を確認するには、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。</td>
</tr>
<tr>
<td>CPUの重大しきい値の超過</td>
<td>警告</td>
<td>x</td>
<td>CPUの重大しきい値を超えた場合。</td>
</tr>
<tr>
<td>CPUの警告しきい値の超過</td>
<td>警告</td>
<td>x</td>
<td>CPUの警告しきい値を超えた場合。</td>
</tr>
<tr>
<td>重複するコンピュータの検出</td>
<td>警告</td>
<td>x</td>
<td>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。</td>
</tr>
<tr>
<td>重複する一意のIDの検出</td>
<td>警告</td>
<td>x</td>
<td>これらのコンピュータは、クラウドのいずれのリソースの管理や、UUID重複のトラブルシューティングについては、Deep Securityのオンラインヘルプまたはドキュメントを参照してください。</td>
</tr>
<tr>
<td>空のRelayグループの割り当て</td>
<td>警告</td>
<td>x</td>
<td>空のRelayグループが割り当てられていない場合は、コンピュータに別のRelayグループを割り当てることなく、空のRelayグループに別のRelayを追加してください。</td>
</tr>
<tr>
<td>イベントの抑制</td>
<td>警告</td>
<td>○</td>
<td>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、一部のイベントが抑制されています。新しいイベントが生成された場合、イベント抑制の状態を確認してください。</td>
</tr>
<tr>
<td>イベントの切り捨て</td>
<td>警告</td>
<td>○</td>
<td>データファイルが大きくなりすぎるとAgent/Applianceのイベントを保存できなくなったり、一部のイベントが抑制されたり、あるいはAgent/Applianceで新しいイベントが送信できなくなった場合に、イベントの切り捨てを有効にします。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。</td>
</tr>
<tr>
<td>ファイルで不正プログラムを検索できませんでした</td>
<td>警告</td>
<td>x</td>
<td>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、原因を特定してください。</td>
</tr>
<tr>
<td>ファイヤーウォールエンジンがオフライン</td>
<td>警告</td>
<td>x</td>
<td>重要なシステムイベントを確認してください。</td>
</tr>
</tbody>
</table>

**管理者ガイド**

アラート

アラートの説明

- アラートが表示され、解決方法が示されます。
- アラートが表示され、解決方法が示されない場合、問題の原因を調査し、解決してください。

アラートの説明

- アラートが表示され、解決方法が示されない場合、問題の原因を調査し、解決してください。
<table>
<thead>
<tr>
<th>アラート</th>
<th>初期設定の重要度</th>
<th>消去可能</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>ファイアウォールルールアラート</td>
<td>警告</td>
<td>○</td>
<td>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。</td>
</tr>
<tr>
<td>ファイアウォールルールの推奨</td>
<td>警告</td>
<td>×</td>
<td>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るか、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る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。</td>
</tr>
<tr>
<td>ハートビートサーバの失敗</td>
<td>警告</td>
<td>×</td>
<td>ハートビートサーバが正常に起動していません。ポート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。ハートビートを使用しない場合は、アラートをオフにできます。</td>
</tr>
<tr>
<td>非互換のAgent/Applianceの推奨</td>
<td>警告</td>
<td>×</td>
<td>Deep Security Managerは、推奨のAgent/Applianceの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たイベントを報告しました。Managerソフトウェアのアップグレードをお勧めします。</td>
</tr>
<tr>
<td>ディスク容量の不足</td>
<td>警告</td>
<td>○</td>
<td>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に空きディスク容量を確保したが、新しいイベントが発生した。侵入防御、ファイアウォール、およびAgent/Applianceのイベントの消去を防ぐために、必要な空きディスク容量を上に確保してください。</td>
</tr>
<tr>
<td>変更監視エンジンがオンライン</td>
<td>警告</td>
<td>×</td>
<td>変更監視エンジンがオンラインで、変更監視エンジンが協力していないことを報告しました。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。</td>
</tr>
<tr>
<td>変更監視情報の収集が遅延しています</td>
<td>警告</td>
<td>×</td>
<td>変更監視情報の収集が遅延しています。変更監視情報の収集が遅延している場合、システムイベントが遅延することが考えられます。変更監視エンジンをオンラインにすることが重要です。</td>
</tr>
<tr>
<td>変更監視ルールの削除の推奨</td>
<td>警告</td>
<td>○</td>
<td>Deep Security Managerは、ネットワークのコンピュータに不要な変更監視ルールが割り当てられていることを検出した。この理由としては、脆弱性のあるアプリケーションがインストールされ、既存の脆弱性にパッチが適用され、変更監視ルールが不要であることが考えられます。コンピュータから削除するには、削除の理由ダイアログボックスを開き、削除の理由をクリックし、削除するルールを削除します。</td>
</tr>
<tr>
<td>変更監視ルールの推奨</td>
<td>警告</td>
<td>○</td>
<td>Deep Security Managerは、ネットワークのコンピュータに不要な変更監視ルールが割り当てられていることを検出した。この理由としては、脆弱性のあるアプリケーションがインストールされ、既存の脆弱性にパッチが適用され、変更監視ルールが不要であることが考えられます。コンピュータから削除するには、削除の理由ダイアログボックスを開き、削除の理由をクリックし、削除するルールを削除します。</td>
</tr>
<tr>
<td>ディスク容量の不足</td>
<td>警告</td>
<td>○</td>
<td>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に空きディスク容量を確保したが、新しいイベントが発生した。侵入防御、ファイアウォール、およびAgent/Applianceのイベントの消去を防ぐために、必要な空きディスク容量を上に確保してください。</td>
</tr>
<tr>
<td>セキュリティ情報の削除の推奨</td>
<td>警告</td>
<td>○</td>
<td>Deep Security Managerは、ネットワークのコンピュータに不要なセキュリティ情報が割り当てられていることを検出した。この理由としては、脆弱性のあるアプリケーションがインストールされ、既存の脆弱性にパッチが適用され、変更監視ルールが不要であることが考えられます。コンピュータから削除するには、削除の理由ダイアログボックスを開き、削除の理由をクリックし、削除するルールを削除します。</td>
</tr>
<tr>
<td>変更監視ルールの削除の推奨</td>
<td>警告</td>
<td>○</td>
<td>Deep Security Managerは、ネットワークのコンピュータに不要な変更監視ルールが割り当てられていることを検出した。この理由としては、脆弱性のあるアプリケーションがインストールされ、既存の脆弱性にパッチが適用され、変更監視ルールが不要であることが考えられます。コンピュータから削除するには、削除の理由ダイアログボックスを開き、削除の理由をクリックし、削除するルールを削除します。</td>
</tr>
</tbody>
</table>

管理者ガイド
アラート
210
<table>
<thead>
<tr>
<th>アラート</th>
<th>初期設定の重要度</th>
<th>消去可能</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>侵入防御ルールの設定が必要</td>
<td>警告</td>
<td>×</td>
<td>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、侵入防御ルールプロパティを開き、[設定]タブを選択してください。</td>
</tr>
<tr>
<td>セキュリティログ監視エンジンがオフライン</td>
<td>重大</td>
<td>×</td>
<td>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、失敗の原因を特定してください。</td>
</tr>
<tr>
<td>セキュリティログ監視ルールの推奨</td>
<td>警告</td>
<td>○</td>
<td>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。</td>
</tr>
<tr>
<td>セキュリティログ監視ルールに設定が必要</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>ディスク容量不足</td>
<td>警告</td>
<td>×</td>
<td>Deep Security Managerノードのディスク容量が残り10%未満でした。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。</td>
</tr>
<tr>
<td>Managerがオンライン</td>
<td>警告</td>
<td>×</td>
<td>Deep Security Managerノードがオンラインです。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。</td>
</tr>
<tr>
<td>Managerの時刻が非同期</td>
<td>重大</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>メモリの重大しきい値の超過</td>
<td>重大</td>
<td>×</td>
<td>メモリの重大しきい値の超過しました。</td>
</tr>
<tr>
<td>メモリの警告しきい値の超過</td>
<td>警告</td>
<td>×</td>
<td>メモリの警告しきい値の超過しました。</td>
</tr>
<tr>
<td>複数の有効化されたApplianceの検出</td>
<td>警告</td>
<td>○</td>
<td>同じESXi上のFilter Driverへの接続が複数検出されたことが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が、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。</td>
</tr>
<tr>
<td>ネットワークエンジンモードの非互換性</td>
<td>警告</td>
<td>×</td>
<td>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をアップグレードしてください。</td>
</tr>
<tr>
<td>新しいダイナミックパターンアップデートがデ</td>
<td>警告</td>
<td>×</td>
<td>新しいパターンアップデートがデ</td>
</tr>
<tr>
<td>ネットワークエンジンモードをタップに設定できないのは、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をアップグレードしてください。</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>新しいバージョンのソフトウェアが利用可能</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>コンピュータ数がデータベースの上限を超</td>
<td>警告</td>
<td>×</td>
<td>有効化されたコンピュータの数が増し、コンピュータ数がデータベースの上限を超えています。さらにコンピュータが追加された場合は、コンピュータをデータベースに追加する必要があ</td>
</tr>
<tr>
<td>保護モジュールライセンスが期限切れ</td>
<td>警告</td>
<td>○</td>
<td>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。</td>
</tr>
<tr>
<td>保護モジュールライセンスがすまもなく期限切れ</td>
<td>警告</td>
<td>×</td>
<td>保護モジュールライセンスが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]画面にライセンスを変更すると削除されます。</td>
</tr>
<tr>
<td>アラート</td>
<td>初期設定の重要度</td>
<td>消去可能</td>
<td>説明</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>推奨設定</td>
<td>警告</td>
<td>○</td>
<td>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た。推奨されている変更点を確認するには、コンピュータのエディタ画面を開き、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のリストで、[削り当て/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、[削り当て解除可能]を表示する設定の表示)フィルタオプションを使用してフィルタします（安全に削り当てを解除できるルールを表示するには、[削り当て解除に推奨される設定の表示]を選択します。</td>
</tr>
<tr>
<td>攻撃の予兆の検出：OSのフィンガープリント調査</td>
<td>警告</td>
<td>○</td>
<td>Agent/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てください。</td>
</tr>
<tr>
<td>攻撃の予兆の検出：ネットワークまたはポートの検索</td>
<td>警告</td>
<td>○</td>
<td>Agent/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。検索の詳細については、コンピュータのイベントを確認してください。</td>
</tr>
<tr>
<td>攻撃の予兆の検出：TCP Null検索</td>
<td>警告</td>
<td>○</td>
<td>Agent/Applianceで、TCP「null」の検索を検出した。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。検索の詳細については、コンピュータのイベントを確認してください。</td>
</tr>
<tr>
<td>攻撃の予兆の検出：TCP SYNFIN検索</td>
<td>警告</td>
<td>○</td>
<td>Agent/Applianceで、TCP「SYNFIN」ポートの検索を検出した。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。検索の詳細については、コンピュータのイベントを確認してください。</td>
</tr>
<tr>
<td>攻撃の予兆の検出：TCP Xmas検索</td>
<td>警告</td>
<td>○</td>
<td>Agent/Applianceで、TCP「Xmas」の検索を検出した。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。検索の詳細については、コンピュータのイベントを確認してください。</td>
</tr>
<tr>
<td>Relayアップデートサービス利用不可</td>
<td>重大</td>
<td>×</td>
<td>Relayのアップデートサービスは、Relayがアップデートサーバ（または別の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している間は利用できません。この状態が解消しない場合、「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。アップデートサーバが利用できない場合またはアップデートが破損している場合、Relayはセキュリティアップデートの取得に失敗します。</td>
</tr>
<tr>
<td>不正プログラムの予約検索がスキップされました</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>ポリシー送信の失敗</td>
<td>重大</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>Smart Protection Serverとの接続失敗</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>ソフトウェアパッケージが見つかりませんでした</td>
<td>重大</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>ソフトウェアアップデートをインポート可能</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>通信不能</td>
<td>重大</td>
<td>×</td>
<td>Deep Security Managerは、設定された期間内にAgent/Applianceのステータスを検査できませんでした。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。</td>
</tr>
<tr>
<td>Agentソフトウェアのアップグレード失敗</td>
<td>警告</td>
<td>○</td>
<td>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。</td>
</tr>
<tr>
<td>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）</td>
<td>警告</td>
<td>×</td>
<td>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サーバを検出した。Filter Driverのアップグレードをお勧めします。</td>
</tr>
<tr>
<td>アラート</td>
<td>初期設定の重要度</td>
<td>消去可能</td>
<td>説明</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ユーザのロックアウト</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>ユーザパスワードがうまくなく有効期限切れ</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>Virtual ApplianceとFilter Driverの互換性なし</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>仮想マシンインタフェースの非同期</td>
<td>警告</td>
<td>×</td>
<td>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。</td>
</tr>
<tr>
<td>保護されていないESXiサーバへの仮想マシンの移動</td>
<td>警告</td>
<td>○</td>
<td>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。</td>
</tr>
<tr>
<td>別のESXiへの移動中に仮想マシンが保護されていません</td>
<td>警告</td>
<td>○</td>
<td>Applianceで保護されている仮想マシンが、別のESXiへの移動中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。</td>
</tr>
<tr>
<td>VMware Toolsがインストールされていません</td>
<td>重大</td>
<td>○</td>
<td>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ません。NSX環境で仮想マシンを保護するにはVMware Toolsが必要です。</td>
</tr>
<tr>
<td>Webレビューイベントアラート</td>
<td>警告</td>
<td>○</td>
<td>アラートを発するために設定されている1台以上のコンピュータで、Webレビューイベントが発生しました。</td>
</tr>
</tbody>
</table>
イベントリスト

- Agent/Applianceイベント (240ページ)
- 不正プログラム対策イベント (243ページ)
- ファイアウォールイベント (246ページ)
- 変更監視イベント (249ページ)
- 侵入防御イベント (244ページ)
- セキュリティログ監視イベント (251ページ)
- システムイベント (215ページ)
## システムイベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>エラー</td>
<td>不明なエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>100</td>
<td>情報</td>
<td>Deep Security Managerの開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>101</td>
<td>情報</td>
<td>ライセンスの変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>102</td>
<td>情報</td>
<td>Trend Micro Deep Securityユーバーアカウントの変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>103</td>
<td>警告</td>
<td>アップデートの確認の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>104</td>
<td>警告</td>
<td>ソフトウェアの自動ダウンロードの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>105</td>
<td>警告</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>106</td>
<td>警告</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>107</td>
<td>情報</td>
<td>ルールアップデートのダウンロードおよび適用</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>108</td>
<td>情報</td>
<td>スクリプト実行</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>109</td>
<td>エラー</td>
<td>スクリプト実行の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>110</td>
<td>情報</td>
<td>システムイベントのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>111</td>
<td>情報</td>
<td>ファイアウォールイベントのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>112</td>
<td>情報</td>
<td>枠入防御イベントのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>113</td>
<td>警告</td>
<td>スケジュールルールアップデートのダウンロード失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>114</td>
<td>情報</td>
<td>スケジュールルールアップデートのダウンロード</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>115</td>
<td>情報</td>
<td>ルールアップデートのダウンロード</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>116</td>
<td>情報</td>
<td>ルールアップデートの適用</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>117</td>
<td>情報</td>
<td>Deep Security Managerのシャットダウン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>118</td>
<td>警告</td>
<td>オフラインのDeep Security Managerがオフライン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>119</td>
<td>情報</td>
<td>Deep Security Managerのオフライン復帰</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>120</td>
<td>エラー</td>
<td>ハートビートサーバの失敗</td>
<td>受信Agentハートビートを待機するManager内のサーバの起動に失敗しました。Managerの受信ハートビートポート(初期設定では4120)が、Managerサーバ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がそのポートにバインドされてエラーが解決します。</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>121</td>
<td>エラー</td>
<td>スケジューラの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>122</td>
<td>エラー</td>
<td>Managerのメッセージスレッドの失敗</td>
<td>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問い合わせてください。</td>
</tr>
<tr>
<td>123</td>
<td>情報</td>
<td>Deep Security Managerの強制シャットダウン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>124</td>
<td>情報</td>
<td>ルールアップデートの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>130</td>
<td>情報</td>
<td>資格情報の生成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>131</td>
<td>警告</td>
<td>資格情報の生成の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>140</td>
<td>情報</td>
<td>コンピュータの検出</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>141</td>
<td>警告</td>
<td>コンピュータの検出の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>142</td>
<td>情報</td>
<td>コンピュータの検出の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>143</td>
<td>情報</td>
<td>コンピュータの検出のキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>150</td>
<td>情報</td>
<td>システム設定の保存</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>151</td>
<td>情報</td>
<td>ソフトウェアの追加</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>152</td>
<td>情報</td>
<td>ソフトウェアの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>153</td>
<td>情報</td>
<td>ソフトウェアのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>154</td>
<td>情報</td>
<td>ソフトウェアのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>155</td>
<td>情報</td>
<td>ソフトウェアプラットフォームの変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>160</td>
<td>情報</td>
<td>認証の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>161</td>
<td>情報</td>
<td>ルールアップデートのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>162</td>
<td>情報</td>
<td>セキュリティ監視イベントのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>163</td>
<td>情報</td>
<td>不正プログラム対策のイベントのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>164</td>
<td>情報</td>
<td>セキュリティアップデートの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>165</td>
<td>エラー</td>
<td>セキュリティアップデートの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>166</td>
<td>情報</td>
<td>新規ソフトウェアの確認の成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>167</td>
<td>エラー</td>
<td>新規ソフトウェアの確認の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>168</td>
<td>情報</td>
<td>手動セキュリティアップデートの成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>169</td>
<td>エラー</td>
<td>手動セキュリティアップデートの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>170</td>
<td>エラー</td>
<td>Managerの利用可能ディスク容量の不足</td>
<td>Managerが引き続き機能するには利用可能ディスク容量が不足しているため、シャットダウンされます。このエラーが発生した場合、Managerはシャットダウンされます。解決するには、ディスク容量を確保してからManagerを再起動してください。</td>
</tr>
<tr>
<td>171</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>172</td>
<td>情報</td>
<td>Webレピュテーションイベントのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>173</td>
<td>情報</td>
<td>不正プログラムの検液ファイルリストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>180</td>
<td>情報</td>
<td>アラートの種類のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>190</td>
<td>情報</td>
<td>アラートの開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>191</td>
<td>情報</td>
<td>アラートの変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>192</td>
<td>情報</td>
<td>アラートの終了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>197</td>
<td>情報</td>
<td>アラートメールの送信</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>198</td>
<td>警告</td>
<td>アラートメールの失敗</td>
<td>1人以上のユーザ宛てにメール通知を生成するように設定されたアラートが発令されましたが、メールを送信できませんでした。SMTPが正しく設定されていることを確認してください。参照 [管理]→[システム設定]→[SMTP] を参照してください。</td>
</tr>
<tr>
<td>199</td>
<td>エラー</td>
<td>アラート処理の失敗</td>
<td>アラート処理に失敗しました。現在のアラートのステータスが正しくない可能性があります。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問い合わせてください。</td>
</tr>
<tr>
<td>248</td>
<td>情報</td>
<td>ソフトウェアアップデート: Relayの無効化要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>249</td>
<td>情報</td>
<td>ソフトウェアアップデート: Relayの有効化要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>250</td>
<td>情報</td>
<td>コンピュータの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>251</td>
<td>情報</td>
<td>コンピュータの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>252</td>
<td>情報</td>
<td>コンピュータのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>253</td>
<td>情報</td>
<td>コンピュータへのポリシーの割り当て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>254</td>
<td>情報</td>
<td>コンピュータの移動</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>255</td>
<td>情報</td>
<td>有効化の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>256</td>
<td>情報</td>
<td>ポリシー送信の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>257</td>
<td>情報</td>
<td>ロック</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>258</td>
<td>情報</td>
<td>ロック解除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>259</td>
<td>情報</td>
<td>無効化の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>260</td>
<td>情報</td>
<td>オープンポートの検索</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重  要  度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>261</td>
<td>警 告</td>
<td>オープンポートの検索の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>262</td>
<td>情 報</td>
<td>オープンポートの検索の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>263</td>
<td>情 報</td>
<td>オープンポートの検索のキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>264</td>
<td>情 報</td>
<td>Agentソフトウェアのアップグレード要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>265</td>
<td>情 報</td>
<td>Agentソフトウェアのアップグレードのキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>266</td>
<td>警 告/エラーのクリア</td>
<td></td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>267</td>
<td>情 報</td>
<td>ステータスの確認の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>268</td>
<td>情 報</td>
<td>イベントの取得の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>270</td>
<td>エ ラ ー</td>
<td>コンピュータの作成の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>271</td>
<td>情 報</td>
<td>Agentソフトウェアのアップグレードのタイムアウト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>272</td>
<td>情 報</td>
<td>Applianceソフトウェアのアップグレードのタイムアウト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>273</td>
<td>情 報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>274</td>
<td>情 報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>275</td>
<td>警 告</td>
<td>重複するコンピュータ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>276</td>
<td>情 報</td>
<td>アップデート: 概要情報</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>280</td>
<td>情 報</td>
<td>コンピュータのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>281</td>
<td>情 報</td>
<td>コンピュータのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>286</td>
<td>情 報</td>
<td>コンピュータのログのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>287</td>
<td>情 報</td>
<td>コンピュータへのRelayグループの割り当て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>290</td>
<td>情 報</td>
<td>グループの追加</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>291</td>
<td>情 報</td>
<td>グループの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>292</td>
<td>情 報</td>
<td>グループのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>293</td>
<td>情 報</td>
<td>インタフェース名の変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>294</td>
<td>情 報</td>
<td>コンピュータブリッジ名の変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>295</td>
<td>情 報</td>
<td>インタフェースの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>296</td>
<td>情 報</td>
<td>インタフェースIPの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重 要 度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>297</td>
<td>情 報</td>
<td>推奨設定の検索要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>298</td>
<td>情 報</td>
<td>推奨設定のクリア</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>299</td>
<td>コンピュータへの資産評価の割り当て</td>
<td></td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>300</td>
<td>情 報</td>
<td>推奨設定の検索完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>301</td>
<td>情 報</td>
<td>Agentソフトウェアの配信の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>302</td>
<td>情 報</td>
<td>Agentソフトウェアの削除の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>303</td>
<td>情 報</td>
<td>コンピュータ名の変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>304</td>
<td>情 報</td>
<td>変更の検索の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>305</td>
<td>情 報</td>
<td>ベースラインの再構築の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>306</td>
<td>情 場</td>
<td>アップデートの要求のキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>307</td>
<td>情 場</td>
<td>変更監視ルールのコンパイルの問題</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>308</td>
<td>情 場</td>
<td>変更監視ルールのコンパイルの問題の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>309</td>
<td>情 場</td>
<td>ディレクトリの追加</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>310</td>
<td>情 場</td>
<td>ディレクトリの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>311</td>
<td>情 場</td>
<td>ディレクトリのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>312</td>
<td>情 場</td>
<td>ディレクトリ同期</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>320</td>
<td>情 場</td>
<td>ディレクトリ同期の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>321</td>
<td>情 場</td>
<td>ディレクトリ同期の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>322</td>
<td>情 場</td>
<td>ディレクトリ同期のキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>323</td>
<td>情 場</td>
<td>ユーザ同期</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>324</td>
<td>情 場</td>
<td>ユーザ同期の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>325</td>
<td>情 場</td>
<td>ユーザ同期のキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>330</td>
<td>情 場</td>
<td>SSL設定の作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>331</td>
<td>情 場</td>
<td>SSL設定の削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重 要 度</td>
<td>イベント</td>
<td>備 考</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>332</td>
<td>情 報</td>
<td>SSL設定のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>350</td>
<td>情 報</td>
<td>ポリシーの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>351</td>
<td>情 報</td>
<td>ポリシーの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>352</td>
<td>情 報</td>
<td>ポリシーのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>353</td>
<td>情 報</td>
<td>ポリシーのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>354</td>
<td>情 報</td>
<td>ポリシーのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>355</td>
<td>情 報</td>
<td>推奨設定の検索のキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>360</td>
<td>情 報</td>
<td>VMware vCenterの追加</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>361</td>
<td>情 報</td>
<td>VMware vCenterの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>362</td>
<td>情 報</td>
<td>VMware vCenterのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>363</td>
<td>情 報</td>
<td>VMware vCenterの同期</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>364</td>
<td>情 報</td>
<td>VMware vCenterの同期の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>365</td>
<td>エ ラ ー</td>
<td>VMware vCenterの同期失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>366</td>
<td>情 報</td>
<td>VMware vCenterの同期要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>367</td>
<td>情 報</td>
<td>VMware vCenterの同期キャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>368</td>
<td>警 告</td>
<td>インタフェースの非同期</td>
<td>これは、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が違うことを示しています。通常、仮想マシンを再起動すると解決します。</td>
</tr>
<tr>
<td>369</td>
<td>情 報</td>
<td>インタフェースの同期</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>370</td>
<td>情 報</td>
<td>Filter Driverのインストール完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>371</td>
<td>情 報</td>
<td>Filter Driverの削除完了</td>
<td>ESXi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。</td>
</tr>
<tr>
<td>372</td>
<td>情 場</td>
<td>Filter Driverのアップグレード</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>373</td>
<td>情 場</td>
<td>Virtual Applianceの配信</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>374</td>
<td>情 場</td>
<td>Virtual Applianceのアップグレード完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>375</td>
<td>警 告</td>
<td>Virtual Applianceのアップグレードの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>376</td>
<td>警 告</td>
<td>保護されていないESXiへの仮想マシンの移動</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>377</td>
<td>警 告</td>
<td>保護されているESXiへの仮想マシンの移動</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>378</td>
<td>警 告</td>
<td>別のESXiへの移動後に仮想マシンが保護されていません</td>
<td>保護されていないESXiに仮想マシンが移動されました。</td>
</tr>
<tr>
<td>379</td>
<td>警 告</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>イベント</td>
<td>備考</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>380</td>
<td>エラー</td>
<td>指定されたESXi上の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。</td>
<td></td>
</tr>
<tr>
<td>381</td>
<td>報告</td>
<td>Filter Driverのオンライン復帰 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>382</td>
<td>報告</td>
<td>Filter Driverのアップグレード要求 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>383</td>
<td>報告</td>
<td>Applianceのアップグレード要求 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>384</td>
<td>警告</td>
<td>ESXiの準備失敗 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>385</td>
<td>警告</td>
<td>Filter Driverのアップグレード失敗 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>386</td>
<td>警告</td>
<td>ESXiからのFilter Driver削除の失敗 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>387</td>
<td>エラー</td>
<td>Filter Driverとの接続失敗 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>388</td>
<td>エラー</td>
<td>Filter Driverとの接続成功 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>389</td>
<td>エラー</td>
<td>複数の有効化されたApplianceの検出 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>390</td>
<td>報告</td>
<td>有効化されたApplianceの複数検出の解決 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>391</td>
<td>エラー</td>
<td>ネットワーク設定とvCenterグローバル設定の非同期 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>392</td>
<td>報告</td>
<td>ネットワーク設定とvCenterグローバル設定の同期 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>393</td>
<td>エラー</td>
<td>不正プログラム対策エンジンがオフライン (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>394</td>
<td>報告</td>
<td>不正プログラム対策エンジンのオンライン復帰 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>395</td>
<td>エラー</td>
<td>Virtual ApplianceとFilter Driverの互換性なし (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>396</td>
<td>報告</td>
<td>Virtual ApplianceとFilter Driverの互換性がない状態の解決 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>警告</td>
<td>VMware NSXコールバック認証失敗 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>398</td>
<td>エラー</td>
<td>VMware Toolsがインストールされていません (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>399</td>
<td>報告</td>
<td>VMware Toolsの未インストール解決 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>報告</td>
<td>サイアーウォールルールの作成 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>401</td>
<td>報告</td>
<td>サイアーウォールルールの削除 (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>402</td>
<td>報告</td>
<td>サイアーウォールルールのアップデート (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>403</td>
<td>報告</td>
<td>サイアーウォールルールのエクスポート (備考はありません)</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>414</td>
<td>情報</td>
<td>ファイアウォールルールのインポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>420</td>
<td>情報</td>
<td>ファイアウォールステートルール設定の作成</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>421</td>
<td>情報</td>
<td>ファイアウォールステートルール設定の削除</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>422</td>
<td>情報</td>
<td>ファイアウォールステートルール設定のアップデート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>424</td>
<td>情報</td>
<td>ファイアウォールステートルール設定のインポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>460</td>
<td>情報</td>
<td>アプリケーションの種類の作成</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>461</td>
<td>情報</td>
<td>アプリケーションの種類の削除</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>462</td>
<td>情報</td>
<td>アプリケーションの種類のアップデート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>463</td>
<td>情報</td>
<td>アプリケーションの種類のエクスポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>464</td>
<td>情報</td>
<td>アプリケーションの種類のインポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>470</td>
<td>情報</td>
<td>侵入防御ルールの作成</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>471</td>
<td>情報</td>
<td>侵入防御ルールの削除</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>472</td>
<td>情報</td>
<td>侵入防御ルールのアップデート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>473</td>
<td>情報</td>
<td>侵入防御ルールのエクスポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>474</td>
<td>情報</td>
<td>侵入防御ルールのインポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>480</td>
<td>情報</td>
<td>変更監視ルールの作成</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>481</td>
<td>情報</td>
<td>変更監視ルールの削除</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>482</td>
<td>情報</td>
<td>変更監視ルールのアップデート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>483</td>
<td>情報</td>
<td>変更監視ルールのエクスポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>484</td>
<td>情報</td>
<td>変更監視ルールのインポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>490</td>
<td>情報</td>
<td>セキュリティログ監視ルールの作成</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>491</td>
<td>情報</td>
<td>セキュリティログ監視ルールの削除</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>492</td>
<td>情報</td>
<td>セキュリティログ監視ルールのアップデート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>493</td>
<td>情報</td>
<td>セキュリティログ監視ルールのエクスポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>494</td>
<td>情報</td>
<td>セキュリティログ監視ルールのインポート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>495</td>
<td>情報</td>
<td>セキュリティログ監視デコダーの作成</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>496</td>
<td>情報</td>
<td>セキュリティログ監視デコダーの削除</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>497</td>
<td>情報</td>
<td>セキュリティログ監視データのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>498</td>
<td>情報</td>
<td>セキュリティログ監視データのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>499</td>
<td>情報</td>
<td>セキュリティログ監視データのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>505</td>
<td>情報</td>
<td>コンテキストの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>506</td>
<td>情報</td>
<td>コンテキストの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>507</td>
<td>情報</td>
<td>コンテキストのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>508</td>
<td>情報</td>
<td>コンテキストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>509</td>
<td>情報</td>
<td>コンテキストのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>510</td>
<td>情報</td>
<td>IPリストの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>511</td>
<td>情報</td>
<td>IPリストの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>512</td>
<td>情報</td>
<td>IPリストのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>513</td>
<td>情報</td>
<td>IPリストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>514</td>
<td>情報</td>
<td>IPリストのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>520</td>
<td>情報</td>
<td>ポートリストの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>521</td>
<td>情報</td>
<td>ポートリストの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>522</td>
<td>情報</td>
<td>ポートリストのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>523</td>
<td>情報</td>
<td>ポートリストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>524</td>
<td>情報</td>
<td>ポートリストのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>525</td>
<td>情報</td>
<td>検索キャッシュ設定の作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>526</td>
<td>情報</td>
<td>検索キャッシュ設定のエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>530</td>
<td>情報</td>
<td>MACリストの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>531</td>
<td>情報</td>
<td>MACリストの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>532</td>
<td>情報</td>
<td>MACリストのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>533</td>
<td>情報</td>
<td>MACリストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>534</td>
<td>情報</td>
<td>MACリストのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>540</td>
<td>情報</td>
<td>プロキシの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>541</td>
<td>情報</td>
<td>プロキシの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>542</td>
<td>情報</td>
<td>プロキシのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>543</td>
<td>情報</td>
<td>プロキシのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>544</td>
<td>情報</td>
<td>プロキシのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>550</td>
<td>情報</td>
<td>スケジュールの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>551</td>
<td>情報</td>
<td>スケジュールの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>552</td>
<td>情報</td>
<td>スケジュールのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>553</td>
<td>情報</td>
<td>スケジュールのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>554</td>
<td>情報</td>
<td>スケジュールのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>560</td>
<td>情報</td>
<td>予約タスクの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>561</td>
<td>情報</td>
<td>予約タスクの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>562</td>
<td>情報</td>
<td>予約タスクのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>563</td>
<td>情報</td>
<td>予約タスクの手動実行</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>564</td>
<td>情報</td>
<td>予約タスクの開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>565</td>
<td>情報</td>
<td>バックアップの完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>566</td>
<td>エラー</td>
<td>バックアップの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>567</td>
<td>警告</td>
<td>未解決アラートの概要の送信中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>568</td>
<td>警告</td>
<td>未解決アラートの概要の送信失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>569</td>
<td>警告</td>
<td>メールの失敗</td>
<td>メール通知を送信できませんでした。SMTPが正しく設定されていることを確認してください([管理]→[システム設定]→[SMTP])。</td>
</tr>
<tr>
<td>570</td>
<td>警告</td>
<td>レポートの送信中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>571</td>
<td>警告</td>
<td>レポートの送信の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>572</td>
<td>エラー</td>
<td>無効なReport Jar</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>573</td>
<td>情報</td>
<td>資産評価の作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>574</td>
<td>情報</td>
<td>資産評価の削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>575</td>
<td>情報</td>
<td>資産評価のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>576</td>
<td>エラー</td>
<td>レポートのアンインストールの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>577</td>
<td>エラー</td>
<td>レポートのアンインストール</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>580</td>
<td>警告</td>
<td>アプリケーションの種類のポードリストの誤った設定</td>
<td>(備考はありません)</td>
</tr>
</tbody>
</table>

管理者ガイド
システムイベント

224
<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>581</td>
<td>警告</td>
<td>アプリケーションの種類のポートリストの誤った設定の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>582</td>
<td>警告</td>
<td>侵入防御ルールで設定が必要</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>583</td>
<td>情報</td>
<td>侵入防御ルールで必要な設定の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>584</td>
<td>警告</td>
<td>設定が必要な変更監視ルール</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>585</td>
<td>情報</td>
<td>変更監視ルールで必要な設定の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>586</td>
<td>警告</td>
<td>セキュリティログ監視ルールで設定が必要</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>587</td>
<td>情報</td>
<td>セキュリティログ監視ルールで必要な設定の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>588</td>
<td>警告</td>
<td>セキュリティログ監視ルールで必要なログファイル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>589</td>
<td>情報</td>
<td>セキュリティログ監視ルールで必要なログファイルの解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>590</td>
<td>警告</td>
<td>不明な予約タスクの種類</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>591</td>
<td>情報</td>
<td>Relayグループの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>592</td>
<td>情報</td>
<td>Relayグループのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>593</td>
<td>情報</td>
<td>Relayグループの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>594</td>
<td>情報</td>
<td>イベントベースタスクの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>595</td>
<td>情報</td>
<td>イベントベースタスクの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>596</td>
<td>情報</td>
<td>イベントベースタスクのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>597</td>
<td>情報</td>
<td>イベントベースタスクの開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>600</td>
<td>情報</td>
<td>ユーザのログオン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>601</td>
<td>情報</td>
<td>ユーザのログオフ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>602</td>
<td>情報</td>
<td>ユーザのタイムアウト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>603</td>
<td>情報</td>
<td>ユーザのロックアウト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>604</td>
<td>情報</td>
<td>ユーザのロック解除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>608</td>
<td>エラー</td>
<td>ユーザセッションの確認の失敗</td>
<td>Managerは、成功したユーザログオン/認証によって開始されたユーザセッションであることを確認できません。ログオンページに戻ります。ユーザは再度認証を実行する必要があります。</td>
</tr>
<tr>
<td>609</td>
<td>エラー</td>
<td>ユーザによる無効な要求</td>
<td>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）。監査データへのアクセスは拒否されます。</td>
</tr>
<tr>
<td>610</td>
<td>情報</td>
<td>ユーザセッションの有効化</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>611</td>
<td>情報</td>
<td>ユーザによるファイヤウォールイベントの表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>613</td>
<td>情報</td>
<td>ユーザによる侵入防御イベントの表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>615</td>
<td>情報</td>
<td>ユーザによるシステムイベントの表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>616</td>
<td>情報</td>
<td>ユーザによる変更監視イベントの表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>617</td>
<td>情報</td>
<td>ユーザによるセキュリティログ監視イベントの表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>618</td>
<td>情報</td>
<td>ユーザによる隔離ファイルの詳細表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>619</td>
<td>情報</td>
<td>ユーザによる不正プログラム対策イベントの表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>620</td>
<td>情報</td>
<td>ユーザによるWebレビューションイベントの表示</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>621</td>
<td>情報</td>
<td>ユーザがテナントとしてログオン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>622</td>
<td>情報</td>
<td>プライマリテナントからのアクセス有効</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>623</td>
<td>情報</td>
<td>プライマリテナントからのアクセス無効</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>624</td>
<td>情報</td>
<td>プライマリテナントからのアクセス許可</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>625</td>
<td>情報</td>
<td>プライマリテナントからのアクセス取り消し済み</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>626</td>
<td>情報</td>
<td>プライマリテナントからのアクセス期限切れ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>650</td>
<td>情報</td>
<td>ユーザの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>651</td>
<td>情報</td>
<td>ユーザの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>652</td>
<td>情報</td>
<td>ユーザのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>653</td>
<td>情報</td>
<td>ユーザパスワードの設定</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>660</td>
<td>情報</td>
<td>役割の作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>661</td>
<td>情報</td>
<td>役割の削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>662</td>
<td>情報</td>
<td>役割のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>663</td>
<td>情報</td>
<td>役割のインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>664</td>
<td>情報</td>
<td>役割のエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>670</td>
<td>情報</td>
<td>連絡先の作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>671</td>
<td>情報</td>
<td>連絡先の削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>672</td>
<td>情報</td>
<td>連絡先のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>700</td>
<td>エラー</td>
<td>Agentソフトウェアのインストール</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>701</td>
<td>エラー</td>
<td>Agentソフトウェアのインストールの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要な度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>702</td>
<td>情報</td>
<td>資格情報の生成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>703</td>
<td>エラー</td>
<td>資格情報の生成の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>704</td>
<td>情報</td>
<td>Agent/Appliance有効化の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>705</td>
<td>エラー</td>
<td>Agent/Appliance有効化の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>706</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>707</td>
<td>警告</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>708</td>
<td>情報</td>
<td>Agent/Appliance無効化の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>709</td>
<td>エラー</td>
<td>Agent/Appliance無効化の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>710</td>
<td>情報</td>
<td>イベントの取得</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>711</td>
<td>情報</td>
<td>Agentソフトウェアの配信</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>712</td>
<td>エラー</td>
<td>Agentソフトウェアの配信の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>713</td>
<td>情報</td>
<td>Agentソフトウェアの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>714</td>
<td>エラー</td>
<td>Agentソフトウェアの削除の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>715</td>
<td>情報</td>
<td>Agent/Applianceのバージョン変更</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>720</td>
<td>情報</td>
<td>ポリシー送信</td>
<td>Agent/Applianceがアップデートされました。</td>
</tr>
<tr>
<td>721</td>
<td>エラー</td>
<td>ポリシー送信の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>722</td>
<td>警告</td>
<td>インターフェースの取得失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>723</td>
<td>警告</td>
<td>インターフェースの取得失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>724</td>
<td>警告</td>
<td>ディスク容量の不足</td>
<td>ディスク容量不足がAgentからレポートされました。Agentのホストの空き容量を増やしてください。</td>
</tr>
<tr>
<td>725</td>
<td>警告</td>
<td>イベントの抑制</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>726</td>
<td>警告</td>
<td>Agent/Appliance-イベントの取得失敗</td>
<td>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なく、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。</td>
</tr>
<tr>
<td>727</td>
<td>警告</td>
<td>Agent/Appliance-イベントの取得失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>728</td>
<td>エラー</td>
<td>イベントの取得失敗</td>
<td>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なく、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 [今すぐイベントを取得] を実行してください。</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>729</td>
<td>情報</td>
<td>イベントの取得失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>730</td>
<td>エラー</td>
<td>オフライン</td>
<td>Managerがコンピュータと通信できません。Agent/Applianceによる保護が無効というわけではありません。詳細については、コンピュータおよびAgent/Applianceのステータスを参照してください。</td>
</tr>
<tr>
<td>731</td>
<td>情報</td>
<td>オンラインに復帰</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>732</td>
<td>エラー</td>
<td>ファイアウォールエンジンがオフライン</td>
<td>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ませんと送受信されています。この状態は、通常、コンピュータのOSプラットフォームへの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。</td>
</tr>
<tr>
<td>733</td>
<td>情報</td>
<td>ファイアウォールエンジンがオンライン復帰</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>734</td>
<td>警告</td>
<td>コンピュータの時計の変更</td>
<td>ポリシーのエディタまたはコンピュータエディタ画面の設定→コンピュータ→[ハートビート]エリアで設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。</td>
</tr>
<tr>
<td>735</td>
<td>警告</td>
<td>前回の設定の検出</td>
<td>Agentの設定が、Managerのレコードで示されて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。</td>
</tr>
<tr>
<td>736</td>
<td>情報</td>
<td>ステータス確認の失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>737</td>
<td>エラー</td>
<td>ステータスの確認の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>738</td>
<td>エラー</td>
<td>検証防衛エンジンがオフライン</td>
<td>検証防衛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ませんと送受信されています。この状態は、通常、コンピュータのOSプラットフォームへの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。</td>
</tr>
<tr>
<td>739</td>
<td>情報</td>
<td>検証防衛エンジンがオンライン復帰</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>740</td>
<td>エラー</td>
<td>Agent/Applianceエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>741</td>
<td>警告</td>
<td>異常な再起動の検出</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>742</td>
<td>警告</td>
<td>通信の問題</td>
<td>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軽減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。</td>
</tr>
<tr>
<td>743</td>
<td>警告</td>
<td>通信の問題の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>745</td>
<td>警告</td>
<td>イベントの切り捨て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>748</td>
<td>エラー</td>
<td>セキュリティログ監視エンジンがオフライン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>749</td>
<td>情報</td>
<td>セキュリティログ監視エンジンのオンライン復帰</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>750</td>
<td>警告</td>
<td>前回の自動再試行</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>755</td>
<td>警告</td>
<td>Deep Security Managerのバージョン互換性の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>756</td>
<td>警告</td>
<td>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）</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>760</td>
<td>警告</td>
<td>Agent/Appliance/バージョン互換性の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>761</td>
<td>報告</td>
<td>Agent/Applianceのアップグレード推奨</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>762</td>
<td>報告</td>
<td>Agent/Applianceのアップグレードが必要</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>763</td>
<td>報告</td>
<td>非互換のAgent/Applianceのバージョン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>764</td>
<td>報告</td>
<td>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）</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>765</td>
<td>報告</td>
<td>コンピュータの再起動が必要</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>766</td>
<td>報告</td>
<td>ネットワークエンジンモードの設定が非互換</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>767</td>
<td>報告</td>
<td>ネットワークエンジンモードのバージョンが非互換</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>768</td>
<td>報告</td>
<td>ネットワークエンジンモードの非互換性の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>769</td>
<td>報告</td>
<td>Agent/Applianceのパートナートリートの拒否</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>770</td>
<td>警告</td>
<td>認識できないクライアントによる接続</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>771</td>
<td>情報</td>
<td>推奨設定の検索失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>772</td>
<td>情報</td>
<td>ベースラインの再構築失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>773</td>
<td>警告</td>
<td>ベースラインの再構築の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>774</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>775</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>776</td>
<td>情報</td>
<td>変更の検索失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>777</td>
<td>警告</td>
<td>変更の検索の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>778</td>
<td>情報</td>
<td>Agentからのリモート有効化の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>779</td>
<td>情報</td>
<td>Agentからのリモート有効化の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>780</td>
<td>情報</td>
<td>不正プログラムの手動検索失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>781</td>
<td>情報</td>
<td>不正プログラムの手動検索の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>782</td>
<td>情報</td>
<td>不正プログラムの予約検索失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>783</td>
<td>情報</td>
<td>不正プログラムの予約検索の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>784</td>
<td>情報</td>
<td>不正プログラムの予約検索タスクのスキップ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>785</td>
<td>情報</td>
<td>不正プログラムの予約検索タスクの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>786</td>
<td>情報</td>
<td>不正プログラム検索のキャンセル失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
</tbody>
</table>
| 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、検索を再試行してください。
| 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、検索を再試行してください。
| 800| 情報 | アラートの消去 | (備考はありません)
| 801| 情報 | エラーの消去 | (備考はありません)
| 850| 警告 | 攻撃の予兆の検出: OSのフィンガープリント調査 | (備考はありません)
| 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 | (備考はありません)
| 852| 警告 | 攻撃の予兆の検出: TCP Null検索 | (備考はありません)
| 853| 警告 | 攻撃の予兆の検出: TCP SYNFIN検索 | (備考はありません)
| 854| 警告 | 攻撃の予兆の検出: TCP Xmas検索 | (備考はありません)
| 900| 情報 | Deep Security Managerの監査の開始 | (備考はありません)
| 901| 情報 | Deep Security Managerの監査のシャットダウン | (備考はありません)
| 902| 情報 | Deep Security Managerのインストール | (備考はありません)
| 903| 情報 | ライセンス関連設定の変更 | (備考はありません)
| 904| 情報 | 診断パッケージの生成 | (備考はありません)
| 905| 情報 | 診断パッケージのエクスポート | (備考はありません)
| 906| 情報 | 診断パッケージのアップロード | (備考はありません)
| 913| エラー | 自動診断パッケージのエラー | (備考はありません)
| 914| 情報 | 隔離ファイルの削除の成功 | (備考はありません)
| 915| 情報 | 隔離ファイルの削除の失敗 | (備考はありません)
| 916| 情報 | 隔離ファイルのダウンロードの成功 | (備考はありません)
| 917| 情報 | 隔離ファイルのダウンロードの失敗 | (備考はありません)
| 918| 情報 | 隔離ファイル管理ユーティリティのダウンロードの成功 | (備考はありません)
| 919| 情報 | 隔離ファイルが見つかりませんでした | (備考はありません)
| 920| 情報 | 使用状況情報の生成 | (備考はありません)
| 921| 情報 | 使用状況情報パッケージのエクスポート | (備考はありません)
| 922| 情報 | 使用状況情報パッケージのアップロード | (備考はありません)
| 923| エラー | 使用状況情報パッケージのエラー | (備考はありません)
<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>924</td>
<td>警告</td>
<td>不正プログラムの隔離の失敗 (仮想マシンの制限を超過)</td>
<td>感染ファイルを隔離できませんでした。この仮想マシンからの隔離ファイルの格納用にVirtual Applianceに割り当てられた最大容量を超しました。</td>
</tr>
<tr>
<td>925</td>
<td>警告</td>
<td>不正プログラムの隔離の失敗 (仮想マシンの制限を超過)</td>
<td>感染ファイルを隔離できませんでした。隔離ファイルの格納用にVirtual Applianceに割り当てられている最大容量を超しました。</td>
</tr>
<tr>
<td>926</td>
<td>警告</td>
<td>スマートスキャン用のSmart Protection Serverへの接続不能</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>927</td>
<td>情報</td>
<td>スマートスキャン用のSmart Protection Serverへの接続不能</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>928</td>
<td>情報</td>
<td>隔離ファイルの復元の成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>929</td>
<td>情報</td>
<td>隔離ファイルの復元の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>930</td>
<td>情報</td>
<td>証明書の承認</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>931</td>
<td>情報</td>
<td>証明書の削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>932</td>
<td>警告</td>
<td>Webレピュテーション用のSmart Protection Serverへの接続不能</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>933</td>
<td>情報</td>
<td>Webレピュテーション用のSmart Protection Serverとの接続</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>934</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>935</td>
<td>エラー</td>
<td>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失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>936</td>
<td>情報</td>
<td>隔離ファイルの送信の成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>937</td>
<td>情報</td>
<td>隔離ファイルの送信の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>940</td>
<td>情報</td>
<td>自動タグルールの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>941</td>
<td>情報</td>
<td>自動タグルールの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>942</td>
<td>情報</td>
<td>自動タグルールのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>943</td>
<td>情報</td>
<td>タグの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>944</td>
<td>情報</td>
<td>タグの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>970</td>
<td>情報</td>
<td>コマンドラインユーティリティの開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>978</td>
<td>情報</td>
<td>コマンドラインユーティリティの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>979</td>
<td>情報</td>
<td>コマンドラインユーティリティのシャットダウン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>980</td>
<td>情報</td>
<td>システム情報のエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>990</td>
<td>情報</td>
<td>Managerノードの追加</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>991</td>
<td>情報</td>
<td>Managerノードの使用停止</td>
<td>備考はありません</td>
</tr>
<tr>
<td>992</td>
<td>情報</td>
<td>Managerノードのアップデート</td>
<td>備考はありません</td>
</tr>
<tr>
<td>995</td>
<td>情報</td>
<td>ソフトウェア安全性評価サービスへの接続が復活</td>
<td>備考はありません</td>
</tr>
<tr>
<td>996</td>
<td>警告</td>
<td>ソフトウェア安全性評価サービスに接続不能</td>
<td>備考はありません</td>
</tr>
<tr>
<td>997</td>
<td>エラー</td>
<td>タグ付けエラー</td>
<td>備考はありません</td>
</tr>
<tr>
<td>998</td>
<td>エラー</td>
<td>システムイベント通知エラー</td>
<td>備考はありません</td>
</tr>
<tr>
<td>999</td>
<td>エラー</td>
<td>内部ソフトウェアエラー</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1101</td>
<td>エラー</td>
<td>プラグインのインストールの失敗</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1102</td>
<td>情報</td>
<td>プラグインのインストール</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1103</td>
<td>エラー</td>
<td>プラグインのアップグレードの失敗</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1104</td>
<td>情報</td>
<td>プラグインのアップグレード</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1105</td>
<td>エラー</td>
<td>プラグインの起動の失敗</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1106</td>
<td>エラー</td>
<td>プラグインのアンインストールの失敗</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1107</td>
<td>情報</td>
<td>プラグインのアンインストール</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1108</td>
<td>情報</td>
<td>プラグイン起動</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1109</td>
<td>情報</td>
<td>プラグイン停止</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1110</td>
<td>エラー</td>
<td>ソフトウェアパッケージが見つかりません</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1111</td>
<td>情報</td>
<td>ソフトウェアパッケージが見つかりました</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1500</td>
<td>情報</td>
<td>不正プログラム検査設定の作成</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1501</td>
<td>情報</td>
<td>不正プログラム検査設定の削除</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1502</td>
<td>情報</td>
<td>不正プログラム検査設定のアップデート</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1503</td>
<td>情報</td>
<td>不正プログラム検査設定のエクスポート</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1504</td>
<td>情報</td>
<td>不正プログラム検査設定のインポート</td>
<td>備考はありません</td>
</tr>
<tr>
<td>1505</td>
<td>情報</td>
<td>ディレクトリリストの作成</td>
<td>備考はありません</td>
</tr>
<tr>
<td>ID</td>
<td>重</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>1506</td>
<td>情報</td>
<td>ディレクトリリストの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1507</td>
<td>情報</td>
<td>ディレクトリリストのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1508</td>
<td>情報</td>
<td>ディレクトリリストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1509</td>
<td>情報</td>
<td>ディレクトリリストのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1510</td>
<td>情報</td>
<td>ファイル拡張子リストの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1511</td>
<td>情報</td>
<td>ファイル拡張子リストの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1512</td>
<td>情報</td>
<td>ファイル拡張子リストのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1513</td>
<td>情報</td>
<td>ファイル拡張子リストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1514</td>
<td>情報</td>
<td>ファイル拡張子リストのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1515</td>
<td>情報</td>
<td>ファイルリストの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1516</td>
<td>情報</td>
<td>ファイルリストの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1517</td>
<td>情報</td>
<td>ファイルリストのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1518</td>
<td>情報</td>
<td>ファイルリストのエクスポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1519</td>
<td>情報</td>
<td>ファイルリストのインポート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1520</td>
<td>情報</td>
<td>不正プログラムの手動検索の保留中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1521</td>
<td>情報</td>
<td>不正プログラムの手動検索の開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1522</td>
<td>情報</td>
<td>不正プログラムの手動検索の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1523</td>
<td>情報</td>
<td>不正プログラムの予約検索の開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1524</td>
<td>情報</td>
<td>不正プログラムの予約検索の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1525</td>
<td>情報</td>
<td>不正プログラムの手動検索キャンセルの実行中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1526</td>
<td>情報</td>
<td>不正プログラムの手動検索キャンセルの完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1527</td>
<td>情報</td>
<td>不正プログラムの予約検索キャンセルの実行中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1528</td>
<td>情報</td>
<td>不正プログラムの予約検索キャンセルの完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1529</td>
<td>情報</td>
<td>不正プログラムの手動検索の一時停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1530</td>
<td>情報</td>
<td>不正プログラムの手動検索の一時停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1531</td>
<td>情報</td>
<td>不正プログラムの予約検索の一時停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1532</td>
<td>情報</td>
<td>不正プログラムの手動検索の一時停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1533</td>
<td>情報</td>
<td>不正プログラムのクリーンアップタスクでコンピュータの再起動が必要</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1534</td>
<td>情報</td>
<td>不正プログラム対策保護でコンピュータの再起動が必要</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1536</td>
<td>情報</td>
<td>不正プログラムのクイック検索の保留中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1537</td>
<td>情報</td>
<td>不正プログラムのクイック検索の開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1538</td>
<td>情報</td>
<td>不正プログラムのクイック検索の完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1539</td>
<td>情報</td>
<td>不正プログラムのクイック検索キャンセルの実行中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1540</td>
<td>情報</td>
<td>不正プログラムのクイック検索キャンセルの完了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1541</td>
<td>情報</td>
<td>不正プログラムのクイック検索の一時停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1542</td>
<td>情報</td>
<td>不正プログラムのクイック検索失敗の解決</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1543</td>
<td>警告</td>
<td>不正プログラムのクイック検索の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1544</td>
<td>情報</td>
<td>不正プログラムのクイック検索の再開</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1545</td>
<td>情報</td>
<td>ファイルで不正プログラムを検索できませんでした</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1550</td>
<td>情報</td>
<td>Webレピュテーション設定のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1551</td>
<td>情報</td>
<td>不正プログラム検索設定のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1552</td>
<td>情報</td>
<td>変更監視設定のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1553</td>
<td>情報</td>
<td>セキュリティログ監視設定のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1554</td>
<td>情報</td>
<td>ファイアウォールステートフール設定のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1555</td>
<td>情報</td>
<td>側入防御設定のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1600</td>
<td>情報</td>
<td>Relayグループのアップデートの要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1601</td>
<td>情報</td>
<td>Relayグループのアップデートの成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1602</td>
<td>エラー</td>
<td>Relayグループのアップデートの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1603</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1604</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1605</td>
<td>警告</td>
<td>不正プログラム対策保護がない、期限切れ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1606</td>
<td>情報</td>
<td>ベースラインの再構築の開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>1661</td>
<td>情報</td>
<td>ベースラインの再構築の一時停止</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1662</td>
<td>情報</td>
<td>ベースラインの再構築の一時停止</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1663</td>
<td>情報</td>
<td>ベースラインの再構築の再開</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1664</td>
<td>警告</td>
<td>ベースラインの再構築の再開</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1665</td>
<td>情報</td>
<td>ベースラインの再構築の完了</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1666</td>
<td>情報</td>
<td>変更の検索の開始</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1667</td>
<td>情報</td>
<td>変更の検索の一時停止</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1668</td>
<td>情報</td>
<td>変更の検索の一時停止</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1669</td>
<td>警告</td>
<td>変更の検索の完了</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1670</td>
<td>警告</td>
<td>変更の検索の停止</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1671</td>
<td>情報</td>
<td>変更の検索の完了</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1672</td>
<td>エラー</td>
<td>変更監視エンジンがオフライン</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1673</td>
<td>情報</td>
<td>変更監視エンジンのオンライン復帰</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1674</td>
<td>エラー</td>
<td>TPMのエラー</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1675</td>
<td>エラー</td>
<td>TPMのエラー</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1676</td>
<td>情報</td>
<td>TPMのレジスタ値の読み込み</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1677</td>
<td>情報</td>
<td>TPMのレジスタ値の読み込み</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1678</td>
<td>警告</td>
<td>TPMのレジスタ値の読み込み</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1679</td>
<td>警告</td>
<td>TPMのレジスタ値の読み込み</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1680</td>
<td>警告</td>
<td>TPMチェックが無効</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1681</td>
<td>情報</td>
<td>TPM情報の信頼性なし</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1700</td>
<td>情報</td>
<td>Agentが検出されませんでした</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1800</td>
<td>エラー</td>
<td>Deep Security Protectionモジュールの障害</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1900</td>
<td>情報</td>
<td>クラウドアカウントの追加</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1901</td>
<td>情報</td>
<td>クラウドアカウントの削除</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1902</td>
<td>情報</td>
<td>クラウドアカウントのアップデート</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1903</td>
<td>情報</td>
<td>クラウドアカウント同期の実行中</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1904</td>
<td>情報</td>
<td>クラウドアカウント同期の完了</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>1905</td>
<td>エラー</td>
<td>クラウドアカウント同期の失敗</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>ID</td>
<td>重 要 度</td>
<td>イベント</td>
<td>備 考</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>1906</td>
<td>情 報</td>
<td>クラウドアカウント同期の要求</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1907</td>
<td>情 報</td>
<td>クラウドアカウント同期のキャンセル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1950</td>
<td>情 報</td>
<td>テナントの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1951</td>
<td>情 報</td>
<td>テナントの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1952</td>
<td>情 場</td>
<td>テナントのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1953</td>
<td>情 場</td>
<td>テナントのデータベースサーバの作成</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1954</td>
<td>情 場</td>
<td>テナントのデータベースサーバの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1955</td>
<td>情 場</td>
<td>テナントのデータベースサーバのアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1957</td>
<td>エ ラ ー</td>
<td>テナントの初期化失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1958</td>
<td>情 場</td>
<td>テナント機能のアップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2000</td>
<td>情 場</td>
<td>検索キャッシュ設定オブジェクトの追加</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2001</td>
<td>情 場</td>
<td>検索キャッシュ設定オブジェクトの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2002</td>
<td>情 場</td>
<td>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アップデート</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2200</td>
<td>情 場</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2201</td>
<td>情 場</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2202</td>
<td>警 告</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2203</td>
<td>情 場</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2204</td>
<td>情 場</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2205</td>
<td>警 告</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2300</td>
<td>情 場</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2301</td>
<td>情 場</td>
<td>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成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2302</td>
<td>警 告</td>
<td>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失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>2303</td>
<td>情報</td>
<td>ソフトウェアアップデート: Webリピュテーションモジュールのダウンロード成功</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2400</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2401</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2402</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2403</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2500</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2501</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2502</td>
<td>警告</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2503</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2600</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2601</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2602</td>
<td>警告</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2603</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2700</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2701</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2702</td>
<td>警告</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2703</td>
<td>情報</td>
<td>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</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>2800</td>
<td>情報</td>
<td>ソフトウェアの自動ダウンロード完了</td>
<td>（備考はありません）</td>
</tr>
<tr>
<td>ID</td>
<td>イベント</td>
<td>備考</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>2801</td>
<td>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</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2802</td>
<td>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</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2803</td>
<td>オンラインヘルプのアップデート開始</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2804</td>
<td>オンラインヘルプのアップデート完了</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2805</td>
<td>オンラインヘルプのアップデート成功</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2806</td>
<td>オンラインヘルプのアップデート失敗</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2900</td>
<td>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</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2901</td>
<td>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</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2902</td>
<td>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</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2903</td>
<td>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</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2904</td>
<td>VMware NSX同期の完了</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2905</td>
<td>VMware NSX同期の失敗</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2906</td>
<td>Agentセルフプロテクションの有効化</td>
<td>¥u0028¥u5099¥u8003¥u306f¥u3042¥u308a¥u307e¥u305b¥u3093¥u0029</td>
<td></td>
</tr>
<tr>
<td>2907</td>
<td>Agentセルフプロテクションの無効化</td>
<td>¥u0028¥u5099¥u8003¥u306f¥u3042¥u308a¥u307e¥u305b¥u3093¥u0029</td>
<td></td>
</tr>
<tr>
<td>2908</td>
<td>Agentセルフプロテクションの有効化</td>
<td>¥u0028¥u5099¥u8003¥u306f¥u3042¥u308a¥u307e¥u305b¥u3093¥u0029</td>
<td></td>
</tr>
<tr>
<td>2909</td>
<td>Agentセルフプロテクションの無効化</td>
<td>¥u0028¥u5099¥u8003¥u306f¥u3042¥u308a¥u307e¥u305b¥u3093¥u0029</td>
<td></td>
</tr>
<tr>
<td>2920</td>
<td>DDAnからのレポートの取得を完了しました</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>2921</td>
<td>DDAnからのレポートの取得に失敗しました</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>3000</td>
<td>ソフトウェアアップデート: SAPモジュールのインストール開始</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>3001</td>
<td>ソフトウェアアップデート: SAPモジュールのインストール成功</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>3002</td>
<td>ソフトウェアアップデート: SAPモジュールのインストール失敗</td>
<td>(備考はありません)</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>3003</td>
<td>情報</td>
<td>ソフトウェアアップデート: SAPモジュールのダウンロード成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3004</td>
<td>情報</td>
<td>SAP VSAがインストールされています</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3005</td>
<td>エラー</td>
<td>SAP VSAがインストールされていません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3006</td>
<td>情報</td>
<td>SAP VSAは最新です</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3007</td>
<td>情報</td>
<td>SAP VSAが最新ではありません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3008</td>
<td>情報</td>
<td>SAP VSA通信チャネルの準備ができています</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3009</td>
<td>情報</td>
<td>SAP VSA通信チャネルの準備ができていません</td>
<td>(備考はありません)</td>
</tr>
</tbody>
</table>
## Agentイベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>エラー</td>
<td>不明なAgent/Appliance-イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1000</td>
<td>エラー</td>
<td>エンジンを開けません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1001</td>
<td>エラー</td>
<td>エンジンコマンドの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1002</td>
<td>警告</td>
<td>エンジンリストオブジェクトエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1003</td>
<td>警告</td>
<td>オブジェクトの削除失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1004</td>
<td>エラー</td>
<td>ドライバのアップグレードの停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1005</td>
<td>警告</td>
<td>ドライバのアップグレード中</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1006</td>
<td>警告</td>
<td>ドライバのアップグレードで再起動が必要</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1007</td>
<td>警告</td>
<td>ドライバのアップグレード成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>1008</td>
<td>エラー</td>
<td>サポートされないカーネル</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2000</td>
<td>情報</td>
<td>ポリシー送信</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2001</td>
<td>警告</td>
<td>無効なファイアウォールルール割り当て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2002</td>
<td>警告</td>
<td>無効なファイアウォールステートフル設定</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2003</td>
<td>エラー</td>
<td>セキュリティ設定の保存失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2004</td>
<td>警告</td>
<td>無効なインタフェース割り当て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2005</td>
<td>警告</td>
<td>無効なインタフェース割り当て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2006</td>
<td>警告</td>
<td>無効な処理</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2007</td>
<td>警告</td>
<td>無効なパケット方向</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2008</td>
<td>警告</td>
<td>無効なルール優先度</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2009</td>
<td>警告</td>
<td>認識のできないIPアドレスの形式</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2010</td>
<td>警告</td>
<td>無効な送信先IPリスト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2011</td>
<td>警告</td>
<td>無効な送信先ポートリスト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2012</td>
<td>警告</td>
<td>無効な送信先IPリスト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2013</td>
<td>警告</td>
<td>無効な送信先ポートリスト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2014</td>
<td>警告</td>
<td>無効なスケジュール</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2015</td>
<td>警告</td>
<td>無効な送信元MACリスト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2016</td>
<td>警告</td>
<td>無効な送信元MACリスト</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2017</td>
<td>警告</td>
<td>無効なスケジュール長</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2018</td>
<td>警告</td>
<td>無効なスケジュール文字列</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2019</td>
<td>警告</td>
<td>認識のできないIPアドレスの形式</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2020</td>
<td>警告</td>
<td>オブジェクトが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2021</td>
<td>警告</td>
<td>オブジェクトが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2022</td>
<td>警告</td>
<td>無効なルールの割り当て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2050</td>
<td>警告</td>
<td>ファイアウォールルールが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2075</td>
<td>警告</td>
<td>トラフィックストリームが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2076</td>
<td>警告</td>
<td>侵入防御ルールが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2077</td>
<td>警告</td>
<td>パターンリストが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2078</td>
<td>警告</td>
<td>トラフィックストリーム変換エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2080</td>
<td>警告</td>
<td>条件付きファイアウォールルールが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2081</td>
<td>警告</td>
<td>条件付き侵入防御ルールが見つかりません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2082</td>
<td>警告</td>
<td>空白の侵入防御ルール</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2083</td>
<td>警告</td>
<td>侵入防御ルールのXMLルール変換エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2085</td>
<td>エラー</td>
<td>セキュリティ設定エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2086</td>
<td>警告</td>
<td>サポートされていないIPマッチタイプ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2087</td>
<td>警告</td>
<td>サポートされていないMACマッチタイプ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2088</td>
<td>警告</td>
<td>無効なSSL資格情報</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>2089</td>
<td>警告</td>
<td>SSL資格情報がありません</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>-------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>3000</td>
<td>警告</td>
<td>無効なMACアドレス</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3001</td>
<td>警告</td>
<td>イベントデータの取得失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3002</td>
<td>警告</td>
<td>過剰なイナメスフェス</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3003</td>
<td>エラー</td>
<td>外部コマンドの実行不能</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3004</td>
<td>エラー</td>
<td>外部コマンド出力の読み取り不能</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3005</td>
<td>エラー</td>
<td>OS呼び出しエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3006</td>
<td>エラー</td>
<td>OS呼び出しエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3007</td>
<td>エラー</td>
<td>ファイルエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3008</td>
<td>エラー</td>
<td>コンピュータ固有のキーエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3009</td>
<td>エラー</td>
<td>Agent/Applianceの手配しないシャットダウン</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3010</td>
<td>エラー</td>
<td>Agent/Applianceデータベースエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3300</td>
<td>警告</td>
<td>イベントデータの取得失敗</td>
<td>Linuxエラー</td>
</tr>
<tr>
<td>3301</td>
<td>警告</td>
<td>イベントデータの取得失敗</td>
<td>Linuxエラー</td>
</tr>
<tr>
<td>3302</td>
<td>警告</td>
<td>イベントデータの取得失敗</td>
<td>Linuxエラー</td>
</tr>
<tr>
<td>3303</td>
<td>警告</td>
<td>イベントデータの取得失敗</td>
<td>Linuxエラー</td>
</tr>
<tr>
<td>3600</td>
<td>警告</td>
<td>Windowsシステムディレクトリの取得失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>3601</td>
<td>警告</td>
<td>ローカルデータ読み取りエラー</td>
<td>Windowsエラー</td>
</tr>
<tr>
<td>3602</td>
<td>警告</td>
<td>ローカルデータ読み取りエラー</td>
<td>Windowsエラー</td>
</tr>
<tr>
<td>3603</td>
<td>警告</td>
<td>ローカルデータ読み取りエラー</td>
<td>Windowsエラー</td>
</tr>
<tr>
<td>3700</td>
<td>警告</td>
<td>同様の再起動の検出</td>
<td>Windowsエラー</td>
</tr>
<tr>
<td>3701</td>
<td>情報</td>
<td>異常な再起動の検出</td>
<td>Windowsエラー</td>
</tr>
</tbody>
</table>

通信関連のイベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000</td>
<td>警告</td>
<td>無効なプロトコルヘッダ</td>
<td>コンテンツ長が範囲外です</td>
</tr>
<tr>
<td>4001</td>
<td>警告</td>
<td>無効なプロトコルヘッダ</td>
<td>コンテンツ長があります</td>
</tr>
<tr>
<td>4002</td>
<td>情報</td>
<td>コマンドセッションの開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>4003</td>
<td>情報</td>
<td>コマンドセッションの設定</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>4004</td>
<td>情報</td>
<td>コマンドの受信</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>4011</td>
<td>警告</td>
<td>Managerへの接続に失敗しました</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>4012</td>
<td>警告</td>
<td>ハートビートの失敗</td>
<td>(備考はありません)</td>
</tr>
</tbody>
</table>

Agent関連のイベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>情報</td>
<td>Agent/Applianceの開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5001</td>
<td>エラー</td>
<td>Agent/Applianceの停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5002</td>
<td>エラー</td>
<td>Agent/Applianceの停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5003</td>
<td>情報</td>
<td>Agent/Applianceの停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5004</td>
<td>警告</td>
<td>Agent/Applianceの停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5005</td>
<td>情報</td>
<td>Agent/Applianceの監査開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5006</td>
<td>情報</td>
<td>Agent/Applianceの監査停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5007</td>
<td>情報</td>
<td>Agent/Applianceの監査停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5008</td>
<td>警告</td>
<td>Filter Driver接続の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5009</td>
<td>警告</td>
<td>Filter Driver接続の成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5010</td>
<td>警告</td>
<td>Filter Driver接続の成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5100</td>
<td>情報</td>
<td>Filter Driverの情報イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5101</td>
<td>情報</td>
<td>Filter Driverの情報イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5102</td>
<td>情報</td>
<td>Filter Driverの情報イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5103</td>
<td>情報</td>
<td>Filter Driverの情報イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5104</td>
<td>情報</td>
<td>Filter Driverの情報イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5105</td>
<td>情報</td>
<td>Filter Driverの情報イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5106</td>
<td>情報</td>
<td>Filter Driverの情報イベント</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5107</td>
<td>情報</td>
<td>Agentセプトの有効化</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>5108</td>
<td>情報</td>
<td>Agentセプトの無効化</td>
<td>(備考はありません)</td>
</tr>
</tbody>
</table>

ログ記録関連のイベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>6000</td>
<td>情報</td>
<td>ログデバイスオープンエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6001</td>
<td>情報</td>
<td>ログファイルオープンエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>----</td>
<td>------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>6002</td>
<td>情報</td>
<td>ログファイル書き込みエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6003</td>
<td>情報</td>
<td>ログディレクトリ作成エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6004</td>
<td>情報</td>
<td>ログファイル検索エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6005</td>
<td>情報</td>
<td>ログディレクトリオープンエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6006</td>
<td>情報</td>
<td>ログファイル削除エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6007</td>
<td>情報</td>
<td>ログファイルの名前変更エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6008</td>
<td>情報</td>
<td>ログ読み取りエラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6009</td>
<td>警告</td>
<td>空き容量不足によるログファイルの削除</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6100</td>
<td>警告</td>
<td>イベントは抑制されました</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6101</td>
<td>警告</td>
<td>イベントの切り捨て</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6102</td>
<td>エラー</td>
<td>ディスク容量の不足</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>6103</td>
<td>警告</td>
<td>Agentの設定パッケージが大きすぎる</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9050</td>
<td>情報</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9051</td>
<td>エラー</td>
<td>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</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9100</td>
<td>情報</td>
<td>セキュリティアップデート成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9101</td>
<td>エラー</td>
<td>セキュリティアップデートの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9102</td>
<td>エラー</td>
<td>セキュリティアップデートの失敗</td>
<td>エラーメッセージに特定の情報が記録されました</td>
</tr>
<tr>
<td>9103</td>
<td>情報</td>
<td>Relay Webサーバの無効化</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9104</td>
<td>情報</td>
<td>Relay Webサーバの有効化</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9105</td>
<td>エラー</td>
<td>Relay Webサーバの有効化の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9106</td>
<td>エラー</td>
<td>Relay Webサーバの無効化の失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9107</td>
<td>エラー</td>
<td>Relay Webサーバの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9108</td>
<td>情報</td>
<td>アップデート元に接続不能</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9109</td>
<td>エラー</td>
<td>コンポーネントのアップデートの失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9110</td>
<td>エラー</td>
<td>不正プログラム対策のライセンスの期限切れ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9111</td>
<td>情報</td>
<td>セキュリティアップデートのロールバック成功</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9112</td>
<td>エラー</td>
<td>セキュリティアップデートのロールバック失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9113</td>
<td>情報</td>
<td>Relayによるすべてのパッケージの複製</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9114</td>
<td>エラー</td>
<td>Relayによるすべてのパッケージの複製に失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9201</td>
<td>情報</td>
<td>変更の検索の開始</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9203</td>
<td>情報</td>
<td>変更の検索の異常終了</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9204</td>
<td>情報</td>
<td>変更の検索の一時停止</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9205</td>
<td>情報</td>
<td>変更の検索の再開</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9206</td>
<td>警告</td>
<td>変更の検索の開始失敗</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>9209</td>
<td>警告</td>
<td>変更の検索の停止</td>
<td>(備考はありません)</td>
</tr>
</tbody>
</table>

Smart Protection Serverのステータスに関するイベント

<table>
<thead>
<tr>
<th>ID</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>9300</td>
<td>警告</td>
<td>Webレピュテーション用のSmart Protection Serverへの接続不能</td>
</tr>
<tr>
<td>9301</td>
<td>情報</td>
<td>Webレピュテーション用のSmart Protection Serverとの接続</td>
</tr>
</tbody>
</table>
## 不正プログラム対策イベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
</tr>
</thead>
<tbody>
<tr>
<td>9001</td>
<td>情報</td>
<td>不正プログラム検索の開始</td>
</tr>
<tr>
<td>9002</td>
<td>情報</td>
<td>不正プログラム検索の完了</td>
</tr>
<tr>
<td>9003</td>
<td>情報</td>
<td>不正プログラム検索の異常終了</td>
</tr>
<tr>
<td>9004</td>
<td>情報</td>
<td>不正プログラム検索の一時停止</td>
</tr>
<tr>
<td>9005</td>
<td>情報</td>
<td>不正プログラム検索の再開</td>
</tr>
<tr>
<td>9006</td>
<td>情報</td>
<td>不正プログラム検索のキャンセル</td>
</tr>
<tr>
<td>9007</td>
<td>警告</td>
<td>不正プログラム検索キャンセルの失敗</td>
</tr>
<tr>
<td>9008</td>
<td>警告</td>
<td>不正プログラム検索開始の失敗</td>
</tr>
<tr>
<td>9009</td>
<td>警告</td>
<td>不正プログラム検索の停止</td>
</tr>
<tr>
<td>9010</td>
<td>エラー</td>
<td>不正プログラムの隔離の失敗 (仮想マシンの制限を超える)</td>
</tr>
<tr>
<td>9011</td>
<td>エラー</td>
<td>不正プログラムの隔離の失敗 (Applianceの制限を超える)</td>
</tr>
<tr>
<td>9012</td>
<td>警告</td>
<td>スマートスキャン用のSmart Protection Serverへの接続不能</td>
</tr>
<tr>
<td>9013</td>
<td>情報</td>
<td>スマートスキャン用のSmart Protection Serverへの接続</td>
</tr>
<tr>
<td>9014</td>
<td>警告</td>
<td>不正プログラム対策保護でコンピュータの再起動が必要</td>
</tr>
<tr>
<td>9015</td>
<td>情報</td>
<td>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</td>
</tr>
<tr>
<td>9016</td>
<td>情報</td>
<td>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</td>
</tr>
<tr>
<td>9017</td>
<td>エラー</td>
<td>ファイルでの不正プログラム検索失敗</td>
</tr>
<tr>
<td>9018</td>
<td>エラー</td>
<td>ファイルでの不正プログラム検索失敗</td>
</tr>
</tbody>
</table>
## 侵入防御イベント

<table>
<thead>
<tr>
<th>ID</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>リージョンサイズの超過</td>
<td>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。</td>
</tr>
<tr>
<td>201</td>
<td>メモリ不足</td>
<td>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バ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。</td>
</tr>
<tr>
<td>202</td>
<td>編集回数の超過</td>
<td>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。</td>
</tr>
<tr>
<td>203</td>
<td>編集範囲の超過</td>
<td>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。</td>
</tr>
<tr>
<td>204</td>
<td>パケットの最大一致数を超過</td>
<td>パケット内でパターンに一致する地点が2,048箇所を超えていました。この制限に達するパケットは通常カーブバケットまたは回退バケットであるため、エラーが返されて接続が破棄されます。</td>
</tr>
<tr>
<td>205</td>
<td>エンジンのコールスタック数の超過</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>206</td>
<td>ランタイムエラー</td>
<td>ランタイムエラーです。</td>
</tr>
<tr>
<td>207</td>
<td>パケットの読み込みエラー</td>
<td>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。</td>
</tr>
<tr>
<td>300</td>
<td>サポートされていない暗号化</td>
<td>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。</td>
</tr>
<tr>
<td>301</td>
<td>マスターキーの生成エラー</td>
<td>マスターキー生成エラーです。</td>
</tr>
<tr>
<td>302</td>
<td>レコードレヤメッセージ（準備ができています）</td>
<td>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。</td>
</tr>
<tr>
<td>303</td>
<td>ハンドシェークメッセージ（準備ができています）</td>
<td>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。</td>
</tr>
<tr>
<td>304</td>
<td>ハンドシェークメッセージの故障</td>
<td>通話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。</td>
</tr>
<tr>
<td>305</td>
<td>メモリの転送不足エラー</td>
<td>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バ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。</td>
</tr>
<tr>
<td>306</td>
<td>サポートされていないSSLバージョン</td>
<td>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。</td>
</tr>
<tr>
<td>307</td>
<td>プレマスターキーの複合化データ化エラー</td>
<td>ClientKeyExchangeメッセージからプレマスターキーを複合化できません。</td>
</tr>
<tr>
<td>308</td>
<td>クライアントによるロールバックの試行</td>
<td>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。</td>
</tr>
<tr>
<td>309</td>
<td>更新エラー</td>
<td>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見つかりませんでした。</td>
</tr>
<tr>
<td>310</td>
<td>鍵の交換エラー</td>
<td>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。</td>
</tr>
<tr>
<td>311</td>
<td>SSLキー交換の上限を超過</td>
<td>キー交換の同時要求数が上限を超えました。</td>
</tr>
<tr>
<td>312</td>
<td>鍵サイズの超過</td>
<td>マスターキ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。</td>
</tr>
<tr>
<td>313</td>
<td>ハンドシェーク内の不正なパラメータ</td>
<td>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。</td>
</tr>
<tr>
<td>314</td>
<td>利用可能なセッションなし</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>315</td>
<td>未サポートの圧縮方法</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>316</td>
<td>サポートされていないアプリケーション層プロトコル</td>
<td>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。</td>
</tr>
<tr>
<td>500</td>
<td>URIパスの深さが超過</td>
<td>区切り文字「/」が多すぎます。パスの深さは最大100です。</td>
</tr>
<tr>
<td>501</td>
<td>無効なトラバーサル</td>
<td>ルートより上位に「../」を使用しようとしました。</td>
</tr>
<tr>
<td>ID</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>502</td>
<td>URIに使用できない文字</td>
<td>URIに無効な文字が使用されています。</td>
</tr>
<tr>
<td>503</td>
<td>不完全なUTF8シーケンス</td>
<td>UTF8シーケンスの途中でURIが終了しました。</td>
</tr>
<tr>
<td>504</td>
<td>無効なUTF8の符号化</td>
<td>無効または規定外のエンコードが試行されました。</td>
</tr>
<tr>
<td>505</td>
<td>無効な16進の符号化</td>
<td>%nnのnnが16進数ではありません。</td>
</tr>
<tr>
<td>506</td>
<td>URIパス長の超過</td>
<td>パス長が512文字を超えています。</td>
</tr>
<tr>
<td>507</td>
<td>不正な文字の使用</td>
<td>無効な文字を使用しています。</td>
</tr>
<tr>
<td>508</td>
<td>二重デコードの攻撃コード</td>
<td>二重デコードの攻撃コードです (%25xx、%25%xxdなど)。</td>
</tr>
<tr>
<td>700</td>
<td>不正なBase64コンテンツ</td>
<td>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。</td>
</tr>
<tr>
<td>710</td>
<td>損傷したDeflate/GZIPコンテンツ</td>
<td>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。</td>
</tr>
<tr>
<td>711</td>
<td>不完全なDeflate/GZIPコンテンツ</td>
<td>不完全なDeflate/GZIPコンテンツです。</td>
</tr>
<tr>
<td>712</td>
<td>Deflate/GZIPチェックサムエラー</td>
<td>Deflate/GZIPチェックサムエラーです。</td>
</tr>
<tr>
<td>713</td>
<td>未サポートのDeflate/GZIP辞書</td>
<td>サポートされていないDeflate/GZIP辞書です。</td>
</tr>
<tr>
<td>714</td>
<td>サポートされていないGZIPヘッダ形式/方法</td>
<td>サポートされていないGZIPヘッダ形式/方法です。</td>
</tr>
<tr>
<td>801</td>
<td>プロトコルデコード検索の上限を超過</td>
<td>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。</td>
</tr>
<tr>
<td>802</td>
<td>プロトコルデコードの制約エラー</td>
<td>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限を満たしていません。</td>
</tr>
<tr>
<td>803</td>
<td>プロトコルデコードエンジンの内部エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>804</td>
<td>プロトコルデコードの構造の超過</td>
<td>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。</td>
</tr>
<tr>
<td>805</td>
<td>プロトコルデコードのスタックエラー</td>
<td>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ーコールが使用されようとしてしまいました。</td>
</tr>
<tr>
<td>806</td>
<td>データの無限ループエラー</td>
<td>(備考はありません)</td>
</tr>
</tbody>
</table>
ファイアウォールイベント

<table>
<thead>
<tr>
<th>ID</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>セッション情報なし</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>不正なフラグ</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>不正なシークエンス</td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>不正なACK</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>内部エラー</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>CEフラグ</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>不正なIP</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>不正なIPデータグラム長</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>フラグメント化</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>不正なフラグメントオフセット</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>最初のフラグメントが最小サイズ未満</td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>範囲外のフラグメント</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>最小オフセット値以下のフラグメント</td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>IPv6パケット</td>
<td></td>
</tr>
<tr>
<td>114</td>
<td>受信接続の上限</td>
<td></td>
</tr>
<tr>
<td>115</td>
<td>送信接続の上限</td>
<td></td>
</tr>
<tr>
<td>116</td>
<td>SYN送信の上限</td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>ライセンスの期限切れ</td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>不明なIPバージョン</td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>不正なパケット情報</td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>内部エンジンエラー</td>
<td></td>
</tr>
<tr>
<td>121</td>
<td>許可されていないUDPコメント</td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>許可されていないICMPコメント</td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>ボリシーで未許可</td>
<td></td>
</tr>
<tr>
<td>124</td>
<td>不正なポートコマンド</td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>SYN Cookieエラー</td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>不正なデータオフセット</td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>IPヘッダなし</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>読み取り不能なイーサネットヘッダ</td>
<td></td>
</tr>
<tr>
<td>129</td>
<td>未定義</td>
<td></td>
</tr>
<tr>
<td>130</td>
<td>送信元および送信先IPが同一</td>
<td></td>
</tr>
<tr>
<td>131</td>
<td>不正なTCPヘッダ長</td>
<td></td>
</tr>
<tr>
<td>132</td>
<td>読み取り不能なプロトコルヘッダ</td>
<td></td>
</tr>
<tr>
<td>133</td>
<td>読み取り不能なIPv4ヘッダ</td>
<td></td>
</tr>
<tr>
<td>134</td>
<td>不明なIPバージョン</td>
<td></td>
</tr>
</tbody>
</table>

※一部抜粋

<table>
<thead>
<tr>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>セッション情報なし</td>
<td>既存の接続に関連付けられていないパケットを受け信しました。</td>
</tr>
<tr>
<td>不正なフラグ</td>
<td>パケットに設定されたフラグが無効です。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可能性があります。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有効になっている必要があります。</td>
</tr>
<tr>
<td>不正なシークエンス</td>
<td>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。</td>
</tr>
<tr>
<td>不正なACK</td>
<td>確認応答番号が無効なパケットが検出されました。</td>
</tr>
<tr>
<td>内部エラー</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>CEフラグ</td>
<td>CWRまたはECEフラグが設定されており、ファイアウォールステートフル設定では、これらのパケットを拒否するように指定されています。</td>
</tr>
<tr>
<td>不正なIP</td>
<td>パケットの送信元IPが無効です。</td>
</tr>
<tr>
<td>不正なIPデータグラム長</td>
<td>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。</td>
</tr>
<tr>
<td>フラグメント化</td>
<td>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の拒否が有効になっています。</td>
</tr>
<tr>
<td>不正なフラグメントオフセット</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>最初のフラグメントが最小サイズ未満</td>
<td>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。</td>
</tr>
<tr>
<td>範囲外のフラグメント</td>
<td>フラグメント化されたパケットシークエ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。</td>
</tr>
<tr>
<td>最小オフセット値以下のフラグメント</td>
<td>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。</td>
</tr>
<tr>
<td>IPv6パケット</td>
<td>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。</td>
</tr>
<tr>
<td>受信接続の上限</td>
<td>受信接続数が最大許容数を超えました。</td>
</tr>
<tr>
<td>送信接続の上限</td>
<td>送信接続数が最大許容数を超えています。</td>
</tr>
<tr>
<td>SYN送信の上限</td>
<td>サーバーコンピュータからのハーフオーブン接続数がファイアウォールステートフル設定で指定された数を超えています。</td>
</tr>
<tr>
<td>ライセンスの期限切れ</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>不明なIPバージョン</td>
<td>IPv4またはIPv6以外のIPパケットが検出されました。</td>
</tr>
<tr>
<td>不正なパケット情報</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>内部エンジンエラー</td>
<td>リソースが不足しています。</td>
</tr>
<tr>
<td>許可されていないUDPコメント</td>
<td>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。</td>
</tr>
<tr>
<td>許可されていないICMPコメント</td>
<td>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。</td>
</tr>
<tr>
<td>ボリシーで未許可</td>
<td>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。</td>
</tr>
<tr>
<td>不正なポートコマンド</td>
<td>FTP制御チャ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。</td>
</tr>
<tr>
<td>SYN Cookieエラー</td>
<td>SYN Cookieの保護メカニズムでエラーが発生しました。</td>
</tr>
<tr>
<td>不正なデータオフセット</td>
<td>データオフセットパラメータが無効です。</td>
</tr>
<tr>
<td>IPヘッダなし</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>読み取り不能なイーサネットヘッダ</td>
<td>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っています。</td>
</tr>
<tr>
<td>未定義</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>送信元および送信先IPが同一</td>
<td>送信元IPと送信先IPが同じです。</td>
</tr>
<tr>
<td>不正なTCPヘッダ長</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>読み取り不能なプロトコルヘッダ</td>
<td>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。</td>
</tr>
<tr>
<td>読み取り不能なIPv4ヘッダ</td>
<td>読み取り不能なIPv4ヘッダがパケットに含まれています。</td>
</tr>
<tr>
<td>不明なIPバージョン</td>
<td>IPバージョンを認識できません。</td>
</tr>
<tr>
<td>ID</td>
<td>イベント</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>135</td>
<td>不正なアダプタ設定</td>
</tr>
<tr>
<td>136</td>
<td>重複しているフラグメント</td>
</tr>
<tr>
<td>137</td>
<td>ACK再送の上限</td>
</tr>
<tr>
<td>138</td>
<td>切断された接続上のパケット</td>
</tr>
<tr>
<td>139</td>
<td>再送の破棄</td>
</tr>
<tr>
<td>140</td>
<td>未定義</td>
</tr>
<tr>
<td>141</td>
<td>ポリシーで未許可(オープンポート)</td>
</tr>
<tr>
<td>142</td>
<td>新しい接続の開始</td>
</tr>
<tr>
<td>143</td>
<td>無効なチェックサム</td>
</tr>
<tr>
<td>144</td>
<td>無効なフック</td>
</tr>
<tr>
<td>145</td>
<td>IPヘッダーソースがゼロ</td>
</tr>
<tr>
<td>146</td>
<td>IPv6ソースがマルチキャスト</td>
</tr>
<tr>
<td>147</td>
<td>無効なIPv6アドレス</td>
</tr>
<tr>
<td>148</td>
<td>最小サイズ以下のIPv6フラグメント</td>
</tr>
<tr>
<td>149</td>
<td>無効なトランスポーサホッヘッダ長</td>
</tr>
<tr>
<td>150</td>
<td>メモリ不足</td>
</tr>
<tr>
<td>151</td>
<td>最大TCP接続数</td>
</tr>
<tr>
<td>152</td>
<td>最大UDP接続数</td>
</tr>
<tr>
<td>200</td>
<td>リージョンサイズの超過</td>
</tr>
<tr>
<td>201</td>
<td>メモリ不足</td>
</tr>
<tr>
<td>202</td>
<td>編集回数の超過</td>
</tr>
<tr>
<td>203</td>
<td>編集範囲の超過</td>
</tr>
<tr>
<td>204</td>
<td>パケットの最大一致数を超過</td>
</tr>
<tr>
<td>205</td>
<td>エンジンのコールスタック数の超過</td>
</tr>
<tr>
<td>206</td>
<td>ランタイムエラー</td>
</tr>
<tr>
<td>207</td>
<td>パケットの読み込みエラー</td>
</tr>
<tr>
<td>300</td>
<td>サポートされていない暗号化</td>
</tr>
<tr>
<td>301</td>
<td>マスターキーの生成エラー</td>
</tr>
<tr>
<td>302</td>
<td>レコードレイヤメッセージ(準備ができていません)</td>
</tr>
<tr>
<td>303</td>
<td>ハンドシェークメッセージ(準備ができていません)</td>
</tr>
<tr>
<td>304</td>
<td>ハンドシェークメッセージの損失</td>
</tr>
<tr>
<td>305</td>
<td>メモリの割り当てエラー</td>
</tr>
<tr>
<td>306</td>
<td>サポートされていないSSLメッセージ</td>
</tr>
<tr>
<td>307</td>
<td>プレイステーションの復号化時のエラー</td>
</tr>
<tr>
<td>ID</td>
<td>イベント</td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
</tr>
<tr>
<td>308</td>
<td>クライアントによるロールバックの試行</td>
</tr>
<tr>
<td>309</td>
<td>更新エラー</td>
</tr>
<tr>
<td>310</td>
<td>鍵の交換エラー</td>
</tr>
<tr>
<td>311</td>
<td>SSL鍵交換の上限を超えた</td>
</tr>
<tr>
<td>312</td>
<td>鍵サイズの超過</td>
</tr>
<tr>
<td>313</td>
<td>ハンドシェイク内の不正なパラメータ</td>
</tr>
<tr>
<td>314</td>
<td>利用可能なセッションなし</td>
</tr>
<tr>
<td>315</td>
<td>末サポートの圧縮方法</td>
</tr>
<tr>
<td>316</td>
<td>サポートされていないアプリケーション層プロトコル</td>
</tr>
<tr>
<td>500</td>
<td>URI/パスの深さが超過</td>
</tr>
<tr>
<td>501</td>
<td>無効なトラバーサルルート</td>
</tr>
<tr>
<td>502</td>
<td>URIに使用できない文字</td>
</tr>
<tr>
<td>503</td>
<td>不完全なUTF8シーケンス</td>
</tr>
<tr>
<td>504</td>
<td>無効なUTF8の符号化</td>
</tr>
<tr>
<td>505</td>
<td>無効な16進の符号化</td>
</tr>
<tr>
<td>506</td>
<td>URI/パス長の超過</td>
</tr>
<tr>
<td>507</td>
<td>不正な文字の使用</td>
</tr>
<tr>
<td>508</td>
<td>二重デコードの攻撃コード</td>
</tr>
<tr>
<td>700</td>
<td>不正なBase64コンテンツ</td>
</tr>
<tr>
<td>710</td>
<td>破損したDeflate/GZIPコンテンツ</td>
</tr>
<tr>
<td>711</td>
<td>不完全なDeflate/GZIPコンテンツ</td>
</tr>
<tr>
<td>712</td>
<td>Deflate/GZIPチェックサムエラー</td>
</tr>
<tr>
<td>713</td>
<td>末サポートのDeflate/GZIP辞書</td>
</tr>
<tr>
<td>714</td>
<td>サポートされていないGZIPヘッダ形式/方法</td>
</tr>
<tr>
<td>801</td>
<td>プロトコルデコード検索の上限を超えた</td>
</tr>
<tr>
<td>802</td>
<td>プロトコルデコードの制約エラー</td>
</tr>
<tr>
<td>803</td>
<td>プロトコルデコードエンジンの内部エラー</td>
</tr>
<tr>
<td>804</td>
<td>プロトコルデコードの構造の制約</td>
</tr>
<tr>
<td>805</td>
<td>プロトコルデコードのスタックエラー</td>
</tr>
<tr>
<td>806</td>
<td>データの無限ループエラー</td>
</tr>
</tbody>
</table>
### 変更監視イベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>8000</td>
<td>情報</td>
<td>完全なベースラインの作成</td>
<td>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。</td>
</tr>
<tr>
<td>8001</td>
<td>情報</td>
<td>部分的なベースラインの作成</td>
<td>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。</td>
</tr>
<tr>
<td>8002</td>
<td>情報</td>
<td>変更の検索の完了</td>
<td>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。</td>
</tr>
<tr>
<td>8003</td>
<td>エラー</td>
<td>変更監視ルール内の不明な環境変数</td>
<td>ルールで ${env.EnvironmentVar} 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。</td>
</tr>
<tr>
<td>8004</td>
<td>エラー</td>
<td>変更監視ルール内の不正なベース値</td>
<td>無効な基本ディレクトリ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、該当する変更監視ルールのIDと名前、および無効な基本変数が含まれます。</td>
</tr>
<tr>
<td>8005</td>
<td>エラー</td>
<td>変更監視ルール内の不明なエンティティ</td>
<td>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のIDと名前、および検出された不明なEntitySetのカンマ区切りのリストが含まれます。</td>
</tr>
<tr>
<td>8006</td>
<td>エラー</td>
<td>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</td>
<td>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のIDと名前、および検出されたサポートされないEntitySet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。</td>
</tr>
<tr>
<td>8007</td>
<td>エラー</td>
<td>変更監視ルール内の不明な機能</td>
<td>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の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「executeable」です。</td>
</tr>
<tr>
<td>8008</td>
<td>エラー</td>
<td>変更監視ルール内のサポートされていない機能</td>
<td>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の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。</td>
</tr>
<tr>
<td>8009</td>
<td>エラー</td>
<td>変更監視ルール内の不明な属性</td>
<td>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のIDと名前、エンティティセットの種類（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。</td>
</tr>
<tr>
<td>8010</td>
<td>エラー</td>
<td>変更監視ルール内のサポートされていない属性</td>
<td>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のIDと名前、エンティティセットの種類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。</td>
</tr>
<tr>
<td>8011</td>
<td>エラー</td>
<td>変更監視ルール内のエンティティセットの不明な属性</td>
<td>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のIDと名前、エンティティセットの種類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。「&lt;FileSet base=&quot;c:\foo&quot;&gt; の代わりに &lt;FileSet dir=&quot;c:\foo&quot;&gt; を記述した場合にこのイベントが記録されます。</td>
</tr>
<tr>
<td>8012</td>
<td>エラー</td>
<td>変更監視ルール内の不明なレジストリ文字列</td>
<td>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の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。</td>
</tr>
<tr>
<td>8013</td>
<td>エラー</td>
<td>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</td>
<td>変更監視ルールXMLの形式が正しくないため、WQLクエリ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。</td>
</tr>
<tr>
<td>8014</td>
<td>エラー</td>
<td>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)</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>8015</td>
<td>警告</td>
<td>適用できない変更監視ルール</td>
<td>プラットフォームの一部、存在しないサブジェク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。</td>
</tr>
<tr>
<td>8016</td>
<td>警告</td>
<td>2番目に優先される変更監視ルール検出</td>
<td>(備考はありません)</td>
</tr>
<tr>
<td>ID</td>
<td>重要度</td>
<td>イベント</td>
<td>備考</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>8050</td>
<td>エラー</td>
<td>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。</td>
<td>(備考はありません)</td>
</tr>
</tbody>
</table>
セキュリティログ監視イベント

<table>
<thead>
<tr>
<th>ID</th>
<th>重要度</th>
<th>イベント</th>
</tr>
</thead>
<tbody>
<tr>
<td>8100</td>
<td>エラー</td>
<td>セキュリティログ監視エンジンのエラー</td>
</tr>
<tr>
<td>8101</td>
<td>警告</td>
<td>セキュリティログ監視エンジンの警告</td>
</tr>
<tr>
<td>8102</td>
<td>情報</td>
<td>セキュリティログ監視エンジンの初期化</td>
</tr>
</tbody>
</table>
変更監視ルールの言語

変更監視ルールの言語は、Deep Securityが監視するシステムコンポーネントおよび関連付けられた属性を記述した、宣言型のXMLベースの言語です。この言語を使用して、システム内に多数存在するコンポーネントの中から監視の対象外とするものを指定することもできます。

変更監視ルールを新しく作成する場合、次の2つの方法があります。ファイルに対する許可されない変更を監視するだけの場合は、「基本ルール」テンプレートを使用します。基本ルールテンプレートの使用方法の詳細については、ユーザインタフェースガイドまたはオンラインヘルプの変更監視ルールのプロパティ画面のドキュメントを参照してください。

コンピュータの他のエンティティ（ディレクトリ、レジストリ値、サービスなど）を監視するルールを作成する場合は、変更監視ルールの言語を使用してルールを作成する必要があります。変更監視ルールの言語を使用して変更監視ルールを新しく作成するには、[ポリシー]→[共通オブジェクト]→[ルール]→[変更監視ルール]→[新しい変更監視ルール]→[コンテンツ]の順に選択し、「カスタム (XML)」を選択します。

エンティティセット

変更監視ルールに含めるシステムコンポーネントは、「エンティティ」と呼ばれます。コンポーネントの各種類は、エンティティのクラスを表します。たとえば、ファイル、レジストリキー、プロセスは、それぞれエンティティのクラスです。変更監視ルールの言語には、エンティティの各クラスに対してエンティティのセット（エンティティセット）を記述するためのタグが用意されています。ルールには次の種類のエンティティセットを使用できます。

- DirectorySet: ディレクトリの変更を検索するルール
- FileSet: ファイルの変更を検索するルール
- GroupSet: グループの変更を検索するルール
- InstalledSoftwareSet: インストールされているソフトウェアの変更を検索するルール
- PortSet: 待機ポートの変更を検索するルール
- ProcessSet: プロセスの変更を検索するルール
- RegistryKeySet: レジストリキーを検索するルール
- RegistryValueSet: レジストリ値を検索するルール
- ServiceSet: サービスの変更を検索するルール
- UserSet: ユーザの変更を検索するルール
- WQLSet: Windows Management Instrumentation WQLクエリ文の結果の変更を検索するルール

1つの変更監視ルールに複数のエンティティセットを含めることができます。たとえば、複数のファイルとレジストリエントリを監視するルール1つで、アプリケーションを保護できます。

このセクションはエンティティセットについての概要説明です。各エンティティセットの詳細については、それぞれのページ（「DirectorySet (261ページ)」、「FileSet (263ページ)」、「GroupSet (266ページ)」、「InstalledSoftwareSet (267ページ)」、「PortSet (269ページ)」、「ProcessSet (272ページ)」、「RegistryKeySet (274ページ)」、「RegistryValueSet (276ページ)」、「ServiceSet (278ページ)」、「UserSet (280ページ)」および「WQLSet (283ページ)」）を参照してください。

階層とワイルドカード

FileSetやRegistryKeySetなどの階層型のデータの種類を表すエンティティセットでは、セクションベースのパターン照合がサポートされます。

- / (スラッシュ): 階層の各レベルに該当する箇所でパターンの各セクションを区切ります
- ** (2個のアスタリスク): ゼロ個以上のセクションに相当します

252
次のワイルドカードがサポートされます。

- ?（疑問符）: 1文字に相当します
- *（1個のアスタリスク）: ゼロ個以上の文字に相当します

次の「エスケープ」文字もサポートされます。

- \（バックスラッシュ）: 直後の文字をエスケープします

「/」の文字でパターンをセクションに分割します。分割したセクションが一致するかぎり、パターンの各セクションが階層のそれぞれの下位レベルに適用されます。たとえば、次のようなパターンがあります。

/a?c/123/*.*.java

これが次のパスに適用された場合

/abc/123/test.java

次のように判定されます。

- 「a?c」は「abc」に一致
- 「123」は「123」に一致
- 「*.java」は「test.java」に一致

このパターンが次のパスに適用された場合

/abc/123456/test.java

次のように判定されます。

- 「a?c」は「abc」に一致
- "「123」は「123456」に一致しないため、そこから先はパターン照合は実行されない

「**」の記号パターンは、ゼロ個以上のセクションと照合します。したがって、次のパターンの場合

/abc/**/*.*.java

「abc/123/test.java」と「abc/123456/test.java」の両方に一致します。また、「abc/test.java」と「abc/123/456/test.java」にも一致します。

構文とコンセプト

このセクションでは、変更監視ルールの例をいくつか示します。以下の例ではFileSetエンティティセットを使用しますが、説明および使用コンポーネントはすべてのエンティティセットに適用できます。変更監視ルールの最小の形は、次のような構文です。

```xml
<FileSet base="C:\Program Files\MySQL">
  ...
</FileSet>
```

「base」属性には、FileSetのベースディレクトリを指定します。ルールに関するすべての項目は、このディレクトリを基準とした相対ディレクトリに保存されます。上記のルールを変更しなければ、「base」以下のすべてのもの（サブディレクトリも含む）について変更が監視されます。

注意: ワイルドカード「*」と「?」を「base」属性の文字列に使用できますが、使用できるのはパスの最後のセクションだけです。したがって、次の記述は有効です。

```xml
base="C:\program files\CompanyName * Web Server"
```

しかし、次のような記述は無効です。
エンティティセット内では、「include」および「exclude」タグを使用してパターン照合を制御できます。これらのタグには、照合するパターンを指定する「key」属性があります。 「key」属性の内容はエンティティセットによって異なります。たとえば、ファイルやディレクトリではパスが「key」属性の内容になりますが、ポートの場合は「プロトコル/IP/ポート番号」の組み合わせになります。

**注意:** 「include/exclude」ルールに記述したパスの構文が無効な場合、Agentによって「変更監視ルールのコンパイルの問題」のイベントが生成され、ルールIDと拡張後のパスがパラメータとして提供されます。C:\teat1\D:\teat2は無効なパスの例ですが、これは、ファイル名に2つのボリュームIDを含めることができないのでです。

### Include

includeタグは、基本的にはホワイトリストのことです。includeタグを使用すると、そのincludeタグ (または他のincludeタグ) に一致するエンティティのみが含まれます。includeタグを追加した次のルールは、「C:\Program Files\MySQL」フォルダとそのサブボリュームフォルダ内にある「*.exe」という名前の付いたファイルについてのみ変更を監視します。

```xml
<FileSet base="C:\Program Files\MySQL">
    <include key="**/*.exe"/>
</FileSet>
```

includeタグの構文を組み合わせることもできます。次のルールは、「C:\Program Files\MySQL」フォルダとそのサブボリュームフォルダ内にある、「*.exe」と「*.dll」という名前の付いたファイルに対する変更を監視します。

```xml
<FileSet base="C:\Program Files\MySQL">
    <include key="**/*.exe"/>
    <include key="**/*.dll"/>
</FileSet>
```

1つのincludeブロック内に複数の条件を含めることもできます。この場合、対象となる所定のエンティティに対してすべての条件が適用されます。次の「include」タグは、名前の末尾に「.exe」の文字があり、先頭に「sample」の文字があるエンティティを含めることが要求します。この条件はもっと簡潔に記述することもできますが、後述の「機能」のセクションで説明されているように、「key」パターンとエンティティの他の機能を組み合わせたときに、この構文の方が汎用性があることがわかります。

```xml
<include>
    <key pattern="**/*.exe"/>
    <key pattern="**/sample*"/>
</include>
```

次の構文は、同じ条件を他の方針で記述したものでです。

```xml
<include key="**/*.exe">
    <key pattern="**/sample*"/>
</include>
```

### Exclude

excludeタグは、ファイルのブラックリストとして機能します。ファイルセットから不要なファイルを除外して、返されないようにします。次の例は、実際にはありませんが、tempファイル以外のすべてのファイルを監視対象にします。

```xml
<FileSet base="C:\Program Files\MySQL">
    <include key="**"/>
    <exclude key="**/*.tmp"/>
</FileSet>
```

次のルールは、EXEとDLLのファイルセットから「MySQLInstanceConfig.exe」を除外します。
include/excludeタグのパターン照合での大文字/小文字の区別は、「casesensitive」属性で制御できます。この属性は次の3つの値をとります。

- true
- false
- platform

この属性の初期設定は「platform」です。これは、パターンの大文字/小文字の区別を実行中のプラットフォームの大文字/小文字の区別と照合します。次の例の場合、Windowsシステムでは「Sample.txt」と「sample.txt」が返されますが、UNIXシステムで返されるのは「Sample.txt」のみです。

```
<FileSet base="C:\Program Files\MySQL">
    <include key="**/*Sample*">
    </include>
</FileSet>
```

次の例では、Windowsの場合もUNIXの場合も「Sample.txt」のみが返されます。

```
<FileSet base="C:\Program Files\MySQL">
    <include key="**/*Sample*" casesensitive="true"/>
</FileSet>
```

注意: 大文字/小文字の区別を「true」に設定するのは、Windowsのように、ほとんどのオブジェクト名に対して大文字/小文字の区別をしないプラットフォームに限られます。

機能

エンティティの種類によっては、「key」以外の機能に基づいてエンティティをファイルセットに含めたり、除外したりすることができます。エンティティの種類によって、機能のセットは異なります。次の例は、すべての実行可能ファイルを含めます。ファイル拡張子を使用した前述の例のようにファイル拡張子には依存せず、ファイルの最初の数百バイトをチェックして、そのOSで実行可能なファイルかどうかを判定します。

```
<FileSet base="C:\Program Files\MySQL">
    <include key="**" executable="true"/>
</FileSet>
```

機能属性は「include」または「exclude」タグに指定する必要があります。複数の条件を指定するinclude/excludeの一部として機能属性を使用するには、include/excludeの囲みタグの属性として指定する必要があります。次の例は、ファイル名に「MySQL」の文字列を含むすべての実行可能ファイルを含めます。

```
#include executable="true">
    <key pattern="**/MySQL*">
</include>
```
上記の例は、次のようにもっと簡潔に記述することができます。

`<include key="**/*MySQL*" executable="true"/>`

機能属性によっては、単にエンティティのいずれかの属性の値を照合するだけのものもあります。そのようなときには、「*」と「?」
のワイルドカードで照合できる場合があります。この方法でinclude/excludeルールに使用できる属性について、およびワイルドカー
ド照合と単純な文字列照合のどちらがそれらの属性でサポートされるかについては、各エンティティセットのヘルプ画面を参照してく
ださい。

**注意:** ワイルドカード照合がサポートされる場合は、属性の文字列の値についての照合になりますが、正規化は行われないので
で注意が必要です。「**」などのエンティティのキー照合に使用できる構造体やコンポーネントを階層に分ける「/」
の使用は適用されません。Windowsのパス名を照合するには、「\」の使用が必要です。これは、チェックの対象とな
る属性の値にこの文字が含まれているためです。これに対し、UNIXシステムではパスの値に「/」が使われるため、
UNIXパスの照合には「/」を使用する必要があります。

次のルールは、「state」属性を使用した機能照合の例です。

```xml
<ServiceSet>
  <include state="running"/>
</ServiceSet>
```

**注意:** state照合ではワイルドカードはサポートされません。

次の例は、バイナリのパスの末尾が「\notepad.exe」となっているプロセスを照合します。

```xml
<ProcessSet>
  <include path="\*\notepad.exe"/>
</ProcessSet>
```

次の例は、コマンドラインが「/sbin/」から始まるプロセスを照合します。

```xml
<ProcessSet>
  <include commandLine="/sbin/*"/>
</ProcessSet>
```

**注意:** ワイルドカードの使用には注意が必要です。「**」のワイルドカード表現は、「base」以下のすべてのサブディレク
トリ内のすべてのファイルを検索します。このような表現のベースラインを構築するには、多くの時間とリソースが必
要です。

**ANDとOR**

複数の条件を指定するinclude/excludeタグと複数のinclude/excludeタグを使用して、論理ANDと論理ORを記述することができま
す。

複数の条件を指定するincludeまたはexcludeを使用してANDを記述するにはいくつかの方法があります。最も簡単な方法は、複数の条
件を1種類の囲みタグで囲む方法です。次の例は、複数の条件を指定する簡単なAND構文です。

```xml
<include>
  <key pattern="**/*MySQL*" />
  <key pattern="**/*.exe"/>
</include>
```

また、囲みタグの属性に条件を記述すると、その条件は、複数の条件を指定する要件の一部として囲まれた条件でグループ化されま
す。次の例は、上記の複数の条件を指定する「include」タグをこのように書き直したものです。

```xml
<include key="**/*.exe"/>
  <key pattern="**/*MySQL*"/>
</include>
```

最後の例は、複数の条件をinclude/excludeタグの属性に記述したものですが、これもANDとして扱われます。
ORは、複数のinclude/excludeタグに条件を含めるだけで記述できます。次のコードは、ファイル名に「.exe」または「.dll」を含むファイルを返します。

```
#include key="**/*.dll" />
#include key="**/*.exe" />
```

### 評価の順序
ルール内での出現順序にかかわらず、まず、すべての「include」が処理されます。オブジェクト名がいずれかの「include」タグに合致すると、「exclude」タグと照合チェックされます。オブジェクト名がいずれかの「exclude」タグと合致すると、監視対象オブジェクトのセットから除外されます。

### エンティティ属性
各エンティティには、監視対象となる属性のセットがあります。エンティティセットに属性が指定されていない（属性のラッパータグがない）場合は、そのエンティティのSTANDARDセットの属性があるものとみなされます（各エンティティセットについては、「簡略記法属性」セクションを参照してください）。

ただし、エンティティセットによっては、エンティティの特定の属性のみが変更監視の対象となります。たとえば、ログファイルの内容の変更は、通常、変更されることが前提として許可されています。しかし、アクセス許可や所有権の変更はレポートの対象にする必要があります。

エンティティセットの「attributes」タグには、こうしたことを記述できます。「attributes」タグには、監視対象とする属性を列挙したタグのセットを指定します。許可される「attribute」タグのセットの内容は、タグのセットを指定するエンティティセットによって異なります。

注意: 「attributes」タグが存在しても属性が指定されていない場合、ルールで定義されたエンティティは、その存在だけが監視されます。

次の例は、「C:\Program Files\MySQL」ディレクトリ内でファイル名に「SQL」の文字列を含む実行ファイルについて、「last modified」、「permissions」、および「owner」の各属性に関する変更を監視します。

```
<FileSet base="C:\Program Files\MySQL" >
  <include key="**/*SQL*" executable="true"/>
  <attributes>
    <lastModified/>
    <permissions/>
    <owner/>
  </attributes>
</FileSet>
```

次の例は、「C:\Program Files\MySQL」内のログファイルの「permissions」と「owner」の属性を監視します。

```
<FileSet base="C:\Program Files\MySQL" >
  <attributes>
    <permissions/>
    <owner/>
  </attributes>
</FileSet>
```

次の例は、属性のSTANDARDセットを監視します（後述の「簡略記法属性」を参照)。

```
<FileSet base="C:\Program Files\MySQL" >
  <include key="**/*.log" />
</FileSet>
```
次の例では、監視対象となる属性がありません。エンティティの存在に関する変更のみが監視対象となります。

```xml
<FileSet base="C:\Program Files\MySQL">
  <attributes/>
  <include key="**/*.log"/>
</FileSet>
```

### 簡略記法属性

簡略記法属性を使用すると、上位レベルの属性を1つ指定するだけで属性のグループを指定できます。通常の属性と同じく、許可される値のセットの内容は、属性を指定するエンティティセットによって異なります。

簡略記法属性が役に立つのは、属性のセットが自然に集まっている場合、属性のセットをすべて列挙することが煩雑な場合、および上位レベルの属性で表された属性のセットが時間とともにまたはシステム構成によって変更される可能性のある場合などです。各ケースの例を以下に示します。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD</td>
<td>エンティティセットを監視するための属性のセット。これは、エンティティセットの「ありうるすべての属性」とは異なります。たとえば、ありうるすべてのハッシュアルゴリズムが含まれることなく、必要とみなされるものだけが含まれます。各エンティティセットの「standard」属性のリストについては、個々のエンティティセットのセクションを参照してください。</td>
</tr>
<tr>
<td>CONTENTS</td>
<td>ファイルの内容のハッシュまたはハッシュのセットを表す簡略記法属性です。SHA-1に初期設定されています。</td>
</tr>
</tbody>
</table>

### onChange

変更をリアルタイムで監視するように、エンティティセットを設定できます。エンティティセットのonChange属性をtrue (初期設定値) に設定すると、エンティティセットによって返されるエンティティは、変更がリアルタイムで監視されます。変更が検出されると、すぐにそのエンティティがベースラインと比較されます。エンティティセットのonChange属性がfalseに設定されている場合、ベースラインが作成されたとき、または予約タスクから、あるいは必要に応じてDeep Security Managerで開始されたときにのみ実行されます。

次の例では、MySQLバイナリをリアルタイムで監視します。

```xml
<FileSet base="C:\Program Files\MySQL" onChange="true">
  <include key="**/*.exe"/>
  <include key="**/*.dll"/>
</FileSet>
```

### 環境変数

環境変数は、エンティティセットで使用されるベース値に含めることができます。環境変数は「${}」で囲みます。変数名の前頭に「env.」の文字列が付けられます。

次の例は、FileSetのベースディレクトリを、PROGRAMFILES環境変数に格納されたパスに設定します。

```xml
<FileSet base="${env.PROGRAMFILES}"/>
```

注意：参照される環境変数の値は、Deep Security Agentの起動時にAgentによって読み込まれて格納されます。環境変数の値が変更されると、変更内容を登録するためにAgentが再起動されます。

参照先の環境変数が見つからない場合、その環境変数を参照しているエンティティセットは検索も監視もされませんが、それ以外の構成は使用されます。変数が存在しないことを示すアラートがトリガーされます。Agentイベント「変更監視ルールのコンパイルの問題」を使用して、Agentが不正な環境変数を報告します。変更監視ルールのIDと環境変数の名が、イベントのパラメータとして提供されます。
レジストリ値

レジストリ値は、エンティティセットで使用されるベース値に含めることができます。レジストリ値は「${}」で囲みます。レジストリ値のパスの先頭には「reg.」が付けられます。次の例は、FileSetのベースディレクトリを、「HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder」レジストリ値に格納されたパスに設定します。

```
<FileSet base="${reg.HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder}"/>
```

次の例は、FileSetのベースディレクトリを、「HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder」レジストリ値に格納されたパスに設定します。

参照先のレジストリ値は、Agentが新しいルールまたは変更されたルールを受信したときに読み込まれます。また、Agentは起動時にすべてのルールをチェックし、参照先のレジストリ値が変更されていた場合は、影響を受けるルールのベースラインを再構築します。

参照先のレジストリ値が見つからない場合、その環境変数を参照しているエンティティセットは検索も監視もされませんが、それ以外の構成は使用されます。変数が存在しないことを通知するアラートが発令されます。Agentは、イベント8012を使用して環境変数の不正な変更を報告します。変更監視ルールのIDとレジストリ値のパスが、パラメータとしてイベントに提供されます。

注意: ワイルドカードは、ベース名の構造体の最後のコンポーネントにのみ使用できます。たとえば、「base="HKLM\Software\ATI*"」は有効で、「HKLM\Software\ATI」と「HKLM\Software\ATI Technologies」の両方を検出します。ただし、「base="HKLM\Software\ATI++"」は無効です。

「..」の使用

親ディレクトリへの参照を示す「..」符号は、Agentの現在のすべてのバージョンでサポートされるようになりました。Agentは、FileSetとDirectorySet要素のベースディレクトリ名の正規化を行いますが、このとき、「..」参照を解決し、Windowsの短い名前を長い名前に変換します。たとえば、Vistaでは、次のFileSetのベースディレクトリは「C:\Users」です。Vista以前のWindowsでは、ベースディレクトリは「C:\Documents and Settings」です。

```
<FileSet base="${env.USERPROFILE}\..">
    <include key="*/Start Menu/Programs/Startup/*"/>
</FileSet>
```

ベストプラクティス

ルールは、重要なオブジェクトと属性のみを含めるように記述してください。こうすることで、オブジェクトの他属性が変更されても、イベントは報告されなくなります。たとえば、変更監視ポリシーで「/bin」ディレクトリ内のファイルのアクセス権と所有権を制限することもできます。変更監視ルールは所有者、グループ、およびアクセス権を監視しますが、lastModifiedやハッシュ値などの属性は監視しません。

変更監視ルールを使用して、不正プログラムや不審なアクティビティの検出、サービスの監視、NTFSデータストリームの使用状況の監視、および通常の場所以外のディレクトリ（'/tmp'や'${env.windir}\temp'など）に置かれた実行可能ファイルの監視などを実施します。

ルールに含めるオブジェクトを指定する場合は、必ず、できるだけ詳細に指定してください。ルールに含めるオブジェクトが少ないほど、短期間でベースラインを作成でき、変更の検査にかかる時間も短くなります。変更される可能性のあるオブジェクトは除外し、監視する属性は必要なものだけに絞ります。

禁止事項

- 「/」、「C:¥」、または「HKLM\Software」などのディレクトリ階層の最上位で、「**/...」を使用すること
- 必要がないのに、データのハッシュの種類を複数使用すること
- 参照先として、HKEY_CURRENT_USER、${env.USERPROFILE}、または${env.HOME}などのユーザ固有の場所を指定すること
これらのいずれかが変更監視ルールに記述されていると、Deep Security Agentでは指定されたパターンに照合するために多数の項目を探索してしまうため、パフォーマンスが低下します。
DirectorySet

DirectorySetタグは、ディレクトリのセットを記述します。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>DirectorySetのベースディレクトリを設定します。タグ内の他の要素はすべて、このディレクトリから相対的に位置付けられます。</td>
<td>はい</td>
<td>なし</td>
<td>文字列値は、構文的に有効なパスに変換されます (パスは存在しなくても構いません)。注意: UNCパスはWindows Agentで許可されますが、それには、リモートシステムでAgentコンピュータの「LocalSystem」アカウントからのアクセスが許可される必要があります。AgentはWindowsサービスの1つであり、LocalSystem (別名: NT AUTHORITY\SYSTEM) として実行されます。ネットワークリソースにアクセスするとき、LocalSystemは、コンピュータの資格情報であるDOMAIN\MACHINESという名前のアカウントを使用します。リモートコンピュータに表示されるアクセスストーンには、そのコンピュータの「Administrators」グループも含まれます。したがってリモート共有は、Agentのコンピュータアカウント、AgentのコンピュータのAdministratorsグループ、または「Everyone」のいずれかの読み取り権限を付与する必要があります。UNCパスへのアクセスをテストするには、この手法を使用して、LocalSystemアカウントのサービスとして実行するWindowsコマンドプロンプトを起動します。それによって、ネットワークおよびローカルのリソースへのアクセスを試したり、LocalSystemアカウントで実行される他のアプリケーションを起動したりできます。baseの値が構文的に有効でない場合は、FileSetは処理されません。それ以外の設定は評価されます。</td>
</tr>
<tr>
<td>onChange</td>
<td>対象のディレクトリをリアルタイムで監視する必要があるかどうかを示します。</td>
<td>×</td>
<td>false, true, false</td>
<td></td>
</tr>
<tr>
<td>followLinks</td>
<td>このDirectorySetはシンボリックリンクを追跡します。</td>
<td>×</td>
<td>false, true, false</td>
<td></td>
</tr>
</tbody>
</table>

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- **Created**: ディレクトリの作成日時のタイムスタンプ
- **LastModified**: ディレクトリの最終アップデート日時のタイムスタンプ
- **LastAccessed**: ディレクトリの最終アクセス日時のタイムスタンプ。Windowsの場合、この値はすぐにアップデートされません。また、パフォーマンスを向上させるために、最終アクセス日時のタイムスタンプの記録を無効にすることができます。詳細については、「ファイルの時刻」を参照してください。LastAccessed属性には、ディレクトリ検索を実行するのにはAgentがそのディレクトリを開く必要があり、これにより最終アクセス日時のタイムスタンプが変更されるという問題もあります。
- **Permissions**: Windowsの場合は、ディレクトリのセキュリティ記述子 (SDDL形式)。ACLをサポートするUNIXシステムの場合は、PosixスタイルのACL。それ以外の場合は、数値 (8進数) 形式のUNIXスタイルのrwxrwxrwxのファイル権限。
- **Owner**: ディレクトリ所有者のユーザID (通常、UNIXでは「UID」と呼ばれます)
- **Group**: ディレクトリ所有者のグループID (通常、UNIXでは「GID」と呼ばれます)
• **Flags**: Windowsのみ。`GetFileAttributes()` Win32 APIから返されるフラグ。Windowsエクスプローラでは、これらをファイルの「属性」（読み取り専用、アーカイブ、圧縮など）とみなします。

• **SymLinkPath**: ディレクトリがシンボリックリンクである場合は、そのリンクのパスがここに格納されます。Windowsでは、SysInternalsの「junction」ユーティリティを使用して、symlinkに相当するWindows機能を作成します。

• **InodeNumber (UNIX/Linuxのみ)**: ファイルに関連付けられているinodeが格納されるディスクのinode番号

• **DeviceNumber (UNIX/Linuxのみ)**: ディレクトリに関連付けられているinodeが格納されるディスクのデバイス番号

**簡略記法による属性**

次に、簡略記法による属性と、それらがマッピングされる属性を示します。

- **STANDARD**:
  - Created
  - LastModified
  - Permissions
  - Owner
  - Group
  - Flags (Windowsのみ)
  - SymLinkPath

**「key」の意味**

keyは、「dir」で指定されたディレクトリを基準とする相対ディレクトリパスに対して照合されるパターンを指定します。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンです。パターン内のセクションは、所定のOSのファイルのセパレータによって区切られたパスのセクションに対して照合されます。

**サブエレメント**

• **Include**
• **Exclude**

これらのエレメントに指定できる属性とサブエレメントについては、include/excludeの一般的な説明 (252ページ) を参照してください。ここでは、このエンティティセットクラスに関連するinclude/excludeに固有の情報を記載します。
FileSetタグは、ファイルのセットを記述します。

### タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>FileSetのベースディレクトリを設定します。タグ内の他のエレメントはすべて、このディレクトリから相対的に位置付けられます。</td>
<td>はい</td>
<td>ファイル名のパス（存在しない場合でも構いません）。注意：UNCパスはWindows Agentで許可されますが、それには、リモートシステムでAgentコンピュータの「LocalSystem」アカウントからのアクセスが許可される必要があります。AgentはWindowsサービスの1つであり、LocalSystem (別名:NT AUTHORITY\SYSTEM) として実行されます。ネットワークリソースにアクセスするとき、LocalSystemは、コンピュータの資格情報であるDOMAINVMACHINESという名前のアカウントを使用します。リモートコンピュータに表示されるアクセスストークンには、そのコンピュータの「Administrators」グループも含まれます。したがってリモート共有は、Agentのコンピュータアカウント、AgentのコンピュータのAdministratorsグループ、または「Everyone」のいずれかに読み取り権限を付与する必要があります。UNCパスへのアクセスをテストするには、この手法を使用して、LocalSystemアカウントのサービスとして実行するWindowsコマンドプロンプトを起動します。それによって、ネットワークおよびローカルのリソースへのアクセスをしたしたり、LocalSystemアカウントで実行される他のアプリケーションを起動したりできます。baseの値が構文的に有効でない場合は、FileSetは処理されません。それ以外の設定は評価されます。</td>
</tr>
<tr>
<td>onChange</td>
<td>対象のファイルをリアルタイムで監視する必要があるかどうかを示します。</td>
<td>いいえ</td>
<td>false, true, false</td>
</tr>
<tr>
<td>followLinks</td>
<td>このFileSetはシンボリックリンクを追跡します。</td>
<td>いいえ</td>
<td>false, true, false</td>
</tr>
</tbody>
</table>

### エンティティセットの属性

次に示すFileSetの属性は、変更監視ルールによって監視可能な属性です。

- **Created**: ファイルの作成時刻のタイムスタンプ
- **LastModified**: ファイルの最終更新時刻のタイムスタンプ
- **LastAccessed**: ファイルの最終アクセス時刻のタイムスタンプ。Windowsの場合、この値はすぐにアップデートされません。また、パフォーマンスを向上させるために、最終アクセス日時のタイムスタンプの記録を無効にすることはできます。詳細については、「ファイルの時刻」を参照してください。LastAccessed属性には、ファイル検索を実行するにはAgentが対象のディレクトリを開く必要があり、これにより最終アクセス日時のタイムスタンプが変更されるという問題もあります。UNIXの場合、ファイルを開くときにO_NOATIMEフラグが使用可能であれば、Agentはこのフラグを使用します。それにより、最終アクセス日時のタイムスタンプがOSによってアップデートされることがなくなり、検索速度を上げることができます。
- **Permissions**: Windowsの場合、ファイルのセキュリティ記述子（SDDL形式）。ACLをサポートするUNIXシステムの場合は、PosixスタイルのACL。それ以外の場合は、数値（8進数）形式のUNIXスタイルのrwxrwxrwxのファイル権限。
- **Owner**: ファイル所有者のユーザID（通常、UNIXでは「UID」と呼ばれます）
• Group: ファイル所有者のグループID (通常、UNIXでは「GID」と呼ばれます)
• Size: ファイルのサイズ
• Sha1: SHA-1ハッシュ
• Sha256: SHA-256ハッシュ
• Md5: MD5ハッシュ
• Flags: Windowsのみ。GetFileAttributes() Win32 APIから返されるフラグ。Windowsエクスプローラでは、これらをファイルの「属性」(読み取り専用、アーカイブ、圧縮など) とみなします。
• SymLinkPath (UNIX/Linuxのみ): ファイルがシンボリックリンクである場合は、そのリンクのパスがここに格納されます。Windows NTFSでは、UNIXライクなシンボリックリンクをサポートしますが、ファイルではなくディレクトリ専用です。WindowsのショートカットオブジェクトはOSでは処理されないため、本当の意味でのシンボリックリンクではありません。Windowsエクスプローラはショートカットファイル (*.lnk) を処理しますが、*.lnkファイルを開くその他のアプリケーションはlnkファイルのコンテンツの表示のみ行います。
• InodeNumber (UNIX/Linuxのみ): ファイルに関連付けられているinodeが格納されるディスクのinode番号
• DeviceNumber (UNIX/Linuxのみ): ファイルに関連付けられているinodeが格納されるディスクのデバイス番号
• BlocksAllocated (Linux/UNIXのみ): ファイルを格納するために割り当てられるブロック数。

簡略記法による属性

次に、簡略記法による属性と、それらがマッピングされる属性を示します。

• CONTENTS: ポリシーまたはコンピュータエディタの[変更監視]→[詳細]で設定されているコンテンツのハッシュアルゴリズムに変換されます。
• STANDARD: Created、LastModified、Permissions、Owner、Group、Size、Contents、Flags (Windowsのみ)、SymLinkPath (Linux/UNIXのみ)

ディレクトリとしてマウントされたドライブ

ディレクトリとしてマウントされたドライブは他のディレクトリと同様に扱われます。ただし、ネットワークドライブである場合、そのドライブは無視されます。

代替データストリーム

NTFSベースのファイルシステムでは、代替データストリームの概念がサポートされます。この機能が使用される場合には、代替ストリームは概念上、ファイル内のファイルのように動作します。

<table>
<thead>
<tr>
<th>注意:</th>
<th>この機能のデモを実行するには、コマンドプロンプトに以下のコマンドを入力します。</th>
</tr>
</thead>
</table>
| echo plain > sample.txt  
echo alternate > sample.txt:s  
more < sample.txt  
more < sample.txt:s |

最初の「more」は、テキスト「plain」のみを表示します。これは、メモ帳などの標準のテキストエディタでファイルを開いた場合に表示されるテキストと同じです。2番目の「more」は、sample.txtの「s」ストリームにアクセスして文責列「alternate」を表示します。

FileSetでは、ストリームが指定されていない場合、すべてのストリームが含まれます。各ストリームは、ベースラインの個別のエンティエティエントリーです。ストリームに対して指定できる属性は次のとおりです。

• size
次の例では、前のデモで使用したストリームが両方とも含まれます。

```xml
<include key="**/sample.txt" />
```

特定のストリームを含めたり除外したりするには、「:」表記を使用します。次の例では、メインのsample.txtストリームではなく、sample.txtの「S」ストリームのみが一致します。

```xml
<include key="**/sample.txt:s" />
```

パターン照合は、ストリーム表記でもサポートされます。次の例では、sample.txtが含まれますが、その代替ストリームはすべて除外されます。

```xml
<include key="**/sample.txt" />
<exclude key="**/*sample.txt:" />
```

「key」の意味

dkeyは、「base」で指定されたディレクトリを基準とする相対ファイルパスに対して照合されるパターンを指定します。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンです。パターン内のセクションは、所定のOSのファイルのセパレータによって区切られたパスのセクションに対して照合されます。

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントについては、include/excludeの【一般的な説明】(252ページ)を参照してください。ここでは、FileSetエンティティセットクラスに関連するinclude/excludeに固有の情報のみを記載します。

FileSetのinclude/excludeに固有的属性

**executable**

ファイルが実行可能かどうかを決定します。これは、ファイルの権限がファイルの実行を許可していることを意味しません。ファイルの内容を確認するのではなく、プラットフォームに応じて、そのファイルが実行可能ファイルであるかどうかを決定します。

注意: これは、Agentがファイルを開き、ファイルの先頭から1KBまたは2KBを検証して有効な実行可能イメージヘッダを探すことが必要になるため、比較的負荷の高い処理です。1つ1つのファイルを開いて読み取ることは、ディレクトリを検索してファイルパターンに基づいてファイル名を照合する処理に比較すると、非常に高い負荷がかかります。結果として、「executable」を使用するinclude/excludeルールでは、この属性を使用しないルールよりも検索に時間がかかります。
GroupSet

GroupSetはグループのセットを表します。これらはローカルグループのみです。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>リアルタイムで監視するかどうかを示します。</td>
<td>いいえ</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

エンティティセットの属性

監視可能なエンティティの属性には次のものがあります。

- **Description**: (Windowsのみ) グループのテキストによる説明。
- **Group**: グループのIDと名前。グループ名はエンティティキーの一部ですが、グループの名前を変更した場合やグループに新しいIDを付けた場合に、グループのIDと名前のペアを監視できることが重要になります。通常、OSはIDに基づいてセキュリティを実施します。
- **Members**: グループメンバーのカンマ区切りのリスト。
- **SubGroups**: (Windowsのみ) グループのサブグループのカンマ区切りのリスト。

簡略記法による属性

- **Standard**: グループメンバーのサブグループ

「key」の意味

このkeyはグループの名前です。これは階層型のEntitySetではありません。パターンはグループ名のみに適用されます。結果として、「**」パターンは適用できません。次の例は、「Administrators」グループの追加と削除を監視します（「Member」属性はSTANDARDセットの一部であるため黙示的に含まれます。明確にリストされる属性はありません）。

```xml
<GroupSet>
  <include key="Administrators" />
</GroupSet>
```

サブエレメント

include/exclude

これらのエレメントに指定できる属性とサブエレメントについては、include/excludeの一般的な説明を参照してください。
InstalledSoftwareSet

インストールされたソフトウェアのセットを表します。インストールされたアプリケーションを一意に識別するために使用される「key」は、プラットフォーム固有の構成ですが、多くの場合、アプリケーション名の簡略名か一意の数値です。

Windowsでは、このkeyは「FogBugz Screenshot_is1」のように読むで意味のわかる形式で、「{90110409-6000-11D3-8CFE-0150048383C9}」のようなGUIDです。これは、HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstallのサブキーを調べることによって確認できます。

Linuxでは、このkeyはRPMパッケージ名であり、次のコマンドを入力すると表示されます。

rpm -qa --qf "%{NAME}\n"

Solarisでは、このkeyはパッケージ名であり、「pkginfo」コマンドを入力すると表示されます。

HP-UXでは、このkeyはアプリケーション名であり、次のコマンドを入力すると表示されます。

/usr/sbin/swlist -a name

タグ属性

次に示すXML属性のタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>リアルタイムで監視するかどうかを示します。</td>
<td>いいえ</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。エンティティの属性の有無は、プラットフォームとアプリケーション自体の両方に依存します。インストールプログラムが、すべての属性の値を設定する必要はありません。

- **Manufacturer**: アプリケーションのパブリッシャまたはマニファクチャ
- **Name**: アプリケーションのフレンドリ名または表示名。Linuxでは使用できません。
- **InstalledDate**: インストールの日付。通常は、YYYY-MM-DD [HH:MM:SS] の形式で返されますが、Windowsの多くのインストーラは日付文字列を別でフォーマットするため、このフォーマットは保証されません。AIXでは使用できません。
- **InstallLocation**: アプリケーションがインストールされるディレクトリ。Windows、Solaris、およびHPUXでのみ利用可能です。
- **Parent**: パッチおよびアップデートの場合、このアイテムの親のkey名を示します。Windowsでのみ利用可能です。
- **Size**: 利用可能な場合、アプリケーションの推定サイズ。Windowsでは、この属性は「HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*」の下の「EstimatedSize」レジストリ値から読み込まれます。その場合の値はKB単位で表されるため、Agentでは1024を掛けてから値を返します。すべてのWindowsアプリケーションで、レジストリのEstimatedSizeフィールドに値が設定されるわけではありません。この属性はAIXでは使用できません。
- **Version**: インストールされたアプリケーションのバージョン。Windowsでは、このパスは、「DisplayVersion」レジストリ値から取得されます。

簡略記法による属性

次に、エンティティの簡略記法による属性と、解釈される属性を示します。
**STANDARD:** InstalledDate、Name、Version

「key」の意味

keyは、インストールされたソフトウェアの名前です。階層型のキーではないため、**パターンは適用できません。Windowsでは、多くの場合、このkeyはGUIDです（特に、Windowsインストーラ（別名MSI）を使用してインストールされたソフトウェアの場合）。GUIDではなく表示名に基づいてinclude/excludeを実行する必要がある場合は、name="XXX"機能を使用します。

次の例では、新しいソフトウェアの追加および削除を監視します。

```xml
<InstalledSoftwareSet>
  <include key="*"/>
  <attributes/>
</InstalledSoftwareSet>
```

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントについては、include/excludeの一般的な説明（252ページ）を参照してください。ここでは、このエンティティセットクラスに関連するinclude/excludeに固有的情報のみを記載します。

InstalledSoftwareSetsのinclude/excludeに固有的属性

**name (Windowsのみ)**

エンティティの「name」属性であるアプリケーション表示名に対して、?および*を使用するワイルドカード照合を実行できます。たとえば、次のとおりです。

```xml
<InstalledSoftwareSet>
  <include name="Microsoft*"/>
</InstalledSoftwareSet>
```

コントロールパネルに表示される表示名が、「Microsoft」で始まるインストール済みアプリケーションすべてに一致します。

**manufacturer**

アプリケーションのパブリッシャまたはマニファクチャに対して、?および*を使用するワイルドカード照合を実行できます。たとえば、次のとおりです。

```xml
<InstalledSoftwareSet>
  <include manufacturer="* Company "/>
</InstalledSoftwareSet>
```

マニファクチャが「Company」で終了するインストール済みアプリケーションすべてに一致します。
PortSet

待機ポートのセットを表します。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>リアルタイムで監視するかどうかを示します。</td>
<td>いいえ</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- **Created**: (Windowsのみ - XP SP2以降およびServer 2003 SP1以降) GetExtendedTcpTable() または GetExtendedUdpTable() APIによって返されます。このTCP/UDPリンクが作成されたバインド処理の発生時刻を示します。

- **Listeners**: プロトコル/アドレス/ポートの組み合わせにおけるアクティブなリスナーの数です。指定されたポートにバインドされているソケットと待機中のソケットの数が反映されます。この数は、プロセスがポートに複数のソケットをバインドしている場合、ポートを待機しているプロセスの数より大きくなることがあります。指定されたポートにバインドされているソケットが1つだけの場合、この属性の値はありません。

- **Path**: (Windowsのみ - XP SP2以降およびServer 2003 SP1以降) ポートを所有するモジュールの短い名前を示します。（存在する場合）。Windowsでは、このバースは、GetOwnerModuleFromXxxEntry() APIから取得されます。Microsoftのドキュメントでは、接続テーブルエントリを所有者モジュールとして解釈することが推奨されています。まれに、返された所有者のモジュール名が、「svchost.exe」などのプロセス名、「RPC」などのサービス名、「timer.dll」などのコンポーネント名である場合があります。

- **Process**: (Windowsのみ - XP SP2以降およびServer 2003 SP1以降) ポートを所有するモジュールの完全パスを示します。（存在する場合）。Windowsでは、このバースは、GetOwnerModuleFromXxxEntry() APIから取得されます。Microsoftのドキュメントでは、接続テーブルエントリを所有者モジュールとして解釈することが推奨されています。

- **ProcessId**: (Windowsのみ - XP SP2以降およびServer 2003 SP1以降) このポートのバインドを発行したプロセスのPIDを示します。

- **User**: (Linuxのみ) ポートを所有するユーザを示します。

「key」の意味

このkeyは、次の形式をとります。

<PROTOCOL>:/<IP ADDRESS>/:<PORT>

たとえば、次のとおりです。

tcp/172.14.207.94/80
udp/172.14.207.94/68

IPV6

IPアドレスがIPv6である場合、keyも同じ形式になりますが、プロトコルはTCP6またはUDP6です。このIPアドレスは、getnameinfo APIによって返されるように、次のようなIPv6表記となります。

「key」の照合

*/72.14.207.9?/80

*/72.14.207.2*/80

次のパターンは、任意のIPアドレスのポート80に一致します。
*/80

次の例では、待機ポートにおける変更を監視しますが、IPV4およびIPV6のTCPのポート80は無視します。

```xml
<PortSet>
  <include key="*"/>
  <exclude key="tcp*/*/80"/>
</PortSet>
```

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントについては、include/excludeの一般的な説明（252ページ）を参照してください。ここでは、このエンティティセットクラスに関連するinclude/excludeに固有の情報のみを記載します。

PortSetのinclude/excludeに固有の属性

これ以外にも、ポートの各種の属性をinclude/excludeでの監視機能で使用できます。これらの監視では、値とポートの属性値を比較します。各種属性のプラットフォームサポートに注意してください。すべての属性がプラットフォーム間またはプラットフォームリビジョン間で利用可能であるとはかぎりません。したがって、include/excludeタグを使用したこれらの監視の使用は制限されます。監視機能では、UNIXのglobスタイルのワイルドカードである*および?がサポートされ、パスのセパレーターまたはその他の文字の正規化は実行されません。監視機能は、属性の値に対する、単純なglobスタイルのパターン照合です。

Path

ポートのpath属性に対する、ワイルドカード一致をチェックします。次の例では、メインのIISバイナリを実行するプロセスによって所有されているポートを監視します。

```xml
<PortSet>
  <include path="*\system32\inetsrv\inetinfo.exe"/>
</PortSet>
```

Process

ポートのprocess属性に対する、ワイルドカード一致をチェックします。次の例では、svchost.exeまたはoutlook.*バイナリを実行するプロセスによって所有されているポートを監視します。

```xml
<PortSet>
  <include process="svchost.exe"/>
```
ポートのuser属性に対する、ワイルドカード一致をチェックします。次の例では、スーパーユーザ (root) によって所有されていたUNIXシステム上のポートを監視します。

```
<PortSet>
  <include user="root"/>
</PortSet>
```
ProcessSet

プロセスのセットを表します。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>リアルタイムで監視するかどうかを示します。</td>
<td>いいえ</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- **CommandLine**: 「ps -f」 (UNIX), 「ps w」 (Linux), またはProcess Explorer (Windows) のように表示される完全なコマンドライン。
- **Group**: プロセスが実行されているグループ。UNIXでは、プロセスの「有効な」グループIDです。グループIDは、時間とともにプロセスが権限を破棄するか、またはプロセスが有効なグループ資格情報を取り替えた場合に、変更されることがあります。Windowsでは、現在のプロセスのプライマリグループであり、TokenInformationClassにTokenPrimaryGroupが指定されたWin32 API GetTokenInformationによって返されます。これは、新しく作成されたオブジェクトでは、初期設定のプライマリグループSIDです。プロセスには、通常、プライマリグループ以外にも1つ以上のグループ資格情報が関連付けられています。これらの追加のグループ資格情報は、Agentによって監視されません。これらの情報は、Process Explorerにおけるプロセスプロパティの「セキュリティ」タブで表示できます。
- **Parent**: このプロセスを作成したプロセスのPID。
- **Path**: プロセスのバイナリへの完全パス。Solaris 8および9、HP-UXでは使用できません。Windowsでは、このパスは、GetModuleFileNameEx() APIから取得されます。LinuxおよびSolaris 10では、このパスはそれぞれシンボリックリンク /proc/{pid}/exeまたは/proc/{pid}/path/a.outから取得されます。
- **Process**: プロセスバイナリの短い名前（パスを含まない名前）。たとえば、「c:\windows\notepad.exe」の場合は「notepad.exe」であり、「/usr/local/bin/httpd」の場合は「httpd」です。
- **Threads**: プロセス内で現在実行中のスレッドの数。HP-UXでは使用できません。
- **User**: プロセスが実行されているユーザ。UNIXでは、プロセスの「有効な」ユーザIDです。このユーザIDは、時間とともにプロセスが権限を破棄するか、またはプロセスが有効なユーザ資格情報を取り替えた場合に、変更されることがあります。

簡略記法による属性

- **STANDARD**: CommandLine, Group, Parent, Path (利用可能な場合), Process, User

「key」の意味

keyは、実行可能ファイルの短い名前である「Process」属性と、PIDを組み合わせたものであります。PIDは、名前とパスのセパレータの後に追加されます。たとえば、Windowsではnotepad.exe¥1234、UNIXではhttpd/1234となります。パスのセパレータを使用することと、key="abc/"のinclude/exclude照合が期待どおりに動作するようになります。
管理者ガイド

ProcessSet

サブエレメント
•

Include

•

Exclude

これらのエレメントに指定できる属性とサブエレメントについては、includeの一般的な説明 (252ページ)を参照してください。ここ
では、このエンティティセットクラスに関連するinclude/excludeに固有の情報のみを記載します。

ProcessSetsのinclude/excludeに固有の属性

次の例は、PIDに関係なく、notepad.exeの実行中のプロセスセットを監視します。
<ProcessSet>
<include key="notepad.exe\*" />
</ProcessSet>
これ以外にも、プロセスの各種の属性をinclude/excludeでの監視機能で使用できます。監視機能では、UNIXのglobスタイルのワイル
ドカードである*および?がサポートされ、パスのセパレータまたはその他の文字の正規化は実行されません。監視機能は、属性の値に
対する、単純なglobスタイルのパターン照合です。
CommandLine
プロセスのcommandLine属性に対する、ワイルドカード一致をチェックします。次の例では、コマンドラインが「*httpd *」に一致
するプロセスが監視されます。
<ProcessSet>
<include commandLine="*httpd *" />
</ProcessSet>
Group
プロセスのgroup属性に対する、ワイルドカード一致をチェックします。数値形式ではなく、テキスト形式のグループ名が使用されま
す。Linuxでデーモングループをテストするには、「2」ではなく「daemon」を使用します。次の例では、root、daemon、lpのいず
れかのグループとして実行されるプロセスを監視します。
<ProcessSet>
<include group="root" />
<include group="daemon" />
<include group="lp" />
</ProcessSet>
Path
プロセスのpath属性に対する、ワイルドカード一致をチェックします。path属性は、一部のプラットフォームでは使用できません。次
の例では、System32の下にバイナリがあるプロセスを監視します。
<ProcessSet>
<include path="*\System32\*" />
</ProcessSet>
User
プロセスのuser属性に対する、ワイルドカード一致をチェックします。数値形式ではなく、テキスト形式のユーザ名が使用されます。
UNIXでスーパーユーザをチェックするには、「0」ではなく「root」を使用します。次の例では、NT AUTHORITY\SYSTEM、NT
AUTHORITY\LOCAL SERVICE、NT AUTHORITY\NETWORK SERVICEなど、組み込みのシステムユーザとして実行される任意のプ
ロセスを監視します。
<ProcessSet>
<include user="NT AUTHORITY\*" />
</ProcessSet>

273


RegistryKeySet

RegistryKeySetタグは、レジストリ内のセットキーを記述します (Windowsのみ)。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>RegistryKeySetのベースキーを設定します。タグ内の他のエレメントはすべて、このキーから相対的に位置付けられます。ベースは、次のいずれかのレジストリブランチ名で始まる必要があります。HKEY_CLASSES_ROOT (またはHKCR), HKEY_LOCAL_MACHINE (またはHKLM), HKEY_USERS (またはHKU), HKEY_CURRENT_CONFIG (またはHKCC)</td>
<td>は</td>
<td>構文的に有効なレジストリパスに解釈される文字列値</td>
</tr>
</tbody>
</table>

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- Owner
- Group
- Permissions
- LastModified (Windowsレジストリでは「LastWriteTime」と呼ばれています)
- Class
- SecurityDescriptorSize

簡略記法による属性

- STANDARD: Group、Owner、Permissions、LastModified

「key」の意味

レジストリキーは、ファイルシステム内のディレクトリのように、レジストリ内に階層的に格納されています。この言語では、キーに対する「キーパス」は、ディレクトリに対するパスのようなどのものだとみなされています。たとえば、Agentの「Deep Security Agent」キーへの「キーパス」は、次のようにになります。

HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent

RegistryValueSetのinclude/excludeの「キー」値は、このキーパスに対して照合されます。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンであり、「/」で区切られたキーパスのセクションに対して照合されます。

サブエレメント

- Include
Excluded

これらのエレメントに指定できる属性とサブエレメントについては、includeの一般的な説明 (252ページ) を参照してください。
### RegistryValueSet

レジストリ値のセットです (Windowsのみ)。

#### タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>RegistryValueSetのベースキーを設定します。タグ内の他のエレメントはすべて、このキーから相対的に位置付けられます。ベースは、レジストリブランチ名で始まる必要があります。HKEY_CLASSES_ROOT (またはHKCR), HKEY_LOCAL_MACHINE (またはHKLM), HKEY_USERS (またはHKU), HKEY_CURRENT_CONFIG (またはHKCC)</td>
<td>は</td>
<td>は（構文的に有効なレジストリキーに解釈される文字列値）</td>
</tr>
</tbody>
</table>

#### エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- Size
- Type
- Sha1
- Sha256
- Md5

#### 簡略記法による属性

- CONTENTS: ポリシーまたはコンピュータエディタの [変更監視]→[詳細] で設定されているコンテンツのハッシュアルゴリズムに変換されます。
- STANDARD: Size, Type, Contents

#### 「key」の意味

レジストリ値はレジストリ内のキーに格納されている名前/値のペアです。レジストリ値が格納されているキーは、さらに別のキーに格納されている場合があります。これは、ファイルシステム内でのディレクトリとファイルの関係によく似ています。この名前では、値に対する「キーパス」は、ファイルに対するパスのようなものとみなされています。たとは、AgentのInstallationFolder値への「キーパス」は、次のようにになります。

HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent\InstallationFolder

RegistryValueSetのinclude/excludeの「キー」値は、このキーパスに対して照合されます。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンであり、「/」で区切られたキーパスのセクションに対して照合されます。
初期設定値

各レジストリキーには、不特定の値（初期設定値）があります。

パターンの末尾に「/」を使用することで、この値を含める/除外することを明示的に指定できます。たとえば、「**/」は、下位の不特定の値すべてに対して照合され、「*Agent/**/」は、「*Agent」に一致するキーの不特定の値すべてに対して照合されます。

注意： レジストリ値の名前には、引用符、バックスラッシュ、「@」記号など、任意の印刷可能な文字が含まれている可能性があります。

Agentは、これらの文字がエンティティのキー名に含まれている場合、バックスラッシュをエスケープ記号として使用して対処しますが、この処理によってエスケープされるのはバックスラッシュ自体だけです。このように処理されるのは、バックスラッシュを含む値名と、レジストリパスの一部として使用されているバックスラッシュを区別できるようにするためです。つまり、バックスラッシュで終了する値名は、初期設定/不特定の値に対して一致するように設計されたルールと一致することになります。

次の表に、レジストリ値の名前と生成されるエンティティキーの例を示します。

<table>
<thead>
<tr>
<th>値</th>
<th>エスケープ形式</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>Hello</td>
<td>HKLM\Software\Sample\Hello</td>
</tr>
<tr>
<td>&quot;Quotes&quot;</td>
<td>&quot;Quotes&quot;</td>
<td>HKLM\Software\Sample&quot;Quotes&quot;</td>
</tr>
<tr>
<td>back\slash</td>
<td>back\slash</td>
<td>HKLM\Software\Sample\back\slash</td>
</tr>
<tr>
<td>trailing\</td>
<td>trailing\</td>
<td>HKLM\Software\Sample\trailing\</td>
</tr>
<tr>
<td>@</td>
<td>@</td>
<td>HKLM\Software\Sample@</td>
</tr>
</tbody>
</table>

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントについては、include/excludeの一般的な説明（252ページ）を参照してください。
ServiceSet

ServiceSetエレメントは、サービスのセットを表します（Windowsのみ）。サービスは、「サービス名」によって識別されます。このサービス名は、サービスの管理ツールに表示される「name」列の値と同じものではありません。サービス名は、サービスのプロパティで確認することができます。多くの場合、「name」列に表示される値よりも短い名前です（この値は、実際にはサービスの「表示名」です）。たとえば、Agentには、「ds_agent」というサービス名と「Trend Micro Deep Security Agent」という表示名があります。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>リアルタイムで監視するかどうかを示します。</td>
<td>いいえ</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- **Permissions**: SDDL形式のサービスのセキュリティ記述子
- **Owner**: サービスの所有者のユーザID
- **Group**: サービスの所有者のグループID
- **BinaryPathName**: Windowsがサービスの開始に使用するパスと、省略可能なコマンドライン引数
- **DisplayName**: サービスの「プロパティ」パネルに表示されるサービスの「表示名」。
- **Description**: 「サービス」パネルに表示される説明
- **State**: サービスの現在の状態。次のいずれかです: stopped、starting、stopping、running、continuePending、pausePending、paused
- **StartType**: サービスの開始方法。次のいずれかです: automatic、disabled、manual
- **LogOnAs**: サービスプロセスの実行時にサービスプロセスにログオンするアカウントの名前
- **FirstFailure**: サービスがはじめて失敗したときに実行される処理。形式は「delayInMsec,action」で、処理はNone、Restart、Reboot、RunCommandのいずれかです。
- **SecondFailure**: サービスが2回目で失敗したときに実行される処理。形式は「delayInMsec,action」で、処理はNone、Restart、Reboot、RunCommandのいずれかです。
- **SubsequentFailures**: サービスが3回目以降で失敗したときに実行される処理。形式は「delayInMsec,action」で、処理はNone、Restart、Reboot、RunCommandのいずれかです。
- **ResetFailCountAfter**: 失敗がない場合に、失敗カウントをゼロリセットするまでの時間 (秒単位)
- **RebootMessage**: 「Reboot」サービスコントローラ処理に対する応答として、サーバのユーザにブロードキャスト配信されるメッセージ
- **RunProgram**: 「RunCommand」サービスコントローラ処理に対する応答として実行されるプロセスの完全なコマンドライン
- **DependsOn**: サービスが依存しているコンポーネントのカンマ区切りのリスト
- **LoadOrderGroup**: このサービスが属しているロード順序グループ。システムのスタートアッププログラムは、ロード順序グループを使用して、他のグループに対して指定された順序どおりにサービスのグループをロードします。ロード順序グループは、レジストリ値HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ServiceGroupOrderに含まれています。
• **ProcessId**: サービスをホストするプロセスの数値ID。1個のWindowsプロセスに多数のサービスが存在する可能性がありますが、独自のプロセスで実行されるサービスについては、この属性を監視することで、サービスの再起動をログに記録することができます。

簡略記法による属性

次に、エンティティの簡略記法による属性と、解釈される属性を示します。

• **STANDARD**: Permissions、Owner、Group、BinaryPathName、Description、State、StartType、LogOnAs、FirstFailure、SecondFailure、SubsequentFailures、ResetFailCountAfter、RunProgram、DependsOn、LoadOrderGroup、ProcessId

「key」の意味

keyはサービスの名前であり、サービスの管理ツールに表示される「name」列と同じである必要はありません (サービスの管理ツールには、サービスの「表示名」が表示されます)。サービス名は、サービスのプロパティで確認することができます。多くの場合、「name」列に表示される値よりも短い名前です。

| 注意: | これは、階層型のエンティティセットではありません。パターンはサービス名のみに適用されます。結果として、**パターンは適用できません。 |

サブエレメント

• **Include**
• **Exclude**

これらのエレメントに指定できる属性とサブエレメントについては、includeの一般的な説明 (252ページ) を参照してください。ここでは、このエンティティセットクラスに関連するinclude/excludeに固有の情報のみを記載します。

ServiceSetのinclude/excludeに固有の属性

**state**

サービスの状態である、stopped、starting、stopping、running、continuePending、pausePending、pausedのいずれかに基づいたinclude/exclude。次例では、実行中のサービスセットの変更について監視します。

```xml
<ServiceSet>
  <include state="running"/>
</ServiceSet>
```
UserSet

UserSetエレメントはユーザのセットを表します。Windowsシステムでは、システムのローカルユーザで動作します。「ローカルユーザーとグループ」MMCスナップインで表示されるユーザと同じです。DSAがドメインコントローラ以外で実行されている場合にのみ、これらがローカルユーザになります。UserSetエレメントはドメインコントローラ上のドメインユーザをすべて列挙しますが、これは非常に大きなドメインでは望ましくない場合があります。

UNIXシステムの場合、監視されるユーザは「getpwent_r()」APIおよび「getspnam_r()」APIで返すように設定されたユーザです。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>onChange</td>
<td>リアルタイムで監視するかどうかを示します。</td>
<td>いいえ</td>
<td>false</td>
<td>true, false</td>
</tr>
</tbody>
</table>

エンティティセットの属性

監視可能なエンティティの属性には次のものがあります。

一般属性

- **cannotChangePassword**: ユーザにパスワードの変更が許可されているかどうかをtrue/falseで示す。
- **disabled**: アカウントが無効になっているかどうかをtrue/falseで示す。Windowsシステムでは、ユーザの「disabled」チェックボックスに反映されます。UNIXシステムでは、ユーザのアカウントが期限切れの場合、またはパスワードが期限切れで変更の猶予期間が経過してしまった場合、これはtrueになります。
- **fullName**: ユーザの表示名。
- **groups**: ユーザの所属するグループのカンマ区切りのリスト。
- **homeFolder**: ホームフォルダまたはホームディレクトリへのパス。
- **lockedOut**: ユーザが明確に、またはパスワードの失敗回数超過によって、ロックされているかどうかをtrue/falseで示す。
- **passwordHasExpired**: ユーザのパスワードが期限切れかどうかをtrue/falseで示す。Windowsの場合、この属性はWindows XP以降のOSでのみ使用できます（AIXでは使用できません）。
- **passwordLastChanged**: 前回ユーザのパスワードが変更された日時のタイムスタンプ。これは、DSAによって1970年1月1日 (UTC) 以降のミリ秒単位で記録されます。この値に基づき、Deep Security Managerはタイムスタンプを現地時間で表示します。UNIXプラットフォームでは、この属性は1日単位の粒度であるため、表示されるタイムスタンプの時間コンポーネントは無意味なものになります（AIXは該当しません）。
- **passwordNeverExpires**: 期限切れにならないパスワードかどうかをtrue/falseで示す。
- **user**: OSが認識しているユーザ名。たとえば、「Administrator」や「root」があります。

Windowsのみの属性

- **description**: ユーザが所属するプライマリグループ。
- **homeDriveLetter**: ユーザのホームフォルダとしてネットワーク共有がマッピングされているドライブの文字。
- **logonScript**: ユーザがログインするたびに実行されるスクリプトへのパス。
• **profilePath**: ローミングまたは必須のWindowsユーザプロファイルが使用されている場合のネットワークパス。

Linuxのみの属性

• **group**: ユーザが所属するプライマリグループ。
• **logonShell**: ユーザのシェルプロセスへのパス。
• **passwordExpiredDaysBeforeDisabled**: ユーザのパスワードが期限切れになり、アカウントが無効になってからの日数（AIXは該当しません）。
• **passwordExpiry**: ユーザのアカウントが期限切れになり、アカウントが無効になる日付。
• **passwordExpiryInDays**: ユーザのパスワードを変更しなくてはならない日までの残り日数。
• **passwordMinDaysBetweenChanges**: パスワードを変更してから次に変更するまでの最小日数。
• **passwordWarningDays**: ユーザのパスワードが期限切れになる前に警告を表示する日数。

簡略記法による属性

• 標準:
  ◦ cannotChangePassword
  ◦ disabled
  ◦ groups
  ◦ homeFolder
  ◦ passwordHasExpired
  ◦ passwordLastChanged
  ◦ passwordNeverExpires
  ◦ user
  ◦ logonScript (Windowsのみ)
  ◦ profilePath (Windowsのみ)
  ◦ group (Linuxのみ)
  ◦ logonShell (Linuxのみ)
  ◦ passwordExpiryInDays (Linuxのみ)
  ◦ passwordMinDaysBetweenChanges (Linuxのみ)

「key」の意味

このkeyはユーザ名です。これは階層型のEntitySetではありません。パターンはユーザ名のみに適用されます。結果として、「**」パターンは適用できません。

次の例は、任意のユーザの作成と削除を監視します(属性は明確に除外されるので、グループメンバーシップは監視対象にはなりません)。

```xml
<UserSet>
<Attributes/>
<include key="*"/>
</UserSet>
```

次の例では、「jsmith」アカウントの追加および削除の監視に加え、アカウントのSTANDARD属性に対する変更の監視も行います(特定の属性リストが含まれていない場合、このEntitySetのSTANDARDセットが自動的に含められるためです)。

```xml
<UserSet>
<Attributes/>
<include key="**"/>
</UserSet>
```
サブエレメント

include/exclude

これらのエレメントに指定できる属性とサブエレメントについては、includeの一般的な説明を参照してください。

UserSetsのinclude/excludeに固有の属性

これ以外にも、ユーザの各種の属性をinclude/excludeでの監視機能で使用できます。これらの監視では、値とユーザの属性値を比較します。各種属性のプラットフォームサポートに注意してください。すべての属性がプラットフォーム間またはプラットフォームリビジョン間で利用可能であるとはかぎりません。したがって、include/excludeエレメントを使用したこれらの監視の使用は制限されます。監視機能では、UNIXのglobスタイルのワイルドカードである*および?がサポートされ、パスのセパレータまたはその他の文字の正規化は実行されません。監視機能は、属性の値に対する、単純なglobスタイルのパターン照合です。

• Disabled: ユーザの無効な属性に対する、true/false一致。次の例は、プライマリグループに「user」または「daemon」のいずれかがあるユーザを監視します。

  <UserSet>
  <include disabled="true"/>
  </UserSet>

• Group: ユーザのgroup属性に対する、ワイルドカード一致。この監視はUNIXシステムにのみ適用できます。次の例は、プライマリグループに「user」または「daemon」のいずれかがあるユーザを監視します。

  <UserSet>
  <include group="users"/>
  <include group="daemon"/>
  </UserSet>

• LockedOut: ユーザのlockedOut属性に対する、true/false一致。

• PasswordHasExpired: ユーザのpasswordHasExpired属性に対する、true/false一致。

• PasswordNeverExpires: ユーザのpasswordNeverExpires属性に対する、true/false一致。
WQLSet

WQLSetエレメントはWindows Management Instrumentation WQLクエリ文の結果セットについて記述します。WQLは、さまざまなオブジェクトクラスに対してSQLに似たクエリを実行し、その結果について、各行にオブジェクト、各列にオブジェクトの特定属性値を格納した表の形式で返します。

注意: WMIクエリの多くは、時間とコンピュータリソースを大量に消費します。完了まで数分かかり何千行もの結果を返すクエリを、不注意で実行してしまうことがあります。WQLSetで使用する前に、すべてのクエリをPowerShellやWMExplorerなどのプログラムを使用してテストすることを強く推奨します。

<table>
<thead>
<tr>
<th>属性</th>
<th>説明</th>
<th>必須</th>
<th>初期設定値</th>
<th>設定できる値</th>
</tr>
</thead>
<tbody>
<tr>
<td>namespace</td>
<td>WMIクエリの名前空間を設定します。</td>
<td>はい</td>
<td>なし</td>
<td>WMIクエリの名前空間を設定します。</td>
</tr>
<tr>
<td>wql</td>
<td>WQLクエリ文字列。</td>
<td>はい</td>
<td>なし</td>
<td>WQLクエリ文字列。</td>
</tr>
<tr>
<td>onChange</td>
<td>対象のファイルをリアルタイムで監視する必要があるかどうかを示します。</td>
<td>いいえ</td>
<td>いいえ</td>
<td>false</td>
</tr>
<tr>
<td>provider</td>
<td>オプションで、使用する別のWMI名前空間プロバイダを指定します。</td>
<td>いいえ</td>
<td>なし</td>
<td>RsopLoggingModeProvider</td>
</tr>
</tbody>
</table>

注意: WMIクエリの多くは、時間とコンピュータリソースを大量に消費します。完了まで数分かかり何千行もの結果を返すクエリを、不注意で実行してしまうことがあります。WQLSetで使用する前に、すべてのクエリをPowerShellやWMExplorerなどのプログラムを使用してテストすることを強く推奨します。
エンティティセットの属性

WQLクエリによって返される各「行」は、変更監視にそれぞれ単一のエンティティとして扱われます。返される列は、エンティティの属性を表します。WMI/WQLは変更可能な仕様であるため、有効な属性やサポートされている属性のセットリストはありません。クエリと、クエリの対象であるWMIオブジェクトのスキーマは、監視対象の属性を決定します。

たとえば、次のWQLSetの場合、

```xml
<WQLSet namespace="Computer" wql="select * from RSOP_SecuritySettings where precedence=1" provider="RsopLoggingModeProvider" />
```

次の属性を返します。

ErrorCode、GPOID、KeyName、SOMID、Setting、Status、id、precedence

一方、次のようなネットワークアダプタにクエリ実行するWQLSetは、

```xml
<WQLSet namespace="root\cimv2" wql="select * from Win32_NetworkAdapter where AdapterTypeId = 0" />
```

次の属性を返します。

AdapterType、AdapterTypeId、Availability、Caption、ConfigManagerErrorCode、ConfigManagerUserConfig、CreationClassName、DeviceID、DeviceName、Description、DeviceID、Index、Installed、MACAddress、Manufacturer、MaxNumberControlled、Name、PNPDeviceID、PowerManagementSupported、ProductName、ServiceName、SystemCreationClassName、SystemName、TimeOfLastReset

Agentの負荷を減らすため、クエリに「select * ...」を使用する代わりに、監視の必要がある属性のみを明確に含めることをお勧めします。WMIスキーマに属性を追加または削除する変更は、その属性が監視対象のセットの一部でないかぎり、オブジェクトに対する変更であるとレポートされない利点もあります。「select * from Win32_Foobar」を使用すると、Win32_Foobarオブジェクトのクラスに新しい属性を追加するWindowsのパッチが適用された場合、次回の変更の検索で、新しい属性が出現したことによるクラスの各オブジェクトに対する変更がレポートされます。

次に、望ましいWindowsシステムのエンティティを返すWMIクエリの例をいくつか示します。

Windowsにマウントされたストレージデバイスに対するクエリ（*を選択すると、通常、返される属性の80%はnullまたは重複する値になります）:

```xml
<WQLSet namespace="root\cimv2" wql="SELECT __Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,FreeSpace FROM Win32_LogicalDisk" />
```

前のクエリに追加して、DriveTypeを指定（「Removable Disk」であるtype2など）することで、特定タイプのマウント済み論理ストレージデバイスを分離できます（リムーバブルUSBストレージドライブなど)。

```xml
<WQLSet namespace="root\cimv2" wql="SELECT __Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,FreeSpace FROM Win32_LogicalDisk WHERE DriveType=2" />
```

(Win32_LogicalDiskクラスの詳細については[こちら]を参照してください)
USBストレージデバイスの注意事項：U3 USBデバイスは、type 2の「Removable Disk」デバイスとtype 3の「Compact Disc」デバイスの両方にマウントされます。また、前出のクエリはストレージデバイス専用です。記憶装置ではないUSBデバイスは含まれません。type 1の「No Root Directory」デバイスとしてUSBメモリカードアダプタが表示されることがあります。type 1の「Unknown」デバイスとして、不良またはWindowsと互換性のないUSBストレージデバイスが表示されることがあります。

ドライブが「F:」である既知のシステムディレクトリすべてに対して、関連する属性のクエリを実行します。

```xml
<WQLSet namespace="root\cimv2" wql="SELECT __Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Caption,FileType,Readable,Writeable FROM Win32_Directory WHERE Drive='F:'" />
```

ドライブが「F:」である既知のシステムファイルすべてに対して、関連する属性のクエリを実行します。

```xml
<WQLSet namespace="root\cimv2" wql="SELECT __Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Name,FileType,Readable,Writeable FROM CIM_DataFile WHERE Drive='F:'" />
```

「key」の意味

keyは、返されるWMIオブジェクトの「__Path」属性で、通常は次の形式です。

SystemName\Namespace\WmiObjectClass.KeyAttribute=Value[,KeyAttribute=Value]

例を挙げます。

\TEST-DESK\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB958215-IE7",ServicePackInEffect="SP0"
\TEST-DESK\ROOT\Rsop\NSF49B36AD_10A3_4F20_9541_B4C471907CE7\Computer:RSOP_RegistryValue.Path="MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText",precedence=1
\TEST-DESK\root\cimv2:BRCM_NetworkAdapter.DeviceID="8"

サブエレメント

include/exclude

これらのエレメントに指定できる属性とサブエレメントについては、「include」と「exclude」の一般的な説明を参照してください。

WQLSetでは通常、「include」サブエレメントと「exclude」サブエレメントは不要です。WQLはAgentおよびホストのWMI実装の両方によって実行される処理の量を制限するため、監視するオブジェクトの正確なセットを指定するためにWQLを使用することが望ましいです。

任意のincludeまたはexcludeサブエレメントを使用すると、クエリによって返されるオブジェクトのセットを減らすことのみ可能で、追加のオブジェクトを返すようにすることがあります。WQLの結果をさらに制限する必要がある場合には、エンティティキーの値に対して一致させる単純なワイルドカードとして「*」および「？」の文字を使用できます。
Agentを手動で無効化/停止/起動する

Agent/Deep Security Virtual Applianceを無効にする

通常、Agent/Applianceの無効化は、現在Agent/Applianceを管理しているDeep Security Managerから実行できます。Deep Security ManagerがAgent/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
   ```

Agentを停止または起動する

**WindowsでAgentを起動または停止するには**
- 停止: コマンドラインで次のコマンドを実行します: `sc stop ds_agent`
- 開始: コマンドラインで次のコマンドを実行します: `sc start ds_agent`

**LinuxでAgentを起動または停止するには**
- 停止: 次のコマンドを実行します: `/etc/init.d/ds_agent stop`
- 開始: 次のコマンドを実行します: `/etc/init.d/ds_agent start`

Deep Security Virtual Applianceを停止または起動する

Applianceの停止または起動は、ホストコンピュータで、ローカルでのみ実行できます。

**LinuxでApplianceを起動または停止するには**
- 停止: 次のコマンドを実行します: `/etc/init.d/ds_agent stop`
- 開始: 次のコマンドを実行します: `/etc/init.d/ds_agent start`
複数ノードでManagerを実行する

Deep Securityは、1個のデータベースを使用して同時に動作する、複数のノードとして実行することができます。Managerを複数のノードとして実行すると、信頼性の向上、冗長化された可用性、事実上無制限のスケーラビリティ、パフォーマンスの強化が実現されます。

各ノードが、すべてのタスクを実行することができます。また、他のノードよりも重要なノードはありません。ユーザは、任意のノードにログオンしてタスクを実行できます。いずれかのノードでエラーが発生しても、タスクが実行されないという結果にはなりません。同様に、いずれかのノードでエラーが発生しても、データの損失という結果にはなりません。


ノードを表示する


注意: Deep Security Managerは、すべてのオンラインManager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。ユーザが多数のアクティビティをすべてジョブとしてパッケージされ、任意のManager上で「実行可能」となります。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。

アクティビティグラフ付きネットワークマップ

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)

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分析します。

![ノード別ジョブのグラフ](image)

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を種類別に分析します。

![種類別ジョブのグラフ](image)

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。

![ノードおよび種類別ジョブの総数のグラフ](image)

ノードを追加する

システムにDeep Security Managerノードを追加するには、新しいコンピュータ上でManagerインストールパッケージを実行します。プロンプトが表示されたら、使用しているデータベースの場所とログイン資格情報を入力します。インストーラがデータベースに接続したら、システムにノードを追加する処理を続けできます。

注意：複数のノードを実行するには、Microsoft SQL ServerまたはOracle Databaseのいずれかを使用している必要があります。
決して複数のインストーラのインスタンスを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。

ノードの使用を停止する

ノードの使用を停止するには

注意：ノードの使用を停止するには、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。

1. Deep Security Managerで、[管理]→[Managerノード]を選択します。
2. 使用を停止するManagerノードをダブルクリックし、[プロパティ]画面を表示します。
3. [オプション]エリアで[使用停止]ボタンをクリックします。
パフォーマンスの要件

次のガイドラインは、各種規模におけるDeep Securityのインストールに必要なインフラストラクチャ要件の概要です。

ディスク容量


これらのイベント収集設定は、ポリシーおよび個別のコンピュータレベルで詳細に設定することができます（「ポリシー、継承、およびオーバーライド (292ページ)」を参照してください）。

ログを初期設定レベルのまま実行する場合、平均的なコンピュータでは、データベースのディスク容量が約50MB必要になります。コンピュータが1000台ある場合は、50GB必要となり、2000台ある場合には100GB必要となります。

注意: 初期設定の場合、消費量の大きい順にファイアウォール、変更監視、セキュリティログ監視の各モジュールによって、通常ほとんどのディスク容量が消費されます。

専用のサーバ


注意: 管理下のコンピュータが1000台以上あるかどうかにかかわらず、冗長性を提供するために、複数のManagerノードを実行した方がよいでしょう。

Deep Security Virtual Appliance

注意: このセクションは、バージョン9.6よりも前のDeep Security Virtual ApplianceおよびFilter Driverを実行している場合のみ該当します。

1台のESXiサーバ上のVirtual Applianceを使用して、台数の制限なく仮想マシンを保護できます。Filter Driverのヒープメモリの最大サイズは、仮想マシンの数に適したサイズに設定する必要があります。

注意: ヒープメモリの初期設定サイズは256MBです。

Filter Driverのヒープメモリの最大サイズを恒久的に増やすためには、コンソールにログインし、「esxcfg-module」コマンドを実行して最大のヒープサイズをバイト単位で設定してください。

式は次のとおりです。

\[\text{仮想マシンの数} \times 3 \text{MB} + \text{仮想マシンの数} \times 512 \text{バイト} \times \text{UDP接続数} + \text{TCP接続数} + vMotion状態設定用に10 \text{MB}\]

50台の仮想マシンでUDP接続とTCP接続の数がそれぞれ5,000の場合、次のようにになります。
50 x 3 = 150MB
50 x 512 x 10000 = 256000000バイト (256MB)
150M + 256MB + 10MB = 416MB
416 x 1048576 = 436207616バイト (必要なヒープメモリの推定サイズ)

値を設定するコマンドは次のようになります。

% esxcfg-module -s DSAFILTER_HEAP_MAX_SIZE=436207616 dvfilter-dsa

設定を確認するには、次のコマンドを実行します。

% esxcfg-module -g dvfilter-dsa

ドライバをリロードすると、設定が有効になります。リロードは、ESXiサーバを再起動するか (推奨)、または次のコマンドを実行してドライバをアンロード/ロードします。

% esxcfg-module -u dvfilter-dsa
% esxcfg-module dvfilter-dsa

**注意:** 前述のアンロード/ロードを行うには、ESXiサーバ上の保護対象の仮想マシンおよびDSVAをすべてシャットダウンする必要があります。
ポリシー、継承、およびオーバーライド

Deep Securityのほとんどのエレメントと設定は、複数の階層レベルで動作します。階層レベルは、親レベルのベースポリシーから始まり、複数レベルの子ポリシーを経由して、最後のレベルは最終的なポリシーの割り当て先であるコンピュータです。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。

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Deep Security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ポリシーのエディタでは、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。
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。カテゴリ内の値は、現在の継承される設定を常に示しています)。

オーバーライド

Windows Server 2008ポリシーは、Windowsポリシーの子ポリシーです。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。

Windows 2008 Serverポリシーを詳しく見てみると、侵入防御も[オン]であることがわかります。[侵入防御]画面を確認すると、一連の侵入防御ルールが割り当てられています。
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。

オーバーライドする設定が多数ある場合は、親ポリシーのプ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。
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。
使用するポート

Deep Security Manager

ポート: 4119 (初期設定)

- 用途:
  - Deep Security Managerコンソールへのアクセス
- プロトコル: TCP
- 接続元:
  - Webブラウザ
  - ESXiサーバ
- 接続先: Deep Security Manager
- プロキシ: ×
- 設定: このポートは、Deep Security Managerのインストール処理時に設定されます。

ポート: 4120 (初期設定)

- 用途: Agent/ApplianceからManagerへの通信。Agent/ApplianceがManagerにイベントを送信すると、Managerは設定のアップデートを送信します。
- プロトコル: TCP
- 接続元: Agent/Appliance
- 接続先: Deep Security Manager
- プロキシ: ×
- 設定: このポートは、Deep Security Managerのインストール処理時に設定されます。

Agent/Appliance

ポート: 4118

- 用途: ManagerからAgent/Applianceへの通信
- プロトコル: TCP
- 接続元: Deep Security Manager
- 接続先: Agent/Appliance
- プロキシ: ×
- 設定: このポートは設定不可です。
Relay

ポート: 4122

- 用途: Agent/ApplianceからRelayへの通信
- プロトコル: TCP
- 接続元: RelayおよびAgent/Appliance
- 接続先: Deep Security Relay
- プロキシ: なし
- 設定: このポートは、Deep Security Managerのインストール処理時に設定されます。

ポート: 4123

- 用途: 内部Relay通信
- プロトコル: TCP
- 接続元: Relay (内部のローカルホスト)
- 接続先: Deep Security Relay
- プロキシ: ×
- 設定: このポートは設定できません。また、外部のコンピュータから認識できません。

SQL Serverデータベースサーバ

ポート: 1433, 1434

- 用途: Managerからデータベースへの通信 (データベースをDeep Security Managerに接続するために必要)
- プロトコル: 1433はTCP、1434はUDP
- 接続元: Deep Security Manager
- 接続先: SQLデータベースサーバ
- プロキシ: ×
- 設定: このポートは、Deep Security Managerのインストール処理時に設定されます。

Oracle Databaseサーバ

ポート: 1521

- 用途: Managerからデータベースへの通信 (Oracleを使用している場合、SQLで必要)
- プロトコル: TCP
- 接続元: Deep Security Manager
- 接続先: Oracle Databaseサーバ
- プロキシ: ×
- 設定: このポートは、Deep Security Managerのインストール処理時に設定されます。
Syslogファシリティ

ポート: 514 (初期設定)

- 用途: Syslog
- プロトコル: UDP
- 接続元: Agent/Appliance
- 接続先: Syslogファシリティ
- プロキシ: ×

設定: このポートは [管理]→[システム設定]→[SIEM] で設定できます。

SMTPサーバ

ポート: 25 (初期設定)

- 用途: メールのアラート
- プロトコル: TCP
- 接続元: Deep Security Manager
- 接続先: 指定のSMTPサーバ
- プロキシ: ×

設定: このポートは [管理]→[システム設定]→[SMTP] で設定できます。

トレンドマイクロのアップデートサーバ

ポート: 80

- 用途: トレンドマイクロのアップデートサーバへの接続
- プロトコル: HTTPおよびSOCKS
- 接続元: Deep Security Manager
- 接続先: トレンドマイクロのアップデートサーバ
- プロキシ: あり (オプション)

設定: プロキシアドレスとポートは [管理]→[システム設定]→[プロキシ] で設定できます。

ポート: 443

- 用途: トレンドマイクロのアップデートサーバへの接続
- プロトコル: HTTPおよびSOCKS
- 接続元: Deep Security Relay
- 接続先: トレンドマイクロのアップデートサーバ
- プロキシ: あり (オプション)

設定: プロキシアドレスとポートは [管理]→[システム設定]→[プロキシ] で設定できます。
LDAPサーバ

ポート: 389, 636, 3268

- 用途: Active Directoryの統合
- プロトコル: TCP
- 接続元: Deep Security Manager
- 接続先: LDAPサーバ
- プロキシ: ×
- 設定: このポートは、[コンピュータ] 画面のディレクトリの追加ウィザードで設定できます。

Smart Protection Network (グローバルサーバ)

ポート: 80

- 用途: Webレビュートーションサービス
- プロトコル: TCP
- 接続元: Deep Security Agent/Appliance
- 接続先: Smart Protection Network
- プロキシ: あり (オプション)
- 設定: プロキシアドレスとポートは、ポリシーまたはコンピュータエディタの [Webレビュートーション]→[Smart Protection] で設定できます。

ポート: 443

- 用途: スマートフィードバックおよびファイルレビュートーションサービス
- プロトコル: TCP
- 接続先: Smart Protection Network
- プロキシ: あり (オプション)
- 設定: Smart Protection Networkのプロキシアドレスとポートは、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]→[Smart Protection] で設定できます。

Smart Protection Server (ローカルインストール)

ポート: 5274

- 用途: Webレビュートーションサービス
- プロトコル: TCP
- 接続元: Deep Security Agent/Appliance
- 接続先: Smart Protection Server
ポート: 443

- 用途: ファイルレピュテーションサービス
- プロトコル: TCP
- 接続元: Deep Security Agent/Appliance
- 接続先: Smart Protection Server
- プロキシ: ×

ソフトウェア安全性評価サービス

ポート: 443

- 用途: ソフトウェア安全性評価サービス
- プロトコル: TCP
- 接続元: Deep Security Manager
- 接続先: ソフトウェア安全性評価サービス
- プロキシ: あり (オプション)
- 設定: ソフトウェア安全性評価サービスのHTTPプロキシは [管理]→[システム設定]→[プロキシ] タブで設定できます。

DNSサーバ

ポート: 53

- 用途: ホスト名のDNS検索
- プロトコル: TCP
- 接続元: Deep Security Manager
- 接続先: DNSサーバ
- プロキシ: ×
- 設定: 設定は不要です。

ESXiサーバ

ポート: 443

- 用途: ESXiへのVirtual Applianceの配置時における、Deep Security ManagerからESXiサーバのポート443への通信
- プロトコル: HTTPS
- 接続元: Deep Security Manager
- 接続先: ESXiサーバ
- プロキシ: ×
設定：設定は不要です。

備考：vCenterは、Virtual Applianceを構成する3つのvmdkをアップロードするため、Deep Security ManagerにESXiのURLを3つ提供します。Deep Security Managerは、ESXiへのHTTPS接続を確立し、vmdkをPOSTします。

ローカルソフトウェア配信Webサーバ

ポート：80または443

用途：Agentを、Deep Security Relayの代わりにこれらのWebサーバからソフトウェアアップデートを要求するように設定できます。

プロトコル：HTTPまたはHTTPS

接続元：Deep Security Agent

接続先：ローカルソフトウェア配信サーバ

プロキシ：x

設定：設定は不要です。ポートは、WebサーバのURLで指定できます。

備考：ソフトウェア配信Webサーバの詳細については、「ソフトウェアアップデートサーバの設定 (196ページ)」を参照してください。
NICチーミング

WindowsとSolarisのAgentをNICチーミング環境にインストールする

「NICチーミング」とは、データ転送速度を向上したり、冗長性を提供するために、複数のイーサネットアダプタを並列配置して使用することです。ここでは、WindowsおよびSolarisにNICチーミング環境を設定し、Deep Security Agentとの互換性を保つ方法を解説します。

Windows

Windows NICチーミングソフトウェアは、1つ目のスレーブインタフェースのMACアドレスを適用する新しい仮想マスターインタフェースを作成します。初期設定では、Windows Agentはインストール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。その結果、NICチーミング環境で、Agentはチャンネルソフトウェアが作成した物理インタフェース、または仮想インタフェースとバインドされます。しかし、Agentは同一MACアドレスを持つ複数のインタフェースでは正常に動作しません。正常に動作させるには、Agentをチャンネルソフトウェアが作成した仮想インタフェースとのみバインドする必要があります。

注意: 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の仮想マスターインタフェースにバインドされます。インストール後は、ネットワークインタフェースをNICチーミングに追加またはNICチーミングから削除するとき、自動的にバインドを調整することができません。これを実行すると、ネットワーク接続の問題や、ホストシステムが適切に保護されない問題が発生することがあります。Agentのネットワークドライバがインストールされているネットワーク環境でネットワークインタフェースを追加または削除した後、そのドライバが仮想インタフェースのみにバインドされ、いずれの物理アダプタにもバインドされていないことを確認してください。

Solaris

SolarisのIPMPフェイルオーバ (active-standby) モードでは、2つのNICが同じハードウェア (MAC) アドレスを共有することができます。Deep Security AgentはMACアドレスを使ってアダプタを識別するため、このようにアドレスが共有されていると、Agentが正常に動作しません。

これを解決するには、各アダプタに一意のMACアドレスを割り当てます。

ifconfigの出力例を次に示します。

```
# ifconfig -a
hme0:flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
   inet 10.20.30.40 netmask 0
   ether 8:0:20:f7:c3:f
hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
   inet 0.0.0.0 netmask 0
   ether 8:0:20:f7:c3:f
```

「ether」行には、アダプタのMACアドレスが表示されます。同一のMACアドレスを示すインタフェースが複数存在し、それが同じサブネットに接続されている場合、次のifconfigコマンドを使用して新しく一意のMACアドレスを設定する必要があります。

```
# ifconfig <インタフェース名> ether <新しいMACアドレス>
```

MACアドレスが競合する可能性は非常に低いですが、snoopコマンドを使用して、選択したMACアドレスと同じものがないことを確認してください。その後、pingコマンドを使用して、サブネットのブロードキャストアドレスへの接続をテストします。

注意: 同じサブネット上に複数のインタフェースがあるSolarisシステムでは、任意のインタフェースを指定するようにパケットのルーティングをOSで指定できます。このため、ファイアウォールステートフル設定のオプションまたは侵入防御ルールは、すべてのインタフェースに同等に適用する必要があります。
Deep Security Virtual Applianceのインタフェース

Deep Security Virtual Applianceのインタフェースにアクセスするには、VMware vSphere Clientを開き、ナビゲーションパネルでApplianceを選択して、[コンソール]タブをクリックします。

システム情報 ([System Information])

Applianceのバージョン番号とビルド番号、このApplianceを管理しているDeep Security ManagerのURL、およびApplianceのタイムゾーンが表示されます。

パスワードの設定 ([Configure Password])

このApplianceコンソールにアクセスするための現在のパスワードです。初期設定のパスワード（「dsva」）は、インストール後に変更する必要があります。

管理ネットワークの設定 ([Configure Management Network])

Applianceのホスト名とIPアドレスが表示されます。最初に、Applianceには初期設定のホスト名「dsva」が与えられます。IPアドレスは、ローカルのDHCPサーバによって割り当てられます。DHCPサーバがない場合は、IPアドレス、ネットマスク、初期設定のゲートウェイ、プライマリDNS、およびセカンダリDNSの情報を手動で入力する必要があります(編集モードに切り替えるには、<Enter>キーを押します)。

| 注意：  | 複数のVirtual Applianceを配置する場合は、DNSの問題が発生するのを避けるために、ホスト名を必ず変更してください。 |
Amazon Web Servicesのリージョンを管理する

Amazon Web Servicesのリージョンを追加する

ユーザが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、クラウドリソースをホストしているAmazon Web Servicesのリージョンが表示されない場合は、dsm_cコマンドラインツールを使用してリージョンをリストに手動で追加する必要があります。

Amazon Web Servicesのリージョンをdsm_cを使用して追加するには

1. Deep Security Managerサーバで、次のコマンドを実行します。

   ```bash
   dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT
   ```

   パラメータは次のとおりです。

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
<th>値のサンプル</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGION</td>
<td>Amazon Web ServicesのリージョンID。</td>
<td>ca-east-1</td>
</tr>
<tr>
<td>DISPLAY</td>
<td>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。</td>
<td>Canada East (Ottawa)</td>
</tr>
<tr>
<td>ENDPOINT</td>
<td>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。</td>
<td>ec2.ca-east-1.amazonaws.com</td>
</tr>
</tbody>
</table>

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。

注意: Amazon Web Servicesのリージョンを手動で追加するときは、信頼された証明書の追加が必要になることがあります。詳細については、「信頼された証明書を管理する (306ページ)」を参照してください。

追加したAmazon Web Servicesのリージョンを表示する

システムに追加したAmazon Web Servicesのリージョンは、dsm_cコマンドラインツールを使用して表示できます。

追加したAmazon Web Servicesのリージョンをdsm_cを使用して表示するには

1. Deep Security Managerサーバで、次のコマンドを実行します。

   ```bash
   dsm_c -action listregions
   ```

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。

追加したAmazon Web Servicesのリージョンを削除する

システムに追加したAmazon Web Servicesのリージョンは、dsm_cコマンドラインツールを使用して削除できます。

該当するリージョンを使用して追加したクラウドアカウントは引き続き使用できますが、そのリージョンを使用して新しいクラウドアカウントを作成することはできなくなります。

追加したAmazon Web Servicesのリージョンをdsm_cを使用して削除するには

1. Deep Security Managerサーバで、次のコマンドを実行します。
dsm_c -action listregions

2. 削除するリージョンのIDをリストから探します。
3. 次のコマンドを実行します。

   dsm_c -action removeregion -region REGION

REGIONパラメータは必須です。

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
<th>値のサンプル</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGION</td>
<td>Amazon Web ServicesのリージョンID。</td>
<td>ca-east-1</td>
</tr>
</tbody>
</table>

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管理する

信頼された証明書をインポートする

コード署名やAmazon Web Services以外のSSL接続に使用する信頼された証明書は、Deep Security Managerを使用してシステムにインポートすることができます。

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] に進みます。
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。

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
<th>値のサンプル</th>
</tr>
</thead>
<tbody>
<tr>
<td>PURPOSE</td>
<td>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。</td>
<td>AWS - Amazon Web Services, DSA - コード署名, SSL - SSL接続</td>
</tr>
<tr>
<td>CERTFILE</td>
<td>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。</td>
<td>/path/to/cacert.pem</td>
</tr>
</tbody>
</table>

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

コード署名やAmazon Web Services以外のSSL接続で使用する信頼された証明書は、Deep Security Managerを使用して表示することができます。

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] に進みます。
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 PURPOSE]
「-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。

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
<th>値のサンプル</th>
</tr>
</thead>
<tbody>
<tr>
<td>PURPOSE</td>
<td>証明書を使用する接続の種類。</td>
<td>AWS - Amazon Web Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DSA - コード署名</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL - SSL接続</td>
</tr>
</tbody>
</table>

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

コード署名やAmazon Web Services以外のSSL接続で使用する信頼された証明書は、Deep Security Managerを使用して削除することができます。

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] に進みます。
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コンソールにログインします。
2. 次のコマンドを実行します。
   
   dsm_c -action listcerts [-purpose PURPOSE]

   「-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。

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
<th>値のサンプル</th>
</tr>
</thead>
<tbody>
<tr>
<td>PURPOSE</td>
<td>証明書を使用する接続の種類。</td>
<td>AWS - Amazon Web Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DSA - コード署名</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL - SSL接続</td>
</tr>
</tbody>
</table>

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。

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
<th>値のサンプル</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>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。</td>
<td>3</td>
</tr>
</tbody>
</table>

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。
サポート

サポートが必要な場合は、以下を参照してください。

サポートページ
プライバシーポリシー

トレンドマイクロ株式会社は、お客さまのプライバシー保護に取り組んでいます。詳細は、http://jp.trendmicro.com/jp/about/privacy/index.htmlのトレンドマイクロのプライバシーに関する声明を参照してください。