Trend Micro Apex Central™

Patch 9

ウィジェットおよびポリシー管理ガイド

エンドポイント向けセキュリティの一元管理

※注意事項

複数年契約について

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

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

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

法人向け製品のサポートについて

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

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

著作権について

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

商標について

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

先得、Trend Micro One、Workforce One、Security Go、Dock 365、TrendConnect、TREND MICRO FORUM、トレンドマイクロ知恵袋、Trend Cloud One、Trend Service One、および Accelerating You は、トレンドマイクロ株式会社の登録商標です。

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

Copyright © 2024 Trend Micro Incorporated. All rights reserved.

P/N: APEM99919/240731_JP (2024/08)

目次

はじめに

パート I：概要

第 1 章：ダッシュボード

第 3 章：ポリシーリソース

パート II：Apex Central

第 4 章：Apex Central ダッシュボードのウィジェット

パート III：Apex One

第 5 章：Apex One ダッシュボードウィジェット

パート IV：Apex One サーバのポリシー設定

第 6 章：Apex One サーバのポリシー設定

パート V：Apex One セキュリティエージェントのポリシー

第 7 章：セキュリティエージェントプログラム設定

第 8 章：アプリケーションコントロールのポリシー設定

第 9 章：挙動監視ポリシー設定

第 10 章：不正プログラム対策ポリシー設定

パート VIII：Deep Discovery のウィジェットとポリシー

第 22 章：Deep Discovery Analyzer および Email Inspector ダッシュボードウィジェット

第 23 章：Deep Discovery Inspector の統合とポリシー設定

パート IX：Deep Security Manager

第 24 章：Deep Security Manager ダッシュボードウィジェット

パート XVI：Trend Micro Mobile Security のウィジェットとポリシー

第 37 章：Trend Micro Mobile Security ダッシュボードウィジェット

索引

はじめに

『Trend Micro Apex Central™ウィジェットおよびポリシー管理ガイド』にようこそ。このドキュメントでは、Apex Central で [ダッシュボード] ウィジェットと [ポリシー管理] を設定する方法について説明します。

このセクションの内容:

ドキュメント

Apex Central のドキュメントには、次の情報が含まれます。

ドキュメント	説明
Readme ファイル	既知の問題の一覧が含まれます。また、オンラインヘルプや印刷ドキュメントにまだ収録されていない最新の製品情報が含まれる場合があります。
管理者ガイド	Apex Central と管理下の製品の設定および管理方法に加えて、Apex Central の概要と機能の説明が記載された PDF ドキュメント
オンラインヘルプ	操作手順、使用のアドバイス、および目的別の作業手順を提供する、WebHelp 形式でコンパイルされた HTML ファイル。このヘルプは、Apex Central 管理コンソールからもアクセスできます。
製品 Q&A	問題解決およびトラブルシューティング情報のオンラインデータベース。既知の製品の問題についての最新情報を提供します。製品 Q&A にアクセスするには、https://success.trendmicro.com/dcx/s/?language=ja を参照してください。

対象読者

このドキュメントは、次のユーザを対象としています。

- Apex Central の管理者: Apex Central のインストール、設定、および管理を担当し、高度なネットワークおよびサーバ管理の知識を持っていることが求められます。
- 管理下の製品の管理者: Apex Central と統合されているトレンドマイクロ製品の管理を担当し、高度なネットワークおよびサーバ管理の知識を持っていることが求められます。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 1. ドキュメントの表記規則

表記	説明
 注意	設定上の注意
 ヒント	推奨事項
 重要	必須の設定や初期設定、および製品の制限事項に関する情報
 警告!	避けるべき操作や設定についての注意

用語

次の表は、Apex Central 付属のドキュメントで使用されている用語を示しています。

用語	説明
管理者 (または Apex Central 管理者)	Apex Central サーバを管理しているユーザ
セキュリティエージェント	エンドポイントにインストールされている管理下の製品プログラム
コンポーネント	セキュリティリスクの検索、検出、および処理を実行するもの

用語	説明
Apex Central 管理コンソールまたは Web コンソール	Apex Central のアクセス、設定、および管理を実行するための Web ベースのユーザインタフェース **注意** 統合された管理下の製品のコンソールは、管理下の製品名で示されます。たとえば、Apex One Web コンソールなどです。
管理下のエンドポイント	管理下の製品であるセキュリティエージェントがインストールされているエンドポイント
管理下の製品	Apex Central と統合されるトレンドマイクロ製品
管理下のサーバ	管理下の製品がインストールされているエンドポイント
サーバ	Apex Central サーバがインストールされているエンドポイント
セキュリティリスク	ウイルス、不正プログラム、スパイウェア、グレーウェア、および Web からの脅威の総称
デュアルスタック	IPv4 アドレスと IPv6 アドレスの両方のアドレスを持つエンティティ
IPv4 シングルスタック	IPv4 アドレスのみを持つエンティティ
IPv6 シングルスタック	IPv6 アドレスのみを持つエンティティ

パート I

概要

第 1 章

ダッシュボード

このセクションでは、Apex Central のダッシュボードタブおよびウィジェットを使用する方法について説明します。

次のトピックがあります。

ダッシュボードについて

ダッシュボードは、Apex Central 管理コンソールを開くかメインメニューの [ダッシュボード] をクリックすると表示されます。ダッシュボードは Apex Central ユーザアカウントごとに完全に独立しています。特定のユーザアカウントに属するダッシュボードを変更しても、その他のユーザアカウントのダッシュボードに影響はありません。

[ダッシュボード] には以下のものがあります。

- タブ
- ウィジェット

タブとウィジェット

ウィジェットは [ダッシュボード] を構成するコンポーネントです。ウィジェットはさまざまなセキュリティ関連イベントに関する特定の情報を提供します。

ウィジェットに表示される情報は、次の場所から取得されます。

- Apex Central データベース
- 登録されている管理下の製品
- Trend Micro Smart Protection Network

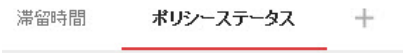
タブはウィジェット用のコンテナを用意します。[ダッシュボード] では、最大 30 のタブがサポートされます。

タブを使用する

タブの管理では、追加、名前の変更、レイアウトの変更、削除、タブ表示の自動切り替えを行います。

手順

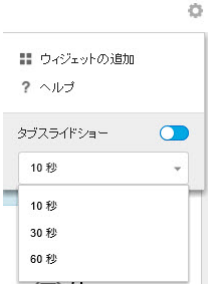
1. [ダッシュボード] に移動します。
2. タブを追加するには、次の手順を実行します。
   a. 追加アイコン (＋) をクリックします。



b. 新しいタブの名前を入力します。

3. タブの名前を変更するには、次の手順を実行します。
   a. タブ名にマウスを重ねて、下矢印をクリックします。

   b. [名前の変更] をクリックして、新しいタブ名を入力します。
4. タブでウィジェットのレイアウトを変更するには、次の手順を実行します。
   a. タブ名にマウスを重ねて、下矢印をクリックします。
   b. [レイアウトの変更] をクリックします。
   c. 表示される画面から新しいレイアウトを選択します。
   d. [保存] をクリックします。
5. タブを削除するには、次の手順を実行します。
   a. タブ名にマウスを重ねて、下矢印をクリックします。
   b. [削除] をクリックし、確認します。
6. タブスライドショーを再生するには、次の手順を実行します。
   a. タブ表示の右にある [設定] ボタンをクリックします。



b. [タブスライドショー] コントロールを有効にします。

c. 次のタブに切り替わるまでの各タブの表示時間を選択します。

ウィジェットを使用する

ウィジェットの管理では、項目の追加、移動、サイズの変更、名前の変更、削除を行います。ウィジェットのデータの収集元となる製品を変更することもできます。

手順

1. [ダッシュボード] に移動します。
2. タブをクリックします。
3. ウィジェットを追加するには、次の手順を実行します。
   a. タブ表示の右にある [設定] ボタンをクリックします。

b. [ウィジェットの追加] をクリックします。

c. 追加するウィジェットを選択します。

- ウィジェットの上部にあるドロップダウンで、カテゴリを選択して選択項目を絞り込みます。
- 画面上の検索テキストボックスで特定のウィジェットを検索できます。

d. [追加] をクリックします。

4. ウィジェットを同じタブ内の別の場所に移動するには、ウィジェットをドラッグアンドドロップします。
5. ウィジェットのサイズを変更するには、カーソルをウィジェットの右端に合わせてから、カーソルを左右に動かします。
6. ウィジェットの名前を変更するには、次の手順を実行します。

a. 設定アイコン (>) をクリックします。

b. 新しいタイトルを入力します。

c. [保存] をクリックします。

7. ウィジェットの製品範囲を変更するには、次の手順を実行します。

a. 設定アイコン (>) をクリックします。

b. [範囲] フィールドの二重矢印ボタン (>>) をクリックします。

c. (オプション) 漏斗アイコン () をクリックして、製品をフィルタ検索します。

d. ウィジェットのデータの収集元となる製品を選択し、[OK] をクリックします。

e. [保存] をクリックします。

8. ウィジェットを削除するには、削除アイコン (>) をクリックします。

[セキュリティ状態] タブ

[セキュリティ状態] タブには、コンプライアンスレベル、重大な脅威の検出、およびネットワーク上で停止した検出に関するデータが統合された、ネットワーク保護ステータスの概要が表示されます。[セキュリティ状態] のグラフを使用して、統合された Active Directory 構造からリスクの高いユーザおよびグループを迅速に特定できます。

注意

サンプルのグラフデータを変更し、社内ネットワークに基づいてサイトまたはレポートラインを表示するには、Active Directory の統合を有効にするか、IP アドレスに基づいてカスタムサイトを作成します。

初期設定では、[セキュリティ状態] タブは [グラフ] 表示 () になっています。グラフのノード、重大な脅威、およびウイルスパターンファイルのコンプライアンス情報を表形式で表示するには、[表データ] 表示 () に切り替えます。

設定アイコン (>) をクリックすると、タブに表示される次の情報が変更されます。

- 組織: 組織の表示名を指定します。
- Active Directory グループ設定: グラフ上のノードが Active Directory の [サイト] または [レポートライン] のどちらを表すかを指定します。

- 表示するグループ: リスクが高いグループを上位何個まで表示するかを選択します。
- 期間: グラフに表示されるデータの時間範囲を指定します。

コンプライアンスインジケータ

[セキュリティ状態] タブのこのセクションには、ウイルスパターンファイルのコンプライアンスレベルまたは情報漏えい対策のコンプライアンスレベルに関する情報が表示されます。

ネットワークのコンプライアンスレベルが変更されると、コンプライアンスインジケータのアイコンの色が変わり、[Active Directory とコンプライアンスの設定] 画面で設定したしきい値が反映されます。

初期設定では、[ウイルスパターンファイルのコンプライアンス] インジケータの情報が表示されます。

注意

コンプライアンスインジケータを変更すると、[セキュリティ状態] のグラフに表示されるコンプライアンスレベルの情報も変更されます。

表示するコンプライアンス情報を変更するには、下矢印アイコン ( ) の横にある選択したコンプライアンスインジケータの名前をクリックし、ドロップダウンから次のいずれかのインジケータを選択します。

インジケータ	説明
ウイルスパターンファイルのコンプライアンス	次の情報が表示されます。 • 対応するウイルスパターンファイルおよびスマートスキャンエージェントパターンファイルのバージョンを使用した、セキュリティエージェントの割合 • 期限切れのパターンファイルを使用しているネットワーク上のエンドポイントの総数 [期限切れのパターンファイルを使用しているエンドポイント] の数をクリックすると、ユーザ/エンドポイントディレクトリ内の感染したエンドポイントに関する詳細情報が表示されます。

インジケータ	説明
情報漏えい対策のコンプライアンス	次の情報が表示されます。 • 情報漏えい対策が有効にされ、許容される脅威の検出数が設定されたセキュリティエージェントの割合 • データ検出で脅威が検出されたエンドポイントの総数 [許容されない脅威が検出されるエンドポイント] の数をクリックすると、ユーザ/エンドポイントディレクトリ内の感染したエンドポイントに関する詳細情報が表示されます。

重大な脅威

[セキュリティ状態] タブの [重大な脅威] には、ネットワーク上で検出された一意の重大な脅威の総数 (脅威の種類別)、影響を受けたユーザの総数、影響を受けた重要なエンドポイントの数 (星のマーク付き) が表示されます。

影響を受けたユーザの数をクリックすると、[ユーザ/エンドポイントディレクトリ] 画面に追加の詳細が表示されます。

重大な脅威の検出には、次の脅威の種類が含まれます。

脅威の種類	説明
ランサムウェア	身代金が支払われない限り、ユーザによるシステムへのアクセスを阻止または制限する不正プログラム
既知の APT (標的型サイバー攻撃)	標的とした対象を執拗に追跡して侵入し、不正行為をする攻撃。単独のイベントではなく、キャンペーン (一定期間にわたって失敗と成功を繰り返しながら対象ネットワークの奥深くに侵入する試み) で行われることが多い。
ソーシャルエンジニアリング攻撃	PDF ファイルなどのドキュメントに存在するセキュリティの脆弱性を悪用する不正プログラムまたはハッカーによる攻撃
脆弱性に対する攻撃	通常、プログラムおよびオペレーティングシステムに存在するセキュリティの弱点を悪用する不正プログラムまたはハッカーによる攻撃
侵入拡大	ディレクトリ、メール、管理サーバ、およびその他の資産の検索してネットワークの内部構造をマップし、そのシステムにアクセスするための認証情報を入手して、攻撃者がシステム間を移動する攻撃

脅威の種類	説明
未知の脅威	Deep Discovery Inspector、エンドポイントのセキュリティ製品、またはその他の仮想アナライザを備えた製品で、リスクレベルが「高」として検出された不審オブジェクト (IP アドレス、ドメイン、ファイル SHA-1 ハッシュ値、メールメッセージ)
C&C コールバック	情報の配信、指示の受信、およびその他の不正プログラムのダウンロードを実行するためのコマンド&コントロール (C&C) サーバとの通信の試行

解決済みのイベント

[セキュリティ状態] タブのこのセクションには、ネットワーク上の解決済みのイベントと未解決のイベントの総数が表示されます。

[n 件の未解決のイベントに影響を受けたユーザ] フィールドの数字をクリックすると、ネットワーク上の未解決のイベントの影響を受けたユーザに関する詳細情報が表示されます。

セキュリティ状態のグラフ

[セキュリティ状態] タブのグラフには、ネットワークの重大な脅威の割合とコンプライアンスレベルの関係が表示されます。x 軸は、サイトまたはレポートライン内のエンドポイントの総数に対する、重大な脅威の割合を示しています。y 軸は、選択したコンプライアンスインジケータのサイトまたはレポートラインのコンプライアンスレベルを示しています。このデータを使用して、統合された Active Directory 構造からリスクの高いユーザおよびグループを迅速に特定できます。

注意

サンプルのグラフデータを変更し、社内ネットワークに基づいてサイトまたはレポートラインを表示するには、Active Directory の統合を有効にするか、IP アドレスに基づいてカスタムサイトを作成します。

ノードにマウスを重ねると、特定のサイトまたはレポートラインのコンプライアンスと重大な脅威の情報が表示されます。ノードの矢印は、指定された期間におけるセキュリティステータスの変化を示します。

- ノードが示す [Active Directory グループ設定] ([サイト]、[レポートライン]) を変更するには、設定アイコン (>) をクリックします。
- また、[Active Directory とコンプライアンスの設定] 画面を使用して、サイトとレポートラインをカスタマイズできます。

初期設定では、過去 7 日間のネットワーク上のすべてのノードの、選択したコンプライアンスインジケータに関する情報が表示されます。

- 表示するコンプライアンス情報を変更するには、別のコンプライアンスインジケータを選択します。
- 表示するデータの [期間] を変更するには、設定アイコン (>) をクリックします。
- ノードをクリックすると、右側の概要パネルに選択したノードの詳細情報が表示されます。

セキュリティ状態の詳細ペイン

[セキュリティ状態] タブの詳細ペインには、コンプライアンスレベル、重大な脅威の検出、およびネットワーク上で解決済みのイベントと未解決のイベントの詳細が表示されます。

初期設定では、過去 7 日間のネットワーク上のすべてのノードの、選択したコンプライアンスインジケータに関する情報が表示されます。

- 表示するコンプライアンス情報を変更するには、別のコンプライアンスインジケータを選択します。
- グラフのノードをクリックすると、選択したノードの情報だけが表示されます。
- 表示するデータの [期間] を変更するには、設定アイコン (>) をクリックします。

表 1-1. コンプライアンス情報

インジケータ	説明

ウイルスパターンファイルのコンプライアンス	対応するウイルスパターンファイルおよびスマートスキャンエージェントパターンファイルのバージョンを使用した、セキュリティエージェントの割合が表示されます。
	
	次の詳細を表示することもできます。
	
	• 管理下のセキュリティエージェント: Apex One またはウイルスバスタービジネスセキュリティサービスのセキュリティエージェントがインストールされているエンドポイントの数
	
	  • パターンファイルに準拠: 対応するパターンファイルおよびスマートスキャンエージェントパターンファイルのバージョンを使用している管理下のセキュリティエージェントの数
	
	  • パターンファイルが古い: 対応するパターンファイルおよびスマートスキャンエージェントパターンファイルのバージョンを使用していない管理下のセキュリティエージェントの数
	
	  • 7 日間オフライン: 管理下の製品のサーバと 7 日以上通信していない管理下のセキュリティエージェントの数
	
	  • 除外: コンプライアンスの計算から除外されているユーザまたはエンドポイントの数
	
	• 管理対象外のエンドポイント: Apex One またはウイルスバスタービジネスセキュリティサービスのセキュリティエージェントがインストールされていないエンドポイントの数
	
	感染したエンドポイントに関する追加の詳細を表示するには、カテゴリを展開して数字をクリックします。

インジケータ	説明

情報漏えい対策のコンプライアンス	情報漏えい対策が有効にされ、許容される脅威の検出数が設定された Apex One セキュリティエージェントの割合が表示されます。
	
	次の詳細を表示することもできます。
	
	• 管理下のセキュリティエージェント: Apex One またはウイルスバスタービジネスセキュリティサービスのセキュリティエージェントがインストールされているエンドポイントの数
	
	  • 許容される脅威検出: 許容される脅威の検出数の範囲内の管理下のセキュリティエージェントの数
	
	  • 許容されない脅威検出: 許容される脅威の検出数を超えている管理下のセキュリティエージェントの数
	
	  • 7 日間オフライン: 管理下の製品のサーバと 7 日以上通信していない管理下のセキュリティエージェントの数
	
	  • 除外: コンプライアンスの計算から除外されているユーザまたはエンドポイントの数
	
	• 管理対象外のエンドポイント: Apex One またはウイルスバスタービジネスセキュリティサービスのセキュリティエージェントがインストールされていないエンドポイントの数
	
	感染したエンドポイントに関する追加の詳細を表示するには、カテゴリを展開して数字をクリックします。

表 1-2. 重大な脅威

セクション	説明
重大な脅威	ネットワーク上で検出された一意の重大な脅威の総数 (脅威の種類別) が表示されます。 ネットワークに影響を与えるすべての重大な脅威の種類が表示されます。 検出された脅威の種類: • 脅威の種類を展開すると、検出のリストが表示されます。 • 検出をクリックすると、[脅威情報] 画面に追加の詳細が表示されます。

セクション	説明
影響を受けたユーザ	重大な脅威の影響を受けたユーザの総数が表示されます。 • セクションを展開すると、影響を受けたユーザが表示されます。 • 影響を受けたユーザをクリックすると、[ユーザ] 情報画面に追加の詳細が表示されます。
感染したエンドポイント	重大な脅威の影響を受けたエンドポイントの総数が表示されます。 • セクションを展開すると、感染したエンドポイントが表示されます。 • 感染したエンドポイントをクリックすると、[エンドポイント] 情報画面に追加の詳細が表示されます。

表 1-3. イベントの総数

データ	説明
イベント総数	検出されたイベントの総数が表示されます。
解決済みのイベント	ネットワーク上の解決済みのイベントの数が表示されます。
未解決のイベント	ネットワーク上の、処理が必要な未解決のイベントの数が表示されます。
影響を受けたユーザ	ネットワーク上の未解決のイベントの影響を受けたユーザの数が表示されます。 数字をクリックすると、影響を受けたユーザの詳細が表示されます。

[概要] タブ

[概要] タブには事前に定義された一連のウィジェットがあり、ネットワークのセキュリティステータスの概要が表示されます。

注意

[概要] タブに表示されるウィジェットは追加、削除、または変更できます。

使用可能なウィジェット:

- 重大な脅威
- 脅威にさらされているユーザ
- 脅威にさらされているエンドポイント
- 製品の接続ステータス
- 製品コンポーネントのステータス
- ランサムウェア対策

重大な脅威のウィジェット

このウィジェットには、ネットワーク上で検出された一意の重大な脅威の種類の総数と、それぞれの脅威の種類における影響を受けたユーザの数および脅威の検出数が表示されます。

設定アイコン (>) をクリックして、初期設定の表示を変更します。

- [概要] タブまたはカスタムタブでは、初期設定で [影響を受けたユーザ] ビューが選択されています。
- [脅威の調査] タブでは、初期設定で [脅威の検出] ビューが選択されています。

注意

- このウィジェットには、重大な脅威の種類が重大度順に示されます。
- ユーザは複数の重大な脅威の種類の影響を受けている可能性があります。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

図 1-1. [影響を受けたユーザ] ビュー

[影響を受けたユーザ] ビューには、それぞれの脅威の種類によって影響を受けた重要なユーザおよびその他のユーザの数が表示されます。

- [重要なユーザ] 列または [その他のユーザ] 列の数字をクリックしてから、表示したい影響を受けたユーザをクリックします。
- [ユーザ/エンドポイントディレクトリ] 画面で、重要なユーザまたはエンドポイントを定義できます。

図 1-2. [脅威の検出] ビュー

[脅威の検出] ビューには、重大な脅威の種類ごとの検出数が表示されます。

- 重大な脅威の種類をクリックすると、その種類の脅威検出が表示されます。
- 特定の脅威検出のハイパーリンクをクリックすると、影響を受けたユーザの詳細が表示されます。同時に、Root Cause Analysis が自動的に開始され、その脅威がネットワーク上の他のエンドポイントに影響を与えたかどうかが調査されます。

重大な脅威の検出には、次の脅威の種類が含まれます。

脅威の種類	説明
ランサムウェア	身代金が支払われない限り、ユーザによるシステムへのアクセスを阻止または制限する不正プログラム
既知の APT (標的型サイバー攻撃)	標的とした対象を執拗に追跡して侵入し、不正行為をする攻撃。単独のイベントではなく、キャンペーン (一定期間にわたって失敗と成功を繰り返しながら対象ネットワークの奥深くに侵入する試み) で行われることが多い。
ソーシャルエンジニアリング攻撃	PDF ファイルなどのドキュメントに存在するセキュリティの脆弱性を悪用する不正プログラムまたはハッカーによる攻撃

脅威の種類	説明
脆弱性に対する攻撃	通常、プログラムおよびオペレーティングシステムに存在するセキュリティの弱点を悪用する不正プログラムまたはハッカーによる攻撃
侵入拡大	ディレクトリ、メール、管理サーバ、およびその他の資産の検索してネットワークの内部構造をマップし、そのシステムにアクセスするための認証情報を入手して、攻撃者がシステム間を移動する攻撃
未知の脅威	Deep Discovery Inspector、エンドポイントのセキュリティ製品、またはその他の仮想アナライザを備えた製品で、リスクレベルが「高」として検出された不審オブジェクト (IP アドレス、ドメイン、ファイル SHA-1 ハッシュ値、メールメッセージ)
C&C コールバック	情報の配信、指示の受信、およびその他の不正プログラムのダウンロードを実行するためのコマンド&コントロール (C&C) サーバとの通信の試行

脅威にさらされているユーザウィジェット

このウィジェットには、セキュリティの脅威が検出されたユーザに関する情報が表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

[重要なエンドポイント] タブまたは [その他のエンドポイント] タブをクリックすると、表示が切り替わります。

この表には、影響を受けたユーザが、最初に重大な脅威の種類の重大度の順に示され、次にユーザの脅威検出数の順に示されます。

- 表示するユーザの [脅威] 列の数字をクリックします。

[最も重大な脅威] 列には、次の脅威の種類が表示されます。

脅威の種類	説明
C&C コールバック	情報の配信、指示の受信、およびその他の不正プログラムのダウンロードを実行するためのコマンド&コントロール (C&C) サーバとの通信の試行

脅威の種類	説明
既知の APT (標的型サイバー攻撃)	標的とした対象を執拗に追跡して侵入し、不正行為をする攻撃。単独のイベントではなく、キャンペーン (一定期間にわたって失敗と成功を繰り返しながら対象ネットワークの奥深くに侵入する試み) で行われることが多い。
侵入拡大	ディレクトリ、メール、管理サーバ、およびその他の資産の検索してネットワークの内部構造をマップし、そのシステムにアクセスするための認証情報を入手して、攻撃者がシステム間を移動する攻撃
ランサムウェア	身代金が支払われない限り、ユーザによるシステムへのアクセスを阻止または制限する不正プログラム
ソーシャルエンジニアリング攻撃	PDF ファイルなどのドキュメントに存在するセキュリティの脆弱性を悪用する不正プログラムまたはハッカーによる攻撃
未知の脅威	Deep Discovery Inspector、エンドポイントのセキュリティ製品、またはその他の仮想アナライザを備えた製品で、リスクレベルが「高」として検出された不審オブジェクト (IP アドレス、ドメイン、ファイル SHA-1 ハッシュ値、メールメッセージ)
脆弱性に対する攻撃	通常、プログラムおよびオペレーティングシステムに存在するセキュリティの弱点を悪用する不正プログラムまたはハッカーによる攻撃

脅威にさらされているエンドポイントウィジェット

このウィジェットには、セキュリティの脅威が検出されたエンドポイントに関する情報が表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

[重要なエンドポイント] タブまたは [その他のエンドポイント] タブをクリックすると、表示が切り替わります。

この表には、影響を受けたユーザが、最初に重大な脅威の種類の重大度の順に示され、次にユーザの脅威検出数の順に示されます。

- 表示するユーザの [脅威] 列の数字をクリックします。

[最も重大な脅威] 列には、次の脅威の種類が表示されます。

脅威の種類	説明
C&C コールバック	情報の配信、指示の受信、およびその他の不正プログラムのダウンロードを実行するためのコマンド&コントロール (C&C) サーバとの通信の試行
既知の APT (標的型サイバー攻撃)	標的とした対象を執拗に追跡して侵入し、不正行為をする攻撃。単独のイベントではなく、キャンペーン (一定期間にわたって失敗と成功を繰り返しながら対象ネットワークの奥深くに侵入する試み) で行われることが多い。
侵入拡大	ディレクトリ、メール、管理サーバ、およびその他の資産の検索してネットワークの内部構造をマップし、そのシステムにアクセスするための認証情報を入手して、攻撃者がシステム間を移動する攻撃
ランサムウェア	身代金が支払われない限り、ユーザによるシステムへのアクセスを阻止または制限する不正プログラム
ソーシャルエンジニアリング攻撃	PDF ファイルなどのドキュメントに存在するセキュリティの脆弱性を悪用する不正プログラムまたはハッカーによる攻撃
未知の脅威	Deep Discovery Inspector、エンドポイントのセキュリティ製品、またはその他の仮想アナライザを備えた製品で、リスクレベルが「高」として検出された不審オブジェクト (IP アドレス、ドメイン、ファイル SHA-1 ハッシュ値、メールメッセージ)
脆弱性に対する攻撃	通常、プログラムおよびオペレーティングシステムに存在するセキュリティの弱点を悪用する不正プログラムまたはハッカーによる攻撃

Apex Central 上位の脅威ウィジェット

このウィジェットには、指定された時間範囲内に検出された不正ファイルと不正 URL に関する情報が表示されます。

表示アイコン () をクリックすると、棒グラフまたは表の形式でデータを表示できます。

グラフまたは表の上部にあるドロップダウンリストを使用して、表示する脅威データの種類を選択します。

- 不正ファイル: ネットワーク上で検出された不正ファイルを検出数で順位付けします。

- 不正 URL: ネットワーク上で検出された不正 URL を検出数で順位付けします。

バー、脅威名、または検出番号をクリックすると、[ログクエリ] 画面が開き、感染したエンドポイント、脅威の詳細、および検出数に関する情報が表示されます。

初期設定では、ログオンしているユーザアカウントがアクセス可能なすべての管理下の製品のトップ 10 の脅威が表示されます。

- 表示されるウィジェットのタイトル、製品範囲、または脅威の数を編集するには、設定アイコン (>) をクリックします。

製品コンポーネントのステータスウィジェット

このウィジェットには、ネットワーク上の管理下の製品またはエンドポイントの、コンポーネントバージョンおよびコンプライアンスステータスが表示されます。このウィジェットは、有効期限が終了したコンポーネントを使用している管理下の製品またはエンドポイントを追跡するために使用します。

初期設定では、Apex Central によって管理されるコンポーネントの最新バージョンと、管理下の製品のコンプライアンスステータスが表示されます。[パターンファイル] と [検索エンジン] のセクションには、コンポーネントがコンプライアンス違反率の高い順にリスト表示されます。[比率] 列をクリックすると、ソート順を変更できます。

[パターンファイル] 列または [検索エンジン] 列のいずれかのコンポーネントをクリックすると、各コンポーネントバージョンを使用している管理下の製品またはエンドポイントの数を示す円グラフが表示されます。

[古いバージョン/すべて] の列の数字をクリックすると、期限切れの管理下の製品、すべての管理下の製品、期限切れのエンドポイント、またはすべてのエンドポイントのコンポーネントバージョンに関する情報が表示されます。

設定アイコン (>) をクリックして、次のオプションを設定します。

注意

[概要] タブのウィジェットには設定アイコン ( ) が表示されません。

- ウィジェットの製品範囲を変更するには、[範囲] フィールドの二重矢印ボタン (>>) をクリックし、データの収集元となる製品を選択します。
- ウィジェットに表示されるコンポーネントを編集するには、[パターンファイル] フィールドまたは [検索エンジン] フィールドからコンポーネントを選択または選択解除します。
- 管理下の製品、エンドポイント、またはその両方のコンプライアンス情報を表示するには、[ソース] を指定します。
- 管理下の製品によって報告されたすべてのコンポーネントのデータを表示するか、Apex Central によって管理されるコンポーネントのデータのみを表示するかを指定するには、[表示] を選択します。

データ	説明
パターンファイル	パターンファイル、テンプレート、またはスパムメール判定ルールの名前が表示されます。
検索エンジン	検索エンジンの名前が表示されます。
最新バージョン	次の情報が表示されます。 • Apex Central によってダウンロードされたコンポーネントの最新バージョン • (管理下の製品によって報告された) ダウンロード可能なコンポーネントの最新バージョン

データ	説明
古いバージョン/すべて	次の情報が表示されます。 • 期限切れ: 期限切れのコンポーネントがある管理下の製品またはエンドポイントの数 [古いバージョン/すべて] 列の最初の数字をクリックすると、期限切れの管理下の製品またはエンドポイントのコンポーネントバージョンに関する情報が表示されます。 • すべて: コンポーネントを使用する管理下の製品またはエンドポイントの総数 [古いバージョン/すべて] 列の 2 番目の数字をクリックすると、すべての管理下の製品またはエンドポイントのコンポーネントバージョンに関する情報が表示されます。 注意 この列は、[ソース] に対して [両方] が選択されている場合に表示されます。
比率	期限切れのコンポーネントがある管理下の製品またはエンドポイントの割合が表示されます。 注意 この列は、[ソース] に対して [両方] が選択されている場合に表示されます。

製品の接続ステータスウィジェット

このウィジェットには、Apex Central サーバに登録されているすべての管理下の製品の接続ステータスが表示されます。

初期設定では、ログオンしているユーザアカウントがアクセス可能な管理下の各製品の接続ステータスと管理下のサーバ名のリストが表示されます。

- 製品の範囲を変更するには、設定アイコン (>) をクリックして、新しい [範囲] を選択します。

- 各接続ステータスの管理下の製品の総数について概要を表示するには、設定アイコン (>) をクリックして、[表示] を [概要] に切り替えます。

[詳細の表示] をクリックして、[ログクエリ] 画面で詳細情報を確認します。

ステータス	説明
有効	製品サービスが実行中であり、Apex Central サーバとの通信が正常に確立されていることを示します。
無効	製品サービスが実行されていないか、Apex Central サーバとの通信が確立できないことを示します。
異常	製品サービスは、ユーザ定義のエージェントの通信タイムアウト間隔で Apex Central サーバと通信していないことを示します。

ランサムウェア対策ウィジェット

このウィジェットには、指定された時間範囲内に試行されたすべてのランサムウェア攻撃の概要が表示されます。

初期設定のビューには、すべてのランサムウェア検出の概要が表示され、感染経路に基づいてすべての試行が分類されます。

- ランサムウェアの検出数をクリックすると、追加の詳細が確認されます。

チャネル	説明
メッセージ	メールのメッセージまたは添付ファイルで検出されたランサムウェアを示します。
Web サイト	Web レピュテーションサービスによって検出されたランサムウェアを示します。
ネットワークトラフィック	Apex One の不審接続監視および Deep Discovery Inspector によって検出されたランサムウェアを示します。
クラウドでの同期	クラウドストレージおよび Office 365 サーバ (Exchange Online、SharePoint Online、および OneDrive) で Cloud App Security によって検出されたランサムウェア、またはクラウドストレージと同期する Apex One セキュリティエージェントのローカルフォルダ内で Apex One によって検出されたランサムウェアを示します。

チャネル	説明
ファイル	ファイルレピュテーションサービスによって検出されたランサムウェアを示します。
挙動	Apex One の挙動監視によって検出されたランサムウェアを示します。

[情報漏えい対策] タブ

[情報漏えい対策] タブには、情報漏えい対策イベント、テンプレート一致、およびイベント発生元に関する情報が表示されるウィジェットが含まれます。

次のウィジェットが事前定義されています。

- 重大度およびステータス別の情報漏えい対策イベント
- ユーザ別の情報漏えい対策イベントの傾向
- ユーザ別の情報漏えい対策イベント
- チャネル別情報漏えい対策イベント
- 情報漏えい対策テンプレート一致
- 情報漏えい対策イベント発生元の上位
- 情報漏えい対策違反ポリシー

ユーザ別の情報漏えい対策イベントの傾向ウィジェット

このウィジェットを使用して、管理下のユーザに基づく情報漏えい対策イベントの傾向の数を確認できます。データは重大度レベル別にフィルタ処理したり、指定された期間に特定のユーザによって実行されたインシデントの総数のみ表示するようにフィルタ処理したりできます。初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。

[期間] ドロップダウンを使用して、データを表示する期間を選択します。

グラフのセクションをクリックすると、[イベント情報] 画面が開き、イベントの概要を確認できます。

ウィジェット上のウィジェット設定をクリックして、追加設定を表示します。

設定	説明
タイトル	フィールドに、ウィジェットの新しくわかりやすいタイトルを入力します。
期間	情報漏えい対策イベントの発生した時間範囲を指定します。
範囲	ウィジェットによって表示されるデータの範囲を指定します。 • 直接管理下のユーザ • すべての管理下のユーザ: データは直接管理されているユーザと直接管理されているユーザの下にいる人々の両方から収集されます。
重大度	データをフィルタするための重大度レベルを指定します。
表示するユーザ	表示する管理下のユーザの数を指定します。

[保存] をクリックして変更を適用し、ウィジェットデータを更新します。

重大度およびステータス別の情報漏えい対策イベントウィジェット

このウィジェットを使用して、重大度レベルとイベントステータスに基づく情報漏えい対策イベント数を確認できます。データは重大度レベル別にフィルタ処理できます。また、新規のイベントおよび重大度の高いイベントの総数も表示できます。初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。

[期間] ドロップダウンを使用して、データを表示する期間を選択します。

任意の列内の数字をクリックすると、[イベント情報] 画面が開き、イベントの概要を確認できます。

特定のイベントを検索するには、[イベント ID] フィールドに ID を入力し、[検索] をクリックします。

ヒント

イベントごとに 1 つずつ ID 番号が割り当てられます。ID 番号は、[イベント詳細のアップデート] イベント通知、または情報漏えい対策ログクエリ内の表のリンクをクリックすることで確認できます。

ウィジェット上のウィジェット設定をクリックして、追加設定を表示します。

設定	説明
タイトル	フィールドに、ウィジェットの新しくわかりやすいタイトルを入力します。
期間	情報漏えい対策イベントの発生した時間範囲を指定します。
範囲	ウィジェットによって表示されるデータの範囲を指定します。 • 直接管理下のユーザ • すべての管理下のユーザ: データは直接管理されているユーザと直接管理されているユーザの下にいる人々の両方から収集されます。
重大度	データをフィルタするための重大度レベルを指定します。

[保存] をクリックして変更を適用し、ウィジェットのデータを更新します。

ユーザ別の情報漏えい対策イベントウィジェット

このウィジェットを使用して、重大度レベルと管理下のユーザに基づく情報漏えい対策イベント数を確認できます。データは重大度レベル別にフィルタ処理できます。また、特定のユーザによって開始された新規のイベントおよび重大度の高いイベントの総数も表示できます。初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。ウィジェットには最大 50 ユーザが表示されます。

[期間] ドロップダウンを使用して、データを表示する期間を選択します。

任意の列内の数字をクリックすると、[イベント情報] 画面が開き、イベントの概要を確認できます。

特定のユーザを検索するには、[ユーザ] フィールドに数文字を入力し、[検索] をクリックします。たとえば、「`ke`」と入力すると、「`ke`」を含むすべてのユーザ名 (「Ken」や「Brooke」など) が表示されます。また、ドメインとユーザ名 (`domain1¥chris` など) を入力することもできます。

注意

ユーザ名には次の文字を使用できません:"[]:;|=+*?/\<&>,

ドメイン名には次の文字を使用できません:*+=|:;"? <&>,

ウィジェット上のウィジェット設定をクリックして、追加設定を表示します。

設定	説明
タイトル	フィールドに、ウィジェットの新しくわかりやすいタイトルを入力します。
期間	情報漏えい対策イベントの発生した時間範囲を指定します。
範囲	ウィジェットによって表示されるデータの範囲を指定します。 • 直接管理下のユーザ • すべての管理下のユーザ: データは直接管理されているユーザと直接管理されているユーザの下にいる人々の両方から収集されます。
重大度	データをフィルタするための重大度レベルを指定します。
表示するユーザ	表示する管理下のユーザの数を指定します。

[保存] をクリックして変更を適用し、ウィジェットデータを更新します。

チャネル別の情報漏えい対策イベントウィジェット

このウィジェットには、情報漏えい対策イベントの総数が表示されます。データはイベントが発生したチャネルの種類別にフィルタ処理できます。

[期間] ドロップダウンを使用して、データを表示する期間を選択します。

[チャネル] ドロップダウンを使用して、イベントが発生したチャネルの種類をフィルタで除外します。

このウィジェットには、情報漏えい対策イベントの数と、イベント総数に対するチャネルの割合が表示されます。このウィジェットには、次のカテゴリ別にデータが表示されます。

データ	説明
P2P	[データの範囲] で指定されている管理下の製品別にピアツーピア情報漏えい対策イベントがすべて表示されます。
IM	[データの範囲] で指定されている管理下の製品別にインスタントメッセージ情報漏えい対策イベントがすべて表示されます。
Web メール	[データの範囲] で指定されている管理下の製品別に Web メール情報漏えい対策イベントがすべて表示されます。
メール通知	[データの範囲] で指定されている管理下の製品別にメール情報漏えい対策イベントがすべて表示されます。
Web アプリケーション	[データの範囲] で指定されている管理下の製品別に Web アプリケーション情報漏えい対策イベントがすべて表示されます。
その他	[データの範囲] で指定されている管理下の製品別に残りの情報漏えい対策イベントがすべて表示されます

[チャネル] 列のリンクまたはグラフのセクションをクリックすると、詳細が表示された画面が開きます。

データ	説明
チャネル	情報漏えい対策イベントが発生したチャネルの種類を示します。
イベント	発生した情報漏えい対策イベントの数を示します。
割合 (%)	イベント総数に対する情報漏えい対策イベントの割合を示します。

ウィジェットに表示される情報を変更するには、 > の順にクリックします。表示されるダイアログボックスで、 をクリックし、ウィジェットがソースとして使用する上位サーバを選択して、[範囲] を指定します。

情報漏えい対策テンプレートの一致ウィジェット

このウィジェットには、ネットワーク上の情報漏えい対策イベントの種類が表示されます。データはテンプレート別にフィルタ処理できます。

[期間] ドロップダウンを使用して、データを表示する期間を選択します。

[テンプレート] 列のリンクやグラフのセクションをクリックすると、詳細が表示された画面が開きます。

データ	説明
テンプレート	情報漏えい対策イベントにより起動されたテンプレートを示します。
イベント	情報漏えい対策イベントの数を示します。
割合 (%)	イベント総数に対する情報漏えい対策イベントの割合を示します。

ウィジェットに表示される情報を変更するには、 > の順にクリックします。表示されるダイアログボックスで、 をクリックし、ウィジェットがソースとして使用する上位サーバを選択して、[範囲] を指定します。

情報漏えい対策イベント発生元の上位ウィジェット

このウィジェットには、ネットワーク上の情報漏えい対策イベント発生元の上位の総数が表示されます。このデータには、ユーザ、メールアドレス、ホスト名、および IP アドレスが含まれ、イベント発生元別にフィルタ処理できます。

[期間] ドロップダウンを使用して、データを表示する期間を選択します。

[表示] ドロップダウンを使用して、表示するデータを選択します。

情報漏えい対策違反ポリシーウィジェット

このウィジェットには情報漏えい対策違反ポリシーが表示されます。このウィジェットは、情報漏えい対策イベントの総数を確認するために使用します。初期設定ではデータがイベント数によってソートされます。データをポリシー名の順にソートするには、[ポリシー] 列のタイトルをクリックします。

[期間] ドロップダウンを使用して、データを表示する期間を選択します。

[イベント] 列のリンクをクリックすると、詳細が表示された画面が開きます。

データ	説明
ポリシー	情報漏えい対策イベントが発生したポリシー名を示します。

データ	説明
イベント	発生した情報漏えい対策イベントの数を示します。

[コンプライアンス] タブ

[コンプライアンス] タブには、管理下の製品またはエンドポイントの、コンポーネントまたは接続のコンプライアンスに関する情報が表示されるウィジェットが含まれます。

次のウィジェットが事前に定義されています。

- 製品アプリケーションのコンプライアンス率
- 製品コンポーネントのステータス
- 製品の接続ステータス
- エージェントの接続ステータス

製品アプリケーションのコンプライアンス率ウィジェット

このウィジェットには、管理下の製品について、製品バージョン、言語、ビルド、およびアップデートステータスが表示されます。これにより、管理者は、管理下の製品について最新のアプリケーションとアップデートが必要なアプリケーションを簡単に特定できます。

表示アイコン () をクリックすると、棒グラフまたは表の形式でデータを表示できます。

[最新バージョン] 列と [古いバージョン] 列の数字をクリックして、画面を開き、詳細情報を確認します。Apex Central によってログクエリが実行され、詳細が表示されます。

データ	説明
製品	Apex Central に登録されている管理下の製品を示します。
バージョン	管理下の製品のバージョンを示します。
言語	管理下の製品の言語のバージョンを示します。

データ	説明
ビルド	管理下の製品のビルド番号を示します。
最新バージョン	最新であるとみなされる製品の数を示します。 ウィジェットを編集して、「最新である」とみなす最小の製品バージョンを指定します。 製品の詳細を確認するには、数字をクリックします。
古いバージョン	「最新でない」製品の数を示します。 製品の詳細を確認するには、数字をクリックします。
最新バージョン率 (%)	「最新である」製品の割合を示します。

初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。

データを表示する方法として棒グラフまたは表を指定します。初期設定では、棒グラフで表示されます。

[編集] をクリックして次のオプションにアクセスします。

- ウィジェットのデータの収集元となる製品を指定するには、[範囲] > [参照] をクリックします。

  データ範囲には、ウィジェットにデータを表示する製品を指定します。この設定は、ウィジェットに表示される情報の有用性に大きく影響する可能性があります。

- [最新バージョンの範囲] ドロップダウンで、製品を「最新である」とみなす、最新ビルドからの製品バージョン数を指定します。

[保存] をクリックして変更を適用し、終了します。

製品コンポーネントのステータスウィジェット

このウィジェットには、ネットワーク上の管理下の製品またはエンドポイントの、コンポーネントバージョンおよびコンプライアンスステータスが表示されます。このウィジェットは、有効期限が終了したコンポーネントを使用している管理下の製品またはエンドポイントを追跡するために使用します。

初期設定では、Apex Central によって管理されるコンポーネントの最新バージョンと、管理下の製品のコンプライアンスステータスが表示されます。[パターンファイル] と [検索エンジン] のセクションには、コンポーネントがコンプライアンス違反率の高い順にリスト表示されます。[比率] 列をクリックすると、ソート順を変更できます。

[パターンファイル] 列または [検索エンジン] 列のいずれかのコンポーネントをクリックすると、各コンポーネントバージョンを使用している管理下の製品またはエンドポイントの数を示す円グラフが表示されます。

[古いバージョン/すべて] の列の数字をクリックすると、期限切れの管理下の製品、すべての管理下の製品、期限切れのエンドポイント、またはすべてのエンドポイントのコンポーネントバージョンに関する情報が表示されます。

設定アイコン (>) をクリックして、次のオプションを設定します。

注意

[概要] タブのウィジェットには設定アイコン ( ) が表示されません。

- ウィジェットの製品範囲を変更するには、[範囲] フィールドの二重矢印ボタン ( ) をクリックし、データの収集元となる製品を選択します。
- ウィジェットに表示されるコンポーネントを編集するには、[パターンファイル] フィールドまたは [検索エンジン] フィールドからコンポーネントを選択または選択解除します。
- 管理下の製品、エンドポイント、またはその両方のコンプライアンス情報を表示するには、[ソース] を指定します。
- 管理下の製品によって報告されたすべてのコンポーネントのデータを表示するか、Apex Central によって管理されるコンポーネントのデータのみを表示するかを指定するには、[表示] を選択します。

データ	説明
パターンファイル	パターンファイル、テンプレート、またはスパムメール判定ルールの名前が表示されます。
検索エンジン	検索エンジンの名前が表示されます。

データ	説明
最新バージョン	次の情報が表示されます。 • Apex Central によってダウンロードされたコンポーネントの最新バージョン • (管理下の製品によって報告された) ダウンロード可能なコンポーネントの最新バージョン
古いバージョン/すべて	次の情報が表示されます。 • 期限切れ: 期限切れのコンポーネントがある管理下の製品またはエンドポイントの数 [古いバージョン/すべて] 列の最初の数字をクリックすると、期限切れの管理下の製品またはエンドポイントのコンポーネントバージョンに関する情報が表示されます。 • すべて: コンポーネントを使用する管理下の製品またはエンドポイントの総数 [古いバージョン/すべて] 列の 2 番目の数字をクリックすると、すべての管理下の製品またはエンドポイントのコンポーネントバージョンに関する情報が表示されます。 注意 この列は、[ソース] に対して [両方] が選択されている場合に表示されます。
比率	期限切れのコンポーネントがある管理下の製品またはエンドポイントの割合が表示されます。 注意 この列は、[ソース] に対して [両方] が選択されている場合に表示されます。

製品の接続ステータスウィジェット

このウィジェットには、Apex Central サーバに登録されているすべての管理下の製品の接続ステータスが表示されます。

初期設定では、ログオンしているユーザアカウントがアクセス可能な管理下の各製品の接続ステータスと管理下のサーバ名のリストが表示されます。

- 製品の範囲を変更するには、設定アイコン (>) をクリックして、新しい [範囲] を選択します。
- 各接続ステータスの管理下の製品の総数について概要を表示するには、設定アイコン (>) をクリックして、[表示] を [概要] に切り替えます。

[詳細の表示] をクリックして、[ログクエリ] 画面で詳細情報を確認します。

ステータス	説明
有効	製品サービスが実行中であり、Apex Central サーバとの通信が正常に確立されていることを示します。
無効	製品サービスが実行されていないか、Apex Central サーバとの通信が確立できないことを示します。
異常	製品サービスは、ユーザ定義のエージェントの通信タイムアウト間隔で Apex Central サーバと通信していないことを示します。

エージェントの接続ステータスウィジェット

このウィジェットには、エージェントの接続ステータスと上位サーバが表示されます。次の管理下の製品のエージェントが表示されます。

- Endpoint Sensor
- Endpoint Encryption
- Trend Micro Mobile Security
- Trend Micro Security (for Mac)
- Apex One
- 仮想パッチ
- ウイルスバスター ビジネスセキュリティサービス

初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。

[オンライン] 列、[オフライン] 列、または [合計] 列の値をクリックすると、詳細情報が表示されます。Apex Central によってログクエリが実行され、情報が表示されます。

データ	説明
サーバ	上位サーバを示します。
オンライン	上位サーバに接続されているエージェントを示します。
オフライン	上位サーバとの接続が切断されているエージェントを示します。
合計	エンドポイントの総数を示します。

ウィジェットに表示される情報を変更するには、 > の順にクリックします。表示されるダイアログボックスで、 をクリックし、ウィジェットがソースとして使用する上位サーバを選択して、[範囲] を指定します。

[脅威の統計] タブ

[脅威の統計] タブには、検出されたセキュリティの脅威の集計が表示されるウィジェットが含まれます。

次のウィジェットが事前定義されています。

- Apex Central 上位の脅威
- Apex Central 脅威の統計
- 脅威の検出結果
- ポリシー違反の検出
- C&C コールバックイベント

Apex Central 上位の脅威ウィジェット

このウィジェットには、指定された時間範囲内に検出された不正ファイルと不正 URL に関する情報が表示されます。

表示アイコン ( ) をクリックすると、棒グラフまたは表の形式でデータを表示できます。

グラフまたは表の上部にあるドロップダウンリストを使用して、表示する脅威データの種類を選択します。

- 不正ファイル: ネットワーク上で検出された不正ファイルを検出数で順位付けします。
- 不正 URL: ネットワーク上で検出された不正 URL を検出数で順位付けします。

バー、脅威名、または検出番号をクリックすると、[ログクエリ] 画面が開き、感染したエンドポイント、脅威の詳細、および検出数に関する情報が表示されます。

初期設定では、ログオンしているユーザアカウントがアクセス可能なすべての管理下の製品のトップ 10 の脅威が表示されます。

- 表示されるウィジェットのタイトル、製品範囲、または脅威の数を編集するには、設定アイコン (>) をクリックします。

Apex Central 脅威の統計ウィジェット

このウィジェットには、ネットワークで検出されたセキュリティの脅威の総数が表示されます。セキュリティの脅威の種類またはセキュリティの脅威が検出されたネットワーク上の場所によってデータをフィルタ処理できます。

- 製品カテゴリ

データ	説明
ファイルサーバ	[データの範囲] で指定されている管理下の製品によって検出されたファイルサーバ上のセキュリティの脅威を示します。
ネットワーク	[データの範囲] で指定されている管理下の製品によって検出されたネットワーク上のセキュリティの脅威を示します。
不明	認識できないセキュリティの脅威を示します。
メール	[データの範囲] で指定されている管理下の製品によって検出されたメールサーバ上のセキュリティの脅威を示します。
デスクトップ	[データの範囲] で指定されている管理下の製品によって検出されたデスクトップ上のセキュリティの脅威を示します。

データ	説明
ゲートウェイ	[データの範囲] で指定されている管理下の製品によって検出されたゲートウェイ上のセキュリティの脅威を示します。
Apex Central サーバ	[データの範囲] で指定されている管理下の製品によって検出された Apex Central サーバ上のセキュリティの脅威を示します。

- 違反の種類

データ	説明
挙動監視	[データの範囲] で指定されている管理下の製品によって検出された挙動監視違反を示します。
コンテンツ違反	[データの範囲] で指定されている管理下の製品によって検出されたコンテンツセキュリティ違反 (スパムメール、ブロックされたキーワードやパターン)を示します。
デバイスコントロール	[データの範囲] で指定されている管理下の製品によって検出されたデバイスコントロール違反を示します。
ファイアウォール違反	[データの範囲] で指定されている管理下の製品によって検出されたファイアウォール違反を示します。
ネットワークコンテンツ検査	[データの範囲] で指定されている管理下の製品によって検出されたネットワークコンテンツ検査違反を示します。
機械学習型検索	[データの範囲] で指定されている管理下の製品別の機械学習型検索の検出結果を示します。
スパイウェア/グレーウェア	[データの範囲] で指定されている管理下の製品によって検出されたスパイウェア/グレーウェアを示します。
不審ファイル	[データの範囲] で指定されている管理下の製品別の不審ファイル検出結果を示します。
ウイルス/不正プログラム	[データの範囲] で指定されている管理下の製品によって検出されたウイルス/不正プログラムを示します。
Web セキュリティ	[データの範囲] で指定されている管理下の製品によって検出された Web セキュリティ違反 (不正な URL、ブロックされた URL)を示します。

注意

ウィジェットに一度に表示できる情報の種類は 1 つのみです。

[検出数] 列のリンクをクリックすると、詳細情報の表示された画面が開きます。Apex Central によってログクエリが実行され、詳細が表示されます。

データ	説明
種類	セキュリティの脅威の種類、またはその脅威を検出した管理下の製品を示します。
検出数	検出されたセキュリティの脅威の数を示します。
割合 (%)	検出されたセキュリティの脅威の総数の割合を示します。

ウィジェットに表示するデータの日付範囲を指定します。

- 今日
- 過去 7 日間
- 過去 14 日間
- 過去 30 日間

ウィジェットにデータを表示する方法を指定します。

- 円グラフ
- 棒グラフ
- 表
- 折れ線グラフ

初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。

ウィジェットに表示される情報を変更するには、 > の順にクリックします。表示されるダイアログボックスで、 をクリックし、ウィジェットがソースとして使用する上位サーバを選択して、[範囲] を指定します。

脅威の検出結果ウィジェット

このウィジェットには、ウィジェット脅威の検出数および検出総数に対する脅威の割合が表示されます。ウィジェットに一度に表示できる情報の種類は 1 つのみです。[検出数] 列のリンクをクリックすると、詳細情報の表示された画面が開きます。Apex Central によってログクエリが実行され、詳細が表示されます。

データ	説明
結果	管理下の製品によって実行された処理、または処理の結果を示します。 注意 脅威の種類が [Web セキュリティ] の場合、この列は表示されません。
ポリシー/ルール	脅威の種類が [Web セキュリティ] の場合に適用されるポリシー/ルールの種類を示します。 注意 脅威の種類がその他の場合、この列は表示されません。
検出数	検出されたセキュリティの脅威の数を示します。
割合 (%)	すべての検出のうち、セキュリティの脅威と判明した検出の割合を示します。

このウィジェットには、次の脅威の種類についての脅威の検出が表示されます。

表 1-4. 脅威の種類

脅威の種類	説明
ウイルス/不正プログラム	[データの範囲] で指定されている管理下の製品別にすべてのファイルに対して実行された処理が表示されます。例: 駆除、アクセス拒否など

脅威の種類	説明
スパイウェア/グレーウェア	[データの範囲] で指定されている管理下の製品別にすべてのファイルに対して実行された処理が表示されます。例: 成功、処理が必要など
コンテンツセキュリティ	[データの範囲] で指定されている管理下の製品別にすべてのメールメッセージに対して実行された処理が表示されます。例: 削除、添付ファイル削除など
Web セキュリティ	[データの範囲] で指定されている管理下の製品別にポリシーを使用してブロックされたすべての Web セキュリティ違反が表示されます。例: ファイルブロック、ファイル名など
ネットワークウイルス	[データの範囲] で指定されている管理下の製品別にすべてのネットワークウイルスに対して実行された処理が表示されます。

表示されるウィジェットのタイトル、製品範囲、または脅威の種類を編集するには、設定アイコン (>) をクリックします。

ポリシー違反の検出ウィジェット

このウィジェットには、Network VirusWall Enforcer デバイスで検出されたポリシー違反が表示されます。[検出数] 列のリンクをクリックすると、詳細情報の表示された画面が開きます。Apex Central によってログクエリが実行され、詳細が表示されます。

データ	説明
種類	セキュリティ上の脅威の種類として [サービス違反] のリストを示します。
更新	最終更新日を示します。
検出数	Network VirusWall Enforcer デバイスで検出されたサービス違反の数を示します。

設定アイコン (>) をクリックして、ウィジェットのタイトルまたは製品の範囲を編集します。

注意

このウィジェットには、Network VirusWall Enforcer で検出されたポリシー違反のみが表示されます。

[保存] をクリックして変更を適用し、終了します。

C&C コールバックイベントウィジェット

このウィジェットには、感染ホストまたはコールバックアドレスに基づく、C&C コールバック回数が表示されます。ウィジェットに一度に表示できる情報の種類は 1 つのみです。表のいずれかのセルの数字をクリックすると、[C&C コールバックイベント] 画面が開き、次のコールバック概要データが示されます。

データ	説明
感染ホスト	影響を受けたホストまたはメールアドレスを示します。
コールバックアドレス	感染ホストがコールバック試行した URL、IP アドレス、またはメールアドレスを示します。
地域/国	C&C サーバが設置されている地域および国を示します。
コールバック試行	コールバックアドレスと感染ホスト間でのコンタクト数を示します。
最新のコールバックアドレス/感染ホスト	最後のコールバック試行がログに記録された URL、IP アドレス、またはメールアドレスを示します。
コールバックアドレス/感染ホスト (列に数字を表示)	コールバック試行に関連付けられた感染ホストまたはコールバックアドレスの数を示します。
検出元	イベントをログに記録した管理下の製品の名前を示します。

設定アイコン (>) をクリックして、次の内容を編集します。

- タイトル: C&C コールバックイベントウィジェットのタイトルを変更します。

- 範囲: >> をクリックして、ウィジェットがソースとして使用する上位サーバを選択します。
- C&C リストのソース: C&C リストのソースとして、[グローバルインテリジェンス]、[仮想アナライザ]、または [ユーザ定義] を選択します。
- 表示する項目: ウィジェットに表示する項目の数を選択します。

[保存] をクリックして変更を適用し、終了します。

第 2 章

ポリシー管理

このセクションでは、管理下の製品とエンドポイントでポリシー管理を実行する方法について説明します。

重要

管理下の各製品にはそれぞれ異なるポリシー設定があり、管理者はこれを指定してポリシーの対象に配信できます。サポートされている管理下の製品とそれぞれのポリシー設定の一覧については、各ポリシー設定画面のオンラインヘルプをご覧ください。

次のトピックがあります。

ポリシー管理

ポリシーを管理することで、管理者は、単一の管理コンソールから管理下の製品およびエンドポイントに製品設定を適用できます。管理者は、対象を選択し、製品設定のリストを設定してポリシーを作成します。

新しい管理下の製品またはエンドポイントでポリシー管理を実行するには、管理下の製品を [新規エンティティ] フォルダから製品ディレクトリ構造の別のフォルダに移動します。

新しいポリシーの作成

重要

管理下の各製品にはそれぞれ異なるポリシー設定があり、管理者はこれを指定してポリシーの対象に配信できます。サポートされている管理下の製品とそれぞれのポリシー設定の一覧については、各ポリシー設定画面のオンラインヘルプをご覧ください。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] リストから製品設定の種類を選択します。

   画面の表示が更新され、選択した管理下の製品に対して作成されているポリシーが表示されます。

   特定の管理下の製品に関するポリシー設定の詳細については、各ポリシー設定画面のオンラインヘルプをご覧ください。

3. [作成] をクリックします。

   [ポリシーの作成] 画面が表示されます。

4. ポリシー名を入力します。

5. 対象を指定します。

   Apex Central には対象の選択方法がいくつかあり、選択方法によってポリシーの動作が異なります。

   注意

   管理下の製品またはエンドポイントを対象に含めるには、管理下の製品またはエンドポイントの製品のバージョンが Apex Central のポリシー管理をサポートしていることを確認します。詳細は管理下の製品の管理者ガイドをご覧ください。

   ポリシーリストでは、次の順序でポリシーの対象が並べられます。

   - 対象の指定: 特定のエンドポイントまたは管理下の製品を選択するには、このオプションを使用します。

     詳細については、53 ページの「ポリシーの対象を指定する」を参照してください。

   - 条件に応じてフィルタ: フィルタ条件に基づいてエンドポイントを自動的に割り当てるには、このオプションを使用します。

     詳細については、49 ページの「条件に応じてフィルタ」を参照してください。

   - [ラベルの選択]: ラベルに基づいてエンドポイントを割り当てるには、このオプションを使用します。

     詳細については、54 ページの「ラベル」 。

   - なし (ドラフトのみ): 対象は選択せずにドラフトとしてポリシーを保存するには、このオプションを使用します。

   ポリシーリストの詳細については、66 ページの「ポリシーリストについて」を参照してください。

6. 管理下の製品の機能をクリックして展開し、機能の設定を行います。この手順を繰り返して、すべての機能を設定します。

   - 各機能にはヘルプトピックへのリンクがあり、その機能の説明と使用方法を確認できます。

- 特定の製品設定では、Apex Central は、管理下の製品から特定の設定オプションを取得する必要があります。管理者が 1 つのポリシーに対して複数の対象を選択した場合、Apex Central は、最初に選択した対象のみから設定オプションを取得できます。正常にポリシー配信を行うには、製品設定が対象間で同期されていることを確認します。
- Apex One セキュリティエージェントのポリシーを作成して以降の子ポリシーの親として使用する場合は、子ポリシーで継承、カスタマイズ、または拡張可能な設定を使用します。
  - セキュリティエージェントの継承、カスタマイズ、拡張可能な設定の一覧については、54 ページの「親ポリシー設定の使用」を参照してください。
  - 子ポリシーの作成の詳細については、59 ページの「ポリシー設定の継承」を参照してください。

7. [配信] または [保存] をクリックします。

   [配信] をクリックすると配信が開始されます。配信されたポリシーは [ポリシー管理] 画面のリストに表示されます。通常、ポリシーが対象に配信されるまでに数分かかります。

   ポリシーリスト内のステータス情報をアップデートするには、[ポリシー管理] 画面の [表示の更新] をクリックします。しばらく待っても配信ステータスが保留中のままの場合は、対象に問題がある可能性があります。Apex Central と対象の間に接続が確立されているかどうかを確認してください。また、対象が正常に機能しているかどうかも確認してください。

   Apex Central から対象にポリシーを配信すると、このポリシーに定義されている設定によって、対象の既存の設定が上書きされます。Apex Central では、24 時間ごとに対象にポリシー設定が適用されます。ローカルの管理者が管理下の製品コンソールから設定を変更することは可能ですが、その変更は Apex Central がポリシー設定を適用するたびに上書きされます。

   - Apex Central では、「対象の指定」を行った場合、24 時間ごとに対象にポリシー設定が適用されます。ローカルの管理者がその適用期間に管理下の製品コンソールを使用して変更を行った場合、対象の製品設定とポリシー設定が一致しない場合があります。

- InterScan Messaging Security Virtual Appliance サーバに配信されたポリシー設定は対象サーバの既存の設定よりも優先され、上書きされることはありません。InterScan Messaging Security Virtual Appliance サーバは、これらのポリシー設定をリストの一番上に保存します。
- Apex Central のポリシーで割り当てられた Apex One セキュリティエージェントが別の Apex One ドメインに移動された場合、そのエージェントの設定は、その Apex One ドメインで定義された設定に一時的に変更されます。Apex Central で再度ポリシーを適用すると、セキュリティエージェント設定はポリシー設定に準拠します。

条件に応じてフィルタ

フィルタ条件に基づいてエンドポイントを自動的に割り当てるには、このオプションを使用します。

このオプションの特徴は次のとおりです。

- 次の管理下の製品でのみ使用できます。
  - Apex One (Mac)
  - Apex One 情報漏えい対策オプション
  - Apex One セキュリティエージェント
  - Mobile Security for Enterprise
  - Trend Micro Endpoint Application Control
- フィルタを使用して、現在の対象およびそれ以降の対象をポリシーに自動的に割り当てます。
- 標準の設定を一連の対象にまとめて配信する場合に便利です。

管理者は、ポリシーリストでフィルタ済みポリシーの優先順位を変更できます。管理者がポリシーリストを並べ替えると、Apex Central は、対象条件および各ポリシー作成者のユーザの役割に基づいて、別のフィルタ済みポリシーに対象を再割り当てします。

Apex Central では、新規のフィルタ済みポリシーには、ポリシーが割り当てられていないエンドポイントのみを割り当てることができます。フィルタ済

みポリシーにすでに割り当てられているエンドポイントを再割り当てするには、条件が一致する別のフィルタ済みポリシーを優先順位のリストの上位に移動します。

Apex Central がフィルタ済みポリシーに対象を割り当てるしくみの詳細については、51 ページの「フィルタ済みポリシーへのエンドポイントの割り当て」を参照してください。

手順

1. [ポリシーの作成] 画面で、[対象] セクションに移動し、[条件に応じてフィルタ] を選択して [フィルタの設定] をクリックします。

   [条件に応じてフィルタ] 画面が表示されます。

2. 次のオプションを選択して、条件を定義します。

条件	説明
キーワードに一致	ホスト名または Apex Central 表示名に基づいてキーワードを定義します。 注意 単一のキーワードで検索する場合は、部分一致検索が可能です。キーワードをコンマで区切ると複数のキーワードで検索できますが、キーワードごとに完全一致した結果のみが表示されます。
IP アドレス	IP アドレスの範囲を定義し、[追加] をクリックします。 注意 • ポリシー管理では、IPv4 アドレスのみがサポートされます。 • 新しい管理下の製品またはエンドポイントが Apex Central に登録された場合、その管理下の製品またはエンドポイントを IP アドレスで検索できるようになるまで約 1 時間かかります。

条件	説明
OS	ドロップダウンリストから 1 つ以上のオペレーションシステムを選択します。
ディレクトリ	次のいずれかのディレクトリを選択して、条件を定義します。 • 製品ディレクトリ: 製品ディレクトリ構造からフォルダを選択します。 • Active Directory: 統合された Active Directory 構造から組織単位を選択します。 • Apex One ドメイン階層: Apex One ドメイン階層のキーワードを 1 つ以上入力します。

3. [保存] をクリックします。

   [ポリシーの作成] 画面が再ロードされます。

フィルタ済みポリシーへのエンドポイントの割り当て

新しいエンドポイントが Apex Central に登録されると、そのエンドポイントは、リスト内のフィルタ済みポリシーに降順で照合されていきます。Apex Central では、次の条件が両方とも満たされた場合に、フィルタ済みポリシーに新しいエンドポイントが割り当てられます。

- 新しいエンドポイントがポリシー内の対象条件に一致する。
- ポリシー作成者に、新しいエンドポイントを管理する権限がある。

同じ処理が、いずれかのポリシーにすでに割り当てられているエンドポイントに適用されますが、ポリシー作成者によって後でそのポリシーは削除されます。

注意

Apex Central に登録されたばかりのエンドポイントおよび削除されたポリシーからリリースされたばかりのエンドポイントの場合、エンドポイントの割り当てが行われない 3 分の更新猶予期間があります。この期間中は、これらのエンドポイントに対してポリシーが一時的に適用されなくなります。

エンドポイントが、いずれのフィルタ済みポリシーの対象条件も満たさない場合、そのエンドポイントはどのポリシーにも関連付けられません。Apex Central では、次の処理を実行するときにこれらのエンドポイントを再度割り当てます。

- フィルタ済みポリシーの新規作成
- フィルタ済みポリシーの編集
- フィルタ済みポリシーの並べ替え
- 日次エンドポイント割り当てスケジュールの使用

  「条件に応じてフィルタ」を行った場合、毎日午後 3:15 にポリシー設定が再適用されます。この処理は、毎日午後 3:15 に 1 回実行されます。OS や IP アドレスなどのプロパティに変更が加えられたエンドポイントには、適切なポリシーに再割り当てされるように、日次スケジュールが必要です。

注意

- エンドポイントが日次エンドポイント割り当てスケジュールの実行中にオフラインになると、これらのエンドポイントのポリシーステータスはオンラインになるまで保留のままになります。
- エンドポイントの Apex One ドメインを変更すると、10 分後に Apex Central からアップデートしたポリシーが配信されます。

前述の処理が実行される場合、Apex Central では、次の条件に基づいてエンドポイントが割り当てられます。

表 2-1. フィルタ済みポリシーへのエンドポイントの割り当て

	新しいエンドポイントまたはポリシーが削除されたエンドポイント	エンドポイント (ポリシーなし)	エンドポイント (ポリシーあり)
新しいポリシーの作成		●	
ポリシーの編集	●	●	●

フィルタ済みポリシーの並べ替え	●	●	●
日次エンドポイント割り当てスケジュールの使用	●	●	●

ポリシーの対象を指定する

特定のエンドポイントまたは管理下の製品を選択するには、このオプションを使用します。

このオプションの特徴は次のとおりです。

- 検索機能または参照機能を使用して特定の対象を指定し、それらの対象をポリシーに手動で割り当てます。
- 管理者が特定の設定を特定の対象のみに配信する場合に便利です。
- ポリシーリストの最上位に留まり、いずれのフィルタ済みポリシーより優先されます。

手順

1. [ポリシーの作成] 画面で、[対象] セクションに移動し、[対象の指定] を選択して [選択] をクリックします。

   [対象の指定] 画面が表示されます。

2. [検索] または [参照] を使用して、対象を見つけます。
   - 検索:次の検索条件を使用して、エンドポイントまたは管理下の製品を検索します。検索結果には、選択した条件すべてに一致するエンドポイントまたは管理下の製品が表示されます。
     - キーワードに一致: ホスト名または Apex Central の表示名に基づいてキーワードを定義します。
     - IP アドレス: IP アドレスの範囲を定義し、[追加] をクリックします。

注意

- ポリシー管理では、IPv4 アドレスのみがサポートされます。
- 新しい管理下の製品またはエンドポイントが Apex Central に登録された場合、その管理下の製品またはエンドポイントを IP アドレスで検索できるようになるまで約 1 時間かかります。

- OS: ドロップダウンリストから 1 つ以上の OS を選択します。
- 参照: 製品ディレクトリまたは Active Directory を参照してエンドポイントまたは管理下の製品を選択し、ポリシーに割り当てます。

3. エンドポイントまたは管理下の製品を選択して、[選択した対象を追加] をクリックします。
4. [処理リストの表示] および [結果の表示] の数値が変わるのを待ちます。
5. [OK] をクリックします。

   [ポリシーの作成] 画面が再ロードされます。

ラベル

ラベルは既存のタグ付けシステムのバリエーションで、フィルタ機能も提供します。タグ/フィルタを使用する場合と同じように、ラベルを作成してエンドポイントに手動で割り当てることができます。自動ラベルルールを作成して、指定した条件に一致するエンドポイントにラベルを自動的に割り当てることもできます。ラベルまたは自動ラベルルールを作成したら、ポリシー、ログクエリ、またはレポートにラベルを使用できます。

親ポリシー設定の使用

Apex Central の管理者は、Apex One セキュリティエージェントの親ポリシーを作成する際に、ポリシーの特定の設定を継承、カスタマイズ、または拡張対象として設定できます。

注意

これらのオプションは、他の管理下の製品では利用できません。

- 親ポリシーから継承
  - 子ポリシーの管理者は設定を変更できません。Apex One 管理者は、Apex One サーバのコンソールから手動で設定を変更できます。ただし、Apex Central から Apex One サーバにポリシーが配信されると、その設定で上書きされます。

    たとえば、Apex Central 管理者は、手動検索から PDF ファイルを除外する親ポリシーを作成できます。
  - 親ポリシーの設定に対する変更はすべて子ポリシーに適用されます。
  - 親ポリシーの権限を [親ポリシーから継承] から [カスタマイズ可能] または [親ポリシーから拡張] に変更すると、子ポリシーの管理者が現在の設定をカスタマイズまたは拡張できるようになります。また、親ポリシーの設定を変更しても子ポリシーに適用されなくなります。
- カスタマイズ可能
  - 親ポリシーの設定を子ポリシーでカスタマイズできます。

    たとえば、親ポリシーで予約検索を毎週実行するように設定されている場合、カスタマイズ可能であれば、子ポリシーの管理者はスケジュールを毎日に変更できます。
  - 親ポリシーの設定に対する変更は子ポリシーに適用されません。
  - 親ポリシーの権限を [カスタマイズ可能] から [親ポリシーから継承] に変更すると、子ポリシーの設定が親ポリシーの現在の設定で上書きされます。また、親ポリシーの設定に対する変更がすべて子ポリシーに適用されるようになります。
- 親ポリシーから拡張
  - 親ポリシーで設定された項目に子ポリシーの管理者が項目を追加できます。

    たとえば、手動検索で 20 個のファイル名を除外するように親ポリシーで設定されている場合、安全で信頼できると判断した 10 個のファイルを子ポリシーに追加できます。

- 親ポリシーで追加または削除された項目は、子ポリシーでも追加または削除されます。必要に応じて、削除された項目を子に追加し直すことができます。
- 親ポリシーの権限を [親ポリシーから拡張] から [親ポリシーから継承] に変更すると、親ポリシーと一致しない子ポリシーの項目は削除されます。また、親ポリシーの項目に対する変更がすべて子ポリシーに適用されるようになります。

次の表に、継承、カスタマイズ、または拡張が可能な親ポリシーの設定を示します。

設定およびパス	利用可能なオプション		
	親ポリシーから継承	カスタマイズ可能	親ポリシーから拡張
検索スケジュール [予約検索設定]→[対象] タブ→[予約] セクション	●	●	
検索するファイル拡張子 [手動検索の設定]/[リアルタイム検索の設定]/[ScanNow の設定]/[予約検索設定]→[対象] タブ→[検索対象ファイル] セクション→[対象の拡張子の選択] オプション	●		●

設定およびパス	利用可能なオプション		
	親ポリシーから継承	カスタマイズ可能	親ポリシーから拡張
検索除外リスト (検索から除外するディレクトリ、ファイル、およびファイル拡張子) [手動検索の設定]/[リアルタイム検索の設定]/[ScanNow の設定]/[予約検索設定]→[検索除外] タブ	●		● 注意 検索除外リストで [親ポリシーから拡張] を選択すると、リストが展開されて [下位ポリシーの制限] セクションが表示されます。親ポリシーの作成者は、このセクションで、子ポリシーで検索からの除外を許可しない項目を指定できます。
承認済みプログラム [挙動監視] → [除外] タブ	●		●
ブロックするプログラム [挙動監視] → [除外] タブ	●		●
除外 機械学習型検索	●		●
信頼済みプログラムリスト 信頼済みプログラムリスト	●		●

ポリシー設定のコピー

管理者は、既存ポリシーの設定をコピーし、新しいポリシーを同じ設定で作成して、その設定を別のエンドポイントまたは管理下の製品に配信できます。

注意

Apex One セキュリティエージェントの子ポリシーの設定はコピーできません。Apex One セキュリティエージェントのポリシーが子と親のどちらであるかは、[親ポリシー] 列で確認できます。ポリシーが子の場合はクリック可能な値が表示され、それ以外の場合は「なし」と表示されます。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] リストから製品設定の種類を選択します。

   画面の表示が更新され、選択した管理下の製品に対して作成されているポリシーが表示されます。

3. リストからポリシーを選択します。

4. [設定のコピー] をクリックします。

   [ポリシーのコピーと作成] 画面が表示されます。

5. [ポリシー名] にポリシーの名前を入力します。

6. [対象] をポリシーに割り当てます。

7. (オプション) 必要に応じて設定を変更します。

8. [配信] をクリックします。

注意

- [配信] をクリックした後で、Apex Central がポリシーを対象に配信するまで 2 分間待ってください。ポリシーリスト内のステータス情報をアップデートするには、[ポリシー管理] 画面の [表示の更新] をクリックします。
- Apex Central では、24 時間ごとに対象にポリシー設定が適用されます。

ポリシー設定の継承

既存の親ポリシーの設定を継承して新しい子ポリシーを作成します。子ポリシーは、コピーしたりその設定を継承したりすることはできません。

このタスクでは、Apex One セキュリティエージェントの親ポリシーが必要になります。Apex One セキュリティエージェントの親ポリシーでは、[親ポリシー] 列に「なし」と表示されています。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] リストから [Apex One セキュリティエージェント] を選択します。

   画面の表示が更新され、選択した管理下の製品に対して作成されているポリシーが表示されます。

3. ローカルで管理される設定が含まれていない親ポリシーを選択します。
4. [設定の継承] をクリックします。

   [ポリシーの継承と作成] 画面が表示されます。

5. [ポリシー名] にポリシーの名前を入力します。
6. [対象] をポリシーに割り当てます。
7. (オプション) カスタマイズまたは拡張が可能な設定を確認し、必要に応じて設定を変更します。確認対象となる設定の一覧については、54 ページの「親ポリシー設定の使用」を参照してください。

注意

親ポリシーで [親ポリシーから継承] オプションが選択されている場合、設定をカスタマイズまたは拡張することはできません。

例:

- 予約検索の設定がカスタマイズ可能な場合、スケジュールを [毎週] から [毎日] に変更できます。
- リアルタイム検索の検索除外リストが拡張可能な場合、安全で信頼できると判断したファイルの名前を追加できます。子ポリシーを作成すると、子ポリシーの検索除外リストにそれらのファイル名が追加されます。

8. [配信] をクリックします。

注意

- [配信] をクリックした後で、Apex Central がポリシーを対象に配信するまで 2 分間待ってください。ポリシーリスト内のステータス情報をアップデートするには、[ポリシー管理] 画面の [表示の更新] をクリックします。
- Apex Central では、24 時間ごとに対象にポリシー設定が適用されます。

ポリシーの変更

管理者は、必要に応じてポリシーの対象や設定を変更できます。root アカウントの所有者はリストのすべてのポリシーを変更でき、それ以外のアカウントの所有者は自分で作成したポリシーだけを変更できます。ポリシーを変更すると、Apex Central から対象にポリシーが配信されます。

重要

管理下の各製品にはそれぞれ異なるポリシー設定があり、管理者はこれを指定してポリシーの対象に配信できます。サポートされている管理下の製品とそれぞれのポリシー設定の一覧については、各ポリシー設定画面のオンラインヘルプをご覧ください。

Apex One セキュリティエージェントの親ポリシーの場合は、特定の機能の対象や設定を変更すると、それらの変更がすべての子ポリシーに適用され、対応する対象に配信されます。親ポリシーの一部の設定では、子ポリシーで可能な変更内容を制御する権限がサポートされます。これらの親ポリシーの権限に対する変更も、子ポリシーに適用されて対象に配信されます。権限をサポートする設定の一覧については、54 ページの「親ポリシー設定の使用」を参照してください。

例:

- 検索スケジュールの権限を [親ポリシーから継承] から [カスタマイズ可能] に変更すると、管理者が子ポリシーの既存のスケジュールをカスタマイズできるようになります。
- 手動検索のファイル拡張子の権限を [親ポリシーから拡張] から [親ポリシーから継承] に変更すると、子ポリシーに管理者が追加したファイル拡張子はすべて削除されます。また、管理者がファイル拡張子を追加することはできなくなります。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] リストから製品設定の種類を選択します。

   画面の表示が更新され、選択した管理下の製品に対して作成されているポリシーが表示されます。

3. [ポリシー] 列のポリシー名をクリックします。

   [ポリシーの編集] 画面が表示されます。

4. ポリシーを変更します。

注意

フィルタ済みポリシーのフィルタ条件を変更すると、対象の割り当てに影響が及ぶ場合があります。Apex Central によって、他のフィルタ済みポリシーに対象が再割り当てされたり、現在のポリシーにさらに対象が追加されたりすることがあります。

5. [配信] をクリックします。

   Apex Central がポリシーを対象に配信するには、時間がかかることがあります。ポリシーリスト内のステータス情報をアップデートするには、[ポリシー管理] 画面で [表示の更新] をクリックします。しばらく待っても配信ステータスが保留中のままの場合は、対象に問題がある可能性があります。Apex Central と対象の間に接続が確立されているかどうかを確認してください。また、対象が正常に機能しているかどうかも確認してください。

   Apex Central では、24 時間ごとに対象にポリシー設定が適用されます。

ポリシーのインポートとエクスポート

ポリシーをバックアップ用にエクスポートしたり、同じバージョンの他の Apex Central サーバにインポートしたりできます。

注意

- エクスポートされるのはポリシー設定で、ポリシーの対象ではありません。
- 親ポリシーはエクスポートまたはインポート後も親のままです。
- 子ポリシーはエクスポートすると親になります。そのため、そのポリシーをインポートすると親になります。
- 既存の子ポリシーと同じ名前のポリシーはインポートできません。既存のポリシーが子でない場合は、インポートしたポリシーで上書きされます。
- 詳細については、次のトピックを参照してください。
  - 46 ページの「新しいポリシーの作成」
  - 59 ページの「ポリシー設定の継承」

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] リストから製品設定の種類を選択します。

   画面の表示が更新され、選択した管理下の製品に対して作成されているポリシーが表示されます。

3. エクスポートするには、1 つ以上のポリシーを選択して [設定のエクスポート] をクリックし、生成されたポリシーファイルを保存します。
   - 1 つのポリシーをエクスポートした場合、生成されるファイルの拡張子は`*.cmpolicy` になります。
   - 複数のポリシーをエクスポートした場合は、それぞれの`.cmpolicy` ファイルを含む圧縮 (`*.zip`) ファイルが生成されます。
4. インポートするには、[設定のインポート] をクリックし、ポリシーファイルを指定してロードします。

- *.zip ファイル全体をインポートすることも、個々の*.cmpolicy ファイルを 1 つずつインポートすることもできます。
- ポリシーがポリシーリストにすでに存在する場合、既存のポリシーを上書きするかどうかを確認するプロンプトメッセージが表示されます。

  続行する場合は、[OK] をクリックします。

画面の表示が更新され、インポートされたポリシーがリストの一番上に表示されます。

ポリシーリストの並べ替えの詳細については、69 ページの「ポリシーリストの並べ替え」を参照してください。

ポリシーの削除

管理者は、リストからポリシーを削除できます。ポリシーが削除されると、そのポリシーに関連付けられていた対象が別のポリシーのフィルタ条件に一致した場合に、それらの対象が Apex Central によって再割り当てされます。フィルタ条件に一致しない対象は、ポリシーが割り当てられていないエンドポイントとなり、これらのエンドポイントでは、管理下の製品の管理者が設定を変更しない限り、削除されたポリシーで定義されていた設定が保持されます。

ポリシーを削除できるのは、そのポリシーの作成者のみです。ただし、root アカウントはリスト内のすべてのポリシーを削除できます。

Apex One セキュリティエージェントのポリシーで、既存の子ポリシーが設定を継承している親ポリシーは削除できません。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] リストから製品設定の種類を選択します。

   画面の表示が更新され、選択した管理下の製品に対して作成されているポリシーが表示されます。

3. 削除するポリシーを選択します。
4. [削除] をクリックします。

   削除を確認する画面が表示されます。
5. [OK] をクリックします。

ポリシーの所有者を変更する

ポリシーの初期設定の所有者は、ポリシーを作成したユーザアカウントです。[ポリシー管理] 画面を使用して、ポリシーの所有者を任意の Apex Central ユーザアカウントに変更できます。また、ポリシーの所有者を Active Directory グループに変更することもできます。このグループはグループ内のすべての Active Directory ユーザをポリシーの所有者として指定します。

重要

ポリシーの所有者を、指定された適用先へのアクセス権がないユーザアカウントに変更する場合、新しい所有者はポリシーの設定を変更できますが、ポリシーデータは表示できません。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。
2. 所有者を変更する 1 つ以上のポリシーを選択します。
3. [所有者の変更] をクリックします。

   [ポリシーの所有者の変更] 画面が表示されます。
4. ドロップダウンリストからユーザアカウントを選択します。
5. [保存] をクリックして、所有者を変更します。

   「管理者」の役割が割り当てられているすべてのユーザアカウントに対して、Apex Central からメール通知が送信されます。

ポリシーリストについて

ポリシーリストには、すべてのユーザによって作成されたポリシーの情報とステータスが表示されます。新しいエンドポイントが Apex Central に登録されると、そのエンドポイントは、リスト内のフィルタ済みポリシーに降順で照合されていきます。Apex Central では、次の条件が両方とも満たされた場合に、フィルタ済みポリシーに新しいエンドポイントが割り当てられます。

- 新しいエンドポイントがポリシーの対象条件に一致する。
- ポリシー作成者に、新しいエンドポイントを管理する権限がある。

次の表は、[ポリシー管理] 画面に表示されるポリシーリストの列について示しています。列をクリックすると、そのデータが並べ替えられます。

表 2-2. ポリシーリスト

列	説明
優先度	ポリシーの優先順位が表示されます。 • Apex Central では、優先順位の最上位から最下位へという順序でポリシーがリストされます。 • 管理者がフィルタ済みポリシーを作成すると、Apex Central では、その新しいポリシーは優先順位が最下位のポリシーとして保存されます。 • 指定済みポリシーは、どのフィルタ済みポリシーよりも優先され、リストの最上位に留まります。管理者は指定済みポリシーを並べ替えることはできません。 • Apex Central では、ドラフトポリシーがリストの最下部に配置されます。
ポリシー	ポリシーの名前が表示されます。

列	説明
ポリシーのバージョン	この列は、Apex One セキュリティエージェントを選択した場合にのみ表示されます。 配信されている最新のポリシーのバージョンが表示されます。  注意 最新のバージョンのポリシーがすべての対象に配信されているとは限りません。特定の対象に配信されている現在のポリシーを確認するには、[配信済み] 列の数字をクリックします。
親ポリシー	この列は、Apex One セキュリティエージェントを選択した場合にのみ表示されます。 ポリシーが子ポリシーの場合 (つまり親ポリシーから設定を継承している場合)、親ポリシーの名前が表示されます。それ以外の場合は「なし」と表示されます。
差異	この列は、Apex One セキュリティエージェントを選択した場合にのみ表示されます。 子ポリシーの場合、親ポリシーから変更された設定の数が表示されます。すべての設定が親ポリシーと同じ場合は、「0」と表示されます。 ポリシーが子ポリシーでない場合は、「なし」と表示されます。

列	説明
所有者	現在ポリシーを割り当てられているユーザが表示されます。 注意 初期設定の所有者は、ポリシーを作成したユーザです。 • ポリシーの所有者を、指定された適用先へのアクセス権がないユーザアカウントに変更する場合、新しい所有者はポリシーの設定を変更できますが、ポリシーデータは表示できません。 • ポリシーを Active Directory グループに割り当てることで、複数の所有者を割り当てることもできます。 詳細については、65 ページの「ポリシーの所有者を変更する」を参照してください。
最終編集者	ポリシーを最後に編集したユーザが表示されます。
最終編集日	この列は、Apex One セキュリティエージェントを選択した場合にのみ表示されます。 ポリシーが最後に編集された日が表示されます。
対象	管理者がポリシーの対象を選択する方法が表示されます。 • 指定済み:参照機能または検索機能を使用して、ポリシーに対して特定の対象を選択します。指定済みポリシーは、ポリシーリストの最上位に留まったままで、フィルタ済みポリシーより優先されます。 • フィルタ済み:フィルタを使用して、現在のエンドポイントおよびそれ以降のエンドポイントをポリシーに自動的に割り当てます。管理者は、フィルタ済みポリシーの優先順位を並べ替えることができます。項目にマウスを重ねるとフィルタ条件が表示され、必要に応じて調整することができます。 • [ラベル]: エンドポイントラベルを使用してエンドポイントをポリシーに割り当てます。 • なし:ポリシー作成者は、対象を選択せずにポリシーをドラフトとして保存しました。

列	説明
配信済み	ポリシー設定が適用されているか、アクティベートされていない製品サービスのある対象の数が表示されます。 ポリシーステータスを表示するには、数をクリックします。
保留中	ポリシー設定が適用されていない対象の数が表示されます。 ポリシーステータスを表示するには、数をクリックします。
オフライン	オフラインエージェントを含む対象の数を表示します。 ポリシーステータスを表示するには、数をクリックします。
問題あり	サポートされていないポリシー配信、ポリシー設定なし、システムエラー、エンドポイントと製品サーバの通信エラー、サポートされていないエンドポイント、ローカルでの設定変更、無効になっている製品サービス、または部分配信が原因で、ポリシー設定が適用されていない対象の数が表示されます。 ポリシーステータスを表示するには、数をクリックします。

注意

[配信済み] と [保留中] の列の数は、管理者が管理権限を持つエンドポイントまたは管理下の製品のみを反映します。

ポリシーリストの並べ替え

管理者は、[並べ替え] ボタンを使用して、フィルタ済みポリシーの順序を変更できます。ポリシーリストを並べ替えると、対象の割り当てに影響が及ぶ場合があります。Apex Central によって、一部の対象が別のフィルタ済みポリシーに再割り当てされる場合があります。

注意

- 指定済みポリシーは影響されないままで、フィルタ済みポリシーよりも常に優先されます。
- この機能は、Apex One 設定の管理でのみ使用できます。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] リストから製品設定の種類を選択します。

   画面の表示が更新され、選択した管理下の製品に対して作成されているポリシーが表示されます。

3. [優先度の再設定] をクリックします。

   [ポリシーの並べ替え] 画面が表示されます。

4. [優先順位] 列の順序を並べ替えます。
5. [保存] をクリックします。

注意

[保存] をクリックした後で、Apex Central が対象を再割り当てするまで 2 分間待ってください。ポリシーリスト内のステータス情報をアップデートするには、[ポリシー管理] 画面の [表示の更新] をクリックします。

ポリシーステータス

ポリシーステータスによって、管理者は Apex Central がポリシーを対象に正常に配信したかどうかを確認できます。

ポリシー配信のステータスを確認するには、次のいずれかの方法を使用します。

- [ポリシー管理] 画面で、ポリシーリスト内の数値をクリックします。[ログクエリ] 画面が表示されます。
- ダッシュボードで、ポリシーステータスウィジェット内の数値をクリックします。[ログクエリ] 画面が表示されます。
- ログクエリを実行します。

次の表は、各ポリシーステータスの説明と対処の提案を示しています。

表 2-3. ポリシーステータス

ポリシーステータス	説明	対処の提案
保留中	Apex Central がポリシーを処理しています。	数分待機して、ステータスを再度確認します。
ポリシーなし	Apex Central は、このエンドポイントまたは管理下の製品にポリシーを割り当てていません。	エンドポイントまたは管理下の製品にポリシーを割り当てます。
配信済み	Apex Central がポリシーを正常に配信しました。	なし
エンドポイントからサーバに接続できません	• エンドポイントは、ポリシー設定を受信しませんでした。 • サーバがビジー状態です。	• エンドポイントの接続ステータスを確認します。 • エンドポイントを社内のネットワークに接続します。 • ポリシーステータスがアップデートされるのを待機します。
適用できない製品設定	管理下の製品で一部のポリシー設定を処理できません。	• ポリシー設定を確認します。 • 最新のポリシーテンプレートバージョンにアップデートします。 • 管理下の製品の設定を確認します。 • [管理下のサーバ] 画面で、管理下の製品の IP アドレスを確認します。 IP アドレスが適切でない場合は、いったん登録解除してから、管理下の製品を Apex Central に登録し直します。 • 管理下の製品の管理者ガイドを参照してください。

ポリシーステータス	説明	対処の提案
サポートされていないエンドポイント	エンドポイントでは、ポリシー設定に指定されている機能でサポートしていないものがあります。	エージェントを、サポートされるバージョンにアップグレードします。
ローカルで変更されている設定	管理下の製品の管理者が管理下の製品のコンソールを使用して変更を加えたために、エンドポイントまたは管理下の製品の設定で、ポリシーに指定されている設定に準拠していないものがあります。	管理下の製品のコンソールで設定を確認します。
アクティベートされていないライセンス	管理下の製品で、ポリシー設定に指定されている一部のサービスのライセンスがアクティベートされていません。	Apex Central 管理コンソールの [ライセンス管理] 画面で関連するサービスのライセンスをアクティベートします。
無効になっている製品サービス	管理下の製品で、ポリシー設定に指定されているサービスの一部が無効にされています。	管理下の製品で関連サービスを有効にします。
一部配信済み	Apex Central がポリシー設定の一部を適用しました。	数分待機して、ステータスを再度確認します。
<Apex Central サーバ名>による管理	現在、別の Apex Central が対象の管理下の製品を管理しています。	[管理下のサーバ] リストから対象の管理下の製品をいったん削除してから、その管理下の製品をリストに追加し直します。
ユーザ名またはパスワードが無効です	認証用のユーザ名またはパスワードが正しくありません。	ユーザ名またはパスワードを確認します。
製品サーバまたは認証情報が無効です	サーバ名または認証情報が正しくありません。	サーバ名および認証情報を確認します。

ポリシーステータス	説明	対処の提案
製品に自動ログオンできません	Apex Central は、対象の管理下の製品へのアクセスにシングルサインオン機能を使用できません。	• 製品ディレクトリでシングルサインオン機能を確認します。 • MCP エージェントの接続ステータスを確認します。 • [管理下のサーバ] リストで、サーバ接続の種類を [自動] から [手動] に変更します。
Web サービスの設定エラーが発生しました	Web サービスエラーが発生しました。	IIS 設定を確認します。
製品通信エラーが発生しました	製品コンソールにアクセスできません。	• 管理下の製品の管理コンソールに接続できるかどうか確認します。 • 管理下の製品の設定を確認します。
製品に接続できません	Apex Central は管理下の製品との接続を確立できません。	• 管理下の製品の接続ステータスを確認します。 • ネットワーク接続を確認します。
サポート対象外の製品バージョン	管理下の製品のバージョンは、サポートされていません。	管理下の製品を、サポートされるバージョンにアップグレードします。
ネットワーク設定エラー	ネットワーク接続でエラーが発生しました。	ネットワーク接続を確認します。
システムエラー。エラー ID: <エラー ID 番号>。	システムエラーが発生しました。	トレンドマイクロのテクニカルサポートに問い合わせてください。

第 3 章

ポリシーリソース

本章では、統合製品/サービスのポリシーリソースについて説明します。

重要

管理下の各製品にはそれぞれ異なるポリシー設定があり、管理者はこれを指定してポリシーの対象に配信できます。サポートされている管理下の製品とそれぞれのポリシー設定の一覧については、各ポリシー設定画面のオンラインヘルプをご覧ください。

次のトピックがあります。

アプリケーションコントロールの条件

セキュリティエージェントポリシールールに割り当てるアプリケーションコントロールの条件を設定します。「許可」条件と「ブロック」を作成して、ユーザが保護されたエンドポイントで実行またはインストールできるアプリケーションを制限できます。また、診断条件を作成してエンドポイントで実行されるアプリケーションを監視した後、使用結果に基づいて条件を調整することもできます。

重要

アプリケーションコントロールの条件は、アプリケーションコントロールポリシーをセキュリティエージェントに配信する前に設定する必要があります。

管理下の各製品にはそれぞれ異なるポリシー設定があり、管理者はこれを指定してポリシーの対象に配信できます。サポートされている管理下の製品とそれぞれのポリシー設定の一覧については、各ポリシー設定画面のオンラインヘルプをご覧ください。

次の表は、[アプリケーションコントロールの条件] 画面で使用可能なタスクの概要を示しています。

タスク	説明
条件の追加	[条件の追加] ドロップダウンボタンをクリックして次のオプションから選択します。 • 許可: クリックして「許可」または「ロックダウン」条件を定義します。 詳細については、78 ページの「許可するアプリケーション条件を定義する」を参照してください。 • ブロック:クリックして「ブロック」または「診断」条件を定義します。 詳細については、81 ページの「ブロックするアプリケーション条件を定義する」を参照してください。 • コピー: 既存の条件を選択し、[コピー] をクリックして既存の設定に基づいた新しい条件を定義します。 • インポート: クリックして、対応するアプリケーションコントロールソースからエクスポートされた ZIP パッケージを選択します。 注意 インポートするパッケージに含まれている条件の名前が既存の条件と一致する場合は、既存の条件を上書きするか、重複する名前の条件のインポートをスキップするかを選択できます。
条件のエクスポート	既存の条件の左側にあるチェックボックスをオンにし、[エクスポート] をクリックして、選択した条件を ZIP パッケージに保存します (`<timestamp>_iACRuleExport.zip`)。

タスク	説明
条件の削除	既存の条件の左側にあるチェックボックスをオンにし、[削除] をクリックして、選択した条件をリストから削除します。 警告! 既存の Apex One セキュリティエージェントポリシーで使用されている条件を選択した場合は、影響を受けるすべてのセキュリティエージェントポリシーからその条件を削除することを確認する必要があります。この処理を取り消すことはできません。
条件の変更	[条件名] をクリックして条件の設定を変更します。 注意 感染したエンドポイントは、次回セキュリティエージェントがサーバに接続したときに変更された条件設定を受信します。
ポリシーの関連付けの表示	[対象のポリシー] 列の値をクリックして、条件を実装するすべての Apex One セキュリティエージェントポリシーのリストを表示します。 ヒント ポリシー名をクリックすると新しいブラウザタブが開き、ポリシー設定を表示または変更できます。

許可するアプリケーション条件を定義する

アプリケーションコントロールでは、特定のアプリケーションの実行を明示的に許可する条件を定義できます。アプリケーションコントロールで特定のアプリケーションがブロックされないように許可条件を定義するか、またはエンドポイントでの実行を許可するすべてのアプリケーションのリストを作成した後にエンドポイントにロックダウンポリシーを配信することができます。ロックダウンモードでは、ユーザは、許可条件に含まれていないアプリケーションを実行、アクセス、またはインストールすることができません。

ロックダウンポリシーの詳細については、**アプリケーションコントロールのポリシー設定**を参照してください

手順

1. ポリシー > ポリシーリソース > アプリケーションコントロールの条件 に移動します。

   [アプリケーションコントロールの条件] 画面が表示されます。

2. [条件の追加] をクリックし、[許可] を選択します。

   [許可条件の設定] 画面が表示されます。

3. 条件に一意の [名前] を入力します。

4. アプリケーションに対する[信頼権限] のレベルを選択します。

権限	説明	使用例
アプリケーションで外部のプロセスを実行できません	アプリケーションは外部のプロセスにアクセスしたり、他のアプリケーションを開始したりできません。	スタンドアロンのアプリケーションにエンドポイントでの実行を許可する一方で、他のプロセスにはアクセスできないようにする場合に使用します。 たとえば、Microsoft Word の実行は許可し、組み込み OLE オブジェクトは実行されないようにします。
アプリケーションで他のプロセスを実行できます	アプリケーションは、ユーザが直接アクセスできない外部のプロセスやアプリケーションを開始できます。	アプリケーションにエンドポイントでの実行を許可し、必要な子プロセスまたはアドオンへのアクセスも許可する場合に使用します。 たとえば、Internet Explorer の実行を許可し、さらにインストール済みプラグインの実行を Internet Explorer に許可します。

権限	説明	使用例
実行権限を継承 (非推奨)	アプリケーションは外部のプロセスやアプリケーションをインストールして開始でき、子アプリケーションも外部のプロセスやアプリケーションをインストールして開始できます。	エンドポイントでのインストールパッケージの実行を許可する場合に使用します。 [実行権限を継承 (非推奨)] では、インストールパッケージがすべてのインストールタスクを実行することを許可し、さらに、インストールされたアプリケーションが必要なプロセスをすべて実行することを許可します。

5. アプリケーションの特定に使用する [照合方法] を選択し、必要な設定を行います。

方法	説明
アプリケーションレピュテーションリスト	トレンドマイクロがテストを実施してセキュリティスコアを割り当てたアプリケーションに条件を適用できます。 詳細については、83 ページの「アプリケーションレピュテーションリスト」を参照してください。
ファイルパス	指定した場所にインストールされた任意のアプリケーションに条件を適用できます。 詳細については、84 ページの「ファイルパス」を参照してください。
証明書	証明書の有効性と属性に基づいてアプリケーションに条件を適用できます。 詳細については、88 ページの「証明書」を参照してください。
ハッシュ値	SHA-1 または SHA-256 ハッシュ値に基づいてアプリケーションに条件を適用できます。 詳細については、89 ページの「ハッシュ値」を参照してください。

方法	説明
悪用されるリスクのあるソフトウェアリスト	トレンドマイクロのテストで有害な可能性があると確認されたアプリケーションを条件に追加することができます。 悪用されるリスクのあるソフトウェアリストは、アプリケーションレピュテーションリストの一部であり、正しく使用されなかった場合に不正な動きをする可能性のあるアプリケーションが含まれています。ネットワークの安全を維持するために、悪用されるリスクのあるソフトウェアリストのアプリケーションをブロックまたは監視することをお勧めします。

6. [保存] をクリックします。

ブロックするアプリケーション条件を定義する

アプリケーションコントロールでは、特定のアプリケーションの実行を明示的にブロックする条件を定義できます。アプリケーションコントロールで特定のアプリケーションが常にブロックされるようにブロック条件を定義することも、ユーザがアクセスするアプリケーションを監視する「診断」条件を作成することもできます。

手順

1. ポリシー > ポリシーリソース > アプリケーションコントロールの条件 に移動します。

   [アプリケーションコントロールの条件] 画面が表示されます。

2. [条件の追加] をクリックし、[ブロック] を選択します。

   [ブロック条件の設定] 画面が表示されます。

3. 条件に一意の [名前] を入力します。

4. 監視ルールを作成するには、[診断モードを有効にする] を選択します。

注意

アプリケーションコントロールは診断条件に一致するアプリケーションをすべてログに記録しますが、それ以上の処理は行いません。アプリケーションの実行は通常どおり許可されます。

5. アプリケーションの特定に使用する [照合方法] を選択し、必要な設定を行います。

方法	説明
アプリケーションレピュテーションリスト	トレンドマイクロがテストを実施してセキュリティスコアを割り当てたアプリケーションに条件を適用できます。 詳細については、83 ページの「アプリケーションレピュテーションリスト」を参照してください。
ファイルパス	指定した場所にインストールされた任意のアプリケーションに条件を適用できます。 詳細については、84 ページの「ファイルパス」を参照してください。
証明書	証明書の有効性と属性に基づいてアプリケーションに条件を適用できます。 詳細については、88 ページの「証明書」を参照してください。
ハッシュ値	SHA-1 または SHA-256 ハッシュ値に基づいてアプリケーションに条件を適用できます。 詳細については、89 ページの「ハッシュ値」を参照してください。
悪用されるリスクのあるソフトウェアリスト	トレンドマイクロのテストで有害な可能性があると確認されたアプリケーションを条件に追加することができます。 悪用されるリスクのあるソフトウェアリストは、アプリケーションレピュテーションリストの一部であり、正しく使用されなかった場合に不正な動きをする可能性のあるアプリケーションが含まれています。ネットワークの安全を維持するために、悪用されるリスクのあるソフトウェアリストのアプリケーションをブロックまたは監視することをお勧めします。

6. [保存] をクリックします。

アプリケーションの照合方法

アプリケーションコントロールでは、色々な方法で許可条件やブロック条件に含めるアプリケーションを特定することができます。

注意

悪用されるリスクのあるソフトウェアリストも用意されていますが、これは変更できません。

悪用されるリスクのあるソフトウェアリストは、アプリケーションレピュテーションリストの一部であり、正しく使用されなかった場合に不正な動きをする可能性のあるアプリケーションが含まれています。ネットワークの安全を維持するために、悪用されるリスクのあるソフトウェアリストのアプリケーションをブロックまたは監視することをお勧めします。

アプリケーションレピュテーションリスト

アプリケーションレピュテーションリストは、トレンドマイクロによってテストされたアプリケーションがすべて含まれているリストです。リストには、最も普及している OS のファイルやバイナリに加え、デスクトップ、サーバ、およびモバイルデバイス向けのアプリケーションも含まれます。トレンドマイクロはこのリストを定期的に更新しています。

重要

常に最新のアプリケーション情報を入手できるように、ソフトウェア安全性評価パターンファイルの定期アップデートを必ずオンにしてください。

ベンダまたはアプリケーションの名前を入力してアプリケーションを検索できます。提供されたデータを使用してアプリケーションを選択してください。

データ	説明
アプリケーション	アプリケーションの名前を示します。 ヒント 各アプリケーションのバージョンの詳細情報を表示するには、アプリケーションレピュテーションリストを展開します。
AIR スコア	アプリケーションの人気とレピュテーションに基づく総合的なセキュリティスコアを示します。

データ	説明
グローバル使用率	グローバルなアプリケーションの普及率を示します。 ヒント 普及率をクリックすると、地域別の内訳が表示されます。

ファイルパス

絶対パス、ストレージの種類、および Perl 互換正規表現 (PCRE) に基づいて、特定のディレクトリの場所を対象とするようにアプリケーションコントロールを設定できます。

特定のパスとストレージの種類のどちらで一致させるか選択し、一致させる文字列の種類 ([文字列] または [正規表現 (PCRE)]) を指定します。条件に適用するファイルパスを入力します。

注意

- [文字列] を指定した場合、アスタリスク (*) ワイルドカードを使用できます。アスタリスクを使用して、指定された文字列の場所のサブディレクトリにある 1 つ以上の文字を表すことができます。
- アプリケーションコントロールではファイルパスを指定する際に、[文字列] または [正規表現 (PCRE)] での一致には環境変数を使用できません。
- ワイルドカード文字を使用して、選択されたストレージの場所の内容全体を表すことはできません。
- 最大 100 のファイルパスを指定できます。

表 3-1. サポートされるストレージの場所

ストレージの場所	環境変数	説明
特定のパス	該当なし	指定されたパスにあるアプリケーションにのみ適用されます。 **注意** この場所の種類を使用する場合、アプリケーションコントロールはデバイスの種類をチェックしません。
任意の組み込みストレージ	$FixedDrives	指定されたパスにあり、内部ストレージデバイス (内部ハードディスクドライブ) に格納されているアプリケーションにのみ適用されます。
任意のローカルストレージ	$LocalDrives	指定されたパスにあり、リムーバブルでないローカルストレージデバイス (内部または外部のハードディスクドライブ) に格納されているアプリケーションにのみ適用されます。
任意のリムーバブルストレージ	$RemovableDrives	指定されたパスにあり、リムーバルストレージデバイス (USB ドライブ、CD/DVD) に格納されているアプリケーションにのみ適用されます。
ネットワークパス	$RemoteDrives	指定されたパスにあり、共有ネットワークリソースに格納されているアプリケーションにのみ適用されます。
Program Files フォルダ	$ProgramFiles	指定されたパスにあり、Program Files フォルダ (初期設定のフォルダ: `C:¥Program Files` と `C:¥Program Files (x86)`) に格納されているアプリケーションにのみ適用されます。
システムボリューム	$SystemDrive	指定されたパスにあり、初期設定の Windows システムドライブに格納されているアプリケーションにのみ適用されます。

ファイルパスの使用例

目標	許可ルール	ブロックルール	結果
すべてのユーザの Downloads フォルダを監視します。	-	1. 診断モードを有効にする 2. 任意のローカルストレージ 3. 文字列 4. `C:\Users\*\Downloads\*`	すべてのユーザの Downloads フォルダにあるアプリケーションにアクセスようとする操作をすべて記録します。 監視: • C:¥Users¥john_doe¥Downloads¥start.exe • C:¥Users¥Administrator¥Downloads¥start.exe
いずれかの Program Files ディレクトリの MyApps サブフォルダにあるフォルダ内のアプリケーションをすべてブロックします。	-	1. Program Files フォルダ 2. 文字列 3. `\MyApps*`	ブロック: • C:¥Program Files(x86)¥MyApps¥start.exe • C:¥Program Files¥MyApps¥start.exe • C:¥Program Files(x86)¥MyApps¥bin¥start.exe 許可: • C:¥Program Files(x86)¥start.exe

目標	許可ルール	ブロックルール	結果
いずれかの Program Files ディレクトリの MyApps サブフォルダにあるフォルダ内のすべてのアプリケーションを許可し、それ以外のアプリケーション/フォルダをすべてブロックします。	1. Program Files フォルダ 2. 文字列 3. `\MyApps*`	1. 任意のローカルストレージ 2. 文字列 3. `C:\Program Files\*` AND 1. 任意のローカルストレージ 2. 文字列 3. `C:\Program Files (x86)\*`	ブロック: • C:¥Program Files(x86)¥start.exe 許可: • C:¥Program Files(x86)¥MyApps¥start.exe • C:¥Program Files¥MyApps¥start.exe • C:¥Program Files(x86)¥MyApps¥bin¥start.exe
いずれかの Program Files ディレクトリの MyApps サブフォルダにあるアプリケーションのみをブロックし、それ以外のアプリケーション/フォルダをすべて許可します。	1. MyApps ディレクトリ内のサブフォルダを許可します。 a. Program Files フォルダ b. 文字列 c. `\MyApps\*\*`	1. Program Files フォルダ 2. 文字列 3. `\MyApps\*`	ブロック: • C:¥Program Files(x86)¥MyApps¥start.exe • C:¥Program Files¥MyApps¥start.exe 許可: • C:¥Program Files(x86)¥start.exe • C:¥Program Files(x86)¥MyApps¥bin¥start.exe

目標	許可ルール	ブロックルール	結果
任意のフォルダ内の特定のアプリケーションファイル名をブロックします。	-	1. 特定のパス 2. 正規表現 (PCRE) 3. `.*\\(?i)test(?-i)\..*`	ブロック: • `C:\MyApps\test.exe` • `C:\Users\guet\AppData\Local\Temp\test.exe` • `C:\Program Files(x86)\MyApps\test.exe`

証明書

証明書の「信頼」レベルおよび特定の属性に基づいてアプリケーションを明示的に対象にするように、アプリケーションコントロールを設定できます。

証明書の「信頼」レベルを選択し、次に証明書の「発行者」または「件名」を指定します。

注意

アプリケーションコントロールでは、証明書の属性を指定する際にワイルドカードとしてアスタリスク (*) を使用できますが、範囲を絞り込むためにワイルドカードを他の文字と組み合わせる必要があります。たとえば、どのフィールドでもワイルドカード文字を単独で使用することはできません。

次の表は、各「信頼」レベルとその説明です。

種類	説明
信頼済み (有効)	信頼された証明書リストに含まれていて、有効期限が切れていない証明書を示します。
信頼済み (有効または期限切れ)	信頼された証明書リストに追加されているが、有効期限が切れている証明書を示します。

種類	説明
信頼されていない/信頼済み (有効または期限切れ)	不明、または信頼された証明書リストに追加されてない証明書を示します。

注意

許可条件とブロック条件では「信頼」レベルの組み合わせは異なります。

ハッシュ値

SHA-1 または SHA-256 のハッシュ値形式を使用してアプリケーションに一致させるようにアプリケーションコントロールを設定できます。手動でハッシュ値を指定するか、生成された値のリストをインポートするかを選択できます。

[入力方式] を選択し、画面上の指示に従います。

入力方式	説明
手動	最大 100 個のハッシュ値 (および説明) を手動で指定できます。

入力方式	説明
インポート	適切な形式 (CSV 形式) のハッシュ値リストを含む ZIP パッケージをインポートできます。 [ハッシュ生成ツール] を使用するか、[CSV サンプル形式] を使用して手動で CSV ファイルを作成するかを選択できます。 **警告!** 各条件セットにインポートできるファイルは 1 つだけです。条件に新しいハッシュ値リストをインポートすると、既存の値がすべて上書きされます。 • ハッシュ生成ツール: 必要なすべてのアプリケーションがインストールされている対象エンドポイントにこのツールをダウンロードし、実行します。このツールは、エンドポイント上で検出されたすべてのアプリケーションのハッシュ値を含む有効な ZIP パッケージを自動的に作成します。 • CSV サンプル形式: サンプルファイルをダウンロードし、指示に従ってハッシュ値リストを入力します。リストが完成したらファイルを ZIP 形式に圧縮し、条件セットにインポートします。 **重要** ハッシュ値リストに SHA-1 と SHA-256 の両方の形式を含めることはできません。ハッシュ値の形式ごとに、個別のハッシュ値ファイルとアプリケーションコントロールの条件を作成する必要があります。

情報漏えい対策について

情報漏えい対策は、組織の機密情報や機密データ (デジタル資産と呼ばれます) を不慮の漏えいや意図的な盗用から保護します。情報漏えい対策を使用すると、次のことを実行できます。

- 保護するデジタル資産の特定
- メールや外部デバイスなどの共通のチャネルを介したデジタル資産の転送を制限または防止するポリシーを作成します。

- 制定されたプライバシー標準へのコンプライアンスの実施

情報漏えい対策は、ポリシーに定義されたルールセットに基づいてデータを評価します。ポリシーによって、不正な転送から保護する必要があるデータが判別され、転送の検出時に情報漏えい対策が実行する処理が決定されます。

重要

管理下の各製品にはそれぞれ異なるポリシー設定があり、管理者はこれを指定してポリシーの対象に配信できます。サポートされている管理下の製品とそれぞれのポリシー設定の一覧については、各ポリシー設定画面のオンラインヘルプをご覧ください。

データ識別子の種類

デジタル資産とは、組織で保護する必要のあるファイルやデータを意味します。デジタル資産は次のデータ識別子を使用して定義することができます。

- パターン: 特定の構造を持つデータ。

  詳細については、91 ページの「パターン」を参照してください。

- ファイル属性: ファイルの種類やサイズなどのファイルのプロパティ。

  詳細については、96 ページの「ファイル属性」を参照してください。

- キーワードリスト: 特別な単語や語句のリスト。

  詳細については、98 ページの「キーワード」を参照してください。

注意

情報漏えい対策テンプレートで使用されているデータ識別子を削除することはできません。データ識別子を削除する前にテンプレートを削除してください。

パターン

パターンは特定の構造を持つデータです。たとえば、クレジットカード番号の多くは 16 桁の「nnnn-nnnn-nnnn-nnnn」という形式で表現されるため、パターンによる検出に適しています。

事前定義済みのパターンとカスタマイズしたパターンを使用できます。

詳細については、92 ページの「事前定義済みのパターン」および 92 ページの「カスタマイズしたパターン」を参照してください。

事前定義済みのパターン

情報漏えい対策には、事前定義済みのパターンが付属しています。これらのパターンは、変更や削除ができません。

これらのパターンは、パターンマッチングと数学的な等式を使用して検証されます。機密と考えられるデータがパターンに一致すると、そのデータに対してさらに検証チェックが実行されることもあります。

事前定義済みのパターンの全リストについては、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

事前定義済みのパターンの設定の表示

注意

事前定義済みのパターンは、変更や削除ができません。

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策データ識別子] に移動します。
2. [パターン] タブをクリックします。
3. パターン名をクリックします。
4. 開いた画面で設定を確認します。

カスタマイズしたパターン

事前定義済みパターンに該当しないパターンを利用したい場合は、カスタマイズしたパターンを作成し、利用する事が出来ます。

パターンは強力な文字列照合ツールです。パターンを作成する前に、以下の注意点をご確認ください。パターンの善し悪しが性能に大きく影響する場合があります。

パターンを作成する際の注意:

- 有効なパターンを定義するための参考として事前定義済みのパターンを参照してください。たとえば、日付を含むパターンを作成する場合は、「日付」に事前定義されたパターンを参照してください。
- 情報漏えい対策は Perl 互換正規表現 (PCRE) で定義されたパターン形式に準拠しています。PCRE の詳細については、次の Web サイトを参照してください。

  http://www.pcre.org/
- 単純なパターンから始めてください。不正なアラームが発生した場合にパターンを修正したり、検出率を高めるためにパターンを調整したりします。

パターンを作成するときには、いくつかの条件の中から選択できます。パターンに選択した条件を満たすデータだけが、情報漏えい対策ポリシーの適用対象となります。各条件オプションの詳細については、93 ページの「カスタマイズしたパターンの条件」を参照してください。

カスタマイズしたパターンの条件

利用可能なオプションを表示してカスタム式を作成します。

表 3-2. カスタマイズしたパターンの条件オプション

条件	ルール	例
なし	なし	米国勢調査局発行の名前 • パターン:[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

条件	ルール	例
特定の文字	パターンには、指定した文字が含まれている必要があります。 さらに、パターン内の文字数は下限値と上限値の範囲に収める必要があります。	米国 - ABA 銀行ルーティング番号 • パターン:[^\d]([0123678]\d{8})[^\d] • 文字: 0123456789 • 最小文字数: 9 • 最大文字数: 9
サフィックス	サフィックスはパターンの最終セグメントを意味します。サフィックスには、指定された文字と特定の文字数が含まれている必要があります。 さらに、パターン内の文字数は下限値と上限値の範囲に収める必要があります。	自宅住所 • パターン:\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • サフィックス文字: 0123456789- • 文字数: 5 • パターン内の最小文字数: 25 • パターン内の最大文字数: 80
単一の区切り文字	パターンは 2 つのセグメントで構成し、1 つの文字で区切る必要があります。文字は 1 バイト長にする必要があります。 さらに、区切り文字の左側の文字数は下限値と上限値の範囲に収める必要があります。区切り文字の右側の文字数は上限値を超えないようにする必要があります。	メールアドレス • パターン:[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • 区切り文字: @ • 左側の最小文字数: 3 • 左側の最大文字数: 15 • 右側の最大文字数: 30

カスタマイズしたパターンの作成

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策データ識別子] に移動します。

2. [パターン] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。
4. パターンの名前を入力します。名前は、100 バイト以下の長さにする必要があり、次の文字を含めることができません。

   - > < * ^ | & ? \ /
5. 長さが 256 バイトを超えない説明を入力してください。
6. 表示するデータを入力します。

   たとえば、ID 番号に関するパターンを作成する場合は、サンプル ID 番号を入力します。このデータは、参照目的にのみ使用し、製品内の他の場所には表示されません。
7. 次の条件のいずれかを選択して、その条件に合わせて追加の設定値を指定します (93 ページの「カスタマイズしたパターンの条件」を参照)。

   - なし
   - 特定の文字
   - サフィックス
   - 単一のセパレータ文字
8. 実際のデータでパターンをテストします。

   [テストデータ] テキストボックスに有効な値を入力して [テスト] をクリックし、結果を確認します。
9. 目的の結果であれば、[保存] をクリックします。

注意

テストが成功した場合にのみ設定を保存します。データを検出できないパターンは、システムリソースを浪費し、性能に影響を与える可能性があります。

カスタマイズしたパターンのインポート

このオプションは、パターンを含んだ適切な形式の.dat ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからパターンをエクスポートすることによって作成できます。

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策データ識別子] に移動します。
2. [パターン] タブをクリックします。
3. [インポート] をクリックしてから、パターンが保存された.dat ファイルを選択します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするパターンがすでに存在する場合は省略されます。

ファイル属性

ファイル属性はファイル独自のプロパティです。データ識別子を定義するときに、ファイルタイプとファイルサイズという 2 つのファイル属性を使用できます。たとえば、ソフトウェア開発会社では、会社のソフトウェアインストーラの共有を、ソフトウェアの開発とテストを担当している開発部門に制限しなければならない場合があります。この場合は、Apex Central 管理者はポリシーを作成して、サイズが 10～40MB の実行可能ファイルが開発以外の部門に転送されるのをブロックできます。

ファイル属性自体は、機密ファイルの識別子に適しているとは言えません。このトピックの例では、他の部門で共有されているサードパーティ製ソフトウェアがブロックされる可能性があります。そのため、ファイル属性と他の情報漏えい対策データ識別子を組み合わせて、機密ファイルの検出対象を絞り込むことをお勧めします。

サポートされるファイルタイプの全リストについては、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

ファイル属性リストの作成

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策データ識別子] に移動します。
2. [ファイル属性] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。
4. ファイル属性リストの名前を入力します。名前は、100 バイト以下の長さにする必要があり、次の文字を含めることができません。

   - > < * ^ | & ? \ /
5. 長さが 256 バイトを超えない説明を入力してください。
6. 目的の実際のファイルタイプを選択します。
7. 含めるファイルタイプがリストに掲載されていない場合は、[ファイル拡張子] を選択し、そのファイルタイプの拡張子を入力します。情報漏えい対策は、実際のファイルタイプではなく指定されたファイル拡張子をチェックします。ファイル拡張子を指定する際のガイドライン:

   - 各拡張子の先頭にはアスタリスク (*) とピリオド (.) を付け、その後に拡張子を指定する必要があります。アスタリスクはワイルドカードであり、ファイルの実際の名前を表しています。たとえば、`*.pol` は `12345.pol` や `test.pol` と一致します。
   - 拡張子にワイルドカードを含めることができます。1 文字のデータを表す場合は疑問符 (?) を使用し、複数の文字を表す場合はアスタリスク (*) を使用します。次の例を参照してください。

     - `*.*m` は、`ABC.dem`、`ABC.prm`、`ABC.sdcm` などのファイルと一致します。

     - `*.m*r` は、`ABC.mgdr`、`ABC.mtp2r`、`ABC.mdmr` などのファイルと一致します。

     - `*.fm?`は、`ABC.fme`、`ABC.fml`、`ABC.fmp` などのファイルと一致します。

- 拡張子の末尾にアスタリスクを追加すると、ファイル名や関係のない拡張子の一部と一致する可能性があるので注意してください。例:*.do*は、abc.doctor_john.jpg や abc.donor12.pdf と一致します。
- 複数のファイル拡張子はセミコロン (;) で区切って入力してください。セミコロンの後に空白を追加する必要はありません。

8. 最小ファイルサイズと最大ファイルサイズをバイト単位で入力します。両方のファイルサイズは、0 より大きい整数にする必要があります。
9. [保存]をクリックします。

ファイル属性リストのインポート

このオプションは、ファイル属性リストを含んだ適切な形式の.dat ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからファイル属性リストをエクスポートすることによって作成できます。

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策データ識別子] に移動します。
2. [ファイル属性] タブをクリックします。
3. [インポート] をクリックしてから、ファイル属性リストが保存された.dat ファイルを選択します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするファイル属性リストがすでに存在する場合は省略されます。

キーワード

キーワードは特殊な単語または語句です。関連するキーワードをキーワードリストに追加することで、特定の種類のデータを識別できます。たとえば、「予後」、「血液型」、「予防接種」、および「医師」は診断書で使用されるキーワードです。診断書ファイルの転送を禁止したい場合は、情報漏えい対策ポ

リシーでこれらのキーワードを使用し、これらのキーワードを含むファイルをブロックするように情報漏えい対策を設定できます。

よく使用される単語を組み合わせて意味のあるキーワードを形成できます。たとえば、「end」、「read」、「if」、および「at」を組み合わせて、「END-IF」、「END-READ」、「AT END」などのソースコードで見られるキーワードを形成できます。

事前定義済みのキーワードリストとカスタマイズしたキーワードリストを使用できます。詳細については、99 ページの「事前定義済みのキーワードリスト」および 100 ページの「カスタムキーワードリスト」を参照してください。

事前定義済みのキーワードリスト

情報漏えい対策には、事前定義済みのキーワードリストが付属しています。これらのキーワードリストは、変更や削除ができません。リストにはそれぞれ固有の条件が組み込まれており、テンプレートに照らしてポリシー違反と見なすかどうかを判別します。

情報漏えい対策の事前定義済みキーワードリストの詳細については、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

キーワードリストの機能

キーワード数条件

キーワードリストにはそれぞれ条件が含まれており、一定数のキーワードがドキュメントに存在すると、リストに照らして違反と見なされます。

キーワード数の条件には、次の値が含まれます。

- すべて:ドキュメントに、リスト内のすべてのキーワードが存在する必要があります。
- いずれか:ドキュメントに、リスト内のキーワードがいずれか 1 つ存在する必要があります。
- 特定の数:ドキュメントに、少なくとも指定された数のキーワードが存在する必要があります。ドキュメント内のキーワードが指定された数より多い場合、違反と見なされます。

距離条件

一部のリストには、違反があるかどうかを判別する「距離」条件が含まれています。「距離」とは、あるキーワードの最初の文字と、別のキーワードの最初の文字との間の文字数を表します。次のエントリについて考えます。

First Name:_John_ Last Name:_Smith_

[フォーム - 名、姓] リストには、50 文字の「距離」条件と、代表的なフォームフィールド「名」と「姓」が含まれています。上記の例では、「First Name」の「F」と「Last Name」の「L」の間の文字数が 18 なので、違反と見なされます。

違反と見なされないエントリの例は、次のとおりです。

The first name of our new employee from Switzerland is John.His last name is Smith.

この例では、「first name」の「f」と「last name」の「l」の間の文字数は 61 です。この場合は距離のしきい値を超えるので、違反とは見なされません。

カスタムキーワードリスト

カスタマイズしたキーワードリストを作成します。どの事前定義済みのキーワードリストも要件を満たさない場合は。

キーワードリストを設定するときに選択可能な条件がいくつかあります。キーワードリストは、情報漏えい対策によるポリシーの適用に関係なく、選択した条件を満たす必要があります。キーワードリストごとに次の条件のいずれかを選択します

- いずれかのキーワード
- すべてのキーワード
- <x> 文字以下のすべてのキーワード
- キーワードの合計スコアがしきい値を超過

条件のルールの詳細については、101 ページの「カスタムキーワードリストの条件」を参照してください。

カスタムキーワードリストの条件

情報漏えい対策テンプレートで使用するカスタムキーワードリストを作成するために使用される基準を表示します。

表 3-3. キーワードリストの基準

条件	ルール
任意のキーワード	キーワードリストの 1 つ以上のキーワードがファイルに含まれている必要があります。
すべてのキーワード	キーワードリストのすべてのキーワードがファイルに含まれている必要があります。
<x>文字以内のすべてのキーワード	キーワードリストのすべてのキーワードがファイルに含まれている必要があります。さらに、各キーワードのペアは、それぞれが<x>文字以内に存在している必要があります。 たとえば、キーワードが WEB、DISK、および USB の 3 つで、指定した文字数が 20 であるとします。 情報漏えい対策がすべてのキーワードを DISK、WEB、USB の順に検出した場合、DISK の「D」から WEB の「W」まで、および「W」から USB の「U」までの文字数は 20 文字以下である必要があります。 次のデータがこの条件に一致します。DISK####WEB############USB 次のデータはこの条件に一致しません。 DISK******************WEB****USB (「D」と「W」の間が 23 文字) この文字数を小さくすると (10 など) 検索時間は短くなりますが、検出範囲は制限される傾向にあります。これは、特に大きなファイルで、機密データが検出される確率が低下します。数字を大きくするほど、対象範囲も広がりますが、検索時間は長くなります。

条件	ルール
キーワードの合計スコアがしきい値を超えています	キーワードリストの 1 つ以上のキーワードがファイルに含まれている必要があります。キーワードが 1 つだけ検出された場合は、そのスコアがしきい値を超える必要があります。キーワードが複数ある場合は、その合計スコアがしきい値を超える必要があります。 各キーワードに、1〜10 のスコアを割り当てます。機密性の高い単語や語句、たとえば総務部で「昇給」などは、比較的高いスコアにします。単独ではあまり重要性が高くない単語や語句のスコアは低くしてもかまいません。 しきい値を設定する場合は、キーワードに割り当てたスコアを考慮します。たとえば、キーワードが 5 つあり、そのうち 3 つの優先度が高い場合、しきい値は優先度の高い 3 つのキーワードの合計スコア以下にすることができます。これは、この 3 つのキーワードさえ検出されれば、そのファイルは脆弱だと十分に判断できるということです。

キーワードリストの作成

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策データ識別子] に移動します。
2. [キーワードリスト] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。
4. キーワードリストの名前を入力します。名前は、100 バイト以下の長さにする必要があり、次の文字を含めることができません。
   - > < * ^ | & ? \ /
5. 長さが 256 バイトを超えない説明を入力してください。
6. 次の条件のいずれかを選択して、その条件に合わせて追加の設定値を指定します。
   - 任意のキーワード
   - すべてのキーワード

- <x> 文字以下のすべてのキーワード
- キーワードの合計スコアがしきい値を超過

7. キーワードを手動でリストに追加するには
   a. 長さが 3 ～ 40 バイトのキーワードを入力して、大文字と小文字を区別するかどうかを指定します。
   b. [追加] をクリックします。
8. [インポート] オプションを使用してキーワードを追加するには

注意

このオプションは、キーワードを含んだ適切な形式の.csv ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからキーワードをエクスポートすることによって作成できます。

   a. [インポート] をクリックしてから、キーワードが保存された.csv ファイルを選択します。
   b. [開く] をクリックします。

      インポートが成功したかどうかを示すメッセージが表示されます。インポートするキーワードがすでにリスト内に存在する場合は省略されます。
9. キーワードを削除するには、そのキーワードを選択して、[削除] をクリックします。
10. キーワードをエクスポートするには

注意

[エクスポート] 機能は、キーワードをバックアップするか、キーワードを別のサーバにインポートする場合に使用します。キーワードリスト内のすべてのキーワードがエクスポートされます。キーワードを個別にエクスポートすることはできません。

a. [エクスポート] をクリックします。

b. 生成された.csv ファイルを任意の場所に保存します。

11. [保存]をクリックします。

キーワードリストのインポート

このオプションは、キーワードリストを含んだ適切な形式の.dat ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからキーワードリストをエクスポートすることによって作成できます。

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策データ識別子] に移動します。
2. [キーワード] タブをクリックします。
3. [インポート] をクリックしてから、キーワードリストが保存された.dat ファイルを選択します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするキーワードリストがすでに存在する場合は省略されます。

情報漏えい対策テンプレート

情報漏えい対策テンプレートは、情報漏えい対策データ識別子と、条件文を形成する論理演算子 (および、または、除外) で構成されます。特定の条件文を満たすファイルやデータのみが情報漏えい対策ポリシーの対象となります。

たとえば、「雇用契約」ポリシーの対象ファイルの条件を、「Microsoft Word ファイル (ファイル属性)」および「特定の法律用語を含む (キーワード)」および「ID 番号を含む (パターン)」のように指定できます。このポリシーを使用すれば、人事担当者が印刷処理を介してファイルを転送できるため、従業員がそのハードコピーに署名できます。メールなどの他の使用可能なチャネル経由の転送はすべてブロックされます。

情報漏えい対策データ識別子の定義が完了していれば、独自のテンプレートを作成できます。事前定義済みのテンプレートを使用することもできます。詳細については、105 ページの「カスタム情報漏えい対策テンプレート」および 105 ページの「事前定義済みの情報漏えい対策テンプレート」を参照してください。

注意

情報漏えい対策ポリシーで使用されているテンプレートを削除することはできません。テンプレートを削除する前にポリシーからテンプレートを削除します。

事前定義済みの情報漏えい対策テンプレート

情報漏えい対策には、次のように、さまざまな規制基準に準拠するために使用可能な事前定義済みのテンプレートが付属しています。これらのテンプレートは、変更や削除ができません。

- GLBA:Gramm-Leach-Billey Act
- HIPAA:Health Insurance Portability and Accountability Act (医療保険の相互運用性と説明責任に関する法律)
- PCI-DSS:Payment Card Industry Data Security Standard (PCI-DSS: カード会員データや取引情報を保護することを目的に作成されたクレジット業界のセキュリティ基準)
- SB-1386:US Senate Bill 1386
- US PII:United States Personally Identifiable Information (米国で個人を特定できる情報)

すべての事前定義済みのテンプレートの目的の一覧、および保護されるデータの例については、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

カスタム情報漏えい対策テンプレート

情報漏えい対策テンプレートを作成するには、データ識別子を設定している必要があります。

情報漏えい対策テンプレートは、データ ID と論理演算子 (And、Or、Except) を組み合わせて条件文を形成します。

条件文と論理演算子の働きと例については、106 ページの「条件文と論理 pperators」を参照してください。

条件文と論理 pperators

カスタム情報漏えい対策テンプレートに条件と演算子を適用します。

情報漏えい対策は左から右に条件文を評価します。条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。

次の表の例を参照してください。

表 3-4. サンプル条件文

条件文	説明と例
[データ識別子 1] および [データ識別子 2] 除外 [データ識別子 3]	ファイルは、[データ識別子 1] と [データ識別子 2] の条件を満たすが、[データ識別子 3] の条件を満たしていない必要があります。 例を以下に示します。 ファイルは、[Adobe PDF 文書] であり、[メールアドレス] を含むが、[キーワードリスト内のすべてのキーワード] を含まない必要があります。
[データ識別子 1] または [データ識別子 2]	ファイルは [データ識別子 1] または [データ識別子 2] の条件を満たす必要があります。 例を以下に示します。 ファイルは、[Adobe PDF 文書] であるか、[Microsoft Word ドキュメント] である必要があります。
除外 [データ識別子 1]	ファイルは [データ識別子 1] の条件を満たしていない必要があります。 例を以下に示します。 ファイルは [マルチメディアファイル] 以外である必要があります。

表の最後の例で示したように、ファイルが条件文内のいずれのデータ識別子の条件も満たさないことが必要な場合は、条件文内の最初のデータ識別子に「除外」演算子を使用できます。ただし、ほとんどの場合、最初のデータ識別子に演算子は使用しません。

テンプレートの作成

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策テンプレート] に移動します。
2. [追加] をクリックします。

   新しい画面が表示されます。
3. テンプレートの名前を入力します。名前は、100 バイト以下の長さにする必要があり、次の文字を含めることができません。

   - > < * ^ | & ? \ /
4. 長さが 256 バイトを超えない説明を入力してください。
5. データ識別子を選択してから、[追加] アイコンをクリックします。

   定義を選択する場合:

   - 複数のエントリを選択するには、<Ctrl> キーを押しながらデータ識別子を選択します。
   - 検索機能は、特定の定義を想定している場合に使用します。データ識別子名のすべてまたは一部を入力できます。
   - テンプレートごとに最大 30 のデータ識別子を含めることができます。
6. 新しいパターンを作成するには、[パターン] をクリックし、[新しいパターンの追加] をクリックします。表示された画面で、パターンを設定します。
7. 新しいファイル属性リストを作成するには、[ファイル属性] をクリックし、[新しいファイル属性の追加] をクリックします。表示された画面で、ファイル属性リストを設定します。

8. 新しいキーワードリストを作成するには、[キーワード] をクリックし、[新しいキーワードの追加] をクリックします。表示された画面で、キーワードリストを設定します。
9. パターンを選択した場合は、出現頻度を入力します。情報漏えい対策がパターンをポリシーの対象とするには、指定された回数だけ出現している必要があります。
10. 定義ごとに論理演算子を選択します。

注意

条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。正しい使用例については、106 ページの「条件文と論理 pperators」を参照してください。

11. 選択したデータ識別子のリストからデータ識別子を削除するには、ごみ箱アイコンをクリックします。
12. [プレビュー] で、条件文を確認し、目的の記述と異なる場合は変更します。
13. [保存]をクリックします。

テンプレートのインポート

このオプションは、正しくフォーマットされた.dat ファイルにテンプレートが保存されている場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからテンプレートをエクスポートすることによって作成できます。

手順

1. [ポリシー] > [ポリシーリソース] > [情報漏えい対策テンプレート] に移動します。
2. [インポート] をクリックしてから、テンプレートが保存された.dat ファイルを選択します。

3. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするテンプレートがすでに存在する場合は省略されます。

IPS ルール

[IPS ルール] 画面には、Apex Central 仮想パッチでサポートされている IPS ルールが表示されます。IPS ルールは、ネットワークパケットの実際の内容 (およびパケットの順序) を検査します。その後、IPS ルール内に設定された条件に基づいて、これらのパケットに対してさまざまな処理が実行されます。処理には、明確に定義されたバイトシーケンスや疑わしいバイトシーケンスの置換から、パケットの完全な破棄や接続のリセットまで含まれます。

- ルールのリストをフィルタするには、[検索] ボックスを使用し、任意の列の文字列全体または一部を指定します。
- IPS ルールのリストを列のデータで並べ替えるには、列見出しをクリックします。
- IPS ルールの詳細なプロパティを表示するには、ルールの [ルール名] 列にあるリンクをクリックします。
- 仮想パッチによる検索から、1 つ以上の送信元エンドポイントからのトラフィックを除外するには、[除外の設定] をクリックして送信元 IP アドレスを指定します。

  注意

  除外リストには最大 100 件のエントリを追加できます。

注意

Apex Central は、手動または自動のコンポーネントをアップデート中に IPS ルールを自動的に Apex One サーバからインポート/アップデートします。

重要

管理下の各製品にはそれぞれ異なるポリシー設定があり、管理者はこれを指定してポリシーの対象に配信できます。サポートされている管理下の製品とそれぞれのポリシー設定の一覧については、各ポリシー設定画面のオンラインヘルプをご覧ください。

次の表では、[IPS ルール] 画面に表示されるルール情報の概要を説明します。

列	説明
識別子	IPS ルールの固有識別子タグを示します。
ルール名	IPS ルールの名前を示します。
アプリケーションの種類	IPS ルールがグループ化されるアプリケーションの種類を示します。
重大度	トレンドマイクロがルールに割り当てる重大度レベルを示します。 **注意** ルールの重大度は、ルールの実装方法または適用方法に影響しません。重大度レベルは、IPS ルールのリストを表示する場合にソート条件として使用できます。
モード	IPS モジュールによって使用されるネットワークエンジン検出モードを示します。モードをクリックして、ルールの設定を行います。
種類	検出された脆弱性の種類を示します。 • スマート: 既知または不明な脆弱性 (ゼロデイ攻撃など) • 攻撃コード: 既知の脆弱性に対する既知の攻撃コード (通常、署名ベース) • 脆弱性: 1 つ以上の攻撃コードが存在する可能性のある既知の脆弱性

列	説明
CVE	MITRE がその脆弱性に割り当てた Common Vulnerabilities and Exposures (CVE®) 識別子を示します。 詳細については、http://cve.mitre.org/を参照してください。
Microsoft	Microsoft がその脆弱性に割り当てた Common Vulnerabilities and Exposures (CVE®) 識別子を示します。
CVSS スコア	National Vulnerability Database に登録されている脆弱性の Common Vulnerability Scoring System (CVSS) 重大度スコアを示します。 詳細については、http://nvd.nist.gov/cvss.cfm を参照してください。
最終更新日	ルールが最後に変更された日時を示します。

IPS ルールのプロパティ

[IPS ルールのプロパティ] 画面には、特定の IPS ルールと脆弱性に関する詳細が表示されます。[一般] タブまたは [脆弱性] をクリックすると、ルールの詳細が表示されます。

次の表では、[一般] タブと [脆弱性] タブに表示される情報について説明します。

表 3-5. 一般情報

データ	説明
識別子	IPS ルールの固有識別子タグを示します。
名前	IPS ルールの名前を示します。
説明	IPS ルールの説明を示します。 注意 Apex One Vulnerability Protection は Trend Micro Vulnerability Protection のスタンドアロンバージョンで使用されるオプションの設定をサポートしません。

データ	説明
アプリケーションの種類	IPS ルールがグループ化されるアプリケーションの種類を示します。
優先度	IPS ルールの優先レベルを示します。優先度の高いルールは、優先度の低いルールより前に適用されます。
重大度	トレンドマイクロがルールに割り当てる重大度レベルを示します。 注意 ルールの重大度は、ルールの実装方法または適用方法に影響しません。重大度レベルは、IPS ルールのリストを表示する場合にソート条件として使用できます。
モード	IPS モジュールによって使用されるネットワークエンジン検出モードを示します。モードをクリックして、ルールの設定を行います。
種類	検出された脆弱性の種類を示します。 • スマート: 既知または不明な脆弱性 (ゼロデイ攻撃など) • 攻撃コード: 既知の脆弱性に対する既知の攻撃コード (通常、署名ベース) • 脆弱性: 1 つ以上の攻撃コードが存在する可能性のある既知の脆弱性
発行済み	ルールの公開日 (ダウンロード日ではありません) を示します。
最終更新日	ルールが最後に変更された日時を示します。

表 3-6. 脆弱性情報

データ	説明
重大度	脆弱性の重大度レベルを示します。
CVSS スコア	National Vulnerability Database に登録されている脆弱性の Common Vulnerability Scoring System (CVSS) 重大度スコアを示します。 詳細については、http://nvd.nist.gov/cvss.cfm を参照してください。

データ	説明
説明	脆弱性の説明を示します。
外部参照先	脆弱性の詳細に関する外部参照先のリンクを示します。

デバイスコントロールで許可されたデバイス

すべての Apex One セキュリティエージェントのポリシー対象に適用されるデバイスコントロールで許可されたデバイスのリストをインポートまたはエクスポートします。

注意

- [デバイスコントロールで許可されたデバイス] リストに追加したデバイスにおける「ブロック」処理または「読み取り」処理を上書きするのは、情報漏えい対策オプションが有効になっているセキュリティエージェントのみです。
- [デバイスコントロールで許可されたデバイス] リストは、情報漏えい対策オプションが無効なセキュリティエージェントおよびデバイスコントロール権限が「ブロック」または「読み取り」に設定されていないセキュリティエージェントには適用されません。

項目	説明
インポート	すべての Apex One セキュリティエージェントエンドポイントで許可する全デバイスのリストが含まれた、適切な形式の CSV ファイルを選択します。 重要 新しいリストをインポートすると、前のリストが完全に上書きされます。既存のリストを保持するには、そのリストをエクスポートした後で、新しい CSV ファイルをインポートします。
前回のインポート	現在のリストがサーバにインポートされた日時を示します。

項目	説明
許可されたデバイスの総数	現在適用されているリストで許可されているデバイスの総数を示します。
エクスポート	現在の許可リストを CSV 形式でエクスポートします。

パート II

Apex Central

第 4 章

Apex Central ダッシュボードのウィジェット

本章では、Apex Central 管理コンソールダッシュボード固有のダッシュボードウィジェットについて説明します。

次のトピックがあります。

Apex Central 上位のファイルベースの脅威ウィジェット

このウィジェットでは、ネットワーク全体で検出されたエンドポイントにある上位の不正ファイルの分布を追跡し、ファイルベースの脅威 (ウイルスやスパイウェア/グレーウェア) の上位 10、25、または 50 件のいずれかの製品検出状況を表示します。

図内の任意のノードをクリックすると、詳細が表示された画面が開きます。Apex Central によってログクエリが実行され、詳細が表示されます。

ウィジェットに表示するデータの日付範囲を指定します。

- 今日
- 1 週間
- 2 週間
- 1 か月

ウィジェットに表示する脅威を指定します。このウィジェットに一度に表示できるファイルベースの脅威は 1 つのみです。初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。

ウィジェット上のウィジェット設定をクリックして、追加設定を表示します。

設定	説明
タイトル	フィールドに、ウィジェットの新しくわかりやすいタイトルを入力します。
範囲	ウィジェットによって表示されるデータの範囲を指定します。 この範囲により、ウィジェットにデータを表示する製品が決定されます。
上位の脅威	表示する脅威の数を指定します。

[保存] をクリックして変更を適用し、ウィジェットのデータを更新します。

エンドポイント保護の検証ウィジェット

このウィジェットには、統合された Active Directory 構造のエンドポイントの、Apex One と Deep Security による保護のステータスが表示されます。

重要

このウィジェットを使用する前に

- Apex One クライアントツリーを Active Directory ツリーと同期します。

  詳しい手順については、Apex One のドキュメントを参照してください。

- [運用管理] > [設定] > [エンドポイント保護の検証] に移動してウィジェットを有効にし、Active Directory サーバ、Apex One サーバ、および Deep Security サーバの接続設定を実行します。

設定アイコン (>) をクリックして、次の内容を設定します。

- Apex One サーバ: ウィジェットのデータの収集元となる Apex One サーバを指定するには、参照ボタン ( ) をクリックします。
- Deep Security サーバ: ウィジェットのデータソースに Deep Security サーバを指定するには、参照ボタン ( ) をクリックします。
- 列: ウィジェットでデータ表に表示する列を指定します。

Active Directory 構造の組織単位をクリックすると、次の情報が表示されます。

列	説明
コンピュータ	エンドポイント名が表示されます。
Apex One	エンドポイントが Apex One または VDI クライアントで保護されているかどうかが表示されます。
Deep Security	エンドポイントが Deep Security エージェントで保護されているかどうかが表示されます。
物理ホスト	仮想エンドポイントが配置されている物理サーバが表示されます。

列	説明
パターンファイル	Apex One または VDI クライアントが使用するパターンファイルのバージョンが表示されます。
検索エンジン	Apex One または VDI クライアントが使用する検索エンジンのバージョンが表示されます。
クライアントのバージョン	クライアントプログラムのバージョンが表示されます。
Deep Security プロファイル	使用中の Deep Security プロファイルが表示されます。
サーバ名	エンドポイントの接続先の Apex One サーバや Deep Security サーバが表示されます。

C&C コールバックを試行するホストウィジェット

このウィジェットには、一意の感染ホスト数の合計が表示され、C&C リストのソース別にこれらのホストがグループ化されます。

初期設定では、現在の日付のデータが表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。[今日]、[1 週間]、[2 週間]、または [1 か月] のデータを表示できます。

データ	説明
グローバルインテリジェンスに一致するホスト	トレンドマイクログローバルインテリジェンスネットワーク (Trend Micro Smart Protection Network など) によって検出された C&C コールバック。
動的アナライザに一致するホスト	動的アナライザ (仮想アナライザ、ネットワークコンテンツ検査エンジンなど) によって検出された C&C コールバック。 アナライザは、Deep Discovery Inspector や Apex One などの製品に組み込まれています。

データ	説明
管理下の製品のユーザ指定リストに一致するホスト	ユーザ定義リストを使用する製品によって検出された C&C コールバック。 ユーザ定義リストの例には、Deep Discovery Inspector の拒否リストなどがあります。

ポリシーステータス

このウィジェットには、ポリシーの配信ステータスが表示されます。

ポリシーの名前またはターゲットの数をクリックすると、新しい [ログクエリ] 画面が表示され、詳細情報を確認できます。

データ	説明
ポリシー	ポリシーの名前が表示されます。
配信ステータス	ポリシー設定に準拠する対象の割合が表示されます。
配信済み	ポリシー設定が適用されているか、アクティベートされていない製品サービスのある対象の数が表示されます。
保留中	ポリシー設定が適用されていない対象の数が表示されます。 注意 HotFix 2575 をインストールしていない場合、[保留中] 列にはオフラインエージェントを含む対象の数が含まれます。
オフライン	オフラインエージェントを含む対象の数を表示します。 重要 この機能には、Hotfix 2575 のインストールが必要です。インストールしていない場合、オフラインエージェントを含む対象の数は [保留中] 列に含まれ、[オフライン] 列は表示されません。

データ	説明
問題あり	サポートされていないポリシー配信、ポリシー設定なし、システムエラー、エンドポイントと製品サーバの通信エラー、サポートされていないエンドポイント、ローカルでの設定変更、無効になっている製品サービス、または部分配信が原因で、ポリシー設定が適用されていない対象の数が表示されます。
エンドポイント/製品 (ポリシーなし)	ポリシーが適用されていないエンドポイントまたは管理下の製品の数を表示します。
エンドポイント/製品の合計	管理者が管理可能なエンドポイントまたは管理下の製品の数を表示します。

クイック起動

このウィジェットには、[製品ディレクトリ] および [ポリシー管理] へのショートカットが表示されます。

一意の感染ホストの時間別推移ウィジェット

このウィジェットには、過去 30 日間に管理下の製品によってログに記録された一意の感染ホストが表示されます。

一意の感染ホストをグループ化し、円として表示します。円のサイズは感染ホストの数を相対的に表しています。

- 小: 1〜5
- 中: 6〜10
- 大: 11 以上

コンピュータアイコンまたはホスト名の上にカーソルを置くと、その他の感染ホストが表示されます。

選択したコールバックアドレスに対してコールバックを試行した感染ホストを表示するには、[コールバックアドレス] ドロップダウンを使用します。

注意

[コールバックアドレス] ドロップダウンには上位 25 件のコールバックアドレスが含まれます。

ウィジェットには、感染ホストから選択したコールバックアドレスに対して試行された最初のコールバックだけが表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下の製品を変更します。表示されるダイアログボックスで、 をクリックし、ソースとして使用する管理下の製品を選択して、[範囲] を指定します。

パート III

Apex One

第 5 章

Apex One ダッシュボードウィジェット

本章では、Apex Central で利用できる Apex One ダッシュボードウィジェットについて説明します。

次のトピックがあります。

Attack Discovery による検出ウィジェット

このウィジェットには、指定された期間に Endpoint Sensor の Attack Discovery 機能でリスクレベルに基づいて生成された検出ログが表示されます

重要
この機能を使用するには、有効な Endpoint Sensor ポリシーをエンドポイントに配信しておく必要があります。

[ルール名] をクリックすると、検出の詳細表示と、すべての関連オブジェクトが表示されます。[影響の診断] ボタンをクリックして、すべての関連オブジェクトを対象に履歴調査を実行することができます。

注意
履歴調査で実行できるのは、特定の条件の種類に基づいた診断のみです。Attack Discovery による検出ウィジェットから履歴調査を実行した場合、利用可能なデータがないオブジェクトは無視されます。

クイック調査ウィジェット

このウィジェットでは、ネットワーク全体の基本的な履歴調査を単一の条件タイプを使用して開始できます。

重要
この機能を使用するには、有効な Endpoint Sensor ポリシーをエンドポイントに配信しておく必要があります。

条件の種類を選択し、値を指定して、[影響の診断] をクリックします[履歴調査] 画面が開き、診断結果が表示されます。

注意

さらに複雑な診断を行うには、[履歴調査] 画面または [ライブ調査] 画面を使用します。

ブロック回数が多い上位のアプリケーション

このウィジェットには、ユーザがアクセスを試行した回数に基づいて、アプリケーションコントロールポリシーに違反している上位のアプリケーションの概要が表示されます。

表示されるアプリケーション数の初期設定を変更するには、設定ボタンを使用します。

IPS イベントの影響を受ける上位のエンドポイントウィジェット

このウィジェットでは、検出された IPS イベントにより特に大きな影響を受けるエンドポイントに関する情報が得られます。IPS イベントは、仮想パッチの IPS ルールによりトリガされます。

[期間] ドロップダウンを使用して、表示するデータの期間を選択します。

表示するエンドポイントの数の初期設定を変更するには、設定アイコン (>) を使用します。

データ	説明
エンドポイント	エンドポイントの名前を示します。
IP アドレス	エンドポイントの IP アドレスを示します。
検出数	エンドポイントで検出された IPS イベントの数を示します。

上位の IPS 攻撃元

このウィジェットでは、ネットワークで検出された IPS イベントについて、攻撃元の上位に関する情報が得られます。IPS イベントは、仮想パッチの IPS ルールによりトリガされます。

[期間] ドロップダウンを使用して、表示するデータの期間を選択します。

表示する攻撃元の数の初期設定を変更するには、設定アイコン (>) を使用します。

データ	説明
攻撃元	既知の攻撃元の IP アドレスを示します。
場所	攻撃元の場所を示します。
検出数	エンドポイントで検出された IPS イベントの数を示します。

上位の IPS イベント

このウィジェットでは、ネットワークで発生した IPS イベントを特に頻繁にトリガした IPS ルールに関する情報が得られます。IPS イベントは、仮想パッチの IPS ルールによりトリガされます。

[期間] ドロップダウンを使用して、表示するデータの期間を選択します。

このほか、2 番目のドロップダウンを使って検出や防御の上位 IPS イベントのみを表示することもできます。

表示する IPS ルールの数の初期設定を変更するには、設定アイコン (>) を使用します。

データ	説明
ルール名	IPS ルールの名前を示します。
重大度	トレンドマイクロがルールに割り当てる重大度レベルを示します。
合計	その IPS ルールによりトリガされた IPS イベントの数を示します。

違反が多い上位のアプリケーションコントロールの条件

このウィジェットには、ユーザが許可されていないアプリケーションへのアクセスを試行した回数に基づいて、違反が多い上位のアプリケーションコントロールの条件の概要が表示されます。

表示される一致件数の初期設定を変更するには、設定ボタンを使用します。

パート IV

Apex One サーバのポリシー設定

本章では、Apex One サーバのポリシー設定を管理する方法について説明します。

第 6 章

Apex One サーバのポリシー設定

本章では、Apex One サーバのポリシー設定を管理する方法について説明します。

Endpoint Sensors サーバを設定する

重要

- Endpoint Sensor 機能を使用するには、専用のライセンスが必要であるほか、追加のシステム要件を満たす必要があります。Endpoint Sensor のポリシーをエンドポイントに配信する前に、正しいライセンスがあることを確認してください。ライセンスの入手方法の詳細については、サポートプロバイダにお問い合わせください。
- サーバポリシーは、オンプレミスの Apex One サーバにのみ適用されます。

手順

1. [製品] で [Apex One サーバ] を選択します。
2. ポリシーを [作成] または [編集] します。
   a. ポリシーを作成するには、[作成] をクリックします。
   b. ポリシーを編集するには、[ポリシー] 列のポリシー名をクリックします。
3. [Endpoint Sensor] を設定します。

オプション	説明
最大メタデータストレージ	メタデータストレージで許容される最大サイズを指定します。サイズは 20〜20,480GB の間で指定します。ストレージサイズの初期設定は 1,024GB (1TB) です。メタデータストレージがこのサイズに達すると、サーバは新しいレコードに対応するために古いレコードを削除します。 **注意** Critical Patch 9601 以降のバージョンを搭載した Apex One では、ストレージサイズの初期設定は 400GB です。

オプション	説明
最大メモリ割り当て	メタデータキャッシュに割り当てられる最大メモリ容量を指定します。サイズは 4〜48GB の間で指定します。現在よりも大きいサイズを新しいサイズとして指定する必要があります。割り当てサイズの初期設定は 4GB です。 注意 メモリサイズは、データアップロードのパフォーマンスや調査速度に影響します。パフォーマンスを向上させるには、該当するサーバのメモリサイズを増やしてください。

4. [配信] または [保存] をクリックします。

パート V

Apex One セキュリティエージェントのポリシー

第 7 章

セキュリティエージェントプログラム設定

ここでは、エンドポイントにインストールしたセキュリティエージェントプログラムを管理する方法について説明します。

この章は次のトピックで構成されます。

追加サービス設定

セキュリティエージェントプログラムで特定の機能を正常に動作させるには、追加サービスを有効にする必要があります。次の表は、使用可能なサービスおよび各サービスを必要とする機能について説明しています。

サービス	説明	機能
不正変更防止サービス (TMBMSRV.exe)	アプリケーションの動作を制御し、プログラムの信頼性を検証します。	• 機械学習型検索 • 挙動監視 • デバイスコントロール • ソフトウェア安全性評価サービス • エージェントセルフプロテクション
ファイアウォールサービス (TmPfw.exe)	ネットワーク接続のアクセス権限を制御します。	• Apex One ファイアウォール
不審接続監視サービス	C&C コールバックに対する高度な保護を実現します。	• ユーザ指定の承認済みおよびブロック済み IP リスト • グローバル C&C IP リスト (ネットワークコンテンツ検査エンジン) • 不正プログラムネットワークフィンガープリント (適合度ルールパターンファイル)
情報漏えい対策オプションサービス (dsagent.exe)	機密データの高度な監視を実現し、エンドポイント上のデバイスアクセスを制限します。	• 情報漏えい対策 • デバイスコントロール (アクセスをブロック) • データ検出 (Apex Central コンソールを使用して管理)
高度な保護サービス (TMCCSF.exe)	高度な検索機能と保護機能を提供します。	• 機械学習型検索 • ブラウザ脆弱性対策 • 挙動監視

セキュリティエージェントの追加サービス設定

手順

1. 次のセクションの [Windows デスクトップ] または [Windows Server プラットフォーム] で必要なサービスを選択して有効にします。
   - 不正変更防止サービス
   - ファイアウォールサービス

     重要
     サービスを有効または無効にすると、エンドポイントが一時的にネットワークから切断されます。切断の影響を最小にするため、就業時間帯は設定の変更を避けてください。
   - 不審接続監視サービス
   - 情報漏えい対策オプションサービス

     重要
     サービスを有効または無効にすると、エンドポイントが一時的にネットワークから切断されます。切断の影響を最小にするため、就業時間帯は設定の変更を避けてください。
   - 高度な保護サービス

   重要
   Windows Server プラットフォームで追加のサービスを有効にすると、サーバのパフォーマンスが低下することがあります。Windows Server プラットフォームでサービスを有効にした後、しばらくはサーバを監視して、パフォーマンスへの影響がないことを確認することをお勧めします。

権限とその他の設定

セキュリティエージェント で、設定のカスタマイズ、通知メッセージの表示、およびセキュリティエージェントの重要なファイルとサービスの保護を行う権限をユーザに付与する設定を行います。

エージェント権限の設定

手順

1. 必要に応じて設定を行います。

セクション	設定
スタンドアロンモード	スタンドアロンモードの有効化: セキュリティエージェントでユーザが次の機能を無効にして、セキュリティエージェントのシステムパフォーマンスに悪影響が及ばないようにすることができます。 • セキュリティエージェントはサーバからポリシー設定を受け取りません。 • セキュリティエージェントはサーバから検索コマンドを開始しません。 • セキュリティエージェントはサーバにログを送信しません。 エンドユーザは、スタンドアロンモードのエージェントで検索やアップデートを手動で開始できます。
検索	• 手動検索の設定: セキュリティエージェントコンソールでユーザが [手動検索] の設定を行うことができます。 • リアルタイム検索の設定: セキュリティエージェントコンソールでユーザが [リアルタイム検索] の設定を行うことができます。 • 予約検索の設定: セキュリティエージェントコンソールでユーザが [予約検索] の設定を行うことができます。

セクション	設定
予約検索	• 予約検索の延期: ユーザが予約検索を延期するか、または実行中の検索を指定した期間停止できます。 注意 ユーザが実行中の検索を停止できるのは 1 回だけです。検索を再開すると、セキュリティエージェントはエンドポイント上のすべてのファイルを再検索します。 • 予約検索のスキップおよび停止: ユーザが実行中の予約検索を 1 回だけスキップまたは停止できます。 注意 予約検索を複数回スキップまたは停止することはできません。システムの再起動後も、次回の予約時刻に基づいて予約検索が再開されます。

セクション	設定
ファイアウォール	• セキュリティエージェントコンソールにファイアウォール設定を表示: セキュリティエージェントコンソールでユーザが [ファイアウォール] の設定を行うことができます。 • ユーザにファイアウォール/IDS/警告メッセージの有効化/無効化の変更を許可: セキュリティエージェントのシステムトレイアイコンに、ファイアウォールの有効化/無効化および IDS モードの有効化/無効化のメニューオプションを表示します。 **注意** Apex One のファイアウォールは、ステートフルインスペクション、高性能なネットワークウイルス検索、および駆除機能を使用して、ネットワーク上のエージェントとサーバを保護します。ファイアウォールとその機能を有効化または無効化する権限をユーザに付与する場合、エンドポイントが侵入やハッカーの攻撃にさらされることを防ぐため、長期間ファイアウォールを無効にしないよう、ユーザに注意してください。 • セキュリティエージェントに Apex One サーバへのファイアウォールログの送信を許可: サーバにファイアウォールログを送信するようにセキュリティエージェントを設定し、ネットワークトラフィックを分析できるようにします。
挙動監視	セキュリティエージェントコンソールに挙動監視設定を表示: セキュリティエージェントコンソールでユーザが [挙動監視] の設定を行うことができます。
信頼済みプログラムリスト	セキュリティエージェントコンソールに信頼済みプログラムリストを表示: セキュリティエージェントコンソールでユーザが [信頼済みプログラムリスト] の設定を行うことができます。

セクション	設定
メール検索	セキュリティエージェントコンソールにメール検索設定を表示: セキュリティエージェントコンソールでユーザが [メール検索] の設定を行うことができます。 有効にすると、メールサーバから取得した、不正な脅威を含む POP3 メールメッセージをリアルタイム検索で検出して処理を実行できます。
プロキシ設定	ユーザにプロキシの設定を許可: 次の場合にのみ、ユーザのプロキシ設定を使用できます。 • セキュリティエージェントで「今すぐアップデート」が実行された場合。 • ユーザが自動プロキシ設定を無効にした場合、またはセキュリティエージェントで自動プロキシ設定を検出できない場合。  警告! ユーザによるプロキシ設定に誤りがあると、アップデート時に問題が発生することがあります。プロキシ設定権限をユーザに付与する際には、注意するよう指示してください。
コンポーネントアップデート	• 「今すぐアップデート」の実行: セキュリティエージェントのシステムトレイアイコンに、[今すぐアップデート] メニューオプションを表示します。 • 予約アップデートの有効化/無効化: セキュリティエージェントのシステムトレイアイコンに、[予約アップデートの有効化/無効化] メニューオプションを表示します。  注意 セキュリティエージェントのメニューにこのメニュー項目が表示されるようにするには、管理者が [その他の設定] タブで [セキュリティエージェントでの予約アップデートの有効化] を選択する必要があります。

セクション	設定
アンロードとロック解除	セキュリティエージェントのアンロードとロック解除権限を持つユーザは、パスワードの有無に関係なく、セキュリティエージェントを一時的に停止することも、高度な Web コンソール機能にアクセスすることもできます。 • パスワードを要求しない • パスワードを要求する: 必要なパスワードと確認用のパスワードを入力します。 注意 パスワードは以下の複雑さの要件を満たしている必要があります。 • 8〜32 文字の長さ • 大文字 (A〜Z)、小文字 (a〜z)、数字 (0〜9)、特殊文字をそれぞれ 1 文字以上含む • 印刷できない ASCII 文字を含まない 重要 [パスワードを要求する] を選択してパスワードを指定しなかった場合は、Apex Central によって次の初期設定のパスワードが適用されます。 • Apex One: サーバインストール時に指定されたパスワード • Apex Oneas a Service: コンソールのプロビジョニングに使用されたアカウント名

セクション	設定
アンインストール	セキュリティエージェントのアンインストール権限を持つユーザは、ローカルエンドポイントのセキュリティエージェントプログラムをアンインストールできます。 • パスワードを要求しない • パスワードを要求する: 必要なパスワードと確認用のパスワードを入力します。 注意 パスワードは以下の複雑さの要件を満たしている必要があります。 • 8〜32 文字の長さ • 大文字 (A〜Z)、小文字 (a〜z)、数字 (0〜9)、特殊文字をそれぞれ 1 文字以上含む • 印刷できない ASCII 文字を含まない 重要 [パスワードを要求する] を選択してパスワードを指定しなかった場合は、Apex Central によって次の初期設定のパスワードが適用されます。 • Apex One: サーバインストール時に指定されたパスワード • Apex Oneas a Service: コンソールのプロビジョニングに使用されたアカウント名

その他のエージェント設定

手順

1. 必要に応じて設定を行います。

セクション	設定
限定機能モードエージェントの変換	限定機能モードのセキュリティエージェントをフル機能モードのセキュリティエージェントに恒久的に変換する:「限定機能モード」でインストールされたセキュリティエージェントですべての機能を有効にします。 重要 この処理を取り消すことはできません。限定機能モードのセキュリティエージェントをフル機能のセキュリティエージェントに変換すると、エージェントプログラムは対象のエンドポイントにインストールされている互換性のない他社製セキュリティソフトウェアをアンインストールします。変換が完了すると、Apex One はセキュリティエージェントの通常の機能に関連する必要なサービスと機能をすべて有効にします。 変換後のエンドポイントで限定機能モードのセキュリティエージェントを使用する必要がある場合は、セキュリティエージェントプログラムをアンインストールしてから限定機能モードのセキュリティエージェントを再インストールしてください。

セクション	設定

アップデート設定	• セキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロード: 指定されたアップデート元に接続できないセキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートを試行するように設定します。
	• セキュリティエージェントでの予約アップデートの有効化: 初期設定で予約アップデートが有効になるようにすべてのセキュリティエージェントを設定します。
	• セキュリティエージェントがアップデートするコンポーネント: セキュリティエージェントにおけるコンポーネントのアップデート方法を制御します。
	  • すべてのコンポーネント (HotFix とエージェントプログラムを含む): セキュリティエージェントはすべてのコンポーネントをアップデートします。
	  • パターンファイル、エンジン、ドライバ: セキュリティエージェントはセキュリティエージェントプログラムのバージョンアップまたは HotFix の配信を行いません。
	  • パターンファイル: セキュリティエージェントはセキュリティエージェントプログラムのバージョンアップ、HotFix の配信、またはエンジンとドライバのアップデートを行いません。

Web レピュテーション設定	Web サイトのブロック時に通知を表示: Web レピュテーションポリシーに違反する URL をブロックした後に、セキュリティエージェントに通知メッセージを表示します。
挙動監視設定	プログラムをブロックした場合、通知を表示: 挙動監視ポリシーに違反するプログラムをブロックした後に、セキュリティエージェントに通知メッセージを表示します。
C&C コンタクトアラート設定	C&C コールバックが検出された場合、通知を表示: C&C コールバックが検出された後に、セキュリティエージェントに通知メッセージを表示します。
隔離の一括復元通知設定	隔離ファイルの復元時に通知を表示: 隔離ファイルの復元後に、セキュリティエージェントに通知メッセージを表示します。
機械学習型検索設定	脅威の検出時に通知を表示: 機械学習型検索で未知の脅威が検出された後に、セキュリティエージェントに通知メッセージを表示します。

セクション	設定
セキュリティエージェントセルフプロテクション	• セキュリティエージェントサービスを保護する: ユーザまたはアプリケーションがセキュリティエージェントサービスを終了できないようにします。 • セキュリティエージェントのインストールフォルダ内のファイルを保護する: ユーザまたはアプリケーションがセキュリティエージェントのインストールフォルダ内のファイルを変更したり削除したりできないようにします。 • セキュリティエージェントのレジストリキーを保護する: ユーザまたはアプリケーションがセキュリティエージェントプログラムで使用するレジストリ値を変更、削除、追加できないようにします。 • セキュリティエージェントプロセスを保護する: ユーザまたはアプリケーションがセキュリティエージェントプロセスを終了できないようにします。 詳細については、153 ページの「セキュリティエージェントセルフプロテクション」を参照してください。
予約検索設定	予約検索の実行前に通知を表示する: 設定された予約検索の開始前に、セキュリティエージェントに通知メッセージを表示します。
検索用のキャッシュ設定	• デジタル署名キャッシュを有効にする: 挙動監視のデジタル署名パターンファイルを使用して手動検索、予約検索、および ScanNow からファイルを除外するようにセキュリティエージェントを設定します。 • 手動検索のキャッシュを有効にする: 検索のパフォーマンスを向上するために、ローカルの手動検索キャッシュを保持し、手動検索、予約検索、および ScanNow の実行中にファイルを除外するようにセキュリティエージェントを設定します。 詳細については、156 ページの「検索用のキャッシュ設定」
POP3 メール検索設定	POP3 メール検索: セキュリティエージェントで POP3 メール検索を有効にします。 詳細については、158 ページの「POP3 メール検索」を参照してください。

セクション	設定
セキュリティエージェントアクセス制限	システムトレイあるいは Windows スタートメニューからセキュリティエージェントコンソールへのアクセスを許可しない: ユーザがシステムトレイまたは Windows スタートメニューを使用してセキュリティエージェントコンソールにアクセスできないようにします。 注意 この設定によってセキュリティエージェントが無効になることはありません。セキュリティエージェントは引き続きバックグラウンドで動作し、セキュリティリスクからコンピュータを保護します。
再起動の通知	感染ファイルの駆除処理を完了するためにエンドポイントの再起動が必要な場合に通知を表示: 不正ファイルの駆除処理を完了するためにユーザがエンドポイントを再起動する必要がある場合に、セキュリティエージェントに通知メッセージを表示します。

セキュリティエージェントセルフプロテクション

セキュリティエージェントセルフプロテクションは、セキュリティエージェントが正常に機能するために必要なプロセスおよびその他のリソースを保護し、プログラムやユーザが不正プログラム対策保護を無効にしようとする試みを阻止するのに役立ちます。

セキュリティエージェントサービスを保護する

Apex One では、次のセキュリティエージェントサービスを停止しようとする操作をすべてブロックします。

- Apex One NT Listener (`TmListen.exe`)
- Apex One NT RealTime Scan (`NTRtScan.exe`)
- Apex One NT Firewall (`TmPfw.exe`)
- Trend Micro Apex One Data Protection Service (`dsagent.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

注意

このオプションを有効にすると、エンドポイントへの他社製品のインストールがセキュリティエージェントによって阻止されることがあります。この問題が発生した場合は、このオプションを一時的に無効にして他社製品をインストールし、その後再びこのオプションを有効化してください。

- Apex One Common Client Solution Framework (TmCCSF.exe)

セキュリティエージェントのインストールフォルダ内のファイルを保護する

他のプログラムまたはユーザによりセキュリティエージェントのファイルが変更または削除されないようにするには、Apex One で <エージェントインストールフォルダ> のルートにある次のファイルをロックします。

- 拡張子が.exe、.dll、および.sys のデジタル署名ファイル
- 次のファイルを含む、デジタル署名のない一部のファイル
  - bspatch.exe
  - bzip2.exe
  - INETWH32.dll
  - libcurl.dll
  - libeay32.dll
  - libMsgUtilExt.mt.dll
  - msvcm80.dll
  - MSVCP60.DLL
  - msvcp80.dll
  - msvcr80.dll
  - OfceSCV.dll
  - OFCESCVPack.exe
  - patchbld.dll
  - patchw32.dll
  - patchw64.dll
  - PiReg.exe
  - ssleay32.dll
  - Tmeng.dll
  - TMNotify.dll
  - zlibwapi.dll

セキュリティエージェントのレジストリキーを保護する

セキュリティエージェントでは、次のレジストリキーおよびサブキーの下のエントリを変更、削除、または新規追加しようとする操作をすべてブロックします。

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP

セキュリティエージェントプロセスを保護する

セキュリティエージェントでは、次の表のプロセスを停止しようとする操作をすべてブロックします。

プロセス	説明
TmListen.exe	Apex One サーバからコマンドと通知を受信して、セキュリティエージェントからサーバへの通信を制御します。
NTRtScan.exe	セキュリティエージェントでリアルタイム検索、予約検索、および手動検索を実行します。
TmPfw.exe	パケットレベルファイアウォール、ネットワークウイルス検索および侵入検知機能を提供します。
TMBMSRV.exe	外部ストレージデバイスへのアクセスを規制し、レジストリキーおよびプロセスへの不正な変更を回避します。
DSAgent.exe	機密データの転送を監視し、デバイスへのアクセスを管理します。
PccNTMon.exe	セキュリティエージェントコンソールを起動します。
TmCCSF.exe	ブラウザ脆弱性対策およびメモリ検索を実行します。

さらに、セキュリティエージェントでは Microsoft のソフトウェア制限ポリシー (SRP) へのプロセスの追加も防止することができます。ソフトウェア制限ポリシーに指定されたアプリケーションは、エンドポイントで実行できません。ソフトウェア制限ポリシーにセキュリティエージェントプロセスが追加されないようにするには、次の手順を実行します。

1. [セキュリティエージェントプロセスを保護する] を有効にします。
2. [不正変更防止サービス] を有効にします。

検索用のキャッシュ設定

セキュリティエージェントでは、検索パフォーマンスを向上するために、デジタル署名や手動検索のキャッシュファイルを作成できます。手動検索の実行時、セキュリティエージェントでは最初にデジタル署名キャッシュファイルが確認され、次に検索から除外するファイルについて手動検索キャッシュファイルが確認されます。検索で多数のファイルが除外されている場合、検索時間は短くなります。

デジタル署名のキャッシュ

デジタル署名キャッシュファイルは、手動検索、予約検索、および ScanNow の実行時に使用されます。エージェントでは、ファイルの署名がデジタル署名キャッシュファイルに追加されている場合、そのファイルは検索されません。

セキュリティエージェントでは、挙動監視に使用される同じデジタル署名パターンファイルを使用して、デジタル署名キャッシュファイルが作成されます。デジタル署名パターンファイルには、トレンドマイクロが信頼できると見なした、検索から除外可能なファイルのリストが含まれています。

注意

Windows Server プラットフォームでは挙動監視は自動的に無効となります。デジタル署名キャッシュを有効にした場合、これらのプラットフォームにインストールされているセキュリティエージェントでは、キャッシュで使用するデジタル署名パターンファイルがダウンロードされ、その他の挙動監視コンポーネントはダウンロードされません。

エージェントでは、スケジュールに従ってデジタル署名キャッシュファイルが作成されます。このファイルは Web コンソールから設定できます。エージェントでは、次の目的でキャッシュが作成されます。

- 最後にキャッシュファイルが作成されてからシステムに導入された、新しいファイルの署名を追加します。
- 変更されたファイルやシステムから削除されたファイルの署名を削除します。

エージェントでは、キャッシュの作成プロセスの間、次のフォルダで信頼できるファイルが確認され、これらのファイルの署名がデジタル署名キャッシュファイルに追加されます。

- %PROGRAMFILES%
- %WINDIR%

キャッシュの作成プロセスは、最小限のシステムリソースしか使用しないため、エンドポイントのパフォーマンスに影響しません。エージェントでは、何らかの理由 (ホストコンピュータの電源が切断された場合や、ワイヤレスエンドポイントの AC アダプタのプラグが抜かれた場合など) で中断されたキャッシュの作成タスクを再開することもできます。

手動検索のキャッシュ

手動検索キャッシュファイルは、手動検索、予約検索、および ScanNow の実行時に使用されます。セキュリティエージェントでは、ファイルのキャッシュが手動検索キャッシュファイルに追加されている場合、そのファイルは検索されません。

検索を実行するたびに、セキュリティエージェントでは、脅威を含まないファイルのプロパティが確認されます。脅威を含まないファイルが特定の期間変更されていない場合 (この期間は変更可能)、セキュリティエージェントでは、このファイルのキャッシュが手動検索キャッシュファイルに追加されます。次の検索の実行時、キャッシュが期限切れになっていなければ、そのファイルは検索されません。

脅威を含まないファイルのキャッシュは、設定された期間を経過すると期限切れになります (この期間も設定可能です)。キャッシュの期限切れ以降に検索が発生した場合、セキュリティエージェントでは、期限切れキャッシュが削除され、ファイルが脅威について検索されます。ファイルが脅威を含まないファイルで、変更されないままの場合、そのファイルのキャッシュがオンデマンドの検索キャッシュファイルに再度追加されます。ファイルが脅威を含まないファイルで、最近変更されている場合、そのファイルのキャッシュは追加されず、そのファイルは次回の検索で再度検索されます。

脅威を含まないファイルのキャッシュは、感染したファイルが検索から除外されないように、期限が定められています。

- 極端に古いパターンファイルは、感染している未変更のファイルを、脅威を含まないファイルとして処理する場合があります。キャッシュが期

限切れにならなければ、この感染ファイルは、変更されてリアルタイム検索で検出されるまでシステム内に残されます。

- キャッシュのファイルが変更され、リアルタイム検索がファイルの変更時に機能しない場合は、キャッシュを期限切れにして、変更されたファイルに対して脅威を検索する必要があります。

手動検索キャッシュファイルに追加されるキャッシュの数は、検索の種類や検索対象によって変わります。たとえば、手動検索でエンドポイント内の 1,000 ファイルのうち 200 ファイルしか検索されなければ、キャッシュの数は少なくなります。

手動検索を頻繁に実行する場合は、手動検索キャッシュファイルによって検索時間が大幅に削減されます。すべてのキャッシュが期限切れでない検索タスクでは、通常 12 分かかる検索が 1 分に削減される場合もあります。ファイルが変更されない日数を減らすことと、キャッシュの期限を延ばすことは、多くの場合パフォーマンスを向上させます。比較的短い時間はファイルは変更されないため、多くのキャッシュがキャッシュファイルに追加される可能性があります。また、キャッシュの期限を長くすることは、より多くのファイルが検索でスキップされることを意味します。

手動検索をほとんど実行しない場合は、次の検索の実行時にキャッシュが期限切れになっている可能性があるため、手動検索キャッシュを無効にすることができます。

POP3 メール検索

セキュリティエージェントにメール検索権限がある場合、セキュリティエージェントコンソールに [メール検索] オプションが表示されます。[メール検索] オプションには、POP3 メール検索が表示されます。

次の表は、POP3 メール検索プログラムについて説明しています。

表 7-1. メール検索プログラム

詳細	説明
目的	POP3 メールメッセージでウイルス/不正プログラムを検索します。

詳細	説明
前提条件	• ユーザが使用するためには、管理者が Web コンソールで有効にする必要があります。 注意 POP3 メール検索を有効にするには、[セキュリティエージェントコンソールにメール検索設定を表示] の権限を有効にする必要があります。 詳細については、144 ページの「エージェント権限の設定」を参照してください。 • ウイルス/不正プログラムに対する処理は、セキュリティエージェントコンソールから設定可能ですが、Web コンソールからは設定できません。
サポートされている検索の種類	リアルタイム検索 メールメッセージが POP3 メールサーバから取得されたときに検索が実行されます。
検索結果	• 検索の完了後に参照できる、検出されたセキュリティリスクに関する情報 • 検索結果はセキュリティエージェントコンソールの [ログ] 画面に表示されない • 検索結果はサーバに送信されない

アップデートエージェント

コンポーネント、ドメイン設定、エージェントプログラム、または HotFix をセキュリティエージェントに配信するタスクを分散するために、セキュリティエージェントをアップデートエージェントに設定し、他のセキュリティエージェントのアップデート元に指定することが可能です。これにより、セキュリティエージェントは適切なタイミングでアップデートを受信でき、Apex One サーバに大量のネットワークトラフィックが集中することもありません。

ネットワークが場所によってセグメント化され、セグメント間のネットワークリンクに大量のトラフィックの負荷がかかっている場合には、それぞれの場所に少なくとも 1 つアップデートエージェントを割り当ててください。

注意

アップデートエージェントからコンポーネントをアップデートするために割り当てられたセキュリティエージェントは、アップデートエージェントから最新コンポーネントおよび設定のみを受信します。ただし、すべてのセキュリティエージェントは Apex One サーバにステータスを報告します。

セキュリティエージェントのアップデートエージェントとしての割り当て

手順

1. アップデートエージェントで共有可能な項目を選択します。
   - コンポーネントのアップデート
   - ドメイン設定
   - セキュリティエージェントプログラムと HotFix

第 8 章

アプリケーションコントロールのポリシー設定

このセクションでは、セキュリティエージェントでアプリケーションコントロールポリシーを設定する方法について説明します。

次のトピックがあります。

アプリケーションコントロール

アプリケーションコントロールを使用すると、特定のエンドポイントの特定のアプリケーションにアクセスできるユーザを管理できます。全体的なエンドポイントベースのポリシーを作成したり、Active Directory と統合されている場合はエンドポイントごとに細かいユーザベースのポリシーを作成したりできます。

ポリシーの対象範囲を決定した後、アプリケーションの一致条件を作成して、どのアプリケーションを許可、ブロック、または監視するかを定義できます。上級ユーザの場合は、「ロックダウン」条件を作成して、信頼されたアプリケーションの実行のみを許可し、ルールで明示的に許可されていないアプリケーションすべてをブロックできます。

アプリケーションコントロールの設定 (エージェント)

アプリケーションコントロールポリシーを設定する前に、必要なアプリケーションコントロールの条件をすべて定義するようにしてください。アプリケーションコントロールポリシーには、エンドポイントまたは特定のユーザに対して「許可」または「ブロック」するアプリケーションを定義する、事前設定された条件の使用が必要となります。

詳細については、76 ページの「アプリケーションコントロールの条件」を参照してください。

手順

1. [アプリケーションコントロールを有効にする] を選択します。
2. [ユーザ定義ルール] セクションで、ログオンしたユーザアカウントに基づいてエンドポイントにルールを割り当てます。

重要

- ユーザベースのアプリケーションコントロールを使用できるのは、Active Directory を統合済みの場合のみです。Active Directory を統合していない場合は、初期設定の「すべてのユーザアカウント」ルールのみに条件を割り当てることができます。
- 初期設定の「すべてのユーザアカウント」ルールは削除できません。

a. 新しいルールを追加するか、既存のルールを変更します。

- 新しいルールを追加するには、[ルールの割り当て] をクリックします。
- 既存のルールを変更するには、表の [ユーザアカウント] 列にある値をクリックします。

[ルールの割り当て] 画面が表示されます。

b. 特定のアプリケーションコントロールの条件を適用する [ユーザアカウント] を指定します。

重要

- ユーザベースのアプリケーションコントロールを使用できるのは、Active Directory を統合済みの場合のみです。Active Directory を統合していない場合は、初期設定の「すべてのユーザアカウント」ルールのみにルールを割り当てることができます。
- ルールごとに最大 30 のユーザまたはグループを割り当てることができます。1 つのポリシーにより多くのユーザを割り当てる必要がある場合は、追加のルールを作成してください。

---

c. 必要な条件の [名前] をクリックして、その条件を [選択した条件] 表に移動します。

d. [保存] をクリックします。

注意

ルールの優先順位を変更するには、変更するルールを選択し、リスト内の別の場所にドラッグしてください。アプリケーションコントロールは、複数のルールに含まれているユーザに最初の一致ルールを適用します。

---

3. [追加処理] セクションで、ユーザが [ユーザ定義ルール] のいずれの条件とも一致しないアプリケーションの実行を試みた場合にアクションコントロールで実行する処理を指定します。

- 許可: 他のすべてのアプリケーションの実行を許可: アプリケーションコントロールは、[ユーザ定義ルール] のいずれの条件とも一致しないアプリケーションに対して何も実行しません。アプリケーションコントロールを使用してアプリケーションの利用をブロックまたは監視する場合に選択します。
- ロックダウン: 前回のインベントリ検索で確認できなかったアプリケーションをすべてブロック: エンドポイントがこのコマンドを受信すると、アプリケーションコントロールは以下の処理を実行します。

  a. アプリケーションコントロールは、エンドポイント内を検索して完全なアプリケーションインベントリを作成します。

  b. アプリケーションコントロールにより、エンドポイントは「ロックダウン」され、以下のアプリケーションへのアクセスが禁止されます。

     - [ユーザ定義ルール] の表で定義された許可条件と正確に一致しないアプリケーション
     - [ユーザ定義ルール] の表で定義された診断条件と正確に一致しないアプリケーション
     - 特定のエンドポイントに対するインベントリ検索の結果にないアプリケーション

  - トレンドマイクロの信頼済みベンダのアプリケーションを除外: 信頼済みベンダのアプリケーションであるとトレンドマイクロの脅威の専門家が判断したアプリケーションをすべて自動的に許可する場合に選択します。
  - 診断モードを有効にする: ロックダウンの適用時に実行が明示的に許可されていないがブロックもされていないアプリケーションへのアクセスをログに記録する場合に選択します。

ヒント

許可ルールに追加しなかったすべてのアプリケーションへのアクセスを完全にブロックする前に、ユーザがどのアプリケーションを必要としているかを特定する場合に、診断モードを使用します。

4. [エージェント通知] セクションで、[アプリケーションがブロックされたときに通知を表示] を選択し、アプリケーションコントロールによってアプリケーションがブロックされたときにエンドポイントで通知が表示されるようにします。

5. [ログ管理] セクションで、次の情報を指定します。

   - ログの最大保存期間 (日数): エンドポイントでログデータが保持される最大日数を指定します。
   - セキュリティエージェントで 1 時間ごとに送信できるログの条件あたりの最大数: 各条件ルールについて、1 つのセキュリティエージェントから Apex One サーバに 1 時間ごとに送信できるログの最大数を指定します。

   注意

   セキュリティエージェントの数やネットワーク設定によっては、サーバに大量のネットワークトラフィックが送られ、パフォーマンスの低下を招く恐れがあります。

重要

別の画面に移動する前に、必ず Apex One セキュリティエージェントポリシーの [配信] または [保存] を実行してください。ポリシー全体を保存しない場合は、変更内容がすべて失われます。

第 9 章

挙動監視ポリシー設定

ここでは、セキュリティエージェントで挙動監視ポリシーを設定する方法について説明します。

この章は次のトピックで構成されます。

挙動監視

挙動監視機能は、エンドポイントの OS またはインストールされたソフトウェアに対して不審な変更が行われていないかどうかを常に監視します。挙動監視では、「不正プログラム挙動ブロック」と「イベント監視」によってエンドポイントが保護されます。さらにこの 2 つの機能を補うものとして、ユーザが設定する「除外リスト」と、「ソフトウェア安全性評価サービス」が使用されます。

重要

Windows Server コンピュータでは、いずれのバージョンでも初期設定で挙動監視が無効になっています。

不正プログラム挙動ブロック

不正プログラム挙動ブロックにより、不正プログラムの挙動を示すプログラムからの追加の脅威に対する保護に必要な層を提供します。不正プログラム挙動ブロックは長時間にわたり、システムイベントを観察します。プログラムが通常とは異なるシーケンスまたは組み合わせの処理を実行すると、不正プログラム挙動ブロックが既知の不正プログラムの挙動を検出して、関連プログラムをブロックします。この機能を使用すると、新たに出現した脅威に対する保護のレベルを向上できます。

不正プログラム挙動監視は次の脅威レベルの検索オプションを提供します。

- 既知の脅威:既知の不正プログラムの脅威に関連付けられた挙動をブロックします。
- 既知および潜在的な脅威: 既知の脅威に関連付けられた挙動をブロックし、潜在的に不正な挙動に対して処理を実行します。

通知が有効になっているプログラムをブロックした後、セキュリティエージェントはエンドポイントに通知を表示します。

ランサムウェア対策

ランサムウェア対策は、「ランサムウェア」によるエージェント上のファイルの不正な変更や暗号化を防止します。ランサムウェアは不正プログラムの一種で、ファイルへのアクセスを制限し、ファイルの復元と引き換えに金銭を要求してきます。

Apex One には、ランサムウェアの脅威から環境を保護する対策として次のオプションが用意されています。

注意

セキュリティエージェントで安全なプロセスが不正プロセスとして検出される確率を少なくするには、エージェントがインターネットにアクセスし、トレンドマイクロのサーバを使用してその他の検証プロセスを実行できるようにします。

オプション	説明
不正な暗号化や変更から文書を保護	ランサムウェアの可能性のある特定のイベントシーケンスを検出するように、挙動監視を設定できます。セキュリティエージェントは、次のすべての条件に該当する場合、不正なプログラムを終了して隔離を試みます。 1. 一定期間内に 3 つのファイルを変更、削除、または名前変更しようとする、安全と認識されていないプロセス 2. 保護されているファイルの拡張子の種類を変更しようとしたプロセス さらに、[不審なプログラムによって変更されたファイルを自動的にバックアップして復元] を有効にすると、ランサムウェアによって暗号化の対象とされやすいファイルのコピーが事前にエンドポイントに作成されます。暗号化プロセスの完了後に Apex One でランサムウェアの脅威が検出されると、影響を受けたファイルの復元を求めるメッセージが表示され、事前にバックアップされていたファイルを復元する事で、データを失うリスクを低減できます。 注意 自動ファイルバックアップを実行するには、クライアントエンドポイントに 100MB 以上のディスク容量が必要です。また、バックアップされるのは 10MB 未満のファイルだけです。 エージェントエンドポイントのバックアップフォルダの場所は、<エージェントインストールフォルダ>¥CCSF¥module¥DRE¥data です。 警告! [不審なプログラムによって変更されたファイルを自動的にバックアップして復元] を有効にしないと、Apex One で新しいランサムウェアの脅威による攻撃を最初に受けたファイルを回復できません。

オプション	説明
ランサムウェアに関連付けられていることの多いプロセスをブロック	多くのランサムウェアは、エンドポイントの特定の場所に実行可能ファイルとして侵入し、ファイルのハイジャックを試みます。該当する場所から開始されるプロセスをブロックすることで、ランサムウェアによるファイルのハイジャックを回避できます。
プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック	プログラム検査は、プロセスを監視して API フックを行うことで、予期しない挙動を示すプログラムを特定します。これにより、不正な実行可能ファイルの全体的な検出率が高くなりますが、システムのパフォーマンスが下がる場合があります。 ヒント [ブロックする脅威] リストから [既知の脅威と潜在的な脅威] を選択すると、プログラム検査によるセキュリティが向上します。

脆弱性対策

脆弱性対策は、プログラム検査と連携して機能し、プログラムの挙動を監視して、プログラムの脆弱性を悪用した攻撃の疑いがある異常な動作を検出します。不審な動作が検出されると、挙動監視によってプログラムのプロセスが終了されます。

重要
脆弱性対策を使用するには、[プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック] を選択する必要があります。

新たに検出されたプログラム対策

挙動監視は Web レピュテーションサービスおよびリアルタイム検索と連携して機能し、Web チャネル、メールアプリケーション、または Microsoft Office マクロスクリプト経由でダウンロードされたファイルの普及度を確認します。「新たに検出された」ファイルが検出された後に、管理者は、ユーザがファイルを実行する前にユーザに確認を求めるように設定することができます。トレンドマイクロでは、ファイルの検出数、または Smart Protection Network により特定されたファイルの存続期間に基づいて、新たに検出されたプログラムを分類します。

挙動監視は各チャネルで次のファイルタイプを検索します。

- Web (HTTP/HTTPS): .exe ファイルを検索します。
- メールアプリケーション: .exe ファイル、および暗号化されていない.zip ファイルや.rar ファイルに含まれる圧縮された.exe ファイルを検索します。

注意

- このプロンプトが表示される前にセキュリティエージェントで HTTP/HTTPS トラフィックを検索できるようにするためには、管理者はエージェントの Web レピュテーションサービスを有効にする必要があります。
- セキュリティエージェントは、処理実行中にメールアプリケーションを介してダウンロードされたファイル名を一致させます。ファイル名が変更されると、ユーザにプロンプトは表示されません。

イベント監視

イベント監視は、不正なソフトウェアおよび不正なプログラムによる攻撃に対して保護するためのより一般的なアプローチを提供します。イベント監視では、システムエリアで特定のイベントを監視して、管理者がこのようなイベントを実行するプログラムを制御できるようにします。不正プログラム挙動ブロックで提供される保護を超える特別なシステム要件がある場合は、イベント監視を使用してください。

次の表は監視対象のシステムイベントの一覧を示しています。

表 9-1. 監視対象のシステムイベント

イベント	説明
AI アプリ対策	このポリシーを設定し、AI 統合アプリケーションおよび関連ファイルを悪意のある改変から保護してください。
システムファイルの複製	多くの不正プログラムは、Windows システムファイルが使用しているファイル名を使って、自分自身または他の不正プログラムのコピーを作成します。これは、通常、システムファイルの上書きまたは置換、検出の回避、またはユーザによる不正ファイルの削除を阻止する目的で実行されます。

イベント	説明
Hosts ファイルの変更	Hosts ファイルは、ドメイン名と IP アドレスを比較し、一致しているかどうかを確認します。不正プログラムの多くは、感染した Web サイト、存在しない Web サイト、または偽の Web サイトに Web ブラウザをリダイレクトするように Hosts ファイルを変更します。
不審な挙動	不審な挙動とは、正規プログラムではまれにしか実行されない特定の処理または処理グループです。不審な挙動を示すプログラムは、注意して使用する必要があります。
Internet Explorer プラグインの追加	スパイウェア/グレーウェアは、多くの場合、ツールバーやブラウザヘルパーオブジェクトを含む不要な Internet Explorer プラグインをインストールします。
Internet Explorer 設定の変更	不正プログラムは、ホームページ、信頼する Web サイト、プロキシサーバの設定、メニュー拡張などの Internet Explorer の設定を変更することがあります。
セキュリティポリシー設定の変更	Windows セキュリティポリシーを変更して、不要なアプリケーションを実行し、システム設定を変更させる場合があります。
DLL (プログラムライブラリ) インジェクション	不正プログラムの多くは、すべてのアプリケーションがプログラムライブラリ (DLL) を自動的にロードするように、Windows を設定します。これにより、アプリケーションが起動するたびに、DLL 内の不正なルーチンが実行されるようになります。
シェル設定の変更	多くの不正プログラムは、Windows シェルの設定を変更し、それらを特定のファイルタイプに関連付けます。ユーザが Windows エクスプローラで関連付けられたファイルを開くと、このルーチンによって不正プログラムが自動的に起動します。不正プログラムは、Windows シェルの設定を変更することで、使用されているプログラムの追跡を可能にしたり、正規のアプリケーションと一緒に自身を起動できるようにしたりします。
サービスの追加	Windows サービスは特殊な機能を持ち、通常はフル管理アクセス権でバックグラウンドで継続して実行されるプロセスです。不正プログラムは、自身をサービスとしてインストールし、隠れた状態のままでいることがあります。

イベント	説明
システムファイルの変更	特定の Windows システムファイルは、スタートアッププログラムやスクリーンセーバの設定を含む、システムの挙動を決定します。多くの不正プログラムは、システムファイルを変更することで、スタートアップ時に自動的に起動し、システムの挙動を制御できるようにします。
ファイアウォールポリシー設定の変更	Windows ファイアウォールポリシーは、ネットワークにアクセス可能なアプリケーション、通信用に開くポート、コンピュータと通信可能な IP アドレスを決定します。多くの不正プログラムは、このポリシーを変更して、自身がネットワークとインターネットへアクセスできるようにします。
システムプロセスの変更	多くの不正プログラムが組み込み Windows システムのプロセスでさまざまな処理を実行します。これらの処理には、実行中のプロセスを終了または変更するものがあります。
スタートアッププログラムの追加	不正なアプリケーションは、通常、Windows レジストリに自動スタートエントリを追加または変更して、コンピュータを起動するたびに自動的に起動します。

イベント監視で監視対象のシステムイベントを検出すると、そのイベントに設定された処理を実行します。

次の表は、管理者が監視対象のシステムイベントで実行できる処理の一覧を示します。

表 9-2. 監視対象のシステムイベントでの処理

処理	説明
診断	セキュリティエージェントは常にイベントに関連したプログラムの実行を許可し、診断用にイベントをログに記録します。 これは、すべての監視対象のシステムイベントのデフォルトの処理です。 **注意** このオプションは、64 ビットシステムのプログラムライブラリインジェクション (DLL インジェクション) イベントではサポートされていません。

処理	説明
許可	セキュリティエージェントは常にイベントに関連したプログラムの実行を許可します。
必要に応じて問い合わせ	セキュリティエージェントはイベントに関連したプログラムの実行を許可または拒否するように求めるメッセージを表示し、プログラムを除外リストに追加します。 特定の期間内にユーザが応答しない場合、セキュリティエージェントは自動的にプログラムの実行を許可します。デフォルトの期間は 30 秒です。 **注意** このオプションは、64 ビットシステムのプログラムライブラリインジェクション (DLL インジェクション) イベントではサポートされていません。
拒否	セキュリティエージェントは常にイベントに関連したプログラムの実行をブロックし、イベントをログに記録します。 通知が有効になっているプログラムをブロックした後、セキュリティエージェントはエンドポイントに通知を表示します。

挙動監視除外リスト

挙動監視除外リストは、セキュリティエージェントが挙動監視を使用して監視しないプログラムのリストです。

- 承認済みプログラム: セキュリティエージェントは、[承認済みプログラム] リスト内のすべてのプログラムを挙動監視検索から除外します。

注意

挙動監視では [承認済みプログラム] リストに追加されたプログラムに対して処理を実行しませんが、他の検索機能 (ファイルベースの検索など) では引き続き、プログラムの実行を許可する前にそのプログラムを検索します。

- ブロックするプログラム: セキュリティエージェントは、[ブロックするプログラム] リスト内のプログラムをすべてブロックします。[ブロックするプログラム] リストを設定するには、イベント監視を有効にします。

除外リストは Web コンソールで設定します。また、セキュリティエージェントコンソールから独自の除外リストを設定する権限をユーザに付与することもできます。

詳細については、144 ページの「エージェント権限の設定」を参照してください。

除外リストでのワイルドカードのサポート

挙動監視の承認済みリストでは、ファイルパス、ファイル名、およびファイル拡張子の除外の種類の定義時にワイルドカード文字を使用できます。次の表を使用して除外リストの書式を適切に設定し、Apex One で正しいファイルとフォルダが検索から除外されるようにしてください。

サポートされるワイルドカード文字は次のとおりです。

- アスタリスク (*): 任意の文字または文字列を表します
- 疑問符 (?): 任意の 1 文字を表します

重要

- 挙動監視の承認済みリストでは、ワイルドカード文字を使用してシステムドライブの名称や UNC アドレスを置き換えることはできません。
- 挙動監視のブロックリストでは、ワイルドカード文字を使用してフォルダを置き換えることはできません。

除外の種類	ワイルドカードの使用法	一致する	一致しない
ディレクトリ	`C:\*` 指定したドライブにあるすべてのファイルとフォルダを除外します	• `C:¥sample.exe` • `C:¥folder¥test.doc`	• `D:¥sample.exe` • `E:¥folder¥test.doc`

除外の種類	ワイルドカードの使用法	一致する	一致しない
特定のフォルダ階層にある特定のファイル	`C:\*\Sample.exe` Sample.exe ファイルが C:¥ディレクトリのいずれかのサブフォルダにある場合にのみ除外します	• C:¥files¥Sample.exe • C:¥temp¥files¥Sample.exe	• C:¥sample.exe
UNC パス	`\\<UNC path>\*\Sample.exe` Sample.exe ファイルが指定した UNC パスのいずれかのサブフォルダにある場合にのみ除外します	• ¥¥<UNC path>¥files¥Sample.exe • ¥¥<UNC path>¥temp¥files¥Sample.exe	• R:¥files¥Sample.exe 理由: ネットワークドライブはサポートされていません。 • ¥¥<UNC path>¥Sample.exe 理由: ファイルが UNC パスのサブフォルダ内にありません。
ファイル名と拡張子	`C:\*.*` C:¥ディレクトリの任意のフォルダおよびサブフォルダにある、任意の拡張子のすべてのファイルを除外します	• C:¥Sample.exe • C:¥temp¥Sample.exe • C:¥test.doc	• D:¥sample.exe • C:¥Sample **注意** C:¥Sample にはファイル拡張子がないため、検索から除外されません。

除外の種類	ワイルドカードの使用法	一致する	一致しない
ファイル名	`C:\*.exe` C:¥ディレクトリの任意のフォルダおよびサブフォルダにある、拡張子が.exe のすべてのファイルを除外します	• C:¥Sample.exe • C:¥temp¥test.exe	• C:¥Sample.doc • C:¥temp¥test.bat • C:¥Sample **注意** C:¥Sample にはファイル拡張子がないため、検索から除外されません。
ファイル拡張子	`C:\Sample.*` C:¥ディレクトリにある、Sample という名前の任意の拡張子のすべてのファイルを除外します	• C:¥Sample.exe	• C:¥Sample1.doc • C:¥temp¥Sample.bat • C:¥Sample **注意** C:¥Sample にはファイル拡張子がないため、検索から除外されません。

除外の種類	ワイルドカードの使用法	一致する	一致しない
特定のディレクトリ構造にあるファイル	`C:\*\*\Sample.exe` C:¥ディレクトリの第 2 階層以下のサブフォルダにある、ファイル名と拡張子が Sample.exe であるすべてのファイルを除外します	• C:¥files¥temp¥Sample.exe • C:¥files¥temp¥test¥Sample.exe	• C:¥Sample.exe • C:¥temp¥Sample.exe • C:¥files¥temp¥Sample.doc
複雑なパスまたはファイル名	`C:\Sam*e??.exe` 名前が次の条件を満たすすべてのファイルを除外します • 先頭が「Sam」である • ファイル名の後ろから 3 文字目が「e」である • ファイル名の先頭の「Sam」と末尾の「e??」の間に少なくとも 1 文字ある • ファイル名の「e」からファイル拡張子までの間の文字数がちょうど 2 文字である • ファイル拡張子が.exe である すべての条件を満たすファイルが C:¥ディレクトリにある場合、そのファイルが挙動監視の検索から除外されます。	• C:¥Sample12.exe • C:¥SamSamSample12.exe	• C:¥SaSmple12.exe 理由: 先頭が「Sam」でありません • C:¥SamSamSam12.exe 理由: 後ろから 3 文字目が「e」でありません • C:¥Same12.exe 理由: 先頭の「Sam」と後ろから 3 文字目の「e」の間に文字がありません • C:¥Sample1.exe 理由:「e」から拡張子までの間の文字数が 2 文字でありません • C:¥Sample12.doc 理由: 拡張子が異なります

除外リストの環境変数のサポート

次の表は、ファイルおよびフォルダをリストに追加する際に使用できる環境変数を示しています。

環境変数	例	対応するパス
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{現在のユーザアカウント}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

挙動監視のルールと除外の設定

ランサムウェア、脆弱性攻撃、および新たに出現した脅威からエンドポイントを保護するように挙動監視ポリシーを設定します。不正プログラムの脅威に共通する挙動を診断またはブロックするには、イベント監視機能を使用します。

注意

Windows Server コンピュータでは、いずれのバージョンでも初期設定で挙動監視が無効になっています。

手順

1. [不正プログラム挙動ブロック] セクションで、次の手順を実行します。
   a. [不正プログラム挙動ブロックを有効にする] を選択し、ブロックする脅威の種類を指定します。
      - 既知の脅威: 既知の不正プログラムの脅威に関連する挙動をブロックします。
      - 既知の脅威と潜在的な脅威: 既知の脅威に関連付けられた挙動をブロックし、潜在的に不正な挙動に対して処理を実行します。
   b. 有効にするランサムウェア対策オプションを選択します。
      - 不正な暗号化や変更から文書を保護: 潜在的なランサムウェアによる文書の暗号化や変更を防止します。
        - 不審なプログラムによって変更されたファイルを自動的にバックアップして復元: ランサムウェアの脅威が検出された場合に、暗号化されたファイルのバックアップコピーをエンドポイントに作成してデータの損失を防止します。

注意

自動ファイルバックアップを実行するには、クライアントエンドポイントに 100MB 以上のディスク容量が必要です。また、バックアップされるのは 10MB 未満のファイルだけです。

      - ランサムウェアに関連付けられていることの多いプロセスをブロック: 既知のランサムウェアに関連付けられているプロセスをブロックして、文書の暗号化や変更を防止します。
      - プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック: プログラム検査は、プロセスを監視して API フッ

クを行うことで、予期しない挙動を示すプログラムを特定します。これにより、不正な実行可能ファイルの全体的な検出率が高くなりますが、システムのパフォーマンスが下がる場合があります。

ヒント

[ブロックする脅威] リストから [既知の脅威と潜在的な脅威] を選択すると、プログラム検査によるセキュリティが向上します。

詳細については、168 ページの「ランサムウェア対策」を参照してください。

c. [脆弱性対策] で [脆弱性攻撃に関連する異常な挙動を示すプログラムを終了] を有効にし、プログラムの潜在的な脆弱性を悪用した攻撃を防止します。

注意

脆弱性対策を使用するには、[プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック] を選択する必要があります。

詳細については、171 ページの「脆弱性対策」を参照してください。

重要

脆弱性対策はリアルタイム検索 (メモリで検出された不正プログラムの変種/亜種を隔離する) と連携して、ファイルレス攻撃からの保護を強化します。

詳細については、198 ページの「リアルタイム検索: [対象] タブ」を参照してください。

2. [新たに検出されたプログラム] セクションで、[Web またはメールアプリケーションチャネルを介してダウンロードされた新たなプログラムを監視する] を有効にし、ダウンロードされたプログラムの実行前にユーザにメッセージを表示するか、Apex One でログへの記録だけを行うかを選択します。
3. [イベント監視] セクションで、次の手順を実行します。

a. [イベント監視を有効にする] を選択します。

b. [詳細な設定を指定] をクリックして、監視するイベントの種類を選択します。

c. 監視するシステムイベントを選択し、選択したイベントごとに処理を選択します。

監視対象のシステムイベントの詳細については、172 ページの「イベント監視」を参照してください。

4. [除外] タブをクリックし、除外リストを設定します。

a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

注意

子ポリシーが [親ポリシーから拡張] に設定されている場合、[子ポリシーの制限] も設定できます。この制限によって、子ポリシーによって特定のオブジェクトがリストに追加されることを防止できます。

b. 表示されるテキストフィールドに、プログラムのフルパスを入力します。

注意

- 複数のエントリを区切るには、セミコロン (;) を使用します。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- [承認済みリスト] にはワイルドカード文字を使用できます。

  詳細については、176 ページの「除外リストでのワイルドカードのサポート」を参照してください。

c. [追加] をクリックします。

d. ブロックするプログラムまたは承認済みプログラムをリストから削除するには、プログラムの横にあるごみ箱アイコン () をクリックします。

注意

Apex One では、承認済みプログラムとブロックするプログラムを合計 1,024 個まで指定できます。

第 10 章

不正プログラム対策ポリシー設定

ここでは、セキュリティエージェントで不正プログラム検索を設定する方法について説明します。

この章は次のトピックで構成されます。

検索方法の種類

セキュリティエージェントでは、セキュリティリスクの検索時に 2 つの検索方法のどちらかを使用できます。1 つはスマートスキャンで、もう 1 つは従来型スキャンです。

- スマートスキャン

  このヘルプでは、スマートスキャンを使用するセキュリティエージェントを「スマートスキャンエージェント」と呼びます。スマートスキャンエージェントは、ローカル検索と、ファイルレピュテーションサービスで提供されるクラウド型クエリを利用できます。

- 従来型スキャン

  スマートスキャンを使用しないエージェントは、「従来型スキャンエージェント」と呼ばれます。従来型スキャンエージェントでは、エンドポイント上にすべてのセキュリティエージェントコンポーネントが格納され、ローカルのすべてのファイルが検索されます。

検索方法の切り替えに関するガイドライン

次の表は、セキュリティエージェントで使用する検索方法を切り替える前の注意事項を示しています。

表 10-1. スマートスキャンへ切り替える際の注意事項

注意事項	詳細
製品ライセンス	必要なすべてのライセンスが新しい検索方法に対してアクティベート済みであることを確認します。
Apex One サーバ	エージェントが Apex One サーバに接続可能であることを確認します。検索方法が切り替わったことが通知されるのは、オンラインエージェントのみです。オフラインエージェントは、オンラインになったときに通知されます。スタンドアロンモードのエージェントは、オンラインになったときに通知されるか、またはエージェントに予約アップデートの権限がある場合には、予約アップデートの実行時に通知されます。 また、Apex One サーバに最新のコンポーネントがインストールされていることも確認し、セキュリティエージェントがそのサーバから正しいパターンファイルをダウンロードできるようにしてください。

注意事項	詳細
切り替えるセキュリティエージェントの数	一度に切り替えるセキュリティエージェントの数を比較的少数にすることで、Apex One サーバおよび Smart Protection Server のリソースを効率的に使用することができます。これらのサーバは、セキュリティエージェントが検索方法を変更しても、他の重要なタスクを実行できます。
タイミング	検索方法を切り替える場合、セキュリティエージェントでは、新しい検索方法に必要なフルパターンファイルをダウンロードする必要があります。 ネットワーク帯域幅への影響とユーザの日常業務の中断を避けるために、就業時間帯を避けて切り替えることを検討してください。検索方法を切り替える際、セキュリティエージェントで [今すぐアップデート] が使用できないように設定をしておくことをお勧めします。
IPv6 のサポート 重要 Apex One サーバにレポートするセキュリティエージェントでのみ使用できます。	スマートスキャンエージェントは、検索クエリを Trend Micro Smart Protection ソースに送信します。 IPv6 シングルスタックのスマートスキャンエージェントからは、次のような IPv4 シングルスタックソースに直接クエリを送信することはできません。 • Smart Protection Server 2.0 (統合またはスタンドアロン) 注意 Smart Protection Server では、バージョン 2.5 以降、IPv6 がサポートされるようになりました。 • Trend Micro Smart Protection Network 同様に、IPv4 シングルスタックのスマートスキャンエージェントからは、IPv6 シングルスタックの Smart Protection Server にクエリを送信することはできません。 スマートスキャンエージェントがこれらのソースに接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

注意事項	詳細
Trend Micro Smart Protection サービス 重要 Apex One サーバにレポートするセキュリティエージェントでのみ使用できます。	従来型スキャンからスマートスキャンにセキュリティエージェントを切り替える場合には、Trend Micro Smart Protection サービスが設定されていることを確認してください。

手動検索

手動検索はオンデマンドの検索であり、ユーザがセキュリティエージェントコンソールで検索を実行するとただちに開始されます。検索にかかる時間は、検索するファイル数やセキュリティエージェントエンドポイントのハードウェアリソースによって異なります。

手動検索設定を、1 つ以上のエージェントおよびドメインに設定および適用するか、またはサーバが管理するすべてのエージェントに設定および適用します。

手動検索設定

次のタブを使用して手動検索を設定します。

- 188 ページの「手動検索: [対象] タブ」
- 191 ページの「手動検索: [処理] タブ」
- 194 ページの「手動検索: [検索除外] タブ」

手動検索: [対象] タブ

手順

1. [検索するファイル] で、次の項目から選択します。

- すべての検索可能ファイル: 検索可能なファイルをすべて検索に含めます。検索不能なファイルとは、パスワードで保護されたファイル、暗号化されたファイル、またはユーザ定義の検索制限を超えるファイルです。

注意

検索可能なファイルをすべて検索する場合、長い時間とリソースが必要になります。

- トレンドマイクロの推奨設定で検索されたファイルタイプ: 実際のファイルタイプに基づいてファイルを検索します。
- 対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください): 拡張子を基準にして検索対象ファイルを手動で指定します。複数のエントリがある場合には、カンマ (,) で区切ります。

注意

親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

2. [設定] で必要な設定を行います。

設定	説明
隠しフォルダの検索	セキュリティエージェントで、エンドポイント上の隠しフォルダを検出して検索できます。
ネットワークドライブの検索	物理的に他のエンドポイントに配置されていても、ローカルエンドポイントに割り当てられているディレクトリを検索します。

設定	説明
圧縮ファイルの検索	アーカイブファイル内の指定された数の圧縮階層を検索します。 注意 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 このオプションを選択して、以下の項目を設定してください。 • 最大階層数: アーカイブファイル内の指定された数の圧縮階層を検索します 注意 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 • 解凍後のサイズが XX MB を超える場合はファイルを検索しない: セキュリティエージェントが圧縮されたアーカイブ内にある各ファイルのサイズをチェックし、各ファイルサイズが設定されたしきい値を超えている場合はファイルの検索をスキップできるようにします • 圧縮ファイル内の最初の XX 個のファイルだけ検索する: 設定したしきい値を超える数のファイルがアーカイブに含まれる場合に、セキュリティエージェントが一部のファイルのみを検索するようにします

設定	説明
OLE オブジェクトの検索	ファイル内の指定された数の Object Linking and Embedding (OLE) 階層を検索します。 [OLE ファイル内の攻撃コードを検出]: OLE セキュリティホールの検出では、Microsoft Office ファイルの攻撃コードを確認することで、不正プログラムをヒューリスティックに特定します。  注意 [OLE オブジェクトの検索] および [[OLE ファイル内の攻撃コードを検出]] の両方のオプションに指定された数の階層を適用できます。
システム領域の検索	エンドポイント上のハードディスクのシステム領域でウイルス/不正プログラムを検索します。

3. [CPU 使用率] で、次の項目から選択します。
   - 高: 検索が速くなり PC への負荷が最も高くなります。
   - 中: 検索の速度も PC への負荷もやや低くなります。
   - 低: 検索に時間がかかりますが PC への負荷が最も低くなります。

手動検索: [処理] タブ

手順

1. [ウイルス/不正プログラム] で必要な設定を行います。
   a. セキュリティ上の脅威を検出した場合にセキュリティエージェントで実行する処理の種類を選択します。
      - [Use AntimalwareScanCore]: ウイルスや不正プログラムに対してあらかじめ設定された一連の処理を使用します。

        詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。

- 潜在的なウイルス/不正プログラムに対する処理のカスタマイズ: 潜在的な不正プログラムの脅威に対してセキュリティエージェントが実行する処理を選択して指定します。

- すべての種類のウイルス/不正プログラムに同じ処理を使用: すべての不正プログラムの脅威に対してセキュリティエージェントが実行する処理を指定します。

- 特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用: 特定のセキュリティ上の脅威に対してセキュリティエージェントが実行する処理を指定します。

  詳細については、229 ページの「検出時の処理のカスタマイズ」を参照してください。

b. [駆除前にファイルをバックアップする] を選択して、エンドポイントの <エージェントインストールフォルダ>¥Backup フォルダに感染ファイルの暗号化されたコピーを作成します。

   ファイルのバックアップコピーを作成すると、元のバージョンのファイルを必要に応じて復元できます。

c. 隔離ディレクトリの場所を指定します。

   - セキュリティエージェントの管理サーバに隔離: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを Apex One サーバに送信します。

   - 隔離ディレクトリ: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを指定された場所に送信します。

   詳細については、230 ページの「隔離ディレクトリ」を参照してください。

d. [ダメージクリーンナップサービス] で、次の項目を設定します。

   - クリーンナップの種類

     - 標準クリーンナップ: セキュリティエージェントでは、標準クリーンナップの間に次のいずれかの処理が実行されます。

- 活動中のトロイの木馬を検出および削除
- トロイの木馬が作成したプロセスを中止
- トロイの木馬が変更したシステムファイルを修復
- トロイの木馬により作成されたファイルとアプリケーションを削除

- 高度なクリーンナップ: 標準クリーンナップの処理の他に、セキュリティエージェントでは、FakeAV と呼ばれる偽セキュリティソフトウェアや特定のルートキットの変種による活動が停止されます。

- 潜在的なウイルス/不正プログラムが検出された場合にクリーンナップを実行: 潜在的な不正プログラムの脅威に対して設定された種類のクリーンナップを実行します。

注意

このオプションは、潜在的なウイルス/不正プログラムに対する処理が、「放置 (ログのみ)」または「アクセス拒否」以外の場合にのみ選択できます。

2. [スパイウェア/グレーウェア] で、スパイウェア/グレーウェアプログラムを検出した場合にセキュリティエージェントが実行する処理を選択します。

- 駆除: 関連するプロセスをすべて終了し、関連付けられているレジストリ値、ファイル、Cookie、およびショートカットを削除します。

注意

スパイウェア/グレーウェアを駆除した後、セキュリティエージェントでスパイウェア/グレーウェアのデータをバックアップし、スパイウェア/グレーウェアに安全にアクセスできると考えられる場合、復元することができます。

- 放置: 検出をログに記録しますが、プログラムの実行は許可します。

3. [高度な不正プログラム検出] セクションで、オプションを選択して必要な設定を行います。

- トレンドマイクロの推奨処理を使用: 検出されたポータブル実行可能ファイルに対してあらかじめ設定された一連の処理を使用します。このオプションを使用することをお勧めします。

  詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。

- 脅威のあるすべての Portable Executable ファイルに同じ処理を使用: 検出されたポータブル実行可能ファイルに対して次のいずれかの処理を適用します。
  - 隔離: 検出されたポータブル実行可能ファイルがシステムによって自動的に隔離されます。
  - 放置: 検出ログがシステムによって生成されますが、検出されたポータブル実行可能ファイルに対して処理は適用されません。

注意

検出されたポータブル実行可能ファイルが検索除外リストにある場合、システムではそのファイルに対して処理が適用されません。

手動検索: [検索除外] タブ

手順

1. [検索除外を有効にする] を選択します。
2. [検索除外リスト (ディレクトリ)] で必要な設定を行います。
   a. [トレンドマイクロ製品がインストールされているディレクトリの除外] を選択して、他のトレンドマイクロ製品に関連付けられているディレクトリが自動的に除外されるようにします。

      詳細については、236 ページの「トレンドマイクロ製品ディレクトリの除外」を参照してください。

   b. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。

- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

注意

子ポリシーが [親ポリシーから拡張] に設定されている場合、[子ポリシーの制限] も設定できます。この制限によって、子ポリシーによって特定のオブジェクトがリストに追加されることを防止できます。

c. 検索から除外するディレクトリパスを入力して、[+] ボタンをクリックします。

セキュリティエージェントは、指定されたディレクトリ (およびサブディレクトリ) にあるファイルを検索しません。

注意

- 検索から除外するディレクトリを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ディレクトリの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

3. [検索除外リスト (ファイル)] で必要な設定を行います。

a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

b. 検索から除外するファイル名または完全なディレクトリパスを含むファイル名を入力して、[+] ボタンをクリックします。

注意

- 検索から除外するファイルを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ファイルの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

4. [検索除外リスト (ファイル拡張子)] で必要な設定を行います。
   a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
      - 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。
   b. 検索から除外するファイル拡張子を選択または入力して、[追加 >] ボタンをクリックします。

注意

- 検索から除外するファイル拡張子を最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- 手動検索、予約検索、および ScanNow の場合、ワイルドカード文字として疑問符 (?) を使用して 1 つの文字を置き換えるか、アスタリスク (*) を使用して複数の文字を置き換えます。たとえば、DOC、DOT、DAT など、D で始まる拡張子を持つすべてのファイルを検索しない場合は、「`D*`」または「`D??`」と入力します。

リアルタイム検索

リアルタイム検索は、継続的に実行される検索です。ファイルの受信時、開かれたとき、ダウンロード時、コピー時、または変更時に毎回、ファイルにセキュリティリスクが存在するかどうかを調べるリアルタイム検索が実行されます。セキュリティエージェントでセキュリティリスクが検出されなかった場合、ユーザはそのファイルへのアクセスを続けることができます。セキュリティエージェントがセキュリティリスクまたは潜在的なウイルス/不正プログラムを検出した場合、通知メッセージが表示され、感染ファイルの名前と該当するセキュリティリスクが示されます。

リアルタイム検索は検索キャッシュを保持し、セキュリティエージェントが起動するたびにキャッシュが再ロードされます。セキュリティエージェントは、セキュリティエージェントのアンロード後に行われたファイルまたはフォルダへの変更を追跡し、変更があったファイルをキャッシュから削除します。

リアルタイム検索設定

手順

1. 次のオプションを選択します。
   - ウイルス/不正プログラム検索を有効にする
   - スパイウェア/グレーウェア検索を有効にする

   注意

   スパイウェア検索を有効にするには、ウイルス/不正プログラムの検索を有効にする必要があります。ウイルスの大規模感染の間、セキュリティエージェントはリアルタイム検索を自動的に有効にするため、大規模感染が解消されるまで検索を無効にすることはできません。リアルタイム検索では、ウイルスがエンドポイント上のファイルやフォルダを変更または削除するのを防ぎます。

2. [対象] の設定を行います。

   詳細については、198 ページの「リアルタイム検索: [対象] タブ」を参照してください。

3. [処理] の設定を行います。

   詳細については、202 ページの「リアルタイム検索: [処理] タブ」を参照してください。

4. [検索除外] の設定を行います。

   詳細については、205 ページの「リアルタイム検索: [検索除外] タブ」を参照してください。

リアルタイム検索: [対象] タブ

手順

1. [ファイルに対するユーザのアクティビティ] で、検索を実行するファイル操作を [次のファイルを検索する] リストから選択します。

   - 作成された/変更された/読み込まれたファイル: エンドポイントで作成、変更、または開かれたすべてのファイルを検索します
   - 作成された/変更されたファイル: エンドポイントで作成または変更されたすべてのファイルを検索します
   - 読み込まれたファイル: エンドポイントで開かれたすべてのファイルを検索します

2. [検索するファイル] で、次の項目から選択します。

   - すべての検索可能ファイル: 検索可能なファイルをすべて検索に含めます。検索不能なファイルとは、パスワードで保護されたファイル、暗号化されたファイル、またはユーザ定義の検索制限を超えるファイルです。

     注意

     検索可能なファイルをすべて検索する場合、長い時間とリソースが必要になります。

   - トレンドマイクロの推奨設定で検索されたファイルタイプ: 実際のファイルタイプに基づいてファイルを検索します。

- 対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください): 拡張子を基準にして検索対象ファイルを手動で指定します。複数のエントリがある場合には、カンマ (,) で区切ります。

注意

親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

3. [設定] で必要な設定を行います。

設定	説明
シャットダウン時にフロッピーディスクを検索	シャットダウン時にフロッピーディスクを検索します。
ネットワークドライブの検索	物理的に他のエンドポイントに配置されていても、ローカルエンドポイントに割り当てられているディレクトリを検索します。
挿入後、USB ストレージデバイスのシステム領域を検索する	ユーザが USB ストレージデバイスを挿入するたびに、USB ストレージデバイスのシステム領域のみを自動的に検索します。
リムーバブルストレージデバイスの接続後、その中のすべてのファイルを検索	ユーザが USB ストレージデバイスを挿入するたびに、USB ストレージデバイス上のすべてのファイルを自動的に検索します。

設定	説明
メモリで検出された不正プログラムの変種/亜種を隔離する	挙動監視によって不審プロセスがシステムメモリで検出されると、リアルタイム検索はそのプロセスをマップして、それが不正プログラムであるかどうかを検索します。不正プログラムであった場合、リアルタイム検索はそのプロセスまたはファイル、あるいはその両方を隔離します。  注意 挙動監視機能では、メモリ検索と脆弱性対策が連動して、ファイルレス攻撃に対する高度な保護を実現します。 詳細については、180 ページの「挙動監視のルールと除外の設定」を参照してください。

設定	説明
圧縮ファイルの検索	アーカイブファイル内の指定された数の圧縮階層を検索します。 **注意** 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 このオプションを選択して、以下の項目を設定してください。 • 最大階層数: アーカイブファイル内の指定された数の圧縮階層を検索します **注意** 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 • 解凍後のサイズが XX MB を超える場合はファイルを検索しない: セキュリティエージェントが圧縮されたアーカイブ内にある各ファイルのサイズをチェックし、各ファイルサイズが設定されたしきい値を超えている場合はファイルの検索をスキップできるようにします • 圧縮ファイル内の最初の XX 個のファイルだけ検索する: 設定したしきい値を超える数のファイルがアーカイブに含まれる場合に、セキュリティエージェントが一部のファイルのみを検索するようにします

設定	説明
OLE オブジェクトの検索	ファイル内の指定された数の Object Linking and Embedding (OLE) 階層を検索します。 [OLE ファイル内の攻撃コードを検出]: OLE セキュリティホールの検出では、Microsoft Office ファイルの攻撃コードを確認することで、不正プログラムをヒューリスティックに特定します。  注意 [OLE オブジェクトの検索] および [[OLE ファイル内の攻撃コードを検出]] の両方のオプションに指定された数の階層を適用できます。
IntelliTrap を有効にする	圧縮ファイルに含まれるボットなどの不正コードが検出されます。
Web およびメールからダウンロードしたファイルに対する CVE セキュリティホールの検索を有効にする	共通脆弱性識別子 (CVE) システムに基づいて、市販の製品の既知の脆弱性を悪用するプロセスをブロックします。

リアルタイム検索: [処理] タブ

手順

1. [ウイルス/不正プログラム] で必要な設定を行います。

   a. セキュリティ上の脅威を検出した場合にセキュリティエージェントで実行する処理の種類を選択します。

      - [Use AntimalwareScanCore]: ウイルスや不正プログラムに対してあらかじめ設定された一連の処理を使用します。

        詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。

- 潜在的なウイルス/不正プログラムに対する処理のカスタマイズ: 潜在的な不正プログラムの脅威に対してセキュリティエージェントが実行する処理を選択して指定します。

- すべての種類のウイルス/不正プログラムに同じ処理を使用: すべての不正プログラムの脅威に対してセキュリティエージェントが実行する処理を指定します。

- 特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用: 特定のセキュリティ上の脅威に対してセキュリティエージェントが実行する処理を指定します。

  詳細については、229 ページの「検出時の処理のカスタマイズ」を参照してください。

b. エンドユーザに対して表示する通知の種類を選択します。

- ウイルス/不正プログラムの検出時に通知を表示: 不正プログラムが検出された場合に、セキュリティエージェントユーザに通知を表示します。

- 潜在的なウイルス/不正プログラムの検出時に通知を表示する: 潜在的な不正プログラムが検出された場合に、セキュリティエージェントユーザに通知を表示します。

c. [駆除前にファイルをバックアップする] を選択して、エンドポイントの <エージェントインストールフォルダ>¥Backup フォルダに感染ファイルの暗号化されたコピーを作成します。

ファイルのバックアップコピーを作成すると、元のバージョンのファイルを必要に応じて復元できます。

d. 隔離ディレクトリの場所を指定します。

- セキュリティエージェントの管理サーバに隔離: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを Apex One サーバに送信します。

- 隔離ディレクトリ: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを指定された場所に送信します。

詳細については、230 ページの「隔離ディレクトリ」を参照してください。

e. [ダメージクリーンナップサービス] で、次の項目を設定します。

- 潜在的なウイルス/不正プログラムが検出された場合にクリーンナップを実行: 潜在的な不正プログラムの脅威に対して設定された種類のクリーンナップを実行します。

注意

このオプションは、潜在的なウイルス/不正プログラムに対する処理が、「放置 (ログのみ)」または「アクセス拒否」以外の場合にのみ選択できます。

2. [スパイウェア/グレーウェア] で、スパイウェア/グレーウェアプログラムを検出した場合にセキュリティエージェントが実行する処理を選択します。

- 駆除: 関連するプロセスをすべて終了し、関連付けられているレジストリ値、ファイル、Cookie、およびショートカットを削除します。

注意

スパイウェア/グレーウェアを駆除した後、セキュリティエージェントでスパイウェア/グレーウェアのデータをバックアップし、スパイウェア/グレーウェアに安全にアクセスできると考えられる場合、復元することができます。

- アクセス拒否: エンドユーザがスパイウェア/グレーウェアコンポーネントを開いたりコピーしたりできないようにします。
- スパイウェア/グレーウェアの検出時にエンドポイントに通知を表示: スパイウェア/グレーウェアが検出された場合に、セキュリティエージェントユーザに通知を表示します。

3. [高度な不正プログラム検出] セクションで、オプションを選択して必要な設定を行います。

- トレンドマイクロの推奨処理を使用: 検出されたポータブル実行可能ファイルに対してあらかじめ設定された一連の処理を使用します。このオプションを使用することをお勧めします。

詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。

- 脅威のあるすべての Portable Executable ファイルに同じ処理を使用: 検出されたポータブル実行可能ファイルに対して次のいずれかの処理を適用します。
  - 隔離: 検出されたポータブル実行可能ファイルがシステムによって自動的に隔離されます。
  - 放置: 検出ログがシステムによって生成されますが、検出されたポータブル実行可能ファイルに対して処理は適用されません。

注意

検出されたポータブル実行可能ファイルが検索除外リストにある場合、システムではそのファイルに対して処理が適用されません。

リアルタイム検索: [検索除外] タブ

手順

1. [検索除外を有効にする] を選択します。
2. [検索除外リスト (ディレクトリ)] で必要な設定を行います。
   a. [トレンドマイクロ製品がインストールされているディレクトリの除外] を選択して、他のトレンドマイクロ製品に関連付けられているディレクトリが自動的に除外されるようにします。

      詳細については、236 ページの「トレンドマイクロ製品ディレクトリの除外」を参照してください。

   b. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
      - 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

注意

子ポリシーが [親ポリシーから拡張] に設定されている場合、[子ポリシーの制限] も設定できます。この制限によって、子ポリシーによって特定のオブジェクトがリストに追加されることを防止できます。

c. 検索から除外するディレクトリパスを入力して、[+] ボタンをクリックします。

セキュリティエージェントは、指定されたディレクトリ (およびサブディレクトリ) にあるファイルを検索しません。

注意

- 検索から除外するディレクトリを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ディレクトリの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

3. [検索除外リスト (ファイル)] で必要な設定を行います。

a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

b. 検索から除外するファイル名または完全なディレクトリパスを含むファイル名を入力して、[+] ボタンをクリックします。

注意

- 検索から除外するファイルを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ファイルの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

4. [検索除外リスト (ファイル拡張子)] で必要な設定を行います。
   a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
      - 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。
   b. 検索から除外するファイル拡張子を選択または入力して、[追加 >] ボタンをクリックします。

注意

- 検索から除外するファイル拡張子を最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- リアルタイム検索では、ワイルドカード文字を使用してファイル拡張子を除外することはできません。

ScanNow

ScanNow は、管理者によって Web コンソールを通してリモートで開始され、1 つ以上のセキュリティエージェントエンドポイントを対象にすることができます。

ScanNow 設定を、1 つ以上のセキュリティエージェントおよびドメインに設定および適用するか、またはサーバが管理するすべてのセキュリティエージェントに設定および適用します。

ScanNow 設定

手順

1. 次のオプションを選択します。
   - ウイルス/不正プログラム検索を有効にする
   - スパイウェア/グレーウェア検索を有効にする

   注意

   スパイウェア検索を有効にするには、ウイルス/不正プログラムの検索を有効にする必要があります。

2. [対象] の設定を行います。

   詳細については、208 ページの「ScanNow: [対象] タブ」を参照してください。

3. [処理] の設定を行います。

   詳細については、211 ページの「ScanNow - [処理] タブ」を参照してください。

4. [検索除外] の設定を行います。

   詳細については、214 ページの「ScanNow - [検索除外] タブ」を参照してください。

ScanNow: [対象] タブ

手順

1. [検索するファイル] で、次の項目から選択します。
   - すべての検索可能ファイル: 検索可能なファイルをすべて検索に含めます。検索不能なファイルとは、パスワードで保護されたファイ

ル、暗号化されたファイル、またはユーザ定義の検索制限を超えるファイルです。

注意

検索可能なファイルをすべて検索する場合、長い時間とリソースが必要になります。

- トレンドマイクロの推奨設定で検索されたファイルタイプ: 実際のファイルタイプに基づいてファイルを検索します。
- 対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください): 拡張子を基準にして検索対象ファイルを手動で指定します。複数のエントリがある場合には、カンマ (,) で区切ります。

注意

親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

2. [設定] で必要な設定を行います。

設定	説明
圧縮ファイルの検索	アーカイブファイル内の指定された数の圧縮階層を検索します。 注意 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 このオプションを選択して、以下の項目を設定してください。 • 最大階層数: アーカイブファイル内の指定された数の圧縮階層を検索します 注意 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 • 解凍後のサイズが XX MB を超える場合はファイルを検索しない: セキュリティエージェントが圧縮されたアーカイブ内にある各ファイルのサイズをチェックし、各ファイルサイズが設定されたしきい値を超えている場合はファイルの検索をスキップできるようにします • 圧縮ファイル内の最初の XX 個のファイルだけ検索する: 設定したしきい値を超える数のファイルがアーカイブに含まれる場合に、セキュリティエージェントが一部のファイルのみを検索するようにします

設定	説明
OLE オブジェクトの検索	ファイル内の指定された数の Object Linking and Embedding (OLE) 階層を検索します。 [OLE ファイル内の攻撃コードを検出]: OLE セキュリティホールの検出では、Microsoft Office ファイルの攻撃コードを確認することで、不正プログラムをヒューリスティックに特定します。  注意 [OLE オブジェクトの検索] および [[OLE ファイル内の攻撃コードを検出]] の両方のオプションに指定された数の階層を適用できます。
システム領域の検索	エンドポイント上のハードディスクのシステム領域でウイルス/不正プログラムを検索します。

3. [CPU 使用率] で、次の項目から選択します。
   - 高: 検索が速くなり PC への負荷が最も高くなります。
   - 中: 検索の速度も PC への負荷もやや低くなります。
   - 低: 検索に時間がかかりますが PC への負荷が最も低くなります。

ScanNow - [処理] タブ

手順

1. [ウイルス/不正プログラム] で必要な設定を行います。
   a. セキュリティ上の脅威を検出した場合にセキュリティエージェントで実行する処理の種類を選択します。
      - [Use AntimalwareScanCore]: ウイルスや不正プログラムに対してあらかじめ設定された一連の処理を使用します。

        詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。

- 潜在的なウイルス/不正プログラムに対する処理のカスタマイズ: 潜在的な不正プログラムの脅威に対してセキュリティエージェントが実行する処理を選択して指定します。

- すべての種類のウイルス/不正プログラムに同じ処理を使用: すべての不正プログラムの脅威に対してセキュリティエージェントが実行する処理を指定します。

- 特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用: 特定のセキュリティ上の脅威に対してセキュリティエージェントが実行する処理を指定します。

  詳細については、229 ページの「検出時の処理のカスタマイズ」を参照してください。

b. [駆除前にファイルをバックアップする] を選択して、エンドポイントの <エージェントインストールフォルダ>¥Backup フォルダに感染ファイルの暗号化されたコピーを作成します。

   ファイルのバックアップコピーを作成すると、元のバージョンのファイルを必要に応じて復元できます。

c. 隔離ディレクトリの場所を指定します。

   - セキュリティエージェントの管理サーバに隔離: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを Apex One サーバに送信します。

   - 隔離ディレクトリ: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを指定された場所に送信します。

   詳細については、230 ページの「隔離ディレクトリ」を参照してください。

d. [ダメージクリーンナップサービス] で、次の項目を設定します。

   - クリーンナップの種類

     - 標準クリーンナップ: セキュリティエージェントでは、標準クリーンナップの間に次のいずれかの処理が実行されます。

- 活動中のトロイの木馬を検出および削除
- トロイの木馬が作成したプロセスを中止
- トロイの木馬が変更したシステムファイルを修復
- トロイの木馬により作成されたファイルとアプリケーションを削除

- 高度なクリーンナップ: 標準クリーンナップの処理の他に、セキュリティエージェントでは、FakeAV と呼ばれる偽セキュリティソフトウェアや特定のルートキットの変種による活動が停止されます。

- 潜在的なウイルス/不正プログラムが検出された場合にクリーンナップを実行: 潜在的な不正プログラムの脅威に対して設定された種類のクリーンナップを実行します。

注意

このオプションは、潜在的なウイルス/不正プログラムに対する処理が、「放置 (ログのみ)」または「アクセス拒否」以外の場合にのみ選択できます。

2. [スパイウェア/グレーウェア] で、スパイウェア/グレーウェアプログラムを検出した場合にセキュリティエージェントが実行する処理を選択します。

- 駆除: 関連するプロセスをすべて終了し、関連付けられているレジストリ値、ファイル、Cookie、およびショートカットを削除します。

注意

スパイウェア/グレーウェアを駆除した後、セキュリティエージェントでスパイウェア/グレーウェアのデータをバックアップし、スパイウェア/グレーウェアに安全にアクセスできると考えられる場合、復元することができます。

- 放置: 検出をログに記録しますが、プログラムの実行は許可します。

3. [高度な不正プログラム検出] セクションで、オプションを選択して必要な設定を行います。

- トレンドマイクロの推奨処理を使用: 検出されたポータブル実行可能ファイルに対してあらかじめ設定された一連の処理を使用します。このオプションを使用することをお勧めします。

  詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。

- 脅威のあるすべての Portable Executable ファイルに同じ処理を使用: 検出されたポータブル実行可能ファイルに対して次のいずれかの処理を適用します。
  - 隔離: 検出されたポータブル実行可能ファイルがシステムによって自動的に隔離されます。
  - 放置: 検出ログがシステムによって生成されますが、検出されたポータブル実行可能ファイルに対して処理は適用されません。

注意

検出されたポータブル実行可能ファイルが検索除外リストにある場合、システムではそのファイルに対して処理が適用されません。

ScanNow - [検索除外] タブ

手順

1. [検索除外を有効にする] を選択します。
2. [検索除外リスト (ディレクトリ)] で必要な設定を行います。
   a. [トレンドマイクロ製品がインストールされているディレクトリの除外] を選択して、他のトレンドマイクロ製品に関連付けられているディレクトリが自動的に除外されるようにします。

      詳細については、236 ページの「トレンドマイクロ製品ディレクトリの除外」を参照してください。

   b. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。

- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

注意

子ポリシーが [親ポリシーから拡張] に設定されている場合、[子ポリシーの制限] も設定できます。この制限によって、子ポリシーによって特定のオブジェクトがリストに追加されることを防止できます。

c. 検索から除外するディレクトリパスを入力して、[+] ボタンをクリックします。

セキュリティエージェントは、指定されたディレクトリ (およびサブディレクトリ) にあるファイルを検索しません。

注意

- 検索から除外するディレクトリを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ディレクトリの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

3. [検索除外リスト (ファイル)] で必要な設定を行います。

a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

b. 検索から除外するファイル名または完全なディレクトリパスを含むファイル名を入力して、[+] ボタンをクリックします。

注意

- 検索から除外するファイルを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ファイルの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

4. [検索除外リスト (ファイル拡張子)] で必要な設定を行います。
   a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
      - 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。
   b. 検索から除外するファイル拡張子を選択または入力して、[追加 >] ボタンをクリックします。

      注意

      - 検索から除外するファイル拡張子を最大 256 個指定できます。
      - リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
      - 手動検索、予約検索、および ScanNow の場合、ワイルドカード文字として疑問符 (?) を使用して 1 つの文字を置き換えるか、アスタリスク (*) を使用して複数の文字を置き換えます。たとえば、DOC、DOT、DAT など、D で始まる拡張子を持つすべてのファイルを検索しない場合は、「`D*`」または「`D??`」と入力します。

予約検索

予約検索は指定された日時に自動的に実行されます。エージェントの予約検索により検索ルーチンを自動化すれば、検索の管理効率を改善できます。

予約検索設定を、1 つ以上のエージェントおよびドメインに設定および適用するか、またはサーバが管理するすべてのエージェントに設定および適用します。

予約検索設定

手順

1. 次のオプションを選択します。
   - ウイルス/不正プログラム検索を有効にする
   - スパイウェア/グレーウェア検索を有効にする

   注意

   スパイウェア検索を有効にするには、ウイルス/不正プログラムの検索を有効にする必要があります。

2. [対象] の設定を行います。

   詳細については、218 ページの「予約検索: [対象] タブ」を参照してください。

3. [処理] の設定を行います。

   詳細については、222 ページの「予約検索: [処理] タブ」を参照してください。

4. [検索除外] の設定を行います。

   詳細については、225 ページの「予約検索: [検索除外] タブ」を参照してください。

予約検索: [対象] タブ

手順

1. [スケジュール] で、予約検索の頻度を指定します。
   - 毎日: 毎日指定された時刻に検索を実行します。
   - 毎週<曜日>: 毎週 1 回、指定された曜日と時刻に検索を実行します。
   - 毎月<日付>: 毎月 1 回、指定された日付と時刻に検索を実行します。
   - 毎月 (曜日) <序数><曜日>: 毎月 1 回、指定された週の曜日と時刻に検索を実行します。

   重要
   指定された月に存在しない日付 (たとえば、2 月に存在しない「30」日) を選択すると、予約検索はその月の最終日に実行されます。

   注意
   親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
   - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
   - カスタマイズ可能: 子ポリシーには、親ポリシーと異なる内容を設定できます。

2. [検索するファイル] で、次の項目から選択します。
   - すべての検索可能ファイル: 検索可能なファイルをすべて検索に含めます。検索不能なファイルとは、パスワードで保護されたファイル、暗号化されたファイル、またはユーザ定義の検索制限を超えるファイルです。

     注意
     検索可能なファイルをすべて検索する場合、長い時間とリソースが必要になります。

- トレンドマイクロの推奨設定で検索されたファイルタイプ: 実際のファイルタイプに基づいてファイルを検索します。
- 対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください): 拡張子を基準にして検索対象ファイルを手動で指定します。複数のエントリがある場合には、カンマ (,) で区切ります。

注意

親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

3. [設定] で必要な設定を行います。

設定	説明
OLE オブジェクトの検索	ファイル内の指定された数の Object Linking and Embedding (OLE) 階層を検索します。 [OLE ファイル内の攻撃コードを検出]: OLE セキュリティホールの検出では、Microsoft Office ファイルの攻撃コードを確認することで、不正プログラムをヒューリスティックに特定します。  注意 [OLE オブジェクトの検索] および [[OLE ファイル内の攻撃コードを検出]] の両方のオプションに指定された数の階層を適用できます。

設定	説明
予約検索の実行 XX 分前にユーザに知らせる	予約検索の開始前にエンドポイントに通知メッセージを表示するには、このオプションを選択します。 注意 この通知メッセージは、[権限およびその他の設定] 画面の [その他の設定] タブで無効にできます。
予約検索を最長 XX 時間 XX 分延期する	予約検索の延期権限を持つユーザが、予約検索を保留または一時停止できる最長の時間を設定します。 注意 予約検索の延期権限は、[権限およびその他の設定] 画面の [権限] タブで付与できます。
検索時間が XX 時間 XX 分以上続いた場合に自動的に予約検索を停止する	設定された時間に達した長時間の予約検索を停止します。
ワイヤレスエンドポイントのバッテリ残量が XX%を下回り、AC アダプタが接続されていない場合は予約検索をスキップする	バッテリ残量が低下している場合にセキュリティエージェントが予約検索を開始しないようにします。
中断された予約検索の再開	ユーザがエンドポイントの電源を切ったために中断された予約検索を指定された時刻に再開します。
実行されなかった予約検索の再開	エンドポイントが実行されていなかったために実行されなかった予約検索を指定された時刻に開始します。

設定	説明
圧縮ファイルの検索	アーカイブファイル内の指定された数の圧縮階層を検索します。 **注意** 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 このオプションを選択して、以下の項目を設定してください。 • 最大階層数: アーカイブファイル内の指定された数の圧縮階層を検索します **注意** 検索する階層が増えると、圧縮されたアーカイブ内に意図的に埋め込まれた不正プログラムが検出される可能性があります。ただし、この場合、システムのパフォーマンスが低下することがあります。 • 解凍後のサイズが XX MB を超える場合はファイルを検索しない: セキュリティエージェントが圧縮されたアーカイブ内にある各ファイルのサイズをチェックし、各ファイルサイズが設定されたしきい値を超えている場合はファイルの検索をスキップできるようにします • 圧縮ファイル内の最初の XX 個のファイルだけ検索する: 設定したしきい値を超える数のファイルがアーカイブに含まれる場合に、セキュリティエージェントが一部のファイルのみを検索するようにします
システム領域の検索	エンドポイント上のハードディスクのシステム領域でウイルス/不正プログラムを検索します。

4. [CPU 使用率] で、次の項目から選択します。
   • 高: 検索が速くなり PC への負荷が最も高くなります。

- 中: 検索の速度も PC への負荷もやや低くなります。
- 低: 検索に時間がかかりますが PC への負荷が最も低くなります。

予約検索: [処理] タブ

手順

1. [ウイルス/不正プログラム] で必要な設定を行います。
   a. セキュリティ上の脅威を検出した場合にセキュリティエージェントで実行する処理の種類を選択します。
      - [Use AntimalwareScanCore]: ウイルスや不正プログラムに対してあらかじめ設定された一連の処理を使用します。

        詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。
        - 潜在的なウイルス/不正プログラムに対する処理のカスタマイズ: 潜在的な不正プログラムの脅威に対してセキュリティエージェントが実行する処理を選択して指定します。
      - すべての種類のウイルス/不正プログラムに同じ処理を使用: すべての不正プログラムの脅威に対してセキュリティエージェントが実行する処理を指定します。
      - 特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用: 特定のセキュリティ上の脅威に対してセキュリティエージェントが実行する処理を指定します。

        詳細については、229 ページの「検出時の処理のカスタマイズ」を参照してください。
   b. エンドユーザに対して表示する通知の種類を選択します。
      - ウイルス/不正プログラムの検出時に通知を表示: 不正プログラムが検出された場合に、セキュリティエージェントユーザに通知を表示します。
      - 潜在的なウイルス/不正プログラムの検出時に通知を表示する: 潜在的な不正プログラムが検出された場合に、セキュリティエージェントユーザに通知を表示します。

c. [駆除前にファイルをバックアップする] を選択して、エンドポイントの <エージェントインストールフォルダ>¥Backup フォルダに感染ファイルの暗号化されたコピーを作成します。

ファイルのバックアップコピーを作成すると、元のバージョンのファイルを必要に応じて復元できます。

d. 隔離ディレクトリの場所を指定します。

- セキュリティエージェントの管理サーバに隔離: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを Apex One サーバに送信します。
- 隔離ディレクトリ: セキュリティエージェントは、すべての感染ファイルの暗号化されたコピーを指定された場所に送信します。

詳細については、230 ページの「隔離ディレクトリ」を参照してください。

e. [ダメージクリーンナップサービス] で、次の項目を設定します。

- クリーンナップの種類
  - 標準クリーンナップ: セキュリティエージェントでは、標準クリーンナップの間に次のいずれかの処理が実行されます。
    - 活動中のトロイの木馬を検出および削除
    - トロイの木馬が作成したプロセスを中止
    - トロイの木馬が変更したシステムファイルを修復
    - トロイの木馬により作成されたファイルとアプリケーションを削除
  - 高度なクリーンナップ: 標準クリーンナップの処理の他に、セキュリティエージェントでは、FakeAV と呼ばれる偽セキュリティソフトウェアや特定のルートキットの変種による活動が停止されます。
- 潜在的なウイルス/不正プログラムが検出された場合にクリーンナップを実行: 潜在的な不正プログラムの脅威に対して設定された種類のクリーンナップを実行します。

注意

このオプションは、潜在的なウイルス/不正プログラムに対する処理が、「放置 (ログのみ)」または「アクセス拒否」以外の場合にのみ選択できます。

2. [スパイウェア/グレーウェア] で、スパイウェア/グレーウェアプログラムを検出した場合にセキュリティエージェントが実行する処理を選択します。

   - 駆除: 関連するプロセスをすべて終了し、関連付けられているレジストリ値、ファイル、Cookie、およびショートカットを削除します。

     注意

     スパイウェア/グレーウェアを駆除した後、セキュリティエージェントでスパイウェア/グレーウェアのデータをバックアップし、スパイウェア/グレーウェアに安全にアクセスできると考えられる場合、復元することができます。

   - 放置: 検出をログに記録しますが、プログラムの実行は許可します。
   - スパイウェア/グレーウェアの検出時にエンドポイントに通知を表示: スパイウェア/グレーウェアが検出された場合に、セキュリティエージェントユーザに通知を表示します。

3. [高度な不正プログラム検出] セクションで、オプションを選択して必要な設定を行います。

   - トレンドマイクロの推奨処理を使用: 検出されたポータブル実行可能ファイルに対してあらかじめ設定された一連の処理を使用します。このオプションを使用することをお勧めします。

     詳細については、228 ページの「トレンドマイクロの推奨処理」を参照してください。

   - 脅威のあるすべての Portable Executable ファイルに同じ処理を使用: 検出されたポータブル実行可能ファイルに対して次のいずれかの処理を適用します。

     - 隔離: 検出されたポータブル実行可能ファイルがシステムによって自動的に隔離されます。

- 放置: 検出ログがシステムによって生成されますが、検出されたポータブル実行可能ファイルに対して処理は適用されません。

注意

検出されたポータブル実行可能ファイルが検索除外リストにある場合、システムではそのファイルに対して処理が適用されません。

予約検索: [検索除外] タブ

手順

1. [検索除外を有効にする] を選選択します。
2. [検索除外リスト (ディレクトリ)] で必要な設定を行います。
   a. [トレンドマイクロ製品がインストールされているディレクトリの除外] を選択して、他のトレンドマイクロ製品に関連付けられているディレクトリが自動的に除外されるようにします。

      詳細については、236 ページの「トレンドマイクロ製品ディレクトリの除外」を参照してください。

   b. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
      - 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

注意

子ポリシーが [親ポリシーから拡張] に設定されている場合、[子ポリシーの制限] も設定できます。この制限によって、子ポリシーによって特定のオブジェクトがリストに追加されることを防止できます。

   c. 検索から除外するディレクトリパスを入力して、[+] ボタンをクリックします。

セキュリティエージェントは、指定されたディレクトリ (およびサブディレクトリ) にあるファイルを検索しません。

注意

- 検索から除外するディレクトリを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ディレクトリの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

3. [検索除外リスト (ファイル)] で必要な設定を行います。
   a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
      - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
      - 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。
   b. 検索から除外するファイル名または完全なディレクトリパスを含むファイル名を入力して、[+] ボタンをクリックします。

注意

- 検索から除外するファイルを最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- ファイルの除外ではワイルドカード文字を使用できます。

  詳細については、236 ページの「ワイルドカードによる除外設定」を参照してください。

4. [検索除外リスト (ファイル拡張子)] で必要な設定を行います。

a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

- 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
- 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

b. 検索から除外するファイル拡張子を選択または入力して、[追加 >] ボタンをクリックします。

注意

- 検索から除外するファイル拡張子を最大 256 個指定できます。
- リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。
- 手動検索、予約検索、および ScanNow の場合、ワイルドカード文字として疑問符 (?) を使用して 1 つの文字を置き換えるか、アスタリスク (*) を使用して複数の文字を置き換えます。たとえば、DOC、DOT、DAT など、D で始まる拡張子を持つすべてのファイルを検索しない場合は、「`D*`」または「`D??`」と入力します。

検出時の処理

検出された不正プログラムの種類に基づいて事前定義済みの一連の検索処理またはカスタム処理を使用するようにセキュリティエージェントを設定できます。

重要

ファイルによっては駆除できないものもあります。

詳細については、次のページを参照してください。

トレンドマイクロの推奨処理

ウイルス/不正プログラムの種類ごとに、異なる検索処理が必要になります。検索処理のカスタマイズには、ウイルス/不正プログラムに関する知識が必要であり、時間と手間のかかる作業になる可能性があります。トレンドマイクロの推奨処理を使用して、この問題に対応することが可能です。

トレンドマイクロの推奨処理とは、ウイルス/不正プログラムに事前に割り当てられている一連の検索処理です。検索処理について詳しくない場合や、ウイルス/不正プログラムに適した検索処理の判断が難しい場合は、トレンドマイクロの推奨処理をお勧めします。

トレンドマイクロの推奨処理を使用する利点は、次のとおりです。

- トレンドマイクロの推奨処理では、トレンドマイクロが推奨する検索処理が使用されます。検出時の処理を設定する手間が省けます。
- ウイルス作成者は、ウイルス/不正プログラムによる攻撃手段を絶えず変えています。トレンドマイクロの推奨処理の設定は、最新の脅威やウイルス/不正プログラムの最新の攻撃手段に対応して保護できるように更新されます。

次の表は、ウイルス/不正プログラムの種類に応じて適用されるトレンドマイクロの推奨処理を示しています。

表 10-2. ウイルス/不正プログラムに適用されるトレンドマイクロの推奨処理

ウイルス/不正プログラム	リアルタイム検索		手動検索/予約検索	
	1 次処理	2 次処理	1 次処理	2 次処理
CVE セキュリティホール	放置 (ログのみ)	該当なし	該当なし	該当なし
ジョークプログラム	隔離	該当なし	隔離	該当なし
トロイの木馬	隔離	該当なし	隔離	該当なし
ウイルス	駆除	隔離	駆除	隔離
テストウイルス	アクセス拒否	該当なし	放置 (ログのみ)	該当なし

ウイルス/不正プログラム	リアルタイム検索		手動検索/予約検索	
	1 次処理	2 次処理	1 次処理	2 次処理
パッカー	隔離	該当なし	隔離	該当なし
その他	駆除	隔離	駆除	隔離
潜在的な不正プログラム	放置 (ログのみ)	該当なし	放置(ログのみ)またはユーザ設定の処理	該当なし

注意

- 潜在的なウイルス/不正プログラムの場合、リアルタイム検索の初期設定の処理は「アクセス拒否」、手動検索および予約検索の初期設定の処理は「放置 (ログのみ)」です。これらが適切な処理ではない場合、「隔離」、「削除」、「拡張子変更」などに変更できます。
- ファイルによっては駆除できないものもあります。
- トレンドマイクロの推奨処理は、スパイウェア/グレーウェア検索には使用できません。

検出時の処理のカスタマイズ

処理	説明
削除	感染ファイルを削除します。
隔離	感染ファイルの名前を変更し、エンドポイントの一時隔離ディレクトリに移動します。 セキュリティエージェントは、次に、隔離されたファイルを指定された隔離ディレクトリ (初期設定では管理サーバにあります) に送信します。 セキュリティエージェントは、このディレクトリに送信される隔離ファイルを暗号化します。 詳細については、230 ページの「隔離ディレクトリ」を参照してください。

処理	説明
駆除	感染したファイルから、ウイルスコード部分を取り除きます。 駆除不可能な場合、セキュリティエージェントは 2 次処理として「隔離」、「削除」、「拡張子変更」、または「放置」のいずれかを実行します。 この処理は、潜在的なウイルス/不正プログラム以外のあらゆる種類のセキュリティ上の脅威に対して実行できます。 **注意** ファイルによっては駆除できないものもあります。詳細については、232 ページの「ウイルス駆除できないファイル」を参照してください。
拡張子変更	感染ファイルの拡張子を `vir` に変更します。ユーザは拡張子変更されたファイルを開くことはできませんが、特定のアプリケーションと関連付ければ開くことは可能です。 拡張子変更された感染ファイルを開くと、ウイルス/不正プログラムが実行されるおそれがあります。
放置	検出された脅威に対して処理は実行せず、検出されたことをログに記録します。
アクセス拒否	セキュリティエージェントで、感染ファイルを開こうとしたり実行しようとしたりする操作を検出した場合、ただちに操作がブロックされます。 ユーザは感染ファイルを手動で削除できます。

隔離ディレクトリ

感染ファイルの処理が「隔離」の場合、セキュリティエージェントはそのファイルを暗号化し、<エージェントインストールフォルダ>\SUSPECT にある一時隔離フォルダに移動します。次に、指定された隔離ディレクトリにファイルを送信します。

注意
暗号化された隔離ファイルにアクセスする必要がある場合には、そのファイルを復元することができます。

初期設定の隔離ディレクトリをそのまま使用します。このディレクトリは Apex One サーバコンピュータに配置され、サーバのホスト名または IP アドレスを含む URL の形式で指定されます。

- サーバが IPv4 と IPv6 の両方のエージェントを管理している場合は、すべてのセキュリティエージェントが隔離ファイルをサーバに送信できるようにホスト名を使用してください。
- サーバの識別に IPv4 アドレスのみが使用されている場合、サーバに隔離ファイルを送信できるのは、IPv4 シングルスタックセキュリティエージェントとデュアルスタックエージェントのみです。
- サーバの識別に IPv6 アドレスのみが使用されている場合、サーバに隔離ファイルを送信できるのは、IPv6 シングルスタックセキュリティエージェントとデュアルスタックエージェントのみです。

URL、UNC パス、あるいは絶対ファイルパスの形式で、別の隔離ディレクトリを指定することもできます。セキュリティエージェントから接続可能なディレクトリを指定する必要があります。たとえば、この代替ディレクトリがデュアルスタックセキュリティエージェントおよび IPv6 シングルスタックエージェントから隔離ファイルを受信する場合は、ディレクトリに IPv6 アドレスが割り当てられている必要があります。代替ディレクトリにはデュアルスタックディレクトリを指定し、ホスト名でそのディレクトリを識別して、ディレクトリを入力する際には UNC パスを使用することをお勧めします。

次の表は、URL、UNC パス、または絶対ファイルパスを使用する状況について説明しています。

表 10-3. 隔離ディレクトリ

隔離ディレクトリ	使用可能な形式	例	備考
管理サーバコンピュータのディレクトリ	URL	`http://<osceserver>`	これは初期設定のディレクトリです。 隔離フォルダのサイズなど、このディレクトリの設定を行います。
	UNC パス	`¥¥<osceserver>¥ofcscan¥Virus`	
他の Apex One サーバコンピュータのディレクトリ (ネットワーク	URL	`http://<osceserver2>`	セキュリティエージェントがこのディレクトリに接続可能であることを確認します。間違ったディレクトリを指定した場合、セキュリ

隔離ディレクトリ	使用可能な形式	例	備考
上に他の Apex One サーバがある場合)	UNC パス	¥¥<osceserver2>¥ofcscan¥Virus	ティエージェントは正しい隔離ディレクトリが指定されるまで、\Suspect フォルダに隔離ファイルを保存します。サーバのウイルス/不正プログラムログには、隔離ファイルを指定された隔離フォルダに移動できなかったことが記録されます。 UNC パスを使用している場合、隔離ディレクトリフォルダが「Everyone」グループで共有されていることと、このグループに対して読み取り/書き込み許可を割り当てていることを確認してください。
ネットワーク上の別のエンドポイント	UNC パス	¥¥<computer_name>¥temp	
セキュリティエージェントの別のディレクトリ	絶対パス	C:¥temp	

ウイルス駆除できないファイル

ウイルス検索エンジンでは、次のファイルを駆除できません。

表 10-4. 駆除できないファイルの解決策

駆除できないファイル	説明と解決策
トロイの木馬に感染したファイル	トロイの木馬は、メッセージの表示、ファイルの消去、ディスクのフォーマットなど、予期しない、または許可されていない一般に不正な処理を実行するプログラムです。トロイの木馬はファイルに感染しないため駆除は必要はありません。 解決策: ダメージクリーンナップエンジンとダメージクリーンナップテンプレートを使用してトロイの木馬を削除します。
ワームに感染したファイル	ワームは、ワーム自体またはその一部の動作可能なコピーを他のエンドポイントシステムに拡散できる自己完結型プログラムまたはプログラムのセットです。伝播には通常、ネットワーク接続やメールの添付ファイルが利用されます。ワームはファイルが自己完結型プログラムであるため駆除できません。 解決策:トレンドマイクロではワームを削除することをお勧めします。

駆除できないファイル	説明と解決策
書き込み保護された感染ファイル	解決策:ファイルを駆除できるよう書き込み保護を解除します。
パスワード保護されたファイル	パスワード保護されたファイルには、パスワード保護された圧縮ファイルや Microsoft Office ファイルが含まれます。 解決策:ファイルを駆除できるようパスワード保護を解除します。
バックアップファイル	RB0～RB9 のような拡張子を持つファイルは感染ファイルのバックアップコピーです。駆除処理中にウイルス/不正プログラムによってファイルが破壊された場合に備えて、駆除処理では感染ファイルのバックアップを作成します。 解決策: 正常に駆除された場合、感染ファイルのバックアップコピーを残しておく必要はありません。エンドポイントが通常どおり機能している場合は、バックアップファイルを削除してもかまいません。
ごみ箱の感染ファイル	システムが稼働中のため、ごみ箱から感染ファイルを削除できない場合があります。
	1. エンドポイントに管理者権限でログオンします。 2. アプリケーションがファイルをロックし、Windows で削除できなくなることを防止するため、実行中のアプリケーションをすべて閉じます。 3. コマンドプロンプトを開きます。 4. 次を入力してファイルを削除します。 `del /s \$Recycle.Bin\*` 5. ファイルが削除されたかどうか確認します。
Windows の一時フォルダまたは Internet Explorer の一時フォルダ内の感染ファイル	エンドポイントが使用しているため、Windows の一時フォルダまたは Internet Explorer の一時フォルダ内の感染ファイルを駆除できない場合があります。駆除するファイルが Windows の動作に必要な一時ファイルである場合もあります。
	1. エンドポイントに管理者権限でログオンします。 2. アプリケーションがファイルをロックし、Windows で削除できなくなることを防止するため、実行中のアプリケーションをすべて閉じます。

駆除できないファイル	説明と解決策

	3. 感染ファイルが Windows の一時フォルダにある場合:
	a. コマンドプロンプトを開きます。
	b. 次を入力してファイルを削除します。
	`del /s \Windows\Temp\*`
	c. エンドポイントを通常モードで再起動します。
	4. 感染ファイルが Internet Explorer の一時フォルダにある場合:
	a. コマンドプロンプトを開き、Internet Explorer の一時フォルダに移動します。
	• Windows 7: `%LocalAppData%¥Microsoft¥Windows¥Temporary Internet Files`
	• Windows 8/8.1: `%LocalAppData%¥Microsoft¥Windows¥INetCache`
	• Windows 10: `%LocalAppData%¥Microsoft¥Windows¥INetCache¥IE`
	b. 次を入力してファイルを削除します。
	`del /s .\*`
	最後のコマンドで Internet Explorer の一時フォルダ内のすべてのファイルが削除されます。
	c. エンドポイントを通常モードで再起動します。

サポートされていない圧縮形式で圧縮されたファイル	解決策:ファイルを解凍します。
現在実行中のロックされたファイル	解決策:ファイルのロックを解除するか、実行が終了するまで待ちます。
破損しているファイル	解決策:ファイルを削除します。

トロイの木馬に感染したファイル

トロイの木馬は、メッセージの表示、ファイルの消去、ディスクのフォーマットなど、予期しない、または許可されていない一般に不正な処理を実行す

るプログラムです。トロイの木馬はファイルに感染しないため駆除は必要はありません。

解決策: セキュリティエージェントでは、ダメージクリーンナップエンジンとダメージクリーンナップテンプレートを使用してトロイの木馬を除去します。

ワームに感染したファイル

ワームは、ワーム自体またはその一部の動作可能なコピーを他のエンドポイントシステムに拡散できる自己完結型プログラムまたはプログラムのセットです。伝播には通常、ネットワーク接続やメールの添付ファイルが利用されます。ワームはファイルが自己完結型プログラムであるため駆除できません。

解決策:トレンドマイクロではワームを削除することをお勧めします。

書き込み保護された感染ファイル

解決策: 書き込み保護を解除して、セキュリティエージェントがファイルを駆除できるようにします。

パスワードで保護されたファイル

パスワードで保護された圧縮ファイルまたはパスワードで保護された Microsoft Office ファイルを追加します。

解決策: パスワード保護を解除し、セキュリティエージェントがこれらのファイルを駆除できるようにします。

バックアップファイル

RB0～RB9 の拡張子が付いたファイルは、感染したファイルのバックアップコピーです。セキュリティエージェントでは、駆除プロセス中にウイルス/不正プログラムによってファイルが破損された場合、感染ファイルのバックアップを作成します。

解決策: セキュリティエージェントが感染ファイルを正常に駆除した場合は、バックアップコピーを保持する必要はありません。エンドポイントが通常どおり機能している場合は、バックアップファイルを削除してもかまいません。

検索除外のサポート

ディレクトリとファイル名を不正プログラム検索から除外する場合は、次のサポート情報を参照してください。

トレンドマイクロ製品ディレクトリの除外

[検索除外リスト (ディレクトリ)] で [トレンドマイクロ製品がインストールされているディレクトリの除外] を選択した場合、セキュリティエージェントは次の製品のディレクトリを自動的に除外します。

- <サーバインストールフォルダ>
- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- InterScan eManager 3.11、5.1、5.11、5.12
- InterScan for Lotus Notes eManager NT
- InterScan for Microsoft Exchange

ワイルドカードによる除外設定

ファイルとディレクトリに対する検索除外リストでは、ワイルドカード文字を使用できます。「?」は任意の 1 文字を表し、「*」は任意の文字列を表します。

ワイルドカード文字は慎重に使用してください。間違った文字を使用すると、意図しないファイルやディレクトリが除外されることがあります。たとえば、C:¥*を検索除外リスト (ファイル) に追加すると、C:¥ドライブ全体が除外されます。

表 10-5. ワイルドカード文字を使用した検索除外

値	除外されるもの	除外されないもの
c:\director*\fil*.txt	c:¥directory¥fil¥doc.txt c:¥directories¥fil¥files¥document.txt	c:¥directory¥file¥ c:¥directories¥files¥ c:¥directory¥file¥doc.txt c:¥directories¥files¥document.txt
c:\director?\file*.txt	c:¥directory¥file¥doc.txt	c:¥directories¥file¥document.txt
c:\director?\file\?.txt	c:¥directory¥file¥1.txt	c:¥directory¥file¥doc.txt c:¥directories¥file¥document.txt
c:*.txt	C:¥ディレクトリ内のすべての .txt ファイル	C:¥ディレクトリ内のその他のすべてのファイルタイプ
[]	サポートされていません	サポートされていません

第 11 章

Web レピュテーションポリシー設定

ここでは、セキュリティエージェントで Web レピュテーションポリシーを設定する方法について説明します。

この章は次のトピックで構成されます。

Web レピュテーション

Web レピュテーションテクノロジは、Web サイトの経過日数、配置場所の変更履歴、および不正プログラムの挙動分析により検出された不審な活動の兆候などの要素に基づいてレピュテーションスコアを割り当てることにより、Web ドメインの信頼性を追跡します。トレンドマイクロでは、Web サイトを継続的に分析して Web レピュテーションスコアをアップデートし、不正と思われるコンテンツにユーザがアクセスできないようにしています。

ユーザが Web サイトにアクセスしようとすると、セキュリティエージェントは Smart Protection ソースに対するクエリを実行して、コンテンツのリスクレベルを特定します。Web サイトへのアクセスを許可するかどうかは、セキュリティエージェントに対して設定された Web レピュテーションポリシーによって決まります。

Web レピュテーションの機能を使用すると、安全または危険と見なされる Web サイトを承認済みリストまたはブロックリストに追加できます。セキュリティエージェントは、これらのリストに追加された Web サイトについて Web レピュテーションスコアを照会せず、アクセスを自動的に許可またはブロックします。

Web レピュテーションポリシーの設定

組織の HTTP 通信を処理するプロキシサーバを設定しており、Web アクセスを許可する前に認証を要求する場合は、プロキシサーバ認証の資格情報を指定します。

手順

1. [外部エージェント] タブを選択して外部エージェントのポリシーを設定するか、[内部エージェント] タブを選択して内部エージェントのポリシーを設定します。
2. [次の OS で Web レピュテーションを有効にする] で、保護する Windows プラットフォームの種類 ([Windows デスクトッププラットフォーム] および [Windows Server プラットフォーム]) を選択します。

ヒント

Web レピュテーション機能を備えたトレンドマイクロ製品 (Trend Micro InterScan Web Security Virtual Appliance など) をすでに使用している場合には、内部エージェントの Web レピュテーションは無効にすることをお勧めします。

3. [診断モードを有効にする] を選択します。

注意

診断モードのセキュリティエージェントでは、すべての Web サイトへのアクセスが許可されます。[セキュリティレベル] の設定に違反する Web サイトへのアクセスについては、セキュリティエージェントでそのイベントがログに記録されます。診断モードを使用すると、Web サイトへのアクセスを監視し、ユーザによるアクセスをブロックする前に Web サイトの安全性を評価できます。アクセスログの評価に基づいて、信頼する Web サイトを承認済み URL リストに追加してから診断モードを無効にすることができます。

4. [HTTPS URL を確認する] を選択します。

重要

HTTPS URL の検索では、HTTP/2 プロトコルもサポートされます。Web レピュテーションで HTTPS URL または HTTP/2 URL を確認する前に、ブラウザごとにいくつかの設定を済ませておく必要があります。

詳細については、245 ページの「HTTPS URL 検索のサポート」を参照してください。

5. Web レピュテーションの検索を、ポート 80、81、および 8080 を通過するトラフィックに制限するには、[共通 HTTP ポートのみを検索] を選択します。初期設定では、Web レピュテーションではすべてのポートのすべてのトラフィックを検索します。

注意

Windows 7、Windows 8、Windows 8.1、Windows 10、または Windows Server 2008 R2、Windows Server 2012、およびそれ以降のプラットフォームではサポートされません。

6. 内部セキュリティエージェントから Smart Protection Server に Web レピュテーションクエリを送信する場合は、[Smart Protection Server にクエリを送信する] を選択します。

   - このオプションを有効にする場合は、次の点に注意してください。
     - エージェントは、Trend Micro Smart Protection ソースリストを参照して、クエリを送信する Smart Protection Server を決定します。
     - Smart Protection Server が使用可能であることを確認します。どの Smart Protection Server も使用できない場合、エージェントは Smart Protection Network にクエリを送信しません。この場合、エージェントが使用できる Web レピュテーションデータソースは承認済み URL リスト/URL ブロックリストのみです。
     - 評価されていない Web サイトはブロックされません。これらの Web サイトの Web レピュテーションデータは Smart Protection Server で保存されません。
   - このオプションを無効にする場合は、次の点に注意してください。
     - エージェントは、Trend Micro Smart Protection Network に Web レピュテーションクエリを送信します。クエリを送信するために、エンドポイントにはインターネット接続が必要です。
     - [トレンドマイクロによってまだ評価されていないページをブロックする] オプションを選択した場合、評価されていない Web サイトがブロックされます。

注意

Web レピュテーションクエリをローカルの Smart Protection Server に送信するよう、内部のオンプレミスセキュリティエージェントを設定するだけです。

7. Web レピュテーションセキュリティレベルを [高]、[中]、[低] から選択します。

注意

Web レピュテーションは、セキュリティレベルに従って URL へのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを低に設定すると、Web レピュテーションは Web からの脅威と認識されている URL のみをブロックします。セキュリティレベルをより高く設定すると、Web からの脅威の検出率が増加しますが、誤検出の可能性も増加します。

8. [トレンドマイクロによってまだ評価されていないページをブロックします] は、[Smart Protection Server にクエリを送信する] オプションを無効にした場合に選択できます。

注意

トレンドマイクロは、安全のために Web ページを積極的に評価していますが、ユーザが新しい Web サイトやあまり利用されない Web サイトにアクセスすると、未評価のページに遭遇する可能性があります。未評価のページへのアクセスをブロックすると、安全性は向上しますが、安全なページへのアクセスもブロックされる場合があります。

9. Web ブラウザの脆弱性および不正なスクリプトを特定し、Web ブラウザをセキュリティ侵害から保護するには、[不正なスクリプトを含むページをブロックする] を選択します。

   Web レピュテーションは、ブラウザ脆弱性対策パターンファイルとスクリプトアナライザパターンファイルの両方を利用して、システムが危険にさらされる前に Web ページを特定してブロックします。

重要

- ブラウザ脆弱性対策機能では、レガシー版 Microsoft Edge、Chromium 版 Microsoft Edge、Mozilla Firefox、Chrome の各ブラウザの HTTP トラフィック分析のみがサポートされます。
- ブラウザ脆弱性対策機能を使用するには、高度な保護サービスを有効にする必要があります。

10. 承認済みリストとブロックリストを設定します。

注意

承認済みリストはブロックリストより優先されます。ある URL が承認済みリストのエントリに一致する場合は、同じ URL がブロックリストにあってもその URL へのアクセスは常に許可されます。

a. [承認済み/ブロックリストを有効にする] を選択します。

b. URL を入力します。

URL では、任意の場所でワイルドカード文字 (*) を使用できます。

例:

- 「`www.trendmicro.com/*`」と入力すると、トレンドマイクロの Web サイト内のすべてのページが Web レピュテーションで承認されます。
- 「`*.trendmicro.com/*`」と入力すると、`trendmicro.com` のサブドメインのすべてのページが Web レピュテーションで承認されます。

IP アドレスを含む URL も入力できます。URL が IPv6 アドレスを含む場合は、アドレスをカッコ () で囲んで指定します。

c. [承認済みリストに追加]、または [ブロックリストに追加] をクリックします。

重要

Web レピュテーションは、承認済みリストとブロックリストにあるアドレスに対しては検索を実行しません。

11. Web レピュテーションのフィードバックを送信するには、[URL の再診断] にある URL をクリックします。ブラウザウィンドウに Trend Micro Site Safety Center が表示されます。
12. セキュリティエージェントからサーバへのレピュテーションログの送信を許可するかどうかを選択します。Web レピュテーションでブロックされている URL を分析して安全と考えられる URL に対して適切な処理を実行する場合には、エージェントからのログの送信を許可してください。

HTTPS URL 検索のサポート

HTTPS 通信では、証明書を使用して Web サーバを識別します。またデータを暗号化することで、漏えいや盗聴から情報を保護します。より安全な手法ですが、HTTPS を使用した Web サイトへのアクセスにも危険はあります。有効なセキュリティ証明書を使用していても、それが感染しているサイトであれば、不正プログラムがホストされていたり個人情報が盗まれる可能性があります。証明書は比較的容易に入手できるため、HTTPS を使用する不正な Web サーバを簡単に設定することもできます。

[HTTPS URL を確認する] を有効にすると、HTTPS を使用する感染しているサイトや不正なサイトにアクセスする危険性を低減できます。Web レピュテーションでは、次のブラウザで HTTPS トラフィックを監視できます。

表 11-1. HTTPS トラフィックでサポートされるブラウザ

ブラウザ	バージョン番号	前提条件
Mozilla Firefox	3.5 以降	なし
Chrome	最新バージョン	
Microsoft Edge	• レガシ • Chromium	

第 12 章

未知の脅威対策

ここでは、まだ特定されていない脅威、対象となる脅威、またはあまり普及していない脅威を検出して保護するようにセキュリティエージェントを設定する方法について説明します。

この章は次のトピックで構成されます。

機械学習型検索

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジを使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどのファイル機能を使用した詳細なファイル分析により未知のセキュリティリスクを検出します。また、不明なプロセスやあまり普及していないプロセスの挙動分析を実行して、ネットワークへの侵入を試みる未知の新しい脅威がないかどうかを判定します。

機械学習型検索は、未知の脅威およびゼロデイ攻撃から環境を保護するのに役立つ強力な検索方法です。

検出の種類	説明
ファイル	不明なファイルやあまり普及していないファイルを検出すると、セキュリティエージェントは、高度な脅威検索エンジン (ATSE) でファイルを検索してファイル特性を抽出し、Trend Micro Smart Protection Network でホストされる機械学習型検索エンジンにレポートを送信します。機械学習型検索では、不正プログラムモデリングにより、サンプルを不正プログラムモデルと比較し、可能性スコアを割り当て、ファイルに含まれる潜在的な不正プログラムの種類を判別します。 インターネット接続が使用できなくなった場合は、機械学習型検索が自動的にローカルモデルに切り替わって未知の脅威からの継続的な保護を実現し、Portable Executable ファイルの脅威に対応します。 機械学習型検索の設定に応じて、ネットワークへの脅威の拡散を防ぐために、セキュリティエージェントは該当するファイルの「隔離」を試みます。

検出の種類	説明
プロセス	不明なプロセスやあまり普及していないプロセスを検出すると、セキュリティエージェントは、CI エンジンを使用してプロセスを監視し、動作レポートを機械学習型検索エンジンに送信します。機械学習型検索では、不正プログラムの動作モデリングにより、サンプルをモデルと比較し、可能性のスコアを割り当て、プロセスが実行する潜在的な不正プログラムの種類を判別します。 プロセスの検出ではスクリプトの実行も監視対象となります。CI エンジンが不審スクリプトの実行を検出すると、機械学習型検索は設定された処理を実行します。 機械学習型検索では、次の種類のスクリプトに対してスクリプトのブロックを実行します。 • cscript • jar • powershell • vbs • wscript 機械学習型検索の設定に応じて、セキュリティエージェントは該当するプロセスまたはスクリプトを「終了」し、プロセスまたはスクリプトを実行したファイルの駆除を試みます。

機械学習型検索設定

注意

機械学習型検索を使用するには、次のサービスを有効にする必要があります。

- 不正変更防止サービス
- 高度な保護サービス

手順

1. [機械学習型検索を有効にする] を選択します。
2. [検出設定] で、機械学習型検索で実行する検出の種類とそれに対する処理を選択します。

検出の種類	処理
ファイル	• 隔離: 機械学習型検索による分析で不正プログラムに似た特性を示すと判定されたファイルを自動的に隔離する場合に選択します。 • ログのみ: 脅威について内部で詳しく調査するために、不明なファイルを検索して機械学習型検索による分析をログに記録する場合に選択します。
プロセス	• 終了: 機械学習型検索による分析で不正プログラムに似た挙動を示すと判定されたプロセスまたはスクリプトを自動的に終了する場合に選択します。 重要 機械学習型検索は、不正なプロセスまたはスクリプトを実行したファイルの駆除を試みます。駆除に失敗した場合、該当するファイルは機械学習型検索によって隔離されます。 • ログのみ: 脅威について内部で詳しく調査するために、不明なプロセスまたはスクリプトを検索して機械学習型検索による分析をログに記録する場合に選択します。

3. [除外] で、機械学習型検索のグローバル除外ファイルリストを設定します。このリストに追加したファイルは、いずれのエージェントでも不正ファイルとして検出されなくなります。

   a. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。

      • 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。

      • 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

注意

子ポリシーが [親ポリシーから拡張] に設定されている場合、[子ポリシーの制限] も設定できます。この制限によって、子ポリシーによって特定のオブジェクトがリストに追加されることを防止できます。

b. [ファイルハッシュを追加] をクリックします。

[ファイルを除外リストに追加] 画面が表示されます。

注意

リストを別のポリシーと共有するには、[インポート] ボタンと [エクスポート] ボタンを使用します。

c. 検索から除外するファイルの SHA-1 ハッシュ値を指定します。

d. 必要に応じて、除外する理由やハッシュ値に関連付けられているファイル名を入力します。

e. [追加] をクリックします。

ファイルハッシュが除外リストに追加されます。

サンプル送信の設定

まだ特定されていない未知の脅威を含む可能性があるファイルオブジェクトが検出された場合、詳しい分析のために仮想アナライザに送信するようにセキュリティエージェントを設定できます。オブジェクトが未知の脅威を含むと判定した場合、仮想アナライザはオブジェクトを不審オブジェクトリストに追加し、そのリストをネットワーク上の他のすべてのセキュリティエージェントに配信します。

不審ファイルには以下が含まれます。

- トレンドマイクロで認識していないプログラム (サポート対象の Web ブラウザまたはメールからダウンロード)
- ヒューリスティック検索で検出されたプロセス (サポート対象の Web ブラウザまたはメールからダウンロード)

- リムーバブルストレージ上のあまり普及していない自動実行プログラム

重要

セキュリティエージェントから送信できるサンプルファイルのサイズは、使用する仮想アナライザの種類に応じて異なります。Deep Discovery Analyzer サーバの場合、サンプルファイルの最大サイズは 50MB です。Deep Discovery Analyzer as a Service アドオンの場合、サンプルファイルの最大サイズは 60MB です。

手順

1. [仮想アナライザへの不審ファイルの送信を有効にする] を選択します。

不審接続監視の設定

セキュリティエージェントでは、エンドポイントとグローバル C&C IP リスト内のアドレス間の接続をすべてブロックしてログに記録できます。ログに記録したうえで、ユーザ指定のブロック IP リストに設定された IP アドレスへのアクセスを許可することもできます。

また、ボットネットやその他の不正プログラムに起因する接続も監視でき、不正プログラムの脅威が検出された場合はこれを駆除できます。

手順

1. トレンドマイクロで確認済みの C&C サーバへの接続を監視するには、[グローバル C&C IP リスト内のアドレスへのネットワーク接続を検出] 設定を有効にし、[ログのみ] または [ブロック] のいずれかを選択します。
   - ユーザ指定ブロック IP リスト内のアドレスへの接続をエージェントに許可するには、[ユーザ指定ブロック IP リスト内のアドレスへのアクセスを許可してログに記録] 設定を有効にします。

注意

ユーザ指定ブロック IP リスト内のアドレスへのアクセスを許可するためには、まず [グローバル C&C IP リスト内のアドレスへのネットワーク接続をログに記録] を有効にする必要があります。

2. [不正プログラムネットワークフィンガープリントを使用して接続を検出] 設定を有効にし、[ログのみ] または [ブロック] のいずれかを選択します。

   - C&C サーバへの接続を止めるには、[C&C コールバックの検出時に不審接続監視元を駆除] 設定を有効にします。セキュリティエージェントは、GeneriClean を使用して不正プログラムの脅威を駆除し、C&C サーバへの接続を終了します。

注意

パケット構造のマッチングで検出された C&C サーバへの接続を止めるためには、まず [不正プログラムネットワークフィンガープリントを使用して接続をログに記録] を有効にする必要があります。

第 13 章

デバイスコントロールポリシー設定

ここでは、セキュリティエージェントでデバイスコントロールポリシーを設定する方法について説明します。

この章は次のトピックで構成されます。

デバイスコントロール

デバイスコントロールは、コンピュータに接続されている外部のストレージデバイスやネットワークリソースへのアクセスを規制します。デバイスコントロール機能により、データの損失や漏えいを防ぐことができ、またファイル検索と併用することでセキュリティリスクからの保護が実現されます。

内部エージェントと外部エージェントに対してデバイスコントロールポリシーを設定できます。通常は、外部エージェントに対してより厳格なポリシーを設定します。

Apex Central には、エンドポイントベースとユーザベースの両方のデバイスコントロールポリシー設定が用意されています。

デバイスコントロール設定

手順

1. [デバイスコントロールを有効にする] を選択します。
   - [外部エージェント] タブで [内部エージェントにすべての設定を適用する] を選択すると、設定を内部エージェントに適用できます。
   - [内部エージェント] タブで [外部エージェントにすべての設定を適用する] を選択すると、設定を外部エージェントに適用できます。
2. デバイスコントロールルールを追加または編集します。
   - ユーザベースのルールの場合:
     - Active Directory のユーザまたはグループアカウントに基づいてルールを作成するには、[追加] をクリックします。
     - Active Directory のユーザまたはグループアカウントに基づいてルールを編集するには、[ユーザアカウント] 列のリンクをクリックします。

重要

ユーザベースのデバイスコントロールルールを使用できるのは、Active Directory を Apex Central と統合した後のみです。

- 初期設定のエンドポイントベースのルールを編集するには、次の手順を実行します。
  - [ユーザアカウント] 列の [すべてのユーザ (初期設定)] リンクをクリックします。

注意

初期設定のエンドポイントベースのルールを削除することはできません。

[デバイスコントロールルール] 画面が表示されます。

3. [ユーザアカウント] で、ルールを適用する Active Directory のユーザまたはグループアカウントの表示名を入力および選択します。

注意

初期設定の [すべてのユーザ (初期設定)] のエンドポイントベースのルールの編集時にユーザまたはグループアカウントを指定することはできません。

4. [ストレージデバイス] で、次の手順を実行します。
   a. 各ストレージデバイスの権限を選択します。

重要

- データ保護が有効になっているセキュリティエージェントのみ、「ブロック」処理を実行できます。データ保護が有効になっていないセキュリティエージェントにポリシーを配信する場合、Apex One はドロップダウンボックスで設定された処理を適用します。
- Apex One は、データ保護が有効になっていない場合でも、サポートしているデバイスモデルのリスト に含まれる USB デバイスに設定されたアクセス権限を自動的に適用します。

権限の詳細については、260 ページの「デバイスに対する権限」を参照してください。

いずれかのストレージデバイスへのアクセスを制限するように選択した場合は、[許可するプログラム] ボタンが表示されます。USB ストレージデバイスの場合は、[ブロック (情報漏えい対策オプション)] を選択すると、[許可する USB デバイス] ボタンが表示されます。

b. (オプション) [許可するプログラム] をクリックして、どの種類のデバイスでもデバイスコントロールによってアクセスが制限されないプログラムのリストを設定します。

[許可するプログラム] 画面が表示されます。

1. デバイスコントロールがユーザのアクセスを許可するプログラムのフルパスまたは信頼済みのデジタル署名プロバイダの情報を入力します。

注意

- デジタル署名プロバイダを指定したときにデバイスコントロールで許可されるのは、発行元が署名したプログラムの実行のみです。

  詳細については、263 ページの「デジタル署名プロバイダの指定」を参照してください。

- プログラムのフルパスを指定したときは、デバイスコントロールの [許可するプログラム] リストでワイルドカード文字を使用できます。

  詳細については、262 ページの「デバイスコントロールの [許可されたプログラム] リストでのワイルドカードのサポート」を参照してください。

---

2. [追加] をクリックします。

   プログラムのフルパスまたは信頼済みのデジタル署名プロバイダの情報がリストに表示されます。

3. プログラムの実行または読み取り/書き込みを許可するかどうかを選択します。

4. [OK] をクリックします。

c. (オプション) [許可する USB デバイス] をクリックして、デバイスコントロールでブロックしない USB デバイスのリストを設定します。

   [許可する USB デバイス] 画面が表示されます。

   1. デバイスのベンダ、モデル、およびシリアル ID をリストに入力します。
   2. さらにデバイスを追加するには、プラス (+) アイコンをクリックします。
   3. [権限] リストで、指定された USB デバイスへのアクセスをデバイスコントロールからユーザに許可する際のアクセスレベルを指定します。
   4. [OK] をクリックします。

d. [USB ストレージデバイスの自動実行機能をブロックする] を選択して、USB デバイスに保存されたプログラムが自動的に実行されないようにします。

e. [デバイスへの不正アクセスの検出時にエンドポイントに通知メッセージを表示] を選択すると、デバイスコントロールによってデバイスへのアクセスが制限されたことをエンドユーザに通知できます。

5. 情報漏えい対策オプション機能がインストールされているセキュリティエージェントの場合は、[モバイルデバイス] および [非ストレージデバイス] に表示されているデバイスへのアクセスを許可するかブロックするかを選択します。

6. [OK] をクリックします。

注意

デバイスコントロールは、初期設定のエンドポイントベースのルール ([すべてのユーザ (初期設定)]) よりも優先して、ユーザベースのすべてのルールを自動的に割り当てます。

---

7. (オプション) デバイスコントロールルールのリストを管理します。

   - 優先度: 矢印をクリックして、ユーザベースのルールの優先度を変更します。

- コピー: ルールを選択して [コピー] をクリックし、ルールの内容を変更します。
- 削除: ルールを選択して [削除] をクリックし、リストからルールを完全に削除します。

デバイスに対する権限

ストレージデバイスに対するデバイスコントロール権限は、次の場合に使用されます。

- USB ストレージデバイス、CD/DVD、フロッピーディスク、およびネットワークドライブへのアクセスを許可する場合。これらのデバイスに対するフルアクセスを付与したり、アクセスレベルを制限したりすることができます。
- 承認済み USB ストレージデバイスのリストを設定する場合。デバイスコントロールでは、承認済みデバイスのリストに追加されている USB ストレージデバイスを除く、すべての USB ストレージデバイスへのアクセスをブロックできます。承認済みデバイスに対するフルアクセスを付与したり、アクセスレベルを制限したりすることができます。

次の表は、ストレージデバイスの権限をリストしたものです。

表 13-1. ストレージデバイスに対するデバイスコントロール権限

権限	デバイス上のファイル	受信ファイル
フルアクセス	許可される操作: コピー、移動、開く、保存、削除、実行	許可される操作: 保存、移動、コピー これは、デバイスにファイルを保存、移動、およびコピーできることを意味します。
変更	許可される操作: コピー、移動、開く、保存、削除 禁止される操作: 実行	許可される操作: 保存、移動、コピー

権限	デバイス上のファイル	受信ファイル
読み取りおよび実行	許可される操作: コピー、開く、実行 禁止される操作: 保存、移動、削除	禁止される操作: 保存、移動、コピー
読み取り	許可される操作: コピー、開く 禁止される操作: 保存、移動、削除、実行	禁止される操作: 保存、移動、コピー
デバイスの内容のみのリスト表示	禁止される操作: すべて デバイスおよびそれに含まれるファイルはユーザに (Windows Explorer などを使用して) 表示されます。	禁止される操作: 保存、移動、コピー
ブロック (情報漏えい対策オプションのインストール後に使用可能)	禁止される操作: すべて デバイスおよびそれに含まれるファイルはユーザに (Windows Explorer などを使用して) 表示されません。	禁止される操作: 保存、移動、コピー

ファイルベースの検索機能は、デバイスの権限を補完し、これらの権限よりも優先される場合があります。たとえば、権限ではファイルを開くことが可能でも、セキュリティエージェントによってファイルが不正プログラムに感染していることが検出された場合、不正プログラムを排除するために特定の検出時の処理がそのファイルに実行されます。検出時の処理が駆除の場合、ファイルは駆除後に開かれます。ただし、検出時の処理が削除の場合、ファイルは削除されます。

次の表は、情報漏えい対策オプションで管理されるモバイルデバイスと非ストレージデバイスに対する権限を示しています。

表 13-2. モバイルデバイスと非ストレージデバイスに対するデバイスコントロール権限

権限	デバイス上のファイル	受信ファイル
許可	許可される操作: コピー、移動、開く、保存、削除、実行	許可される操作: 保存、移動、コピー これは、デバイスにファイルを保存、移動、およびコピーできることを意味します。
ブロック	禁止される操作: すべて デバイスおよびそれに含まれるファイルはユーザに (Windows Explorer などを使用して) 表示されません。	禁止される操作: 保存、移動、コピー

ヒント

情報漏えい対策オプションのデバイスコントロールでは、すべての 64 ビットプラットフォームをサポートします。セキュリティエージェントでサポートされていないシステムで不正変更防止監視を行うには、デバイスの権限を「ブロック」に設定して、これらのデバイスへのアクセスを制限します。

デバイスコントロールの [許可されたプログラム] リストでのワイルドカードのサポート

プログラムのパスと名前は 259 文字以内で指定する必要があり、英数字 (A～Z、a～z、0～9) のみを使用できます。プログラム名のみを指定することはできません。

ワイルドカード文字は、ドライブ文字およびプログラム名に使用できます。ドライブ文字など 1 文字のデータを表す場合は、疑問符 (?) を使用します。プログラム名など複数文字のデータを表す場合は、アスタリスク (*) を使用します。

注意

フォルダ名にワイルドカードを使用することはできません。フォルダは正確な名前を指定する必要があります。

ワイルドカードの正しい使用例を次に示します。

表 13-3. ワイルドカードの正しい使用例

例	一致するデータ
?:\Password.exe	任意のドライブの直下にある「Password.exe」ファイル
C:\Program Files\Microsoft*.exe	C:\Program Files 内のファイル拡張子がある任意のファイル
C:\Program Files*.*	C:\Program Files 内のファイル拡張子がある任意のファイル
C:\Program Files\a?c.exe	C:\Program Files 内で、「a」で始まり「c」で終わる 3 文字の名前を持つ任意の.exe ファイル
C:*	ファイル拡張子に関係なく、C:\ドライブ直下の任意のファイル

ワイルドカードの間違った使用例を次に示します。

表 13-4. ワイルドカードの間違った使用例

例	理由
??:\Buffalo\Password.exe	?? は 2 文字を表しますが、ドライブ文字は 1 文字の英文字に限定されています。
*:\Buffalo\Password.exe	*は複数文字のデータを表しますが、ドライブ文字は 1 文字の英文字に限定されています。
C:*\Password.exe	フォルダ名にワイルドカードを使用することはできません。フォルダは正確な名前を指定する必要があります。
C:\?\Password.exe	

デジタル署名プロバイダの指定

プロバイダから提供されるプログラムを信頼する場合は、デジタル署名プロバイダを指定します。たとえば、「Microsoft Corporation」、「Trend Micro, Inc.」のように入力します。デジタル署名プロバイダは、プログラムのプロパティで確認できます (たとえば、プログラムを右クリックして [プロパティ] を選択します)。

第 14 章

検索除外リスト

ここでは、複数の検索機能に適用する検索除外リストを設定する方法について説明します。

この章は次のトピックで構成されます。

スパイウェア/グレーウェアの承認済みリスト

セキュリティエージェントには、「承認済み」のスパイウェア/グレーウェアのリストが用意されています。このリストには、スパイウェアまたはグレーウェアとして処理しないファイルまたはアプリケーションが含まれます。検索時に特定のスパイウェア/グレーウェアが検出されると、セキュリティエージェントではこの承認済みリストをチェックし、リスト内に一致する項目がある場合は処理を実行しません。

承認済みリストを、1 つ以上のセキュリティエージェントおよびドメインに適用するか、またはサーバが管理するすべてのセキュリティエージェントに適用します。承認済みリストをすべての検索の種類に適用するということは、手動検索、リアルタイム検索、予約検索、および ScanNow の際に同じ承認済みリストを使用するということを意味します。

スパイウェア/グレーウェアの承認済みリストの管理

手順

1. [スパイウェア名] テーブルで、スパイウェア/グレーウェア名を選択します。複数の名前を選択するには、<Ctrl> キーを押しながら選択します。
   - また、[検索] にキーワードを入力して、[検索開始] をクリックすることもできます。キーワードに一致する名前でテーブルが更新されます。
2. [追加] をクリックします。

   これらの名前が [承認済みリスト] テーブルに移動します。
3. 承認済みリストから名前を削除するには、名前を選択して [削除] をクリックします。複数の名前を選択するには、<Ctrl> キーを押しながら選択します。

信頼済みプログラムリスト

アプリケーションコントロール、挙動監視、デバイスコントロール、Endpoint Sensor、およびリアルタイム検索で信頼済みプロセスの検索を省略するようにセキュリティエージェントを設定できます。信頼済みプログラムリストにプログラムを追加すると、そのプログラムとそのプログラムによって開始さ

れたプロセスはリアルタイム検索の対象から除外されます。信頼するプログラムをリストに追加すると、エンドポイントの検索パフォーマンスが向上します。

信頼済みプログラムリストに追加したプログラムは、以降、次の検索の対象から自動的に除外されます。

- アプリケーションコントロール (Apex Central コンソールでのみ設定可能)
- 挙動監視
- デバイスコントロール
- Endpoint Sensor (Apex Central コンソールでのみ設定可能)
- リアルタイム検索: ファイルチェックとプロセス検索

信頼済みプログラムリストの設定

信頼済みプログラムリストは、プログラムとそのプログラムで呼び出されるすべての子プロセスをアプリケーションコントロール、挙動監視、デバイスコントロール、Endpoint Sensor、およびリアルタイム検索から除外します。

手順

1. 親ポリシーを設定する場合は、他のユーザによる子ポリシーの設定方法を指定します。
   - 親ポリシーから継承: 子ポリシーには、親ポリシーの設定をそのまま使用する必要があります。
   - 親ポリシーを拡張: 子ポリシーでは、親ポリシーから継承した設定に新たな設定を追加できます。

   注意

   子ポリシーが [親ポリシーから拡張] に設定されている場合、[子ポリシーの制限] も設定できます。この制限によって、子ポリシーによって特定のオブジェクトがリストに追加されることを防止できます。
2. 検索から除外するプログラムのフルパスを入力します。

3. [信頼済みプログラムリストに追加] をクリックします。
4. リストからプログラムを削除するには、[削除] アイコンをクリックします。

第 15 章

Endpoint Sensor のポリシー設定

本章では、セキュリティエージェントで Endpoint Sensor ポリシーを設定する方法について説明します。

次のトピックがあります。

Endpoint Sensor

Endpoint Sensor は強力な監視/調査ツールで、脅威の有無、場所、および検出ポイントを特定します。詳細なシステムイベント記録と履歴分析を使用した履歴調査を実行して、ネットワーク内の隠れた脅威を検出し、すべての感染エンドポイントを特定できます。Root Cause Analysis レポートを生成することで、エンドポイントに脅威が侵入した時点からの不正プログラムの性質とアクティビティを把握することができます。

さらに、共有の IOC ファイルや YARA ルールを使用して、ライブ調査も実行できます。ライブ調査では、エンドポイントを詳細に検索し、それまで認識されていなかった脅威と潜在的な標的型サイバー攻撃を特定します。

Endpoint Sensor を設定する

重要

Endpoint Sensor 機能を使用するには、専用のライセンスが必要であるほか、追加のシステム要件を満たす必要があります。Endpoint Sensor のポリシーをエンドポイントに配信する前に、正しいライセンスがあることを確認してください。ライセンスの入手方法の詳細については、サポートプロバイダにお問い合わせください。

Apex One オンプレミスと Apex One as a Service セキュリティエージェントの両方を管理している環境の場合、一部機能が Apex One as a Service とは異なることがあります。Apex One as a Service セキュリティエージェントは引き続きトレンドマイクロのサーバにデータを送信しますが、調査機能が Apex Central as a Service コンソールのものとは異なる場合があります。

手順

1. [Endpoint Sensor を有効にする] を選択します。
2. [イベント記録を有効にする] を選択してエージェントエンドポイントのシステムイベントログの収集を開始します。(オンプレミスのみ)

   Endpoint Sensor は、調査を実行する際にリアルタイムのイベントログを使用して危険性の高いエンドポイントを特定します。影響を受けた

Windows エンドポイントを特定したら、詳細な Root Cause Analysis を実行し、想定される攻撃経路についてより詳細に把握することができます。

オプション	説明
最大データベースサイズ (オンプレミスのみ)	Endpoint Sensor がエンドポイントのイベントログを保存するために使用できるデータベースサイズの上限を指定します。エージェントのデータベースがサイズの上限に達すると、Endpoint Sensor では、新しいイベントエントリ用にスペースを空けるために古いログが削除されます。
履歴調査の実行用にログデータのサブセットを送信 (オンプレミスのみ)	サーバに送信される情報は、エンドポイントのドメイン、ファイル、プロセスなどのメタデータで構成されます。このデータは、Endpoint Sensor による履歴調査で、感染エンドポイントを特定するために使用されます。 • アップロード頻度: エージェントがメタデータをサーバにアップロードする頻度を指定します。 **注意** ネットワークによっては、頻繁にアップロードを行うとネットワークのパフォーマンスに影響することがあります。 • 追加のハッシュタイプ: SHA-256 および MD5 のハッシュについても Endpoint Sensor で計算を行ってサーバに送信するかどうかを指定します。初期設定では、Endpoint Sensor は SHA1 ハッシュのみを送信します。 **注意** 追加のハッシュタイプを選択すると、より多くのデータベース容量が必要になります。
Attack Discovery を有効にしてエンドポイントに対する既知の攻撃の痕跡を検出する	Attack Discovery では、トレンドマイクロの脅威インテリジェンスを使用して攻撃の痕跡 (IoA) の挙動を分析し、既知の IoA を検出すると情報を記録します。

第 16 章

仮想パッチのポリシー設定

本章では、セキュリティエージェントで仮想パッチのポリシーを設定する方法について説明します。

次のトピックがあります。

仮想パッチ

仮想パッチとの統合により、パッチの正式リリース前に仮想パッチを自動で適用することで Apex One ユーザを保護します。トレンドマイクロは、ネットワークパフォーマンスとセキュリティの優先事項に基づいて、推奨される侵入防御ルールを保護対象のエンドポイントに提供します。

仮想パッチを設定する

手順

1. [仮想パッチを有効にする] を選択します。
2. IPS を設定します。
   a. [IPS ルール] タブをクリックします。
   b. 検索プロファイルとして次のいずれかを選択します。
      - 推奨: 既知の脆弱性の問題から保護します。関連性が高いデータが提供され、エンドポイントのパフォーマンスへの影響は少なくなります。
      - アグレッシブ: [推奨] 検索プロファイルの内容に加え、不審なネットワークアクティビティに対する IPS ルールが追加で適用されます。

      重要
      アグレッシブ検索を有効にすると、重要ではないログが大量に生成されてエンドポイントのパフォーマンスに影響する可能性があります。[推奨] プロファイルを使用することを強くお勧めします。

   c. (オプション) ビューを選択して、IPS ルールをステータスでフィルタします。

ビュー	説明
すべて	すべての IPS ルールが表示されます。

ビュー	説明
初期設定 (有効)	選択した検索プロファイルの初期設定で有効になっている IPS ルールのみが表示されます。
初期設定 (無効)	選択した検索プロファイルの初期設定で無効になっている IPS ルールのみが表示されます。
ユーザ定義 (有効)	ユーザが有効にした IPS ルールのみが表示されます。
ユーザ定義 (無効)	ユーザが無効にした IPS ルールのみが表示されます。

d. [ステータス] ドロップダウンコントロールから選択してルールのステータスを変更します。

- 初期設定 (有効): 選択した検索プロファイルに対応するルールが初期設定で有効になります。検索プロファイルで定義されたルールのステータスを適用する場合に選択します。
- 初期設定 (無効): 選択した検索プロファイルに対応するルールが初期設定で無効になります。検索プロファイルで定義されたルールのステータスを適用する場合に選択します。
- ユーザ定義 (有効): ルールを有効にする場合に選択します。
- ユーザ定義 (無効): ルールを無効にする場合に選択します。

3. ネットワークエンジンを設定します。

a. [ネットワークエンジン設定] タブをクリックします。

b. ネットワークエンジン検出モード*を選択します。

注意

選択したネットワークエンジン検出モードを使って詳細ログポリシーを設定することもできます。

- インライン: パケットのライブストリームは仮想パッチネットワークエンジンを直接通過します。パケットがプロトコルスタックの上位に進む前にすべてのルールがネットワークトラフィックに適用されます。

- タップ (検出のみ): パケットのライブストリームは複製され、メインストリームを迂回します。

c. 次の設定を行います。

設定	説明
ESTABLISHED タイムアウト	ESTABLISHED 状態が続いて接続を終了するまでの時間
LAST_ACK タイムアウト	LAST_ACK 状態が続いて接続を終了するまでの時間
コールドスタートタイムアウト	ステートフル機能が開始される前に確立された接続に属することができる非 SYN パケットを許可する時間
UDP タイムアウト	UDP 接続の最大継続時間
最大 TCP 接続数	同時 TCP 接続の最大数
最大 UDP 接続数	同時 UDP 接続の最大数
ステータスコードの無視	無視するイベントの種類を 3 つまで選択します

設定	説明
詳細ログポリシー	次の設定から選択します。 • 放置 (バイパス): イベントにフィルタを適用しません。上記の [ステータスコードの無視] 設定およびその他の詳細設定をオーバーライドします。ただし、Apex One サーバに定義された他のログ設定はオーバーライドしません • ネットワークエンジン検出モード*: ネットワークエンジン検出モードに [タップ (検出のみ)] を選択した場合には [タップモード]、ネットワークエンジン検出モードに [インライン] を選択した場合には [標準] が、それぞれ使用されます • 標準: 再送の破棄を除くすべてのイベントがログに記録されます • 下位互換性モード: サポート目的でのみ使用します • 詳細モード: [標準] と同じですが、再送の破棄イベントも記録します • ステートフルおよび正規化の抑制: 再送の廃棄、接続範囲外、無効なフラグ、無効なシーケンス、無効な ACK、未承諾の UDP、未承諾の ICMP、ポリシーの許可外を無視します • ステートフル, 正規化およびフラグメントの抑制: [ステートフルおよび正規化の抑制] で無視されるものすべてに加えて、フラグメンテーション関連のイベントも無視します • ステートフル, フラグおよび確認の抑制: [ステートフル、正規化、フラグメントの抑制] で無視されるものすべてに加えて、検証機能に関連したイベントも無視します • タップモード: 再送の廃棄、接続範囲外、無効なフラグ、無効なシーケンス、無効な ACK、ACK 再送の上限、切断された接続上のパケットを無視します [ステートフルおよび正規化の抑制]、[ステートフル, 正規化およびフラグメントの抑制]、[ステートフル, フラグおよび確認の抑制]、および [タップモー

設定	説明
	ド] で無視されるイベントをより包括的にまとめたリストについては、278 ページの「詳細ログポリシーモード」を参照してください。

4. [保存] をクリックして設定を適用します。

詳細ログポリシーモード

次の表に、より複雑な 4 つの詳細ログポリシーモードで無視されるイベントの種類を示します。

モード	無視されるイベント
ステートフルおよび正規化の抑制	接続範囲外
	無効なフラグ
	無効なシーケンス
	無効な ACK
	未承諾の UDP
	未承諾の ICMP
	ポリシーの許可外
	再送の破棄
ステートフル, 正規化およびフラグメントの抑制	接続範囲外
	無効なフラグ
	無効なシーケンス
	無効な ACK
	未承諾の UDP
	未承諾の ICMP
	ポリシーの許可外

モード	無視されるイベント
	CE フラグ
	無効な IP
	無効な IP データグラム長
	フラグメント化
	無効なフラグメントオフセット
	最初のフラグメントが小さすぎる
	範囲を超えたフラグメント
	フラグメントオフセットが小さすぎる
	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
	ライセンスの有効期間が切れました
	IP バージョン不明
	無効なパケット情報
	ACK 再送の上限
	切断された接続上のパケット
	再送の破棄
ステートフル, フラグおよび確認の抑制	接続範囲外
	無効なフラグ
	無効なシーケンス
	無効な ACK
	未承諾の UDP

モード	無視されるイベント
	未承諾の ICMP
	ポリシーの許可外
	CE フラグ
	無効な IP
	無効な IP データグラム長
	フラグメント化
	無効なフラグメントオフセット
	最初のフラグメントが小さすぎる
	範囲を超えたフラグメント
	フラグメントオフセットが小さすぎる
	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
	ライセンスの有効期間が切れました
	IP バージョン不明
	無効なパケット情報
	無効なデータオフセット
	IP ヘッダなし
	読み取り不能なイーサネットヘッダ
	未定義
	送信元と送信先の IP が同じ
	無効な TCP ヘッダ長

モード	無視されるイベント
	読み取り不能なプロトコルヘッダ
	読み取り不能な IPv4 ヘッダ
	不明な IP バージョン
	ACK 再送の上限
	切断された接続上のパケット
	再送の破棄
タップモード	接続範囲外
	無効なフラグ
	無効なシーケンス
	無効な ACK
	ACK 再送の上限
	切断された接続上のパケット
	再送の破棄

パート VI

Apex One 情報漏えい対策ポリシー

第 17 章

Apex One データ検出ダッシュボードウィジェット

本章には、Apex Central でサポートされる Apex One データ検出ダッシュボードウィジェットのヘルプトピックが含まれています。

次のトピックがあります。

機密ファイルポリシー検出の上位ウィジェット

このウィジェットには、データ検出ポリシー違反の検出と、ルールを実行した機密ファイルに関する情報が表示されます。

注意

初期設定では、ユーザのアカウントに表示権限がある、すべての管理下の製品のデータがウィジェットに表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

- カスタムの時間範囲または時間間隔を指定するには、設定アイコン (>) をクリックし、[範囲] に対して [ユーザ指定] を選択します。

検出を実行するルールを指定するには、[ルール] ドロップダウンを使用します。

- 表示するルールの数を指定するには、設定アイコン (>) をクリックし、[表示するルール] ドロップダウンから選択します。
- 残りのデータを集計するには、設定アイコン (>) をクリックし、[残りのデータを「その他」として表示する] を選択します。

表示アイコン ( ) をクリックすると、表、棒グラフ、円グラフ、または折れ線グラフの形式でデータを表示できます。

初期設定では、次の情報が表に表示されます。

列名	説明
ルール名	機密ファイルによって実行されたルールを表示します。
検出数	ルールが実行された回数を表示します。 [検出数] の列名をクリックすると、検出数の順で並べ替えられます。 数字をクリックすると、検出の発生日時や検出された機密ファイルなど、検出の詳細が表示されます。

列名	説明
割合	ルールが実行された回数を、検出数の合計に対するパーセンテージで表示します。

詳細情報を表示するには、[検出数] 列の数をクリックするか、グラフのセクションをクリックします。

データ	説明
受信日時	Apex Central がデータを受信した日時
生成	検出が発生した日時
ルール	実行されたルール
エンドポイント	ルールを実行したエンドポイント
ドメイン	ルールを実行したドメイン
ユーザ (アカウント)	ルールを実行したユーザ
ユーザドメイン	ユーザが属するドメイン
ファイルパス	機密ファイルのファイルパス
ファイル	機密ファイルの名前
テンプレート	ルールが属するテンプレート
処理	機密ファイルに対して実行された処理

機密ファイルを使用しているエンドポイントの上位ウィジェット

このウィジェットには、データ検出ポリシー違反の検出を実行した機密ファイルを使用しているエンドポイントに関する情報が表示されます。

注意

初期設定では、ユーザのアカウントに表示権限がある、すべての管理下の製品のデータがウィジェットに表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

- カスタムの時間範囲または時間間隔を指定するには、設定アイコン (>) をクリックし、[範囲] に対して [ユーザ指定] を選択します。

検出を実行するルールを指定するには、[ルール] ドロップダウンを使用します。

- 表示するテンプレートの数を指定するには、設定アイコン (>) をクリックして、[表示するエンドポイント] ドロップダウンから選択します。
- 残りのデータを集計するには、設定アイコン (>) をクリックし、[残りのデータを「その他」として表示する] を選択します。

表示アイコン ( ) をクリックすると、表、棒グラフ、または円グラフの形式でデータを表示できます。

初期設定では、次の情報が表に表示されます。

列名	説明
エンドポイント	ルールを実行した機密ファイルを使用しているエンドポイントを表示します。
検出数	ルールが実行された回数を表示します。 [検出数] の列名をクリックすると、検出数の順で並べ替えられます。
割合	ルールが実行された回数を、検出数の合計に対するパーセンテージで表示します。

詳細情報を表示するには、[検出数] 列の数をクリックするか、グラフのセクションをクリックします。

データ	説明
受信日時	Apex Central がデータを受信した日時
生成	検出が発生した日時
ルール	実行されたルール
エンドポイント	ルールを実行したエンドポイント

データ	説明
ドメイン	ルールを実行したドメイン
ユーザ (アカウント)	ルールを実行したユーザ
ユーザドメイン	ユーザが属するドメイン
ファイルパス	機密ファイルのファイルパス
ファイル	機密ファイルの名前
テンプレート	ルールが属するテンプレート
処理	機密ファイルに対して実行された処理

データ検出テンプレート一致の上位ウィジェット

このウィジェットには、データ検出テンプレートポリシー違反 (時間別推移) の上位に関する情報が表示されます。

注意

初期設定では、ユーザのアカウントに表示権限がある、すべての管理下の製品のデータがウィジェットに表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

- カスタムの時間範囲または時間間隔を指定するには、設定アイコン (>) をクリックし、[範囲] に対して [ユーザ指定] を選択します。

検出を実行するルールを指定するには、[ルール] ドロップダウンを使用します。

- 表示するテンプレートの数を指定するには、設定アイコン (>) をクリックして、[表示するテンプレート] ドロップダウンから選択します。
- 残りのデータを集計するには、設定アイコン (>) をクリックし、[残りのデータを「その他」として表示する] を選択します。

表示アイコン ( ) をクリックすると、表、棒グラフ、または円グラフの形式でデータを表示できます。

初期設定では、次の情報が表に表示されます。

列名	説明
テンプレート	機密ファイルによって実行されたテンプレートを表示します。
検出数	テンプレートが実行された回数を表示します。 [検出数] の列名をクリックすると、検出数の順で並べ替えられます。
割合	テンプレートが実行された回数を検出総数の割合で表示します。

詳細情報を表示するには、[検出数] 列の数をクリックするか、グラフのセクションをクリックします。

データ	説明
受信日時	Apex Central がデータを受信した日時
生成	検出が発生した日時
ルール	実行されたルール
エンドポイント	ルールを実行したエンドポイント
ドメイン	ルールを実行したドメイン
ユーザ (アカウント)	ルールを実行したユーザ
ユーザドメイン	ユーザが属するドメイン
ファイルパス	機密ファイルのファイルパス
ファイル	機密ファイルの名前
テンプレート	ルールが属するテンプレート
処理	機密ファイルに対して実行された処理

機密ファイルの上位ウィジェット

このウィジェットには、データ検出ポリシー違反 (時間別推移) の検出を実行した機密ファイルの上位に関する情報が表示されます。

注意

初期設定では、ユーザのアカウントに表示権限がある、すべての管理下の製品のデータがウィジェットに表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

- カスタムの時間範囲または時間間隔を指定するには、設定アイコン (>) をクリックし、[範囲] に対して [ユーザ指定] を選択します。

検出を実行するルールを指定するには、[ルール] ドロップダウンを使用します。

- 表示する検出の数を指定するには、設定アイコン (>) をクリックして、[表示する機密ファイル] ドロップダウンから選択します。
- 残りのデータを集計するには、設定アイコン (>) をクリックし、[残りのデータを「その他」として表示する] を選択します。

表示アイコン ( ) をクリックすると、表、棒グラフ、または円グラフの形式でデータを表示できます。

初期設定では、次の情報が表に表示されます。

列名	説明
ファイル	漏えいされた可能性のある機密ファイルを表示します。
検出数	機密ファイルが漏えいされた可能性のある回数を表示します。 [検出数] の列名をクリックすると、検出数の順で並べ替えられます。
割合	機密ファイルが漏えいされた可能性がある回数を検出総数の割合で表示します。

詳細情報を表示するには、[検出数] 列の数をクリックするか、グラフのセクションをクリックします。

データ	説明
受信日時	Apex Central がデータを受信した日時

データ	説明
生成	検出が発生した日時
ルール	実行されたルール
エンドポイント	ルールを実行したエンドポイント
ドメイン	ルールを実行したドメイン
ユーザ (アカウント)	ルールを実行したユーザ
ユーザドメイン	ユーザが属するドメイン
ファイルパス	機密ファイルのファイルパス
ファイル	機密ファイルの名前
テンプレート	ルールが属するテンプレート
処理	機密ファイルに対して実行された処理

第 18 章

Apex One データ検出ポリシー設定

本章では、Apex Central で Apex One データ検出ポリシーを設定する方法について説明します。

次のトピックがあります。

データ検出ポリシーを作成する

データ検出では、データベース、エンドポイント、および文書管理システムで機密情報が検索されます。データ検出ウィジェットには、企業のポリシーに対する情報漏えい対策コンプライアンスが表示されます。データ検出ポリシーとウィジェットを使用することで、管理者は、ネットワークに対する修復処理を実行できます。

注意

エンドポイントのドライブまたはディレクトリの完全検索を実行すると、エンドユーザにとってシステムパフォーマンスの大幅な低下が生じる可能性があります。

手順

1. [データ検出を有効にする] を選選択します。
2. [追加] をクリックします。

   [データ検出ポリシー設定] 画面が表示されます。
3. [このルールを有効にする] を選択します。
4. ルールの名前を指定します。
5. 対象フォルダを設定します。
   a. [対象フォルダ] タブをクリックします。

      注意

      Windows 共有フォルダ、または USB デバイスや DVD などのリムーバブルデバイスをルートフォルダにすることはできません。
   b. [ファイルパス] セクションで、ファイルの検索場所を指定します。

注意

データ検出では、次のディレクトリに配置された autoexec.bat ファイルは検索されません。

- ¥Documents and Settings¥*¥Application Data¥
- ¥Documents and Settings¥*¥Local Settings¥
- ¥Documents and Settings¥*¥Cookies¥
- ¥Program Files¥
- ¥Windows¥
- ¥Winnt¥
- ¥Users¥*¥AppData¥
- ¥ProgramData¥

c. [ファイルタイプ除外] セクションで、検索で除外するファイルタイプを指定します。

- 検索対象: 検索するファイルまたはファイルタイプを指定します。
- 検索対象外: データ検出で検索しないファイル、ファイルタイプ、またはフォルダを指定します。

注意

- データ検出では、次のワイルドカード文字がサポートされます。
  - *: *の前後のすべての文字を表します。
  - ?: 1 つの文字または 1 つのダブルバイト文字を表します。
- 複数のエントリはパイプ (|) で区切り、次の形式を使用します。
  - ファイルの場合: *.<ファイル拡張子> (例: *.exe|*.doc)
  - フォルダの場合: ファイルパスを指定します (例: *\Test*|C:\My-Docs\)

テンプレートを設定します。

6. テンプレートを設定します。

   a. [テンプレート] タブをクリックします。

   b. [利用可能なテンプレート] リストからテンプレートを選択して、[追加] をクリックします。

      テンプレートを選択する場合:

      - 複数のエントリを選択するには、テンプレート名をクリックして、名前をハイライトします。
      - 特定のテンプレートを指定できる場合は、検索機能を使用します。テンプレートの名前の全体または一部を入力して検索できます。

      注意

      - 1 つのルールには最大 500 個のテンプレートを使用することができます。
      - 目的のテンプレートが [利用可能なテンプレート] リストにない場合は、[ポリシー] > [ポリシーリソース] > [情報漏えい対策テンプレート] の順に選択し、新しいテンプレートを作成します。

7. 処理を設定します。

   a. [処理] タブをクリックします。

   b. [監視] を選択して分析のために検出結果を記録します。

8. 検索のスケジュールを設定します。

   a. [スケジュール] タブをクリックします。

   b. 検索の頻度を指定します。

   c. 検索の開始時間を指定します。

9. [保存] をクリックして設定を適用します。

第 19 章

Apex One 情報漏えい対策のポリシー設定

ここでは、セキュリティエージェントの情報漏えい対策のポリシーを設定する方法について説明します。

この章は次のトピックで構成されます。

情報漏えい対策

従来のセキュリティソリューションは、外部のセキュリティ上の脅威がネットワークに侵入するのを防ぐことに重点を置いていました。今日のセキュリティ環境では、それだけでは不十分です。デジタル資産と呼ばれる組織の機密データや重要データを権限のない部外者に公開するデータ侵害が頻繁に発生するようになりました。データ侵害は、社員の過失や不注意、データアウトソーシング、コンピューティングデバイスの盗難または紛失、不正な攻撃などが原因で発生します。

データ侵害の影響は次のとおりです。

- ブランドの評判に傷を付ける
- 組織に対する顧客の信頼を損ねる
- 問題を解決したり、規制違反の罰金を支払ったりするための余分なコストが発生する
- 知的財産が盗まれた場合にはビジネスチャンスや収益が失われる

データ侵害の流行や悪影響により、現在の組織は、デジタル資産保護をセキュリティインフラストラクチャの必須要素と見なしています。

情報漏えい対策は、組織の機密データを不慮の流失や意図的な漏えいから守ります。情報漏えい対策により、管理者は次のことを実行できます。

- データ識別子を使用して保護する必要がある機密情報の識別
- メールや外部デバイスなどの一般的な転送チャネルを通したデジタル資産の転送を制限または阻止するポリシーの作成
- 制定されたプライバシー標準へのコンプライアンスの実施

機密情報の漏えいの危険性を監視するには、まず次の点について確認する必要があります。

- どのデータを無許可のユーザから保護する必要があるか。
- 機密データはどこにあるか。
- 機密データはどのような方法で送受信されるか。
- どのユーザが機密データへのアクセスや機密データの送信を許可されているか。

- セキュリティの違反が発生した場合にどのような処理を実行する必要があるか。

この重要な監査では、通常は、複数の部署や、組織の機密情報に詳しいユーザを対象にします。

機密情報とセキュリティポリシーをすでに定義している場合は、データ識別子と企業ポリシーの定義を始めることができます。

情報漏えい対策ポリシーの設定

手順

1. [外部エージェント] タブをクリックして外部エージェントのポリシーを設定するか、[内部エージェント] タブをクリックして内部エージェントのポリシーを設定します。

   注意

   エージェントの位置を設定していない場合は設定します。エージェントは、これらの位置設定を使用して、適用される正しい情報漏えい対策ポリシーを判断します。

2. [情報漏えい対策を有効にする] を選択します。
3. 次のいずれかを選択します。
   - [外部エージェント] タブで [内部エージェントにすべての設定を適用する] を選択すると、情報漏えい対策のすべての設定を内部エージェントに適用できます。
   - [内部エージェント] タブで [外部エージェントにすべての設定を適用する] を選択すると、情報漏えい対策のすべての設定を外部エージェントに適用できます。
4. [ルール] タブで、情報漏えい対策がポリシーに適用するルールを管理します。

タスク	説明
新しいルールの追加	[追加] をクリックして、ポリシーに適用するルールを作成します。 詳細については、300 ページの「情報漏えい対策ルールの設定」を参照してください。
既存のルール設定のコピー	既存のルールを選択し、[コピー] をクリックして [情報漏えい対策ポリシー設定] 画面を開きます。必要に応じてルール設定を変更します。
既存のルールの削除	既存のルールを選択し、[削除] をクリックしてリストからルールを削除します。
既存のルールの変更	既存のルールのルール名をクリックして設定を変更します。
既存のルールの有効化/無効化	[有効] 列の下にあるボタンをクリックし、ポリシーのルールを有効または無効にします。

注意

ポリシーに含めることのできるルールは最大 40 個です。

5. [除外] タブをクリックし、必要な除外設定を行います。

   詳細については、307 ページの「情報漏えい対策の除外」を参照してください。

情報漏えい対策ルールの設定

注意

情報漏えい対策は優先順位に従ってルールおよびテンプレートを処理します。ルールが「放置 (ログのみ)」に設定されている場合、情報漏えい対策はリスト内の次のルールを処理します。ルールが「ブロック」または「理由申請」に設定されている場合、情報漏えい対策はユーザ処理をブロックまたは承認し、そのルール/テンプレートをそれ以上処理しません。

手順

1. [このルールを有効にする] を選択します。
2. ルールの名前を指定します。

   ここからテンプレートの設定に移ります。
3. [テンプレート] タブをクリックします。
4. [利用可能なテンプレート] リストからテンプレートを選択して、[追加] をクリックします。

   テンプレートを選択する場合:

   - テンプレート名をクリックして名前を強調表示し、複数のエントリを選択します。
   - 検索機能は、特定のテンプレートを想定している場合に使用します。テンプレート名のすべてまたは一部を入力できます。

   注意

   ルールごとに最大 200 のテンプレートを含めることができます。

   ここからチャネルの設定に移ります。
5. [チャネル] タブをクリックします。
6. ルールを適用するチャネルを選択します。

   チャネルの詳細については、303 ページの「ネットワークチャネル」、および 305 ページの「システムチャネルとアプリケーションチャネル」を参照してください。
7. いずれかのネットワークチャネルを選択した場合は、転送範囲を選択してください。

   - すべての転送
   - ローカルエリアネットワークの外部への転送のみ

   302 ページの「ネットワークチャネルの転送範囲と送信先」を参照してください。転送範囲の詳細、転送範囲に応じた送信先の振る舞い、および送信先を正しく定義する方法については。

8. [メールクライアント] を選択した場合は、次の手順に従ってください。
   a. [除外] をクリックします。
   b. 監視対象および監視対象外の内部メールドメインを指定します。

      監視対象および対象外のメールドメインの詳細については、303 ページの「メールクライアント」を参照してください。
9. [リムーバブルストレージ] を選択した場合は、次の手順に従ってください。
   a. [除外] をクリックします。
   b. ベンダで識別する監視対象外のリムーバブルストレージデバイスを追加します。デバイスモデルおよびシリアル ID は任意です。

      USB デバイスの承認済みリストでは、アスタリスク (*) ワイルドカードを使用できます。任意のフィールドをアスタリスク (*) で置き換えると、他のフィールドを満たすデバイスをすべて含めることができます。

      たとえば [ベンダ]-[モデル]-*は、シリアル ID に関係なく、指定したベンダの特定のモデルタイプのすべての USB デバイスを承認済みリストに配置します。
   c. さらにデバイスを追加するには、プラス (+) アイコンをクリックします。

   ここから処理の設定に移ります。
10. [処理] タブをクリックします。
11. 1 次処理と追加処理を選択します。処理の詳細については、306 ページの「情報漏えい対策の処理」を参照してください。
12. [テンプレート]、[チャネル]、および[処理] の設定後、[保存] をクリックします。

ネットワークチャネルの転送範囲と送信先

情報漏えい対策で監視する必要のあるネットワークチャネルを介したデータ転送は、その転送範囲と送信先によって定義します。監視を必要とする転送では、転送を許可またはブロックする前に、データ識別子が存在するかどう

かが確認されます。監視を必要としない転送では、データ識別子が存在するかどうかは確認されず、転送がただちに許可されます。

ネットワークチャネル

情報漏えい対策は、次のネットワークチャネルを介したデータ転送を監視できます。

- メールクライアント
- FTP
- HTTP および HTTPS
- IM アプリケーション
- SMB プロトコル
- Web メール

監視するデータ転送を特定するには、情報漏えい対策でチェックする転送の範囲を設定する必要があります。選択した範囲に応じて、すべてのデータ転送を監視することも、ローカルエリアネットワーク (LAN) 外部の転送のみを監視することもできます。

メールクライアント

情報漏えい対策では、さまざまなメールクライアント経由で送信されるメールを監視します。また、データ識別子について、メールの件名、本文、および添付ファイルをチェックします。サポートしているメールクライアントの一覧については、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

監視は、ユーザがメールを送信しようとしたときに実行されます。メールにデータ識別子が含まれている場合は、情報漏えい対策によってそのメールが許可またはブロックされます。

監視対象外の内部メールドメインおよび監視対象のメールサブドメインを定義できます。

- 対象外のメールドメイン: 監視対象外ドメインに送信されるメールの転送は、ただちに許可されます。

注意

対象外のメールドメインへのデータ転送と、処理が「監視」に指定された監視対象のメールサブドメインへのデータ転送は、転送が許可される点で似ています。唯一の違いは、情報漏えい対策が対象外のメールドメインについて転送ログを記録しない点です。監視対象のメールサブドメインの場合、転送は常にログに記録されます。

- 監視対象のメールサブドメイン: 情報漏えい対策は、監視対象サブドメインへのメール転送を検出すると、ポリシーの処理をチェックします。この処理に応じて、転送が許可またはブロックされます。

注意

監視対象チャネルにメールクライアントを選択した場合、監視するメールはポリシーと一致する必要があります。一方、監視対象のメールサブドメインに送信されるメールは、ポリシーに一致しなくても自動的に監視されます。

ドメインは次の任意の形式を使用して指定します。複数のドメインはカンマで区切って入力してください。

- X400 形式。例: /O=Trend/OU=USA、/O=Trend/OU=China
- メールドメイン。例: `example.com`

SMTP プロトコルで送信されるメールメッセージの場合、送信先の SMTP サーバが次のリストに存在するかどうかがチェックされます。

1. 監視対象
2. 監視対象外
3. 対象外のメールドメイン
4. 監視対象のメールサブドメイン

これは、メールが監視対象のリストに含まれている SMTP サーバに送信される場合、そのメールが監視されることを意味します。SMTP サーバが監視対象のリストに含まれていない場合は、他のリストが確認されます。

他のプロトコルで送信されるメールの場合、次のリストのみが確認されます。

1. 対象外のメールドメイン
2. 監視対象のメールサブドメイン

システムチャネルとアプリケーションチャネル

情報漏えい対策は、次のシステムおよびアプリケーションチャネルを監視できます。

- クラウドストレージサービス
- CD/DVD
- ピアツーピアアプリケーション
- PGP 暗号化
- プリンタ
- リムーバブルストレージ
- 同期ソフトウェア (ActiveSync)
- Windows クリップボード

デバイスリストツール

エンドポイントに接続された外部デバイスを照会するには、エンドポイントごとにデバイスリストツールをローカルで実行します。このツールは、エンドポイントの外部デバイスを検索し、デバイス情報をブラウザ画面に表示します。この情報は、情報漏えい対策やデバイスコントロールのデバイス設定を指定するときに使用できます。

デバイスリストツールの実行

手順

1. デバイスリストツールを用意します。
   - 対象エンドポイントにセキュリティエージェントがインストールされている場合は、`C:¥Windows¥System32¥dgagent¥listDeviceInfo.exe` に移動します。

2. エンドポイントで、listDeviceInfo.exe を実行します。
3. 表示されたブラウザ画面でデバイス情報を確認します。情報漏えい対策とデバイスコントロールでは次の情報が使用されます。
   - ベンダ (必須)
   - モデル (オプション)
   - シリアル ID (オプション)

情報漏えい対策の処理

情報漏えい対策は、データ識別子の転送を検出すると、該当する情報漏えい対策ポリシーをチェックして、ポリシーに設定された処理を実行します。

次の表は、情報漏えい対策の処理をリストしたものです。

表 19-1. 情報漏えい対策の処理

処理	説明
処理	
放置	転送を許可し、ログに記録します。
ブロック	転送をブロックし、ログに記録します。
追加処理	
エージェントユーザに通知する	データの転送と、データがブロックされたかどうかを知らせる通知メッセージを表示します。
データを記録する	1 次処理に関係なく、機密情報を<セキュリティエージェントインストールフォルダ>¥DLPLite¥Forensic に記録します。情報漏えい対策によってフラグが付けられた機密情報を評価する場合にこの処理を選択します。 記録される機密情報は、ハードディスク容量を大量に消費する可能性があります。そのため、このオプションは機密性の高い情報に対してのみ有効にすることをお勧めします。
理由申請	「ブロック」処理を実行する前にユーザに確認メッセージを表示します。ユーザは、機密データを転送する理由を申

処理	説明
注意 このオプションは、[ブロック] 処理を選択した場合にのみ使用できます。	請して「ブロック」処理を無効にできます。次のいずれかの理由を選択できます。 • この操作は確立された業務プロセスの一部です。 • このデータ転送は管理者から承認されています。 • このファイルには機密データは含まれません。 • その他: テキストフィールドに任意の理由を入力します。

情報漏えい対策の除外

情報漏えい対策の除外設定は、ポリシー内で定義されたすべてのルールを含め、ポリシー全体に適用されます。情報漏えい対策では、デジタル資産を検索する前に、すべての送信に除外設定を適用します。特定の送信がいずれかの除外ルールに一致すると、除外の種類に応じて、情報漏えい対策によって送信データがただちに許可または検索されます。

監視対象外および監視対象の定義

[チャネル] タブで設定された転送範囲に基づいて監視対象外および監視対象を定義します。[すべての転送] での監視対象外および監視対象の定義方法の詳細については、308 ページの「転送の範囲: すべての転送」を参照してください。[ローカルエリアネットワークの外部への転送のみ] での監視対象外および監視対象の定義方法の詳細については、309 ページの「転送の範囲: ローカルエリアネットワークの外部への転送のみ」を参照してください。

監視対象および監視対象外を定義する際は、次のガイドラインに従ってください。

1. 次の定義方法があります。
   - IP アドレス
   - ホスト名
   - FQDN
   - ネットワークアドレスとサブネットマスク (例: 10.1.1.1/32)

注意

サブネットマスクの場合、情報漏えい対策では CIDR (Classless Inter-Domain Routing) タイプのポートのみサポートされます。これは、255.255.255.0 の代わりに、32 のような数字のみ入力できることを意味します。

2. 特定のチャネルを送信先に指定する場合は、対象チャネルの初期設定のポート番号、または会社で定義されたポート番号を含めます。たとえば、ポート 21 は一般に FTP トラフィック用、ポート 80 は HTTP 用、およびポート 443 は HTTPS 用です。送信先とポート番号はコロンで区切ってください。
3. ポートの範囲を含めることもできます。すべてのポートを含めるには、ポート範囲は無視してください。

   送信先のポート番号とポート範囲の例を次に示します。

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. 複数指定する場合はカンマで区切ります。

転送の範囲: すべての転送

情報漏えい対策では、ホストコンピュータから外部へ転送されるデータを監視します。

注意

外部エージェントにはこのオプションを選択することをお勧めします。

ホストコンピュータの外部にある特定の送信先へのデータ転送を監視しないようにするには、次の項目を定義します。

- 監視対象外: この送信先に転送されるデータは監視されません。

注意

監視対象外へのデータ転送と、処理が「監視」に指定された監視対象へのデータ転送は、転送が許可される点で似ています。唯一の違いは、情報漏えい対策が監視対象外について転送ログを記録しない点です。監視対象の場合、転送は常にログに記録されます。

- 監視対象: 監視対象外の中で監視を必要とする特別な送信先です。この送信先の指定には、次の制限があります。
  - 監視対象外を定義した場合のオプションです。
  - 監視対象外を定義していない場合には設定できません。

例:

次の IP アドレスが会社の法務部に割り当てられているとします。

- `10.201.168.1〜10.201.168.25`

現在、法務部の常勤社員を除く、全従業員の在籍証明書の転送を監視するポリシーを作成しています。この作業では、転送範囲として [すべての転送] を選択し、さらに次のいずれかを設定できます。

オプション	手順
オプション 1	1. 監視対象外に `10.201.168.1〜10.201.168.25` を追加します。 2. 法務部の非常勤社員の IP アドレスを監視対象に追加します。この IP アドレスは、`10.201.168.21〜10.201.168.23` の 3 つと仮定します。
オプション 2	法務部の常勤社員の IP アドレスを監視対象外に追加します。 • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

監視対象および監視対象外の定義方法のガイドラインについては、307 ページの「監視対象外および監視対象の定義」を参照してください。

転送の範囲: ローカルエリアネットワークの外部への転送のみ

情報漏えい対策では、ローカルエリアネットワーク (LAN) 外の送信先へ転送されるデータを監視します。

注意

内部エージェントにはこのオプションを選択することをお勧めします。

「ネットワーク」は、会社またはローカルのネットワークを指します。これには、現在のネットワーク (エンドポイントおよびネットマスクの IP アドレス) および次の標準のプライベート IP アドレスが含まれます。

- クラス A: `10.0.0.0`〜`10.255.255.255`
- クラス B: `172.16.0.0`〜`172.31.255.255`
- クラス C: `192.168.0.0`〜`192.168.255.255`

この転送範囲を選択した場合、次のように定義できます。

- 監視対象外: 安全と考えられ、監視を必要としない LAN 外部の送信先を定義します。

  注意

  監視対象外へのデータ転送と、処理が「監視」に指定された監視対象へのデータ転送は、転送が許可される点で似ています。唯一の違いは、情報漏えい対策が監視対象外について転送ログを記録しない点です。監視対象の場合、転送は常にログに記録されます。

- 監視対象: LAN 内部の監視を必要とする送信先を定義します。

監視対象および監視対象外の定義方法のガイドラインについては、307 ページの「監視対象外および監視対象の定義」を参照してください。

解凍ルール

圧縮ファイルに含まれるファイルを、デジタル資産について検索できます。情報漏えい対策は、次のルールを条件として、内部のファイルを検索する圧縮ファイルを決定します。

- 解凍ファイルのサイズが次の値を超える場合 — __ MB (1〜10240 MB)
- 圧縮階層数が次の値を超える場合 — __ (1-20)
- 検索対象ファイル数が次の値を超える場合 — __ (1-2000)

パート VII

Apex One (Mac) のウィジェットとポリシー

第 20 章

Apex One (Mac) ダッシュボードウィジェット

本章では、Apex Central でサポートされる Apex One (Mac) ダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

キーパフォーマンスインジケータウィジェット

Apex Central の [ダッシュボード] 画面にあるこのウィジェットを使用して、選択した条件に基づく Apex One (Mac) キーパフォーマンスインジケータ (KPI) を表示します。

ウィジェットを [ダッシュボード] 画面に追加する方法の詳細については、Apex Central または Control Manager のドキュメントを参照してください。

ヒント

初期設定では、このウィジェットは 15 回発生したイベントを「重要」( )、30 回発生したイベントを「重大」( ) としてマークします。必要に応じて、イベントしきい値をカスタマイズしてイベントを重要または重大とマークしてください。

キーパフォーマンスインジケータの設定

Apex Central または Control Manager の [ダッシュボード] で [Apex One (Mac) キーパフォーマンスインジケータ] ウィジェットにアクセスし、以下のインジケータ関連タスクを実行します。

表 20-1. KPI ウィジェットのインジケータタスク

タスク	手順
新しいインジケータを追加する	1. [インジケータの追加] をクリックします。[インジケータの追加] 画面が表示されます。 2. [名前] ドロップダウンリストからオプションを選択し、必要に応じて設定をカスタマイズします。 3. [保存] をクリックします。
インジケータを編集する	1. リスト内のインジケータをクリックします。[インジケータの編集] 画面が表示されます。 2. 設定をカスタマイズします。 3. [保存] をクリックします。

タスク	手順
インジケータを削除する	1. リスト内のインジケータをクリックします。[インジケータの編集] 画面が表示されます。 2. [削除] をクリックします。 3. [OK] をクリックします。
イベントしきい値を指定する	1. [インジケータの追加] または [インジケータの編集] 画面で、[アラートを有効にする] を選択します。 2. イベントの種類ごとに、イベントの最小発生件数を入力します。 3. [保存] をクリックします。 注意 次の両方の条件に当てはまる場合、[件数] 列に重要または重大アイコンが表示されます。 • このインジケータに対応するイベント発生件数がしきい値以上である。 • [アラートを有効にする] が選択されている。

ウィジェットの設定

Apex Central または Control Manager の [ダッシュボード] 画面で、ウィジェットの右上にあるメニューから [ウィジェット設定] を選択し、以下のタスクを実行します。

表 20-2. KPI のウィジェット設定

タスク	手順
ウィジェットタイトルを編集する	テキストフィールドにウィジェットタイトルを入力します。

タスク	手順
毎日のアップデート時間を設定する	ドロップダウンリストから、毎日ウィジェットデータを生成する時間を選択します。 ヒント ウィジェットデータを手動で更新するには、更新 ( ) アイコンをクリックします。

第 21 章

Apex One (Mac) のポリシー設定

本章では、Apex Central で Trend Micro Apex One (Mac) のポリシーを設定する方法について説明します。

次のトピックがあります。

検索用のキャッシュ設定

検索を実行するたびに、エージェントは変更されたファイルのキャッシュをチェックし、前回のエージェントの起動以降にファイルが変更されたかどうかを確認します。

- ファイルが変更されている場合、エージェントはファイルを検索し、それを検索されたファイルのキャッシュに追加します。
- ファイルが変更されていない場合、エージェントは、そのファイルが検索されたファイルのキャッシュに存在するかどうかを確認します。
  - 検索されたファイルのキャッシュに存在する場合、ファイルの検索は省略されます。
  - ファイルが検索されたファイルのキャッシュに存在しない場合、エージェントは承認済みファイルのキャッシュを確認します。

注意

承認済みファイルのキャッシュには、Apex One (Mac) が信頼できると見なしたファイルが含まれます。信頼できるファイルとは、一連のバージョンのパターンファイルで検索され、毎回安全であると宣言されたファイル、もしくは長期間未変更のままの安全なファイルです。

  - 承認済みファイルのキャッシュに存在する場合、ファイルの検索は省略されます。
  - ファイルが承認済みファイルのキャッシュに存在しない場合、エージェントはファイルを検索し、それを検索されたファイルのキャッシュに追加します。

検索エンジンまたはパターンファイルが更新されるたびに、キャッシュのすべてまたは一部が消去されます。

検索が頻繁に実行され、多数のファイルがキャッシュに含まれる場合は、検索時間が大幅に短縮されます。

検索の実行頻度が低い場合は、キャッシュ機能を無効にすることをお勧めします。

デバイスコントロール

デバイスコントロールを使用すると、エンドポイントに接続された外部ストレージデバイスやネットワークリソースへのアクセスを制御できます。デバイスコントロールを使用するとデータの紛失や漏えいを防止でき、ファイル検索と組み合わせて使用することで、セキュリティリスクから保護することができます。

内部エージェントと外部エージェントに対してデバイスコントロールポリシーを設定できます。通常は、外部エージェントに対してより厳格なポリシーを設定します。

ポリシーはエージェントツリーできめ細かく設定できます。各ポリシーは、エージェントグループや個々のセキュリティエージェントに適用できます。1 つのポリシーをすべてのセキュリティエージェントに適用することもできます。

デバイスコントロールを設定する

手順

1. [外部エージェント] タブをクリックして外部エージェントの設定を行うか、[内部エージェント] タブをクリックして内部エージェントの設定を行います。
2. [デバイスコントロールを有効にする] を選択します。
3. [デバイス] で、ストレージデバイスごとに権限を選択します。

   権限の詳細については、320 ページの「ストレージデバイスに対する権限」を参照してください。
4. (オプション) USB ストレージデバイスの権限が [ブロック] になっている場合は、[USB ストレージデバイス承認済みリスト] で承認済みデバイスのリストを設定できます。ユーザはこれらのデバイスにアクセスでき、管理者は権限を使用してアクセスレベルを制御できます。

   a. デバイスのベンダを入力します。

   b. デバイスモデルとシリアル ID を入力します。

   c. デバイスの権限を選択します。

権限の詳細については、320 ページの「ストレージデバイスに対する権限」を参照してください。

注意

承認済みリストの USB ストレージデバイスには、[デバイス] セクションの USB ストレージデバイスに設定された権限よりも高いレベルの権限が必要です。

5. [通知] で、[新しいデバイスが検出された場合にエージェントエンドポイントに通知メッセージを表示する] オプションを選択すると、新しいストレージデバイスがエンドポイントに接続されたときに通知が表示されます。通知には、新しいストレージデバイスのアクセス権限が表示されます。
6. [配信] をクリックします。

ストレージデバイスに対する権限

ストレージデバイスに対するデバイスコントロール権限は、次の場合に使用されます。

- USB ストレージデバイス、CD/DVD、SD カード、ネットワークドライブ、および Thunderbolt SATA ストレージデバイスへのアクセスを許可する場合。これらのデバイスへのフルアクセスを許可したり、アクセスレベルを制限したりすることができます。
- 承認済み USB ストレージデバイスのリストを設定する場合。デバイスコントロールでは、承認済みデバイスのリストに追加されている USB ストレージデバイスを除く、すべての USB ストレージデバイスへのアクセスをブロックできます。承認済みデバイスに対するフルアクセスを付与したり、アクセスレベルを制限したりすることができます。

次の表は、ストレージデバイスの権限をリストしたものです。

表 21-1. ストレージデバイスに対するデバイスコントロール権限

権限	デバイス上のファイル	受信ファイル
フルアクセス	許可される操作: コピー、移動、開く、保存、削除、実行	許可される操作: 保存、移動、コピー これは、デバイスにファイルを保存、移動、およびコピーできることを意味します。
読み取り専用	許可される操作: コピー、開く 禁止される操作: 保存、移動、削除、実行	禁止される操作: 保存、移動、コピー
ブロック	禁止される操作: すべて デバイスとデバイスに含まれるファイルは、ユーザには (Finder などに) 表示されません。	禁止される操作: 保存、移動、コピー

注意

読み取り専用権限はネットワークドライブには適用できません。

Endpoint Sensor

Endpoint Sensor は強力な監視/調査ツールで、脅威の有無、場所、および検出ポイントを特定します。詳細なシステムイベント記録と履歴分析を使用した履歴調査を実行して、ネットワーク内の隠れた脅威を検出し、すべての感染エンドポイントを特定できます。Root Cause Analysis レポートを生成することで、エンドポイントに脅威が侵入した時点からの不正プログラムの性質とアクティビティを把握することができます。

Endpoint Sensor を設定する

重要

Endpoint Sensor 機能を使用するには、専用のライセンスが必要であるほか、追加のシステム要件を満たす必要があります。Endpoint Sensor のポリシーをエンドポイントに配信する前に、正しいライセンスがあることを確認してください。ライセンスの入手方法の詳細については、サポートプロバイダにお問い合わせください。

手順

1. [Endpoint Sensor を有効にする] を選択します。

機械学習型検索設定

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジを使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどのファイル機能を使用した詳細なファイル分析により未知のセキュリティリスクを検出します。また、不明なプロセスやあまり普及していないプロセスの挙動分析を実行して、ネットワークへの侵入を試みる未知の新しい脅威がないかどうかを判定します。

機械学習型検索は、未知の脅威およびゼロデイ攻撃から環境を保護するのに役立つ強力な検索方法です。

この機能を有効にするには、[機械学習型検索を有効にする] を選択します。

権限とその他の設定

セキュリティエージェントの重要なファイルとフォルダを保護するようにセキュリティエージェントを設定します。

セクション	説明
セキュリティエージェントセルフプロテクション	セキュリティエージェントで使用するファイルが他のプログラムやユーザによって変更または削除されないようにするには、[セキュリティエージェントで使用するファイルの保護] を選択します。 この機能によって保護されるファイルとフォルダのリストについては、323 ページの「保護対象のセキュリティエージェントのファイル」を参照してください。

保護対象のセキュリティエージェントのファイル

セキュリティエージェントセルフプロテクション機能を有効にすると、セキュリティエージェントのファイルが他のプログラムやユーザによって変更または削除されないように、Apex One (Mac) によって次のファイルとフォルダがロックされます。

- /Library/Application Support/TrendMicro/common
- /Library/Application Support/TrendMicro/Kext
- /Library/Application Support/TrendMicro/TmccMac
- /Library/Application Support/TrendMicro/TmccUpdate
- /Library/Application Support/TrendMicro/Plug-in
- /Library/Application Support/TrendMicro/Tools
- /Library/LaunchDaemons/com.trendmicro.icore.*
- /Library/LaunchDaemons/com.trendmicro.tmsm.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.launcher.plist
- /Application/TrendMicroSecurity.app

注意

Apex One (Mac) では`/Library/Application Support/TrendMicro/Tools` フォルダにファイルを追加できますが、このフォルダからファイルを削除することはできません。

検索方法の種類

Apex One (Mac) セキュリティエージェントでのセキュリティリスクの検索には、2 つの検索方法のいずれかを使用できます。検索方法には、スマートスキャンと従来型スキャンがあります。

- スマートスキャン

  このドキュメントでは、スマートスキャンを使用するセキュリティエージェントを「スマートスキャンエージェント」と呼びます。スマートスキャンエージェントでは、ローカル検索と、ファイルレピュテーションサービスが提供するインターネットクエリを使用できます。

  これは初期設定の検索方法の種類です。

- 従来型スキャン

  スマートスキャンを使用しないエージェントは、「従来型スキャンエージェント」と呼ばれます。従来型スキャンエージェントでは、エージェントエンドポイント上にすべての Apex One (Mac) コンポーネントが保管され、ローカルのすべてのファイルが検索されます。

検索方法の比較

次の表は、2 つの検索の種類を比較したものです。

表 21-2. 従来型スキャンとスマートスキャンの比較

比較の基本	従来型スキャン	スマートスキャン
検索の動作	従来型スキャンエージェントは、ローカルエンドポイントで検索を実行します。	• スマートスキャンエージェントは、ローカルエンドポイントで検索を実行します。 • セキュリティエージェントが検索中にファイルのリスクを特定できない場合、検索クエリを Smart Protection ソースに送信してリスクを検証します。 • セキュリティエージェントは検索クエリの結果を「キャッシュ」することにより、検索のパフォーマンスを向上させます。

比較の基本	従来型スキャン	スマートスキャン
使用中のコンポーネントとアップデートされたコンポーネント	Mac ヒューリスティックパターンファイルとスマートスキャンエージェントパターンファイルを除く、アップデート元で使用可能なすべてのコンポーネント	パターンファイルとスパイウェア監視パターンファイルを除く、アップデート元で使用可能なすべてのコンポーネント
標準のアップデート元	Apex One (Mac) サーバ	Apex One (Mac) サーバ

スマートスキャンから従来型スキャンへ切り替える

次の表は、エージェントを従来型スキャンに切り替える際のその他の注意点を示しています。

表 21-3. 従来型スキャンに切り替える際の注意点

注意点	詳細
切り替えるセキュリティエージェントの数	比較的少数のセキュリティエージェントを同時に切り替えると、Apex One (Mac) サーバのリソースと Smart Protection Server のリソースを有効活用できます。セキュリティエージェントが検索方法を変更する間、これらのサーバは他の重大なタスクを実行できます。
タイミング	従来型スキャンに切り替えると、セキュリティエージェントは Apex One (Mac) サーバからウイルスパターンファイルおよびスパイウェア監視パターンファイルの製品版をダウンロードする可能性があります。これらのパターンファイルは、従来型スキャンエージェントによってのみ使用されます。 ダウンロード処理を短時間で完了できるよう、ピーク時間を避けて切り替えを実施することを検討してください。また、サーバからのセキュリティエージェントのアップデートが 1 件も予定されていないタイミングを推奨します。

注意点	詳細
エージェントツリーの設定	検索方法は、root、ドメイン、または個々のエージェントレベルで実行できる細かい設定です。従来型スキャンに切り替えると、次のことを実行できます。 • 新しいグループを作成し、その検索方法として従来型スキャンを割り当てます。このグループに移動するセキュリティエージェントは、従来型スキャンを使用します。セキュリティエージェントを移動する場合、[新しいグループの設定を選択したエージェントに適用する] の設定を有効にします。 • グループを選択し、従来型スキャンを使用するように設定します。そのグループに属するスマートスキャンエージェントは従来型スキャンに切り替わります。 • 1 つまたは複数のスマートスキャンエージェントをグループから選択し、それを従来型スキャンに切り替えます。 注意 グループの検索方法に変更を加えると、個々のセキュリティエージェントに設定してある検索方法がオーバーライドされます。

従来型スキャンからスマートスキャンへ切り替える

セキュリティエージェントを従来型スキャンからスマートスキャンに切り替える場合は、Apex One サーバで Smart Protection サービスが設定済みであることを確認してください。詳細については、Apex One のドキュメントを参照してください。

次の表は、セキュリティエージェントをスマートスキャンに切り替える場合のその他の注意点を示しています。

表 21-4. スマートスキャンに切り替える場合の注意点

注意点	詳細
製品ライセンス	スマートスキャンを使用する場合は、Apex One サーバで次のサービスのライセンスを有効にしてあることと、そのライセンスの有効期限が過ぎていないことを確認してください。 • ウイルス対策 • Web レピュテーションおよびスパイウェア対策
Apex One (Mac) サーバ	セキュリティエージェントが Apex One (Mac) サーバに接続できることを確認します。スマートスキャンに切り替えるように通知されるのはオンラインのセキュリティエージェントだけです。オフラインのセキュリティエージェントはオンラインになったときに通知されます。スタンドアロンのセキュリティエージェントは、オンラインになったとき、またはセキュリティエージェントに予約アップデート権限がある場合は予約アップデートが実行されたときに通知されます。
切り替えるセキュリティエージェントの数	一度に切り替えるセキュリティエージェントの数を少なくすることで、Apex One (Mac) サーバのリソースを効率よく使用できます。セキュリティエージェントが検索方法を変更している間も、Apex One (Mac) サーバはその他の重要なタスクを実行できます。
タイミング	初めてスマートスキャンに切り替えるときは、セキュリティエージェントは Apex One (Mac) サーバから Mac ヒューリスティックパターンファイルとスマートスキャンエージェントパターンファイルの完全版をダウンロードする必要があります。スマートスキャンパターンファイルはスマートスキャンエージェントのみが使用します。 ダウンロード処理を短時間で完了できるよう、ピーク時間を避けて切り替えを実施することを検討してください。また、サーバからのセキュリティエージェントのアップデートが 1 件も予定されていないタイミングを推奨します。

注意点	詳細
エージェントツリーの設定	検索方法は、ルート、グループ、または個々のエージェントレベルで設定できます。スマートスキャンに切り替えるときには、次の操作を実行できます。 • 新しいグループを作成し、検索方法としてスマートスキャンを割り当てる。このグループに追加するすべてのセキュリティエージェントでスマートスキャンが使用されます。セキュリティエージェントを移動するときは、設定の [新しいグループの設定を選択したエージェントに適用する] を有効にしてください。 • グループを選択し、スマートスキャンを使用するように設定する。このグループに属している従来型スキャンエージェントは、スマートスキャンに切り替わります。 • グループから 1 つまたは複数の従来型スキャンエージェントを選択し、スマートスキャンに切り替える。 **注意** グループの検索方法に変更を加えると、個々のセキュリティエージェントに設定してある検索方法がオーバーライドされます。
IPv6 のサポート	スマートスキャンエージェントは、Smart Protection ソースに検索クエリを送信します。 IPv6 シングルスタックスマートスキャンエージェントは、次のような IPv4 シングルスタックソースにクエリを直接送信することはできません。 • Smart Protection Server 3.0 (統合またはスタンドアロン) • Trend Micro Smart Protection Network 同様に、IPv4 シングルスタックスマートスキャンエージェントは、IPv6 シングルスタック Smart Protection Server にクエリを送信できません。 スマートスキャンエージェントがソースに接続するためには、IP アドレスを変換できるデュアルスタックプロキシサーバ (DeleGate など) が必要です。

検索の種類

Apex One (Mac) では、エンドポイントをセキュリティリスクから保護するために次の検索の種類が用意されています。

検索の種類	説明
リアルタイム検索	エンドポイント上のファイルを受信、開く、ダウンロード、コピー、および変更したときに自動的に検索されます。 329 ページの「リアルタイム検索」を参照してください。
手動検索	ユーザが要求したファイル (またはファイルのセット) を検索する手動の検索です。 334 ページの「手動検索」を参照してください。
予約検索	管理者が設定したスケジュールに従って、エンドポイント上のファイルが自動的に検索されます。 340 ページの「予約検索」を参照してください。
検索開始	1 つ以上の対象エンドポイント上にあるファイルを検索する、管理者が開始する検索です。

リアルタイム検索

リアルタイム検索は、持続的で継続的な検索です。ファイルが受信、オープン、ダウンロード、コピー、または変更されるたびに、リアルタイム検索はファイルを検索して、セキュリティリスクがないかどうか確認します。Apex One (Mac) でセキュリティリスクが検出されない場合、ファイルはその場所に残され、ユーザは引き続きファイルにアクセスできます。Apex One (Mac) でセキュリティリスクが検出された場合は、通知メッセージが表示され、感染ファイルの名前と該当するセキュリティリスクが表示されます。

1 つまたは複数のエージェントおよびグループ、またはサーバが管理するすべてのセキュリティエージェントに、リアルタイム検索を設定して適用します。

リアルタイム検索の設定

手順

1. チェックボックスをオンにして、リアルタイム検索を有効にします。

2. [対象] タブをクリックし、ファイルのアクティビティと検索の詳細を設定します。

   詳細については、330 ページの「リアルタイム検索: [対象] タブ」を参照してください。

3. [処理] タブをクリックし、Apex One (Mac) でセキュリティリスクが検出されたときに実行する処理を設定します。

   詳細については、331 ページの「リアルタイム検索: [処理] タブ」を参照してください。

リアルタイム検索: [対象] タブ

手順

1. [ファイルに対するユーザのアクティビティ] で、リアルタイム検索を実行するファイルに対するアクティビティを指定します。次のオプションから選択します。

   - 次のファイルを検索: 作成された/変更されたファイル: エンドポイントに取り込まれた新しいファイル (ファイルのダウンロード後など)、または変更されたファイルを検索します。
   - 次のファイルを検索: 読み込まれた/実行されたファイル: ファイルが開かれたときに検索します。
   - 次のファイルを検索: 作成された/変更された/読み込まれた/実行されたファイル
   - 次のファイルを検索: 作成された/変更された/実行されたファイル

   たとえば、3 番目のオプションを選択した場合、エンドポイントにダウンロードされた新しいファイルが検索され、セキュリティリスクが検出されない場合には現在の場所に残されます。この残されたファイルは、ユーザがそのファイルを開いたとき、およびユーザがそのファイルを変更した場合は変更内容が保存される前に、検索されます。

2. [検索設定] で、次のオプションを 1 つ以上選択します。

   - 圧縮ファイルの検索: アーカイブファイル内の個々のファイルを検索します

詳細については、332 ページの「サポートされる圧縮ファイルの種類」を参照してください。

- ネットワークドライブの検索: 他のエンドポイントに物理的に配置されていて、ローカルエンドポイントにマッピングされているディレクトリを検索します

リアルタイム検索: [処理] タブ

[処理] タブでは、セキュリティ上の脅威が検出されたときに Apex One (Mac) で実行する処理を設定します。

手順

1. [処理] で、検出時の処理を指定します。

オプション	説明
トレンドマイクロの推奨処理を使用	トレンドマイクロの推奨処理とは、セキュリティリスクの種類ごとに事前に割り当てられている一連の検索処理です。特定の種類のセキュリティリスクに適した検出時処理の判断が難しい場合は、トレンドマイクロの推奨処理を使用することを推奨します。 トレンドマイクロの推奨処理の設定は、最新のセキュリティリスクや最新の攻撃手段からエンドポイントを保護できるようにパターンファイルで絶えず更新されます。
すべての種類のセキュリティリスクに同じ処理を使用	このオプションは、潜在的なウイルス/不正プログラムを除くすべての種類のセキュリティリスクに同じ処理を実行する場合に選択します。潜在的なウイルス/不正プログラムに対する処理は常に「放置」です。 1 次処理として「駆除」を選択していて駆除に失敗した場合、Apex One (Mac) が実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。 検索時の処理の詳細は、332 ページの「検出時の処理」を参照してください。

2. リアルタイム検索中に Apex One (Mac) でセキュリティリスクが検出されたときに通知メッセージを表示するには、[ウイルス/不正プログラムが検出された場合にエージェントエンドポイントに通知メッセージを表示する] を選択します。

サポートされる圧縮ファイルの種類

Apex One (Mac) は次の種類の圧縮ファイルをサポートしています。

拡張子	種類
.zip	Pkzip によって作成されるアーカイブ
.rar	RAR によって作成されるアーカイブ
.tar	Tar によって作成されるアーカイブ
.arj	ARJ 圧縮アーカイブ
.hqx	BINHEX
.gz、.gzip	Gnu ZIP
.Z	LZW/圧縮 16 ビット
.bin	MacBinary
.cab	Microsoft キャビネットファイル
Microsoft 圧縮/MSCOMP	
.eml、mht	MIME
.td0	Teledisk 形式
.bz2	Unix BZ2 Bzip 圧縮ファイル
.uu	UUEncode
.ace	WinAce

検出時の処理

特定の検索の種類でセキュリティリスクを検出したときに、Apex One (Mac) が実行する処理を指定します。

Apex One (Mac) による検出時の処理は、セキュリティリスクを検出した検索の種類によって異なります。たとえば、Apex One (Mac) で手動検索 (検索の種類) によってセキュリティリスクが検出された場合は、感染ファイルが駆除 (処理) されます。

Apex One (Mac) がセキュリティリスクに対して実行可能な処理は次のとおりです。

ウイルス検出時の処理	詳細
削除	Apex One (Mac) は感染ファイルをエンドポイントから削除します。
隔離	感染ファイルの名前を変更し、そのファイルをエンドポイントの隔離ディレクトリ (<エージェントのインストールフォルダ>/common/lib/vsapi/quarantine) に移動します。 隔離ディレクトリに移動した隔離ファイルに対して、ユーザ指定の処理に基づいて、さらに別の処理を実行できます。隔離ファイルに対して実行できる処理には、削除、駆除、復元があります。ファイルの復元とは、処理を何も実行せずにファイルを元の場所に戻すことです。ユーザは、実際には無害な場合にファイルを復元できます。ファイルの駆除とは、隔離ファイルからセキュリティリスクを削除して、駆除が正常に実行された場合にそのファイルを元の場所に戻すことです。
駆除	Apex One (Mac) は、感染ファイルからセキュリティリスクを削除したうえで、ユーザにファイルへのアクセスを許可します。 ファイルを駆除できない場合は、2 次処理として、隔離、削除、放置のいずれかを実行します。2 次処理を設定するには、[エージェント管理] > [設定] > {検索の種類} に移動し、[処理] タブをクリックします。

ウイルス検出時の処理	詳細
放置	Apex One (Mac) は、感染ファイルに対する処理を実行せず、検出したセキュリティリスクをログに記録します。ファイルは元の場所に残ります。 Apex One (Mac) は、誤検出を防止するため、潜在的なウイルス/不正プログラムの種類に感染したファイルに対して常に「放置」を実行します。その後の解析で潜在的なウイルス/不正プログラムが実際にセキュリティリスクであることが確認されると、新しいパターンファイルがリリースされ、Apex One (Mac) で適切な検出時処理を実行できるようになります。実際には無害であることが確認されると、その潜在的なウイルス/不正プログラムは以降は検出されません。 たとえば、「123.pdf」というファイルで「x_probable_virus」が検出された場合、Apex One (Mac) は検出時に処理を実行しません。「x_probable_virus」がトロイの木馬プログラムであることが確認されると、新しいウイルスパターンファイルがリリースされます。新しいパターンファイルがロードされると、Apex One (Mac) は「x_probable_virus」がトロイの木馬のプログラムとして検出するようになり、トロイの木馬のプログラムに対する処理が「削除」の場合、「123.pdf」は削除されます。 注意 この処理は、リアルタイム検索に対しては使用できません。
アクセス拒否	Apex One (Mac) では、感染ファイルを開いたり、実行したりしようとする操作を検出すると、その操作を即時にブロックします。 ユーザは感染ファイルを手動で削除できます。

手動検索

手動検索はオンデマンドの検索であり、ユーザがエージェントコンソールで検索を実行するとただちに開始されます。検索にかかる時間は、検索するファイル数やエンドポイントのハードウェアリソースによって異なります。

手動検索の設定は、1 つ以上のセキュリティエージェントおよびグループに設定および適用するか、またはサーバが管理するすべてのセキュリティエージェントに設定および適用します。

手動検索の設定

手順

1. [対象] タブをクリックし、検索の詳細と CPU 使用率を設定します。

   詳細については、335 ページの「手動検索: [対象] タブ」を参照してください。

2. [処理] タブをクリックし、Apex One (Mac) でセキュリティリスクが検出されたときに実行する処理を設定します。

   詳細については、336 ページの「手動検索: [処理] タブ」を参照してください。

手動検索: [対象] タブ

手順

1. [検索するファイル] で、次の項目から選択します。

   - 検索可能なすべてのファイル: すべてのファイルを検索します。検索できないファイルには、パスワードで保護されたファイル、暗号化されたファイル、ユーザ指定の検索制限を超えるファイルがあります。

     注意

     すべてのファイルの検索には多くの時間とリソースを消費するため、状況によっては不要な場合もあります。このため、セキュリティエージェントで検索するファイルの数を制限することも可能です。

   - Mach-O ファイルのみを検索: エンドポイント上の Mach-O ファイルのみを検索します。Apex One (Mac) セキュリティエージェントは、その他の種類のファイルに含まれる不正プログラムを検索しません。

注意

このオプションを選択する場合は、OS X および macOS プラットフォームを標的とする最新の不正プログラムによる攻撃から保護するためにスマートスキャン機能を有効にする必要があります。

2. [検索設定] で、次のオプションを 1 つ以上選択します。
   - 圧縮ファイルの検索: アーカイブファイル内の個々のファイルを検索します

     詳細については、332 ページの「サポートされる圧縮ファイルの種類」を参照してください。
   - ネットワークドライブの検索: 他のエンドポイントに物理的に配置されていて、ローカルエンドポイントにマッピングされているディレクトリを検索します
   - Time Machine の検索: Time Machine ドライブ上のファイルのみを検索します

     注意

     手動検索および予約検索の [Time Machine の検索] オプションを有効にした場合、不正プログラムの脅威は検出されますが、処理 (駆除、隔離、削除) は実行されなくなります。これは、Mac OS の権限の制限によるものです。検索処理が設定されている場合、製品ログには失敗として記録されます。
3. [CPU 使用率] セクションで必要な設定を行います。
   - 高: 検索が速くなり PC への負荷が最も高くなります。
   - 低: 検索に時間がかかりますが PC への負荷が最も低くなります。

手動検索: [処理] タブ

[処理] タブでは、セキュリティ上の脅威が検出されたときに Apex One (Mac) で実行する処理を設定します。

オプション	説明
トレンドマイクロの推奨処理を使用	トレンドマイクロの推奨処理とは、セキュリティリスクの種類ごとに事前に割り当てられている一連の検索処理です。特定の種類のセキュリティリスクに適した検出時処理の判断が難しい場合は、トレンドマイクロの推奨処理を使用することを推奨します。 トレンドマイクロの推奨処理の設定は、最新のセキュリティリスクや最新の攻撃手段からエンドポイントを保護できるようにパターンファイルで絶えず更新されます。
すべての種類のセキュリティリスクに同じ処理を使用	このオプションは、潜在的なウイルス/不正プログラムを除くすべての種類のセキュリティリスクに同じ処理を実行する場合に選択します。潜在的なウイルス/不正プログラムに対する処理は常に「放置」です。 1 次処理として「駆除」を選択していて駆除に失敗した場合、Apex One (Mac) が実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。 検索時の処理の詳細は、332 ページの「検出時の処理」を参照してください。

サポートされる圧縮ファイルの種類

Apex One (Mac) は次の種類の圧縮ファイルをサポートしています。

拡張子	種類
.zip	Pkzip によって作成されるアーカイブ
.rar	RAR によって作成されるアーカイブ
.tar	Tar によって作成されるアーカイブ
.arj	ARJ 圧縮アーカイブ
.hqx	BINHEX
.gz、.gzip	Gnu ZIP

拡張子	種類
.Z	LZW/圧縮 16 ビット
.bin	MacBinary
.cab	Microsoft キャビネットファイル
Microsoft 圧縮/MSCOMP	
.eml、mht	MIME
.td0	Teledisk 形式
.bz2	Unix BZ2 Bzip 圧縮ファイル
.uu	UUEncode
.ace	WinAce

検出時の処理

特定の検索の種類でセキュリティリスクを検出したときに、Apex One (Mac) が実行する処理を指定します。

Apex One (Mac) による検出時の処理は、セキュリティリスクを検出した検索の種類によって異なります。たとえば、Apex One (Mac) で手動検索 (検索の種類) によってセキュリティリスクが検出された場合は、感染ファイルが駆除 (処理) されます。

Apex One (Mac) がセキュリティリスクに対して実行可能な処理は次のとおりです。

ウイルス検出時の処理	詳細
削除	Apex One (Mac) は感染ファイルをエンドポイントから削除します。

ウイルス検出時の処理	詳細
隔離	感染ファイルの名前を変更し、そのファイルをエンドポイントの隔離ディレクトリ (<エージェントのインストールフォルダ>/common/lib/vsapi/quarantine) に移動します。 隔離ディレクトリに移動した隔離ファイルに対して、ユーザ指定の処理に基づいて、さらに別の処理を実行できます。隔離ファイルに対して実行できる処理には、削除、駆除、復元があります。ファイルの復元とは、処理を何も実行せずにファイルを元の場所に戻すことです。ユーザは、実際には無害な場合にファイルを復元できます。ファイルの駆除とは、隔離ファイルからセキュリティリスクを削除して、駆除が正常に実行された場合にそのファイルを元の場所に戻すことです。
駆除	Apex One (Mac) は、感染ファイルからセキュリティリスクを削除したうえで、ユーザにファイルへのアクセスを許可します。 ファイルを駆除できない場合は、2 次処理として、隔離、削除、放置のいずれかを実行します。2 次処理を設定するには、[エージェント管理] > [設定] > {検索の種類} に移動し、[処理] タブをクリックします。

ウイルス検出時の処理	詳細
放置	Apex One (Mac) は、感染ファイルに対する処理を実行せず、検出したセキュリティリスクをログに記録します。ファイルは元の場所に残ります。 Apex One (Mac) は、誤検出を防止するため、潜在的なウイルス/不正プログラムの種類に感染したファイルに対して常に「放置」を実行します。その後の解析で潜在的なウイルス/不正プログラムが実際にセキュリティリスクであることが確認されると、新しいパターンファイルがリリースされ、Apex One (Mac) で適切な検出時処理を実行できるようになります。実際には無害であることが確認されると、その潜在的なウイルス/不正プログラムは以降は検出されません。 たとえば、「123.pdf」というファイルで「x_probable_virus」が検出された場合、Apex One (Mac) は検出時に処理を実行しません。「x_probable_virus」がトロイの木馬プログラムであることが確認されると、新しいウイルスパターンファイルがリリースされます。新しいパターンファイルがロードされると、Apex One (Mac) は「x_probable_virus」がトロイの木馬のプログラムとして検出するようになり、トロイの木馬のプログラムに対する処理が「削除」の場合、「123.pdf」は削除されます。 注意 この処理は、リアルタイム検索に対しては使用できません。
アクセス拒否	Apex One (Mac) では、感染ファイルを開いたり、実行したりしようとする操作を検出すると、その操作を即時にブロックします。 ユーザは感染ファイルを手動で削除できます。

予約検索

予約検索は指定された日時に自動的に実行されます。セキュリティエージェントの予約検索を使用して日々の検索を自動化することで、検索をより効率的に管理できます。

予約検索の設定は、1 つ以上のセキュリティエージェントおよびグループに設定および適用するか、またはサーバが管理するすべてのセキュリティエージェントに設定および適用します。

予約検索の設定

手順

1. チェックボックスをオンにして、予約検索を有効にします。
2. [対象] タブをクリックし、検索の詳細、CPU 使用率、および検索スケジュールを設定します。

   詳細については、341 ページの「予約検索: [対象] タブ」を参照してください。
3. [処理] タブをクリックし、Apex One (Mac) でセキュリティリスクが検出されたときに実行する処理を設定します。

   詳細については、343 ページの「予約検索: [処理] タブ」を参照してください。

予約検索: [対象] タブ

手順

1. [スケジュール] で、予約検索を実行する頻度 (毎日、毎週、毎月) や時刻を設定します。

   毎月の予約検索では、29 日、30 日、31 日を選択した場合、これらの日付がない月では、Apex One (Mac) によってその月の最終日に予約検索が実行されます。
2. [検索するファイル] で、次の項目から選択します。
   - 検索可能なすべてのファイル: すべてのファイルを検索します。検索できないファイルには、パスワードで保護されたファイル、暗号化されたファイル、ユーザ指定の検索制限を超えるファイルがあります。

注意

すべてのファイルの検索には多くの時間とリソースを消費するため、状況によっては不要な場合もあります。このため、セキュリティエージェントで検索するファイルの数を制限することも可能です。

- トレンドマイクロの推奨設定で検索されたファイルタイプ: 不正コードが含まれている可能性のあるファイルのみを検索します。これには無害な拡張子名で偽装されたファイルも含まれます。
- パスまたはフルパスを指定: 検索するファイルまたはディレクトリを手動で指定します。例: `/Shared/Files/mytext.txt` または `/Shared/Files`。

3. [検索設定] で、次のオプションを 1 つ以上選択します。
   - 圧縮ファイルの検索: アーカイブファイル内の個々のファイルを検索します

     詳細については、332 ページの「サポートされる圧縮ファイルの種類」を参照してください。
   - Time Machine の検索: Time Machine ドライブ上のファイルのみを検索します

     注意

     手動検索および予約検索の [Time Machine の検索] オプションを有効にした場合、不正プログラムの脅威は検出されますが、処理 (駆除、隔離、削除) は実行されなくなります。これは、Mac OS の権限の制限によるものです。検索処理が設定されている場合、製品ログには失敗として記録されます。
4. [CPU 使用率] セクションで必要な設定を行います。
   - 高: 検索が速くなり PC への負荷が最も高くなります。
   - 低: 検索に時間がかかりますが PC への負荷が最も低くなります。

予約検索: [処理] タブ

[処理] タブでは、セキュリティ上の脅威が検出されたときに Apex One (Mac) で実行する処理を設定します。

手順

1. [処理] で、検出時の処理を指定します。

オプション	説明
トレンドマイクロの推奨処理を使用	トレンドマイクロの推奨処理とは、セキュリティリスクの種類ごとに事前に割り当てられている一連の検索処理です。特定の種類のセキュリティリスクに適した検出時処理の判断が難しい場合は、トレンドマイクロの推奨処理を使用することを推奨します。 トレンドマイクロの推奨処理の設定は、最新のセキュリティリスクや最新の攻撃手段からエンドポイントを保護できるようにパターンファイルで絶えず更新されます。
すべての種類のセキュリティリスクに同じ処理を使用	このオプションは、潜在的なウイルス/不正プログラムを除くすべての種類のセキュリティリスクに同じ処理を実行する場合に選択します。潜在的なウイルス/不正プログラムに対する処理は常に「放置」です。 1 次処理として「駆除」を選択していて駆除に失敗した場合、Apex One (Mac) が実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。 検索時の処理の詳細は、332 ページの「検出時の処理」を参照してください。

2. [予約検索権限] で、ユーザによる予約検索の保留またはスキップを許可するかどうかを指定します。

権限	説明
予約検索の延期	「予約検索の延期」権限を持つユーザは、次の処理を実行できます。 • 予約検索を実行前に延期し、延期期間を指定できます。予約検索は 1 回だけ延期できます。 • 予約検索が進行中の場合、ユーザは検索を停止して後で再開できます。ユーザは、検索を再開するまでの経過時間を指定します。検索を再開すると、前に検索されたファイルがすべて再検索されます。予約検索を停止して再開できるのは 1 回だけです。 次に対応する時間数および分数を設定します。 • 最大延期期間 • 検索を再開するまでの最大経過時間
予約検索のスキップおよび停止	この権限を持つユーザは、次の処理を実行できます。 • 予約検索が実行される前にそれをスキップできます。 • 予約検索の実行中にそれを停止できます。

3. [予約検索設定] で、通知とバッテリ電力の設定を指定します。

設定	説明
予約検索の実行前に通知を表示	このオプションを有効にすると、予約検索を実行する数分前に、エンドポイントに通知メッセージが表示されるようになります。このメッセージでは、検索のスケジュール (日時)、およびユーザの予約検索権限 (予約検索の保留、スキップ、または停止など) が通知されます。 通知メッセージを表示するタイミングを分数で設定します。
予約検索を自動停止するまでの経過時間: __ 時間 __ 分	指定した時間が経過してもセキュリティエージェントによる検索が完了しない場合に検索を停止します。検索中に検出されたセキュリティリスクはセキュリティエージェントを通じてただちにユーザに通知されます。

設定	説明
ノート PC のバッテリ残量が__%よりも少なく、AC アダプタが接続されていない場合は、予約検索をスキップする	ノート PC のバッテリ残量が少なく、AC アダプタが電源に接続されていない場合、予約検索をスキップします。バッテリ残量が少なくても、AC アダプタが電源に接続されている場合は、検索が続行されます。バッテリ残量が少なくなっても、実行中の検索は中止されません。

サポートされる圧縮ファイルの種類

Apex One (Mac) は次の種類の圧縮ファイルをサポートしています。

拡張子	種類
.zip	Pkzip によって作成されるアーカイブ
.rar	RAR によって作成されるアーカイブ
.tar	Tar によって作成されるアーカイブ
.arj	ARJ 圧縮アーカイブ
.hqx	BINHEX
.gz、.gzip	Gnu ZIP
.Z	LZW/圧縮 16 ビット
.bin	MacBinary
.cab	Microsoft キャビネットファイル
Microsoft 圧縮/MSCOMP	
.eml、mht	MIME
.td0	Teledisk 形式
.bz2	Unix BZ2 Bzip 圧縮ファイル
.uu	UUEncode
.ace	WinAce

検出時の処理

特定の検索の種類でセキュリティリスクを検出したときに、Apex One (Mac) が実行する処理を指定します。

Apex One (Mac) による検出時の処理は、セキュリティリスクを検出した検索の種類によって異なります。たとえば、Apex One (Mac) で手動検索 (検索の種類) によってセキュリティリスクが検出された場合は、感染ファイルが駆除 (処理) されます。

Apex One (Mac) がセキュリティリスクに対して実行可能な処理は次のとおりです。

ウイルス検出時の処理	詳細
削除	Apex One (Mac) は感染ファイルをエンドポイントから削除します。
隔離	感染ファイルの名前を変更し、そのファイルをエンドポイントの隔離ディレクトリ (<エージェントのインストールフォルダ>/common/lib/vsapi/quarantine) に移動します。 隔離ディレクトリに移動した隔離ファイルに対して、ユーザ指定の処理に基づいて、さらに別の処理を実行できます。隔離ファイルに対して実行できる処理には、削除、駆除、復元があります。ファイルの復元とは、処理を何も実行せずにファイルを元の場所に戻すことです。ユーザは、実際には無害な場合にファイルを復元できます。ファイルの駆除とは、隔離ファイルからセキュリティリスクを削除して、駆除が正常に実行された場合にそのファイルを元の場所に戻すことです。
駆除	Apex One (Mac) は、感染ファイルからセキュリティリスクを削除したうえで、ユーザにファイルへのアクセスを許可します。 ファイルを駆除できない場合は、2 次処理として、隔離、削除、放置のいずれかを実行します。2 次処理を設定するには、[エージェント管理] > [設定] > {検索の種類} に移動し、[処理] タブをクリックします。

ウイルス検出時の処理	詳細
放置	Apex One (Mac) は、感染ファイルに対する処理を実行せず、検出したセキュリティリスクをログに記録します。ファイルは元の場所に残ります。 Apex One (Mac) は、誤検出を防止するため、潜在的なウイルス/不正プログラムの種類に感染したファイルに対して常に「放置」を実行します。その後の解析で潜在的なウイルス/不正プログラムが実際にセキュリティリスクであることが確認されると、新しいパターンファイルがリリースされ、Apex One (Mac) で適切な検出時処理を実行できるようになります。実際には無害であることが確認されると、その潜在的なウイルス/不正プログラムは以降は検出されません。 たとえば、「123.pdf」というファイルで「x_probable_virus」が検出された場合、Apex One (Mac) は検出時に処理を実行しません。「x_probable_virus」がトロイの木馬プログラムであることが確認されると、新しいウイルスパターンファイルがリリースされます。新しいパターンファイルがロードされると、Apex One (Mac) は「x_probable_virus」がトロイの木馬のプログラムとして検出するようになり、トロイの木馬のプログラムに対する処理が「削除」の場合、「123.pdf」は削除されます。 注意 この処理は、リアルタイム検索に対しては使用できません。
アクセス拒否	Apex One (Mac) では、感染ファイルを開いたり、実行したりしようとする操作を検出すると、その操作を即時にブロックします。 ユーザは感染ファイルを手動で削除できます。

検索除外

検索除外を設定すると、検索のパフォーマンスを向上させ、既知の無害なファイルの検索をスキップできるようになります。特定の種類の検索を実行するときに、Apex One (Mac) は検索除外リストをチェックして、検索から除外するエンドポイント内のファイルを決定します。

検索除外リスト	詳細
ファイル	Apex One (Mac) では、次に該当するファイルは検索しません。 • 検索除外リストに指定したディレクトリパスの下にあるファイル • 検索除外リストに指定したファイルのフルパス (ディレクトリパスとファイル名) に一致するファイル
ファイル拡張子	Apex One (Mac) は、ファイルの拡張子がこの除外リストに含まれているいずれかのファイル拡張子に一致する場合、そのファイルを検索しません。

検索除外リスト設定

検索除外リストの詳細については、「347 ページの「検索除外」」を参照してください。

手順

1. チェックボックスをオンにして検索除外を有効にします。
2. [検索除外リスト (ファイル)] を設定するには
   a. ファイルのフルパスまたはディレクトリパスを入力し、[追加] をクリックします。

      注意:

      • ファイル名のみを入力することはできません。
      • 最大 64 のパスを指定できます。次の表の例を参照してください。

パス	詳細	例

ファイルのフルパス	エンドポイント上の特定のファイルを除外します。	• 例 1:
		`/file.log`
		• 例 2:
		`/System/file.log`

パス	詳細	例

ディレクトリパス	特定のフォルダおよびそのサブフォルダにあるすべてのファイルを除外します。	• 例 1:
		`/System/`
		検索から除外されるファイルの例:
		• `/System/file.log`
		• `/System/Library/file.log`
		検索されるファイルの例:
		• `/Applications/file.log`
		• 例 2:
		`/System/Library`
		検索から除外されるファイルの例:
		• `/System/Library/file.log`
		• `/System/Library/Filters/file.log`
		検索されるファイルの例:
		• `/System/file.log`

- フォルダ名の代わりにアスタリスクワイルドカード (*) を使用します。

  次の表の例を参照してください。

パス	ワイルドカードの使用例
ファイルのフルパス	`/Users/Mac/*/file.log` 検索から除外されるファイルの例: • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` 検索されるファイルの例: • `/Users/file.log` • `/Users/Mac/file.log`

ディレクトリパス	• 例 1:
	`/Users/Mac/*`
	検索から除外されるファイルの例:
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	検索されるファイルの例:
	• `/Users/doc.html`
	• 例 2:
	`/*/Components`
	検索から除外されるファイルの例:
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	検索されるファイルの例:
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- フォルダ名の部分一致はサポートされていません。たとえば、`/Users/*user/temp` と入力して、「end_user」や「new_user」な

ど、フォルダ名の末尾が「user」であるフォルダ内のファイルを除外することはできません。

b. パスを削除するには、そのパスを選択して [削除] をクリックします。

3. [検索除外リスト (ファイル拡張子)] を設定するには

a. ファイル拡張子をピリオドなしで入力し、[追加] をクリックします。たとえば、`pdf` と入力します。最大 64 のファイル拡張子を指定できます。

b. ファイル拡張子を削除するには、そのファイル拡張子を選択して [削除] をクリックします。

信頼済みプログラムリスト

セキュリティエージェントは、リアルタイム検索やイベント記録時に信頼済みプロセスの検索をスキップするよう設定できます。信頼済みプログラムリストにプログラムを追加すると、セキュリティエージェントでは、そのプログラムとそのプログラムで開始されるすべてのプロセスがリアルタイム検索とイベント記録の対象から除外されます。エンドポイントに対する検索のパフォーマンスを向上させるには、信頼済みプログラムリストに信頼するプログラムを追加してください。

注意

信頼済みプログラムリストに追加するファイルの要件は次のとおりです。

- システムディレクトリに格納されていない。
- 有効なデジタル署名がある。

信頼済みプログラムリストにプログラムを追加すると、セキュリティエージェントでは、そのプログラムが自動的に次の処理から除外されます。

- リアルタイム検索のファイル確認
- リアルタイム検索のプロセス検索
- イベント記録

信頼済みプログラムリストを設定する

信頼済みプログラムリストは、プログラムおよびそのプログラムから呼び出されるすべての子プロセスをリアルタイム検索から除外します。

手順

1. 検索から除外するプログラムのフルパスを入力します。
2. [+追加] をクリックします。
3. リストからプログラムを削除するには、[削除] アイコンをクリックします。

アップデート設定

最新のセキュリティリスクに対するセキュリティエージェントの保護状態を維持するには、エージェントのコンポーネントを定期的にアップデートします。コンポーネントが著しく古い場合や、大規模感染が発生したときにもセキュリティエージェントをアップデートしてください。セキュリティエージェントが Apex One (Mac) サーバまたはアップデートサーバから長期間アップデートを実行できないでいると、エージェントのコンポーネントは著しく古くなります。

エージェントのアップデート方法

セキュリティエージェントをアップデートする方法はいくつかあります。

アップデート方法	説明
管理者が開始する手動アップデート	次の Web コンソール画面からアップデートを開始します。 • [エージェント管理] 画面。 • [概要] 画面。

アップデート方法	説明
自動アップデート	• サーバでアップデートが完了すると、アップデートを促す通知が、サーバからセキュリティエージェントへすぐに送信されます。 • アップデートは、設定したスケジュールに従って実行できます。1 つまたは複数のセキュリティエージェントおよびドメインに、またはサーバが管理するすべてのセキュリティエージェントに適用されるスケジュールを設定できます。 詳細については、355 ページの「エージェントのアップデートの設定」を参照してください。
ユーザが開始する手動アップデート	ユーザがエンドポイントからアップデートを開始します。

エージェントのアップデート元

初期設定では、セキュリティエージェントは Apex One (Mac) サーバからコンポーネントをダウンロードします。Apex One (Mac) サーバからアップデートする際、セキュリティエージェントにはコンポーネントだけでなくアップデート済みの設定ファイルもダウンロードされます。セキュリティエージェントでは、新しい設定を適用するために設定ファイルが必要です。Web コンソールで Apex One (Mac) の設定を変更するたびに、設定ファイルが変更されます。

セキュリティエージェントをアップデートする前に、Apex One (Mac) サーバに最新のコンポーネントがあるかどうかを確認してください。

Apex One (Mac) サーバを使用できない場合は、トレンドマイクロのアップデートサーバからダウンロードするように、1 つ、複数、またはすべてのセキュリティエージェントを設定します。

詳細については、355 ページの「エージェントのアップデートの設定」を参照してください。

注意

エージェントに IPv6 アドレスのみが割り当てられている場合は、エージェントのアップデートにおける IPv6 の制限事項について、354 ページの「IPv6 シングルスタックエージェントの制限事項」を参照してください。

エージェントのアップデートにおける注意事項と留意事項

- セキュリティエージェントでは、アップデートの実行時にプロキシ設定を使用できます。プロキシ設定は、エージェントコンソールで設定されます。
- アップデートの実行中、エンドポイントのメニューバー上のセキュリティエージェントアイコンによって、製品がアップデートされていることが示されます。セキュリティエージェントプログラムのアップグレードが利用可能な場合、セキュリティエージェントではアップデートが実行されてから、最新プログラムバージョンまたはビルドへのアップグレードが実行されます。アップデートが完了するまで、ユーザはコンソールからいずれのタスクも実行することはできません。
- [概要] 画面にアクセスして、すべてのセキュリティエージェントがアップデートされたかどうかを確認します。

IPv6 シングルスタックエージェントの制限事項

次の表は、セキュリティエージェントに IPv6 アドレスのみが割り当てられている場合の制限事項を示しています。

表 21-5. IPv6 シングルスタックエージェントの制限事項

項目	制限事項
上位サーバ	IPv6 シングルスタックエージェントを IPv4 シングルスタックサーバで管理することはできません。
アップデート	IPv6 シングルスタックエージェントを、次のような IPv4 シングルスタックのアップデート元からアップデートすることはできません。 • トレンドマイクロのアップデートサーバ • IPv4 シングルスタック Apex One (Mac) サーバ
Web レピュテーションクエリ	IPv6 シングルスタックエージェントは、Web レピュテーションクエリを Trend Micro Smart Protection Network に送信できません。
プロキシ接続	IPv6 シングルスタックエージェントは、IPv4 シングルスタックプロキシサーバ経由で接続することはできません。

項目	制限事項
エージェント配信	Apple Remote Desktop は、エージェントを IPv6 シングルスタックエンドポイントに配信できません。こうしたエンドポイントは常にオフラインと表示されるためです。

これらの制限事項のほとんどは、IPv4 アドレスと IPv6 アドレスを変換できる DeleGate などのデュアルスタックプロキシサーバを設定することで克服できます。エージェントと接続先のエンティティとの間にプロキシサーバを配置してください。

エージェントのアップデートの設定

エージェントのアップデートの詳細については、352 ページの「アップデート設定」を参照してください。

手順

1. [Apex One (Mac) サーバに接続できない場合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ダウンロードする] を選択して、エージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロードできるようにします。

   注意

   セキュリティエージェントに IPv6 アドレスのみが割り当てられている場合は、エージェントのアップデートにおける IPv6 の制限事項について、354 ページの「IPv6 シングルスタックエージェントの制限事項」を参照してください。

2. [エージェントにコンポーネントのアップデートを許可するが、エージェントプログラムのアップグレードと HotFix のインストールを禁止する] を選択して、コンポーネントのアップデートは続行し、エージェントはアップグレードしないようにします。
3. 予約アップデートを設定するには、次の手順を実行します。
   a. [予約アップデートを有効にする] を選択します。
   b. スケジュールを設定します。

c. [毎日] または [毎週] を選択する場合は、アップデートの時刻と Apex One (Mac) サーバがセキュリティエージェントにコンポーネントのアップデートを通知する時間を指定します。たとえば、開始時刻が午後 12 時で、時間が 2 時間の場合、サーバはすべてのオンラインのセキュリティエージェントに対して午後 12 時から午後 2 時までランダムに、コンポーネントをアップデートするよう通知します。この設定では、すべてのオンラインのセキュリティエージェントが指定された開始時刻に同時にサーバに接続することを防ぐため、サーバに向かうトラフィックの量が著しく減少します。

Web レピュテーション

Web レピュテーションテクノロジは、Web サイトの経過期間、場所の変更の履歴、および不正プログラムの動作分析により発見される不審な活動の兆候などの要素に基づいてレピュテーションスコアを採点することで、Web ドメインの信頼性を追跡します。これにより継続的にサイトを検索し、感染した Web サイトにユーザがアクセスするのを防ぎます。

セキュリティエージェントは、Smart Protection ソースにクエリを送信して、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、エンドポイントに適用される特定の Web レピュテーションポリシーに関連付けられています。使用しているポリシーに応じて、セキュリティエージェントによって Web サイトへのアクセスがブロックまたは許可されます。

Web レピュテーションの設定

Web レピュテーション設定には、Apex One (Mac) が Web サイトへのアクセスをブロックするか許可するかを指定するポリシーが含まれます。使用するポリシーを決定するために、Apex One (Mac) はセキュリティエージェントの場所をチェックします。セキュリティエージェントが Apex One (Mac) サーバに接続できる場合、セキュリティエージェントの場所は「内部」になります。サーバに接続できない場合、セキュリティエージェントの場所は「外部」です。

手順

1. 外部のセキュリティエージェントのポリシーを設定するには

a. [外部エージェント] タブをクリックします。

b. [Web レピュテーションポリシーを有効にする] を選択します。

ポリシーが有効になると、外部のセキュリティエージェントは Web レピュテーションクエリを Smart Protection Network に送信します。

注意

エージェントに IPv6 アドレスのみが割り当てられている場合は、Web レピュテーションクエリにおける IPv6 の制限事項について、354 ページの「IPv6 シングルスタックエージェントの制限事項」を参照してください。

---

c. 使用可能な Web レピュテーションのセキュリティレベルとして、[高]、[中]、[低] のいずれかを選択します。

注意

Apex One (Mac) は、セキュリティレベルに従って URL へのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを [低] に設定した場合、Apex One (Mac) は Web からの脅威であることが判明している URL のみをブロックします。セキュリティレベルを高くするほど、Web 脅威の検出率は高くなりますが、誤検出の可能性も高くなります。

---

d. Web レピュテーションのフィードバックを送信するには、表示されている URL をクリックします。トレンドマイクロの Web レピュテーションクエリシステムがブラウザウィンドウに表示されます。

2. 内部のセキュリティエージェントのポリシーを設定するには

a. [内部エージェント] タブをクリックします。

b. [Web レピュテーションポリシーを有効にする] を選択します。

ポリシーが有効になると、内部のセキュリティエージェントは Web レピュテーションクエリを以下のいずれかの場所に送信します。

- [Smart Protection Server にクエリを送信する] オプションが有効な場合は、Smart Protection Server。

- [Smart Protection Server にクエリを送信する] オプションが無効な場合は、Trend Micro Smart Protection Network。

注意

エージェントに IPv6 アドレスのみが割り当てられている場合は、Web レピュテーションクエリにおける IPv6 の制限事項について、354 ページの「IPv6 シングルスタックエージェントの制限事項」を参照してください。

c. 内部のセキュリティエージェントから Web レピュテーションクエリを Smart Protection Server に送信するには、[Smart Protection Server にクエリを送信する] を選択します。

- このオプションを有効にすると、セキュリティエージェントは Apex One セキュリティエージェントによって使用されている Smart Protection ソースリストを参照して、クエリの送信先となる Smart Protection Server を決定します。
- このオプションが無効な場合、セキュリティエージェントは Web レピュテーションクエリを Smart Protection Network に送信します。エンドポイントからクエリを送信するためにはインターネット接続が必要です。

d. 使用可能な Web レピュテーションのセキュリティレベルとして、[高]、[中]、[低] のいずれかを選択します。

注意

Apex One (Mac) は、セキュリティレベルに従って URL へのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを [低] に設定した場合、Apex One (Mac) は Web からの脅威であることが判明している URL のみをブロックします。セキュリティレベルを高くするほど、Web 脅威の検出率は高くなりますが、誤検出の可能性も高くなります。

セキュリティエージェントは、セキュリティレベルに関係なく、未評価の Web サイトをブロックしません。

e. Web レピュテーションのフィードバックを送信するには、表示されている URL をクリックします。トレンドマイクロの Web レピュテーションクエリシステムがブラウザウィンドウに表示されます。

f. セキュリティエージェントに、Web レピュテーションログのサーバへの送信を許可するかどうかを選択します。Apex One (Mac) によってブロックされた URL を解析し、アクセスしても安全だと考えられる URL に対して適切な処理を実行する場合には、セキュリティエージェントからのログの送信を許可します。

承認済み URL リストと URL ブロックリストの設定

安全と考える Web サイトを承認済みリストに、管理者が危険と判断する Web サイトをブロックリストに追加します。Apex One (Mac) でこれらの Web サイトのいずれかへのアクセスが検出されると、アクセスは自動的に許可またはブロックされ、Smart Protection ソースにクエリは送信されなくなります。

手順

1. Apex One (Mac) Web コンソールにアクセスします。
2. [エージェント] > [グローバルエージェント設定] > [Web レピュテーションの承認済み URL リスト/URL ブロックリスト] に移動します。
3. テキストボックスに URL を指定します。ワイルドカード文字 (*) は URL の任意の位置に追加できます。

   例:

   - `www.trendmicro.com/*`は、www.trendmicro.com ドメインにあるすべてのページを指定します。
   - `*.trendmicro.com/*`は、trendmicro.com のいずれかのサブドメインのすべてのページを指定します。

   IP アドレスを含む URL を入力できます。URL に IPv6 アドレスが含まれる場合は、アドレスを角括弧で囲みます。
4. [承認済みリストに追加] または [ブロックリストに追加] をクリックします。
5. エントリを削除するには、[表示] ドロップダウンリストからオプションを選択し、URL の横のアイコンをクリックします。

6. [配信] をクリックします。

パート VIII

Deep Discovery のウィジェットとポリシー

第 22 章

Deep Discovery Analyzer および Email Inspector ダッシュボードウィジェット

本章では、Apex Central でサポートされる Deep Discovery Analyzer および Deep Discovery Email Inspector ダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

Deep Discovery Analyzer ウィジェット

このセクションでは、Apex Central でサポートされるすべての Deep Discovery Analyzer ウィジェットのヘルプトピックについて説明します。

仮想アナライザの概要ウィジェット

このウィジェットには、仮想アナライザに送信されたサンプルの総数と、そのうちリスクのあるサンプルの数が表示されます。1 つ以上の Deep Discovery Analyzer アプライアンスから取得されたデータが表示される場合もあります。ウィジェットには、データが表形式と円グラフで表示されます。

ラベル	説明
送信数	仮想アナライザに送信されたサンプルの総数が表示されます。
確認されたリスク数	送信されたサンプルのうちリスクが確認されたサンプルの総数が表示されます。
リスク高	送信されたサンプルのうち、リスク高のサンプルの総数が表示されます。
リスク中	送信されたサンプルのうち、リスク中のサンプルの総数が表示されます。
リスク低	送信されたサンプルのうち、リスク低のサンプルの総数が表示されます。
リスクのあるイベントの割合(%)	送信されたサンプルのうち、リスクが確認されたサンプルの割合が表示されます。
不正イベントの分布	円グラフに、リスク高、リスク中、リスク低のサンプルの割合が表示されます。

期間を変更するには、ウィジェット左上の [範囲] ドロップダウンリストからオプションを選択します。

登録されているすべての Deep Discovery Analyzer アプライアンスからのデータを表示するのか、特定のアプライアンスのデータを表示するのかを切り替えるには、ウィジェット左上の [表示] ドロップダウンリストからオプションを選択します。

アプライアンスを選択したら、送信サンプルの総数、リスク高/中/低のサンプル数、円グラフの一部をクリックして、詳細を確認できます。

Deep Discovery Email Inspector ウィジェット

このセクションでは、Apex Central でサポートされるすべての Deep Discovery Email Inspector ウィジェットのヘルプトピックについて説明します。

高度な脅威を含むメールメッセージウィジェット

高度な脅威を含むメールメッセージウィジェットには、Deep Discovery Email Inspector によって検出される、特性に不正または疑わしい点が見られるすべてのメールメッセージが表示されます。疑わしい特性には、変則的な動作、誤データや偽データ、不審または不正な動作パターン、追加調査が必要なシステム侵入を疑わせる文字列などが含まれます。

このグラフは選択した期間に基づいて作成されています。Y 軸はメールメッセージ件数を示しています。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、高リスクメッセージの件数と期間が表示されます。

凡例の項目をクリックすると、そのメトリックに関連するデータが表示または非表示になります。

[検出されたメッセージの表示] をクリックすると、すべて検出が表示されます。

高度な脅威のメール受信者の上位ウィジェット

高度な脅威のメール受信者の上位ウィジェットには、Deep Discovery Email Inspector で不審メッセージを受信した数が上位の受信者が表示されます。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

第 23 章

Deep Discovery Inspector の統合とポリシー設定

本章では、Apex Central と Deep Discovery Inspector を統合し、Apex Central のコンソールでポリシーを管理する方法について説明します。

次のトピックがあります。

Deep Discovery Inspector の統合の概要

このトピックでは、Apex Central と Deep Discovery Inspector のサポートされるバージョン間の統合範囲について説明します。

統合機能	5.0
登録	Deep Discovery Inspector 管理コンソール (MCP エージェント経由) から
シングルサインオン	サポート対象
ライセンス管理	なし
コマンド追跡	サポート対象
Apex Central から配信されるコンポーネント	すべてのコンポーネント
Apex Central から管理および配信されるポリシー	• 375 ページの「拒否リスト/許可リスト」 • 376 ページの「監視対象ネットワークグループを追加する」 • 378 ページの「登録済みサービスを追加する」 • 379 ページの「仮想アナライザを設定する」
ユーザ/エンドポイントディレクトリに表示される情報	なし
ログクエリ	ログクエリを実行して製品情報およびログを表示するときに、次のデータビューのいずれかを選択します。 • 製品のステータス情報 • Deep Discovery 情報
製品に固有のダッシュボードウィジェット	• 372 ページの「Deep Discovery Inspector システムのステータスウィジェット」 • 370 ページの「Deep Discovery Inspector によって影響が検出されたホストウィジェット」

統合機能	5.0
他の管理下の製品と共有されているダッシュボードウィジェット	なし
静的レポートテンプレート	Trend Micro Deep Discovery Inspector レポート
カスタムレポートテンプレート (事前定義済み)	• TM-Deep Discovery Inspector ホストへの影響の重大度概要 • TM-Deep Discovery Inspector 脅威の兆候の検出概要
イベント通知	高度な脅威アクティビティ • C&C コールバックアラート • C&C コールバックアウトブレイクアラート • 仮想アナライザによるリスク高の検出 • リスク高ホストの検出 • 既知の標的型攻撃の挙動の兆候 • 文書内の潜在的な攻撃コードの検出 • ルートキットまたはハッキングツールの検出 • SHA-1 拒否リストの検出 • ワームまたはファイル感染型ウイルスの拡散の検出 • 相関関係のあるイベントの検出
情報漏えい対策 (DLP) インシデントの管理	該当なし
不審オブジェクトと IOC ファイルの管理	• 不審オブジェクトを Apex Central に送信します。 • 不審オブジェクトを Apex Central と同期します。

Deep Discovery Inspector によって影響が検出されたホストウィジェット

このウィジェットには、影響を受けたホストで確認された Deep Discovery Inspector の検出に関する情報が表示されます。

初期設定では、[検出数] によって上位 10 の重大度の高いホストのみが表示されます。

ウィジェットでホストを検出数で表示するか、検出日時で表示するかを切り替えるには、設定アイコン (>) をクリックし、次のいずれかを選択します。

- 検出数: ドロップダウンから、ホストの数を選択します (上位 10、25、50 件)
- 検出日時: ドロップダウンから、ホストの数を選択します (最新の 10、25、50、100 件)。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

- [検出数] でホストを表示する場合は、今日、1 週間、2 週間、または 1 か月のデータを表示できます。
- [検出日時] でホストを表示する場合は、今日または 1 週間のデータのみを表示できます。

[検出日時] でホストを表示している場合は、[重大度] ドロップダウンを使用して重大度レベルを指定することもできます。

列	説明
IP アドレス	影響を受けたホストの IP アドレスが表示されます。
ホスト名	影響を受けたホストの名前が表示されます。
ネットワークグループ	監視対象ネットワークのグループ名を表示し、攻撃がネットワークの内部、外部のどちらから来たのかを判断します。

列	説明
検出数	影響を受けたホスト上で確認されたイベント数が表示されます。 • [検出数] 列の数をクリックすると、[検出数] 画面で追加情報を表示できます。 • [詳細] 列の [表示] リンクをクリックすると、シングルサインオンを使用して Deep Discovery Inspector にログオンし、[検出ログクエリの詳細] 画面を表示できます。 ログが削除されている場合は、その旨を知らせるメッセージが表示されます。
最新の検出	Deep Discovery Inspector でリスクの兆候または既知のリスクを最後に検出した日時が表示されます。

Deep Discovery Inspector によって影響が検出されたホストの検出数

Deep Discovery Inspector によって影響が検出されたホストウィジェットの [検出数] 列の値をクリックすると、ホストに関連する情報を含む表が表示されます。

表 23-1. ホストに関連する情報

列名	情報
日付	Deep Discovery Inspector が検出ログを生成した日付と時刻が表示されます。
重大度	重大度評価が表示されます。 • 高: 不正であるか危険性の高い接続に関連することが判明済み • 中: レピュテーションサービスに通知されていない IP アドレス/ドメイン/URL • 低: レピュテーションサービスが過去の侵入またはスパムメールとの関連を示唆 • 情報: ほとんどの場合、安全なオブジェクト
検出	ルールの説明または不正プログラムの名前が表示されます。

列名	情報
脅威の種類	次のいずれかが表示されます。 • ファイルパターン • 不正な挙動 • 不審挙動 • 攻撃コード • グレーウェア • Web レピュテーション • 悪影響を及ぼすアプリケーション
送信元 IP	不審オブジェクトの送信元の IP アドレスが表示されます。
送信先 IP	不審オブジェクトが目的とする送信先の IP アドレスが表示されます。
プロトコル	不審オブジェクトが送信元から送信先に転送される際に使用されたプロトコルが表示されます。
ファイル名	サンプルから抽出されたファイル名が表示されます。
ログ元	サンプルを分析した Deep Discovery Inspector のホスト名が表示されます。
詳細	[表示] をクリックすると、別のウィンドウが開き、Deep Discovery Inspector の不審オブジェクトに関連する詳細な分析が表示されます。

Deep Discovery Inspector システムのステータスウィジェット

このウィジェットは、選択した Deep Discovery Inspector アプライアンスに関して、リソース使用率および仮想アナライザの処理待ちのサンプル数を表示するために使用します。

初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品/サーバのデータがウィジェットに表示されます。

設定アイコン (>) をクリックして、次の内容を設定します。

- タイトル: 新しく指定する、ウィジェットのわかりやすいタイトルを入力します。

- 範囲: すべての製品 :表示するデータの収集元となる製品を指定するには、[>>] をクリックします。

ウィジェットに表示される次のシステムリソースデータで、Deep Discovery Inspector のすべてのリソースが仕様通りに動作していることを確認します。

列	説明
サーバ名	Deep Discovery Inspector アプライアンスごと。 • 詳細なステータスを表示: このオプションをクリックして製品ステータスの詳細を表示します。[詳細なステータスを表示] のデータは、[製品ステータス] ログクエリでも表示できます。 この表には、CPU 使用率の割合、メモリおよびディスクの割合および実際の使用率、および仮想アナライザの処理待ちのサンプル数が表示されます。トラブルシューティングに役立つように、[製品のホスト名]、[製品の IP アドレス]、[接続ステータス]、[製品バージョン] の各フィールドを参照してください。Deep Discovery Inspector は Apex Central に対して、5 分ごとにシステムステータスのアップデートを送信します。 が表示されている場合、Apex Central は、Deep Discovery Inspector システムのステータスの最新ログを受信していません。Deep Discovery Inspector が有効で接続されていることを確認してください。 • ログオンコンソール: このオプションをクリックして Deep Discovery Inspector 管理コンソールにアクセスします。ログオン情報は必要ありません。
CPU 使用率	サーバによって使用されている CPU の割合。 • は、サーバの CPU 平均が 80%を超えたときに表示されます。 **注意** CPU 使用率、メモリとディスクの使用量、および処理待ちサンプル数の制限は設定できません。アラートが解決しない場合は、Deep Discovery Inspector/仮想アナライザアプライアンスのアップグレードを検討してください。

列	説明
メモリ使用量	サーバ上で使用可能なメモリの割合。 • は、メモリ使用量が 80%を超えたときに表示されます。 注意 CPU 使用率、メモリとディスクの使用量、および処理待ちサンプル数の制限は設定できません。アラートが解決しない場合は、Deep Discovery Inspector/仮想アナライザアプライアンスのアップグレードを検討してください。
ディスク使用量	サーバ上で使用可能なディスク容量の割合。 • は、ディスク使用量が 80%を超えたときに表示されます。 注意 CPU 使用率、メモリとディスクの使用量、および処理待ちサンプル数の制限は設定できません。アラートが解決しない場合は、Deep Discovery Inspector/仮想アナライザアプライアンスのアップグレードを検討してください。
処理待ちのサンプル	仮想アナライザの処理待ちのサンプル数。 • は、仮想アナライザの処理待ちのサンプル数が 40 個を超えたときに表示されます。 注意 CPU 使用率、メモリとディスクの使用量、および処理待ちサンプル数の制限は設定できません。アラートが解決しない場合は、Deep Discovery Inspector/仮想アナライザアプライアンスのアップグレードを検討してください。

Deep Discovery Inspector ポリシーの設定

このセクションでは、[ポリシーの作成] 画面での Deep Discovery Inspector ポリシーの設定方法について説明します。

拒否リスト/許可リスト

[拒否リスト/許可リスト] 画面は、[拒否リスト]、[許可リスト]、[インポート/エクスポート] のタブに分かれています。

表 23-2. [拒否リスト/許可リスト] のタブ

タブ	説明
拒否リスト	Deep Discovery Inspector は、拒否リスト内のエントリへの接続の監視、または監視とリセットを行います。
許可リスト	Deep Discovery Inspector は、許可リスト内のエントリへの接続を許可します。 ヒント 許可リストを使用して、拒否リストによる誤検知の数を減少させます。
インポート/エクスポート	拒否リストまたは許可リストのエントリをインポートまたはエクスポートします。

カスタム拒否リストを作成する

手順

1. [拒否リスト] タブを選択します。
2. [拒否リスト] にエンティティを追加するには、[追加] を選択します。

   [拒否リストへの項目の追加] 画面が表示されます。
3. [拒否リストへの項目の追加] 画面で、情報を確認し、コメントがあれば追加して、[保存] をクリックします。

カスタム許可リストを作成する

手順

1. [許可リスト] タブを選択します。
2. [許可リスト] にエンティティを追加するには、[追加] を選択します。

   [許可リストへの項目の追加] 画面が表示されます。
3. [許可リストへの項目の追加] 画面で、情報を確認し、コメントがあれば追加して、[保存] をクリックします。

カスタム拒否リストまたは許可リストをインポート/エクスポートする

手順

1. [インポート/エクスポート] タブを選択します。
2. 現在の拒否リストまたは許可リストをエクスポートするには、リストを選択して [エクスポート] をクリックします。
3. 現在の拒否リストまたは許可リストを上書きするには、リストを選択して保存場所を参照し、[インポート] をクリックします。

   現在選択されているリストは上書きされます。

監視対象ネットワークグループを追加する

IP アドレスを使用して、監視対象となるネットワークのグループを作成し、攻撃がネットワークの内部、外部のどちらから来たのかを Deep Discovery Inspector が判断できるようにします。

手順

1. [追加] をクリックします。
2. グループ名を指定します。

ヒント

IP アドレスが属するネットワークを簡単に見分けられるように、グループにはわかりやすい名前を付けます。たとえば、「Finance network」、「IT network」、「Administration」などを使用します。

3. テキストボックスに IP アドレスの範囲 (最高 1,000 個の IP アドレス範囲) を指定します。

   Deep Discovery Inspector には、最初から Default という管理対象ネットワークが設定されています。このネットワークには、プライベートネットワークについて、Internet Assigned Numbers Authority (IANA) により予約されている次の IP アドレスブロックが含まれます。

   - 10.0.0.0 - 10.255.255.255
   - 172.16.0.0 - 172.31.255.255
   - 192.168.0.0 - 192.168.255.255

注意

- Default を削除しなかった場合、新たに監視対象となるネットワークを追加するときに、これらの IP アドレスを指定する必要はありません。
- IP アドレスの範囲を指定するには、ダッシュを使用します。

  例: 192.168.1.0-192.168.1.255.
- IP アドレスのサブネットマスクを指定するには、スラッシュを使用します。

  例:192.168.1.0/255.255.255.0 または 192.168.1.0/24
- サブグループのレイヤは 3 つまで追加できます。

4. ネットワークグループのネットワークゾーンを選択します。
   - 信頼する ―これはセキュリティで保護されたネットワークです
   - 信頼しない ―ネットワークのセキュリティには多少の疑いがあります。

5. [追加] をクリックします。
6. [完了] をクリックします。

登録済みサービスを追加する

社内使用を目的とするサービス、または信頼できると見なされたサービスに対応する各種サーバを追加して、ネットワークプロファイルを作成します。ネットワーク内の信頼されたサービスを指定することで、許可されていないアプリケーションやサービスの検出が可能になります。

ネットワークプロファイルの精度を確保するため、信頼できるサービスのみを追加してください。サービスは 1,000 個まで追加できます。

手順

1. ドロップダウンリストからサービスを選択します。

表 23-3. サービスの種類

サービス	説明
DNS	DNS サーバとして使用されるネットワークサーバ
FTP	FTP サーバとして使用されるネットワークサーバ
HTTP プロキシ	HTTP プロキシサーバとして使用されるネットワークサーバ
SMTP	SMTP サーバとして使用されるネットワークサーバ
SMTP オープンリレー	SMTP オープンリレーサーバとして使用されるネットワークサーバ
ソフトウェアアップデートサーバ	Windows Server Update Services (WSUS) を実行するネットワークサーバ、またはリモート配信を行うサーバ
セキュリティ監査サーバ	脆弱性と安全ではない構成の両方を検出するために使用されるネットワークサーバ

サービス	説明
Active Directory	Active Directory サーバとして使用されるネットワークサーバ
ドメインコントローラ	ドメインコントローラサーバとして使用されるネットワークサーバ
データベースサーバ	データベースサーバとして使用されるネットワークサーバ
認証サーバ - Kerberos	Kerberos 認証の提供に使用されるネットワークサーバ
ファイルサーバ	共有ファイルアクセスの場所の提供に使用されるネットワークサーバ
Web サーバ	Web サーバとして使用されるネットワークサーバ
コンテンツ管理サーバ	コンテンツの管理に使用されるネットワークサーバ
Radius サーバ	Radius 認証サーバとして使用されるネットワークサーバ

登録サービス名は、[定義された登録済みサービス] セクションに表示されます。

2. サーバ名を指定します。
3. IP アドレスを指定します。
4. [追加] をクリックします。

仮想アナライザを設定する

脅威ファイルの分析を有効または無効にするには、このオプションを使用します。

手順

1. 管理ポートがインターネットにアクセスできることを確認してください。データの照会に、仮想アナライザがこのポートを使用することがあります。
2. 仮想アナライザの設定ウィンドウで [仮想アナライザへのファイル送信] をオンにします。
3. 分析モジュールを選択します。
   - [内部アナライザ] で、ネットワークの種類を選択します。

     表 23-4. アナライザネットワークの種類

モジュールオプション	説明
管理ネットワーク	管理ポートを通じて、仮想アナライザトラフィックを管理するには、このネットワークの種類を選択します。
カスタムネットワーク/専用ネットワーク	仮想アナライザトラフィック専用ポートを設定するには、このネットワークの種類を選択します。ポートが外部ネットワークに直接接続できることを確認してください。
ネットワークなし/独立したネットワーク	環境が外部ネットワークに接続されていないときに、仮想アナライザ内で仮想アナライザトラフィックを分離するには、このネットワークの種類を選択します。

表 23-5. カスタムネットワーク/専用ネットワークオプション

オプション	処理
仮想アナライザポート	仮想アナライザポートを選択します。 **注意** Deep Discovery Inspector のデータポートとは異なる仮想アナライザポートを割り当てます。
IPv4 の設定	[自動 (DHCP を使用)] が選択されています。この設定は変更できません。

- [外部アナライザ] には、仮想アナライザの IP アドレスと API キーを指定します。

ヒント

外部アナライザ (Deep Discovery Inspector Advisor または Deep Discovery Analyzer) には、内部アナライザ (仮想アナライザ) よりも高いパフォーマンスが期待されます。

4. (オプション) 内部の仮想アナライザの場合、専用のプロキシを有効にして設定します。

注意

プロキシを設定するには、ネットワークの種類として管理ネットワークまたはカスタムネットワークを選択する必要があります。

a. [プロキシ設定] で、[専用のプロキシ設定を使用する] を選択します。

b. [サーバアドレス] に、プロキシサーバの IP アドレス、ホスト名、または FQDN を入力します。

c. ポート番号を入力します。

d. (オプション) プロキシサーバの認証情報を入力します。

5. (オプション) 内部仮想アナライザの場合は、[Mac OS の脅威の可能性があるファイルを、分析用にトレンドマイクロのクラウドサンドボックスに送信します。] を選択します。
6. [ファイル送信] オプションを設定します。
   a. 最大ファイルサイズを指定します。この設定を変更すると、Deep Discovery Inspector のパフォーマンスが影響を受ける可能性があります。
   b. ソフトウェア安全性評価サービス (CSSS) を有効にします。

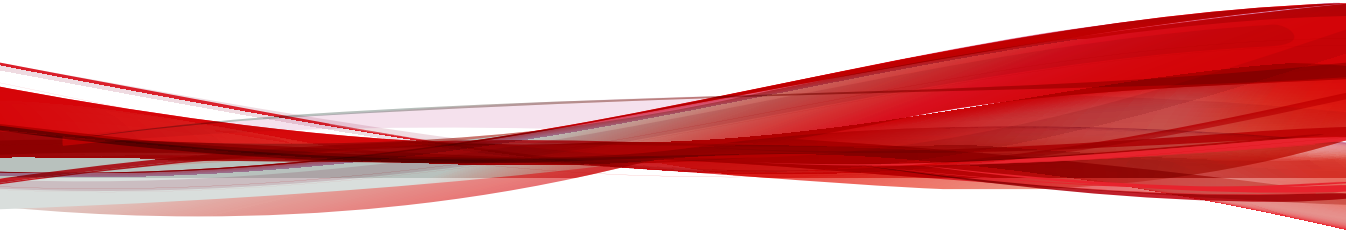
   

   注意

   ソフトウェア安全性評価サービス (CSSS) は、安全なファイルを登録したトレンドマイクロのクラウドデータベースです。Deep Discovery Inspector は、トレンドマイクロのデータセンターにクエリを送信してチェックします。

パート IX

Deep Security Manager



第 24 章

Deep Security Manager ダッシュボードウィジェット

本章では、Apex Central でサポートされるの Deep Security Manager ダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

Deep Security 不正プログラム対策イベント履歴ウィジェット

このウィジェットには、指定された時間範囲内に発生した不正プログラム対策イベントの件数が表示されます。

バーをクリックすると、Deep Security Manager の [イベント] ページが表示され、指定されたイベントの種類および期間について不正プログラム対策イベントがフィルタされて表示されます。凡例のイベントの種類をクリックして、グラフ表示を変更することもできます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

Deep Security 不正プログラム対策のステータス (不正プログラム) ウィジェット

このウィジェットには、エンドポイントで検出された不正プログラムの脅威うち最も一般的な 5 つが表示されます。

Deep Security Manager コンソールで追加の詳細を表示するには、[合計] 列の数をクリックします。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

Deep Security のウィジェットで選択可能な Deep Security インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Deep Security サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

データ	説明
不正プログラム名	不正プログラムの脅威の名前
駆除できなかった数	Deep Security で駆除できなかった脅威の出現件数
合計	時間範囲内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の時間範囲におけるイベント数
傾向	前回の期間から今回の期間への割合の変化

Deep Security アプリケーションの種類別のアクティビティ (検出) ウィジェット

このウィジェットには、IPS (検出) イベントに関連付けられている上位 5 つのアプリケーションの種類が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示され、特定のアプリケーションの種類に関連付けられている IPS (検出) イベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

データ	説明
アプリケーションの種類名	アプリケーションの種類の名前
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security アプリケーションの種類別のアクティビティ (防御) ウィジェット

このウィジェットには、IPS (防御) イベントに関連付けられている上位 5 つのアプリケーションの種類が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示され、特定のアプリケーションの種類に関連付けられている IPS (防御) イベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

データ	説明
アプリケーションの種類名	アプリケーションの種類の名前
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security コンポーネントの概要ウィジェット

このウィジェットには、使用可能な Deep Security コンポーネントのアップデートのバージョン番号と、最新バージョンにアップデート済みのエンドポイントの割合が表示されます。

重要

このウィジェットには、Deep Security 7.5 以降のデータのみが表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
コンポーネント	Deep Security コンポーネントの名前
現在のバージョン	Deep Security Manager で現在使用可能なバージョン
アップデート済みの割合	最新バージョンにアップデートされている管理対象コンピュータの割合 **注意** すべての管理対象コンピュータにアップデートを適用できるわけではありません。

ウィジェットには、次のコンポーネントのバージョン番号が表示されます。

コンポーネント	説明
スマートスキャンエージェントパターンファイル	Deep Security Virtual Appliance に送信される、サイズの小さい不正プログラムパターン検出ファイル。これらのパターンとの比較によってコンピュータ上の疑わしいファイルが検出されると、そのファイルは確認のため、スマートスキャンサーバ上のより厳密なパターンファイルと比較されます。
パターンファイル	ウイルスシグネチャを識別するために Deep Security Virtual Appliance で使用されるファイル。ウイルスシグネチャとは、ウイルスの存在を示すビットとバイトの一意のパターンのことです。
IntelliTrap パターンファイル	IntelliTrap は、パッカーなどの他の不正プログラムの特性と組み合わせて、リアルタイム圧縮を使用するファイルに隠れている可能性のある不正プログラムを検索します。
スパイウェア監視パターンファイル	スパイウェアの検出パターンファイル
ウイルス検索エンジン	ウイルス検索の実行時にウイルスパターンをファイルに適用するエンジン

コンポーネント	説明
Deep Security ルールアップデート	DPI ルールは、既知および未知の攻撃から脆弱性を保護することで、侵入検知および侵入防御 (IDS/IPS) の保護機能を提供します。

Deep Security 機能の概要ウィジェット

このウィジェットは、Deep Security モジュールそれぞれの最新アクティビティを表示します。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

このウィジェットには、複数の管理下のサーバから集計された情報が表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

ヒント

複数の管理下のサーバから集計されていないデータを表示するには、各管理下のサーバごとに新しいウィジェットを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
モジュール	Deep Security モジュール
保護されているコンピュータ	このモジュールで現在保護されている管理対象コンピュータの数とそのすべての管理対象コンピュータの割合
イベント数	指定された期間にモジュールによって生成されたイベント数
傾向	前回の期間からのイベント数の変化率

データ	説明
コンピュータの総数	Deep Security によって管理されるコンピュータの総数

Deep Security ファイアウォールのアクティビティ (検出) ウィジェット

このウィジェットには、検出モードで動作中に、イベントを実行した件数が最も多かったファイアウォールルールの上位 5 個が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示されますが、特定のルールによって実行されたファイアウォールイベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
理由	ルールの名前
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security ファイアウォールのアクティビティ (防御) ウィジェット

このウィジェットには、防御モードで動作中に、イベントを実行した件数が最も多かったファイアウォールルールの上位 5 個が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示されますが、特定のルールによって実行されたファイアウォールイベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
理由	ルールの名前
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security ファイアウォールイベント履歴ウィジェット

このウィジェットには、指定された時間範囲内に Deep Security Manager によって検出されたファイアウォールイベントの件数が表示されます。グラフには、検出モードと防御モードの両方のファイアウォールルールによって実行されたイベントが表示されます。

Deep Security Manager コンソールで追加の詳細を表示するには、バーをクリックします。凡例のイベントの種類をクリックして、グラフ表示を変更することもできます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

Deep Security のウィジェットで選択可能な Deep Security インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Deep Security サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

Deep Security 変更監視のアクティビティウィジェット

このウィジェットには、イベントを実行した件数が最も多かった変更監視ルールの上位 5 個が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示され、特定のルールによって実行された変更監視イベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
理由	ルールの名前

データ	説明
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security 変更監視イベント履歴ウィジェット

このウィジェットには、指定された期間に変更監視検索によって記録されたイベントの重大度レベルが表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

Deep Security IPS イベント履歴ウィジェット

このウィジェットには、指定された時間範囲内に Deep Security によって検出された IPS イベントの件数が表示されます。グラフには、検出モードと防御モードの両方の IPS ルールによって実行されたイベントが表示されます。

バーをクリックすると、Deep Security Manager の [イベント] ページが表示され、指定されたモードおよび時間範囲内の IPS イベントがフィルタされて表示されます。また、凡例のモード ([検出] または [防御]) をクリックして、グラフ表示を変更することもできます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意
ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント
このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

Deep Security IPS のアクティビティ (検出) ウィジェット

このウィジェットには、検出モードで動作中に、イベントを実行した件数が最も多かった IPS ルールの上位 5 個が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示され、特定のルールによって実行された IPS (検出) イベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意
ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
理由	ルールの名前
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security IPS のアクティビティ (防御) ウィジェット

このウィジェットには、防御モードで動作中に、イベントを実行した件数が最も多かった IPS ルールの上位 5 件が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示され、特定のルールによって実行された IPS (防御) イベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
理由	ルールの名前
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security セキュリティログ監視のアクティビティウィジェット

このウィジェットには、イベントを実行した件数が最も多かったセキュリティログ監視ルールの上位 5 件が表示されます。

[合計] 列の値をクリックすると、Deep Security Manager の [イベント] 画面が表示され、特定のルールによって実行されたログ監視イベントがフィルタされて表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
理由	ルールの名前
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への変化率

Deep Security セキュリティログ監視イベントの履歴ウィジェット

このウィジェットは、指定された時間範囲内にセキュリティログ監視ルールによって実行されたイベントの件数を表示します。

バー ([検出] または [防御]) をクリックすると、Deep Security Manager の [イベント] ページが表示され、指定されたイベントの種類および期間についてセキュリティログ監視イベントがフィルタされて表示されます。凡例のイベントの種類をクリックして、グラフ表示を変更することもできます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

Deep Security 攻撃の予兆検索イベント履歴ウィジェット

このウィジェットは、指定された時間範囲内に、攻撃の予兆の検出の設定によって実行されたイベントの件数を表示します。

バーをクリックすると、Deep Security Manager の [イベント] ページが表示され、指定されたイベントの種類および期間について攻撃の予兆の検出イベントがフィルタされて表示されます。凡例のイベントの種類をクリックして、グラフ表示を変更することもできます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

ヒント

このウィジェットには、単一の Deep Security サーバのデータのみが表示されます。複数の Deep Security サーバを監視するには、サーバごとに新しいウィジェットを作成します。

Deep Security ステータスの概要ウィジェット

このウィジェットには、重大なアラートと警告アラートの件数、およびネットワーク全体のエンドポイントのステータスが表示されます。

このウィジェットには、複数の管理下のサーバから集計された情報が表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

ヒント

複数の管理下のサーバから集計されていないデータを表示するには、各管理下のサーバごとに新しいウィジェットを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

表 24-1. アラート

データ	説明
重大なアラート	重大なアラートの件数 注意 アラートの重大または警告の分類は、Deep Security Manager の管理コンソールでユーザが設定できます。

データ	説明
警告アラート	警告アラートの件数 注意 アラートの重大または警告の分類は、Deep Security Manager の管理コンソールでユーザが設定できます。

表 24-2. コンピュータステータス

データ	説明
管理 (緑)	保護されており、エラーや警告はありません。
未管理 (青)	保護されていません。
ロック (灰色)	ロックされています。コンピュータがロック状態の間、Deep Security Manager は Agent/Appliance とは通信せず、コンピュータ関連のアラートは発令されません。
重大 (赤)	エラー状態です。
警告 (黄)	警告状態です。

Deep Security Web レピュテーションイベント履歴ウィジェット

このウィジェットには、指定された時間範囲内に Web レピュテーションサービスによって実行されたイベントの件数が表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
警告	URL が、不正、または脅威の既知の発信源であると確認されました。
非常に不審	URL が、不正、または脅威の発信源となる可能性があります。
兆候	URL が、スパムメールに関連付けられているか、感染している可能性があります。
ブロック	URL が管理者によってブロックされました。
未評価	URL は、まだトレンドマイクロによってテストされていません。 トレンドマイクロは積極的に Web ページの安全性をテストしていますが、ユーザが新しい Web サイトやあまり一般的でない Web サイトにアクセスすると、まだテストされていないページに遭遇することがあります。

Deep Security Web レピュテーションの URL のアクティビティウィジェット

このウィジェットには、イベントを実行した件数が最も多かった Web レピュテーションサービス URL の上位 5 件が表示されます。

設定アイコン (>) をクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。表示された画面で、管理下のサーバをソースとして使用するよう選択し、[保存] をクリックします。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

データ	説明
URL	URL
合計	期間内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の期間におけるイベント数
傾向	前回の期間から今回の期間への割合の変化

パート x

Endpoint Application Control のウィジェットとポリシー

第 25 章

エンドポイントアプリケーションコントロールダッシュボードウィジェット

本章では、Apex Central でサポートされるすべてのエンドポイントアプリケーションコントロールのダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

Endpoint Application Control キーパフォーマンスインジケータウィジェット

このウィジェットには、選択した条件に基づいて Endpoint Application Control キーパフォーマンスインジケータが表示されます。カスタマイズ可能なテンプレートを使用して、はじめて検出されたアプリケーション、ソフトウェア安全性評価リストにないアプリケーション、停止されたエージェントの平均、接続していないエンドポイントの平均、ブロックルールとロックダウンルールを表示できます。

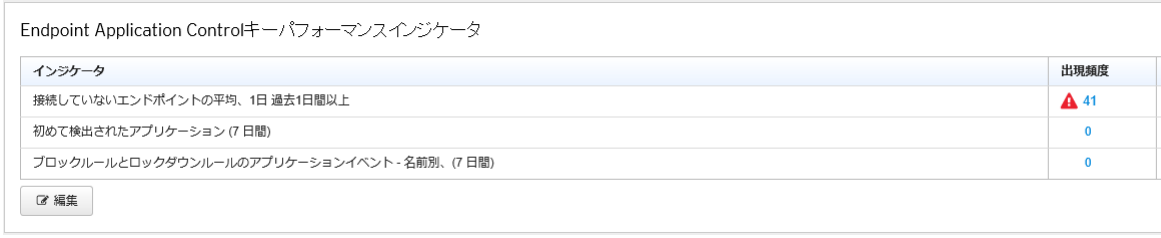


図 25-1. KPI ウィジェットの例

初期設定では、このウィジェットは 5 回発生したイベントを「重要」( )、10 回発生したイベントを「重大」( ) としてマークします。オプションで、イベントを「重要」または「重大」とマークするためにイベントのしきい値をカスタマイズできます。

「**インジケータタスクの追加または編集**」の表を参照してください。

[ダッシュボード] に移動して、ウィジェットの右上のメニューから [ウィジェット設定] を選択し、次のタスクを実行します。

表 25-1. KPI ウィジェット設定タスク

タスク	手順
ウィジェットが使用するインジケータの傾向計算を編集する	このウィジェットは、[変更] 列に傾向を表示します。インジケータの傾向は、現在の期間と以前の期間の平均値を比較して計算されます。 [傾向計算] の下に、平均値を算出する以前の期間数を入力します。 初期設定値は 1 です。

[ダッシュボード] に移動してこのウィジェットを検索し、[編集] をクリックしてインジケータに関連する次のタスクを実行します。タスクが完了したら、[完了] をクリックします。

表 25-2. KPI ウィジェットインジケータタスク

タスク	手順
新規インジケータを追加する	1. [インジケータの追加] をクリックします。 [インジケータの追加] 画面が表示されます。 2. テンプレートを選択して、必要に応じて設定をカスタマイズし、[保存] をクリックします。 「インジケータタスクの追加または編集」の表を参照してください。
インジケータを編集する	1. リスト内のインジケータをクリックします。 [インジケータの編集] 画面が表示されます。 2. 設定をカスタマイズし、[保存] をクリックします。 「インジケータタスクの追加または編集」の表を参照してください。
インジケータを削除する	インジケータの左の  をクリックし、[削除] をクリックします。

表 25-3. インジケータタスクの追加または編集

タスク	手順
インジケータに名前を付ける	[タイトル] で、名前を入力します。 ヒント このフィールドを空白のままにした場合は、初期設定の名前が設定されます。
テンプレートを選択する	[テンプレート] で、テンプレートを選択します。 テンプレートについての情報を参照してください。
期間を編集する	[期間] で、インジケータのデータの期間を選択します。
しきい値アイコンを表示する	[しきい値を有効にする] を選択します。
しきい値アイコンを非表示にする	[しきい値を有効にする] をクリアします。
「重要」( ) のしきい値を設定する	[イベントを [重要] としてマーク] の下に、イベントの最小発生回数を入力します。 次の内容が当てはまる場合、[出現頻度] 列にこのアイコンが表示されます。 • このインジケータと一致するイベントの発生回数はしきい値以上である。 • [しきい値を有効にする] が選択されている。
「重大」( ) のしきい値を設定する	[イベントを [重大] としてマーク] の下に、イベントの最小発生回数を入力します。 次の内容が当てはまる場合、[出現頻度] 列にこのアイコンが表示されます。 • このインジケータと一致するイベントの発生回数はしきい値以上である。 • [しきい値を有効にする] が選択されている。

このウィジェットには、次のインジケータのカスタマイズ可能なテンプレートが含まれています。

「テンプレート」	「ログの種類」	「集約単位」 データ列で集計した出現頻度	「期間」(初期設定)
初めて検出されたアプリケーション	信頼されたアプリケーション 重要 このデータは、ログの種類の「既知のアプリケーション」に一致します。		7 日
ソフトウェア安全性評価リストにないアプリケーション	ポリシー処理		7 日
停止されたエージェントの平均	クライアントサンプリング 重要 このデータは、データソースの「ユーザとエンドポイント」に一致します。		1 日

「テンプレート」	「ログの種類」	「集約単位」 データ列で集計した出現頻度	「期間」(初期設定)
接続していないエンドポイントの平均	クライアントサンプリング 重要 このデータは、データソースの「ユーザとエンドポイント」に一致します。		直近の 1 日に 1 日以上
ブロックルールとロックダウンルールのアプリケーションイベント	ポリシー処理	• エンドポイント名 • 名前 (初期設定) • ユーザ名	7 日
ブロックルールのアプリケーションイベント	ポリシー処理	• エンドポイント名 • 名前 (初期設定) • ユーザ名	7 日
ロックダウンルールのアプリケーションイベント	ポリシー処理	• エンドポイント名 • 名前 (初期設定) • ユーザ名	7 日
検出された分類されていないアプリケーション	ポリシー処理		7 日

Endpoint Application Control ルール管理

このウィジェットには、Endpoint Application Control のルールに含まれているルールの種類とルール名のリストが表示されます。

Endpoint Application Control にルールを追加するには、[ルールの追加] をクリックし、追加するルールの種類を選択します。

ルール	説明
許可	信頼されたアプリケーションに対する許可を拡張する場合は、許可ルールを使用します。
ブロック	実行前または実行後にアプリケーションをブロックする場合は、ブロックルールを使用します。
ロックダウン	現在インストールされているすべてのアプリケーションを許可する場合は、ロックダウンルールを使用します。したがって、最新の完全なインベントリが必要です。

Endpoint Application Control ユーザとエンドポイントの概要ウィジェット

このウィジェットには、選択した基準に基づいて、Endpoint Application Control のユーザとエンドポイントの検出サマリが表示されます。カスタマイズ可能なテンプレートを使用して、エージェント接続、エージェントバージョン、エンドポイントの Windows バージョン、ポリシー、ポリシーアップ

デート、およびルールを表示できます。テンプレートは、カスタム設定を使用して変更します。

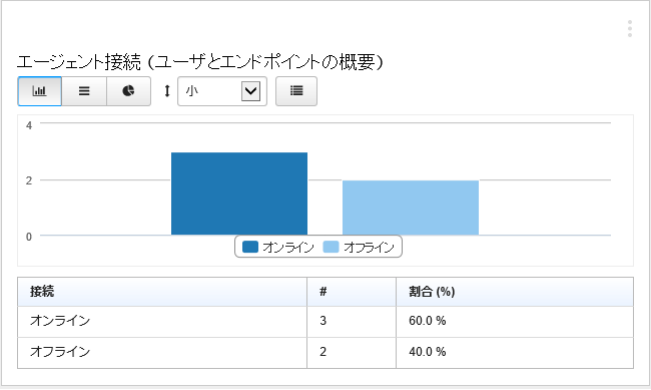
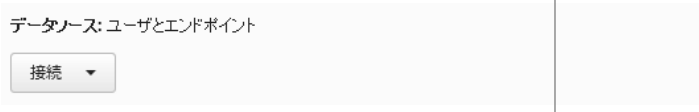
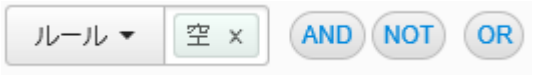


図 25-2. ユーザとエンドポイントの概要ウィジェットの例

[ダッシュボード] に移動して、ウィジェットの右上のメニューから [ウィジェット設定] を選択し、次のタスクを実行します。

表 25-4. ユーザとエンドポイントの概要ウィジェットの設定タスク

タスク	手順
ウィジェットに名前を付ける	[タイトル] で、名前を入力します。 ヒント このフィールドを空白のままにした場合は、初期設定の名前が設定されます。
テンプレートを選択する	[テンプレート] で、テンプレートを選択します。

タスク	手順
データソースを編集する	[詳細] を選択します。 [データソース] で、ウィジェットによって表示されるデータのデータソースを選択します。  図 25-3. データソース
表示される結果を制限する	[詳細] を選択します。 [結果を以下に制限] で、動的検索を使用します。 
グラフの種類を変更する	[表示] で、次のグラフの種類のいずれかを選択します。 • データポイント付きの折れ線グラフの場合は、 を選択します。 • 横のヒストグラムの場合は、 を選択します。 • 円グラフの場合は、 を選択します。(初期設定) • データ表の場合は、 を選択します。 注意 (グラフの下にデータ表を表示) が選択されている場合、このコントロールは利用できません。

タスク	手順
グラフのサイズを変更する	グラフの種類の右側で、次のいずれかのグラフのサイズを選択します。 • 約 1 単位の高さのグラフの場合、[小] を選択します。 • 約 2 単位の高さのグラフの場合、[中] を選択します。(初期設定) • 約 4 単位の高さのグラフの場合、[大] を選択します。  図 25-4. グラフサイズ
凡例の場所を変更する	[凡例] で、次の場所のいずれかを選択します。 • なし • 下位 (初期設定) • 右 • 上位 • 左 注意 (データを円グラフとして表示) が選択されている場合、このコントロールは利用できません。
ウィジェットのグラフコントロールを表示する	[ツールバー] チェックボックスをオンにします。(初期設定)
ウィジェットのグラフコントロールを非表示にする	[ツールバー] チェックボックスをオフにします。
グラフの下のデータ概要テーブルを表示する	[グラフの下のデータ概要テーブル] をオンにします。

タスク	手順
グラフの下のデータ概要テーブルを非表示にする	[グラフの下のデータ概要テーブル] をオフにします。(初期設定)
新しいテンプレートとして設定を保存する	[テンプレート] で、 ➕ [現在の設定をテンプレートとして保存] を選択します。
ウィジェットを削除する	ウィジェットの右上のメニューから、[ウィジェットを閉じる] を選択します。 ウィジェットと、ウィジェットの設定に対して行ったカスタマイズが削除されます。

このウィジェットには、次のカスタマイズ可能なテンプレートが含まれています。

注意

一度に表示できるテンプレートは 1 つだけです。

「テンプレート」	「データソース」	範囲	「アドバンス」 データ列 (初期設定)
エージェント接続	ユーザとエンドポイント	すべて (ユーザによる設定は不可)	接続済み
エージェントバージョン	ユーザとエンドポイント	トップ 3	エージェントバージョン
エンドポイントの Windows バージョン	ユーザとエンドポイント	トップ 3	Windows バージョン
ポリシー	ユーザとエンドポイント	トップ 3	ポリシー
ポリシーアップデート	ユーザとエンドポイント	すべて (ユーザによる設定は不可)	ポリシーアップデート

「テンプレート」	「データソース」	範囲	「アドバンス」 データ列 (初期設定)
ルール	ユーザとエンドポイント	トップ 3	ルール

Endpoint Application Control のアプリケーション、ルール、およびポリシーイベントウィジェット

このウィジェットは、選択した条件に基づいて、Endpoint Application Control のアプリケーションイベントの検出サマリを表示するために使用します。

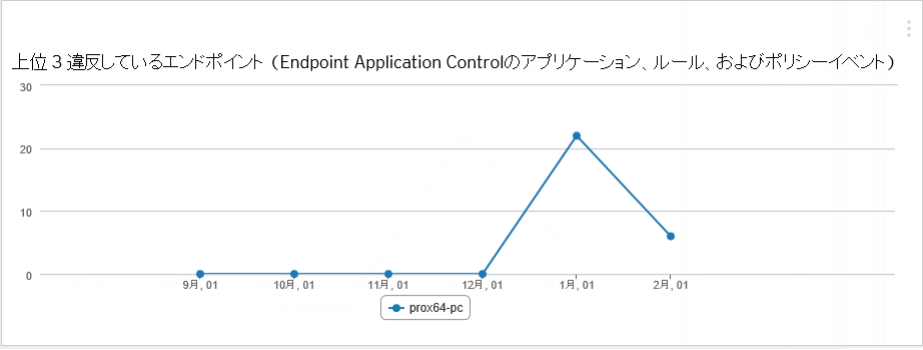


図 25-5. アプリケーション、ルール、およびポリシーイベントウィジェットの例

[ダッシュボード] に移動して、ウィジェットの右上のメニューから [ウィジェット設定] を選択し、次のタスクを実行します。

表 25-5. アプリケーション、ルール、およびポリシーイベントウィジェットの設定タスク

タスク	手順
ウィジェットに名前を付ける	[タイトル] で、名前を入力します。 ヒント このフィールドを空白のままにした場合は、初期設定の名前が設定されます。

タスク	手順
テンプレートを選択する	[テンプレート] で、テンプレートを選択します。 テンプレートについての情報を参照してください。
データ範囲を編集する	[ログの種類] で、ウィジェットによって表示されるデータの範囲を選択します。  図 25-6. データの範囲
期間を編集する	[期間] で、ウィジェットのデータの期間を選択します。
データソースを編集する	1. [詳細] を選択します。 このウィジェットに追加の設定が表示されます。 2. [ログの種類] で、ウィジェットによって表示されるデータのデータソースを選択します。  図 25-7. データソース
表示される結果を制限する	[詳細] を選択します。 [結果を以下に制限] で、動的検索を使用します。 

タスク	手順
グラフの種類を変更する	[表示] で、次のグラフの種類のいずれかを選択します。 • データポイント付きの折れ線グラフの場合は、  を選択します。(初期設定) • 縦のヒストグラムの場合は、  を選択します。 • 横のヒストグラムの場合は、  を選択します。 • 円グラフの場合は、  を選択します。 • データ表の場合は、  を選択します。  注意  (グラフの下にデータ表を表示) が選択されている場合、このコントロールは利用できません。

タスク	手順
グラフのサイズを変更する	グラフの種類の右側で、次のいずれかのグラフのサイズを選択します。 • 約 1 単位の高さのグラフの場合、[小] を選択します。 • 約 2 単位の高さのグラフの場合、[中] を選択します。(初期設定) • 約 4 単位の高さのグラフの場合、[大] を選択します。  図 25-8. グラフサイズ 注意 (データを表として表示) が選択されている場合、このコントロールは利用できません。
凡例の場所を変更する	[凡例] で、次の場所のいずれかを選択します。 • なし • 下位 (初期設定) • 右 • 上位 • 左 注意 (データを円グラフとして表示) または (データを表として表示) が選択されている場合、このコントロールは利用できません。

タスク	手順
ウィジェットのグラフコントロールを表示する	[ツールバー] チェックボックスをオンにします。
ウィジェットのグラフコントロールを非表示にする	[ツールバー] チェックボックスをオフにします。(初期設定)
グラフの下のデータ概要テーブルを表示する	[グラフの下のデータ概要テーブル] をオンにします。
グラフの下のデータ概要テーブルを非表示にする	[グラフの下のデータ概要テーブル] をオフにします。(初期設定)
新しいテンプレートとして設定を保存する	[テンプレート] で、 ➕ [現在の設定をテンプレートとして保存] を選択します。

このウィジェットには、次のカスタマイズ可能なテンプレートが含まれています。

注意

一度に表示できるテンプレートは 1 つだけです。

「テンプレート」	「ログの種類」	範囲 (初期設定)	「期間」(初期設定)	「アドバンス」データ列 (初期設定)	「アドバンス」動的検索 (初期設定)
ルールなしのアプリケーション	アプリケーションイベント 重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	名前	ルールが空である
適用済みポリシー	アプリケーションイベント 重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	ポリシー	ポリシーが空ではない

「テンプレート」	「ログの種類」	範囲 (初期設定)	「期間」(初期設定)	「アドバンス」データ列 (初期設定)	「アドバンス」動的検索 (初期設定)
ブロック済みアプリケーション	アプリケーションイベント  重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	名前	実行された処理がブロックされる
使用されているアプリケーション	アプリケーションイベント  重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	名前	実行された処理が許可される

「テンプレート」	「ログの種類」	範囲 (初期設定)	「期間」(初期設定)	「アドバンス」 データ列 (初期設定)	「アドバンス」 動的検索 (初期設定)
違反ポリシー	アプリケーションイベント  重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	ポリシー	ポリシーが空ではない および 実行された処理がブロックされる
違反ルール	アプリケーションイベント  重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	名前	ルールが空ではない および 実行された処理がブロックされる

「テンプレート」	「ログの種類」	範囲 (初期設定)	「期間」(初期設定)	「アドバンス」データ列 (初期設定)	「アドバンス」動的検索 (初期設定)
違反しているエンドポイント	アプリケーションイベント 重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	エンドポイント名	実行された処理がブロックされる
違反しているユーザ	アプリケーションイベント 重要 このデータは、ログの種類の「ポリシー処理」に一致します。	トップ 3	過去 14 日間	ユーザ名	実行された処理がブロックされる

第 26 章

Endpoint Application Control のポリシー設定

次の Endpoint Application Control のポリシー設定を使用して、Apex Central から Endpoint Application Control エージェントを管理できます。

ポリシールール

[ルール] を展開して、以下のタスクを実行します。

タスク	手順
このポリシーに割り当てられているルールのリストを表示する	ポリシーに割り当てられているルールは、[ルールの割り当て] ボタンの下の表に表示されます。 ヒント ルールで明示的にブロックされていない限り、ソフトウェア安全性評価で安全と見なされた OS アプリケーションは許可されます。
ルールをこのポリシーに割り当てる	[ルールの割り当て] をクリックして、次のいずれかを実行します。 • ポリシーに割り当てる既存のルールを選択するには、 [既存] を選択します。[ポリシーへの既存ルールの割り当て] 画面が表示されます。割り当てるルール (複数可) を選択して、[ルールの割り当て] をクリックします。
選択したルールをこのポリシーから削除します。	リストから 1 つ以上のルールを選択し、[選択した対象を削除] をクリックしてから、もう一度 [選択した対象を削除] をクリックします。

次の表は、以下の設定オプションの概要を示しています。

ポリシーの設定	詳細
Windows ディレクトリのすべてのアプリケーションを常に許可 (ブロックルールとロックダウンルールをオーバーライド) する	初期設定では、Endpoint Application Control はすべてのアプリケーションを Windows ディレクトリに格納することを許可します。この機能は、Windows の初期設定パスの許可ルールに似ており、ブロックルールまたはロックダウンルールを上書きします。

ポリシーの設定	詳細
エンドポイントの切断中は自動的にロックダウンルールを適用する	切断されたエンドポイントは新しいポリシーを受信したり、適用したりできません。初期設定では、これは切断されたエンドポイントで現在のポリシーの適用が継続されることを意味します。
不審オブジェクトに対する保護を有効にする (Apex Central に対する契約が必要)	Endpoint Application Control は、一致したエンドポイントを不審オブジェクトから保護します。
互換性は高いが機能は限られたユーザレベルのブロック方法を使用する	カーネルレベルのブロックは、ファイルアクセスをブロックすることでアプリケーションが起動できないようにします。この方法ではセキュリティは向上しますが、承認済みのアプリケーションが必要とする特定のファイルへのアクセスも予期せずにブロックされたり一時的に遅延したりする可能性があります。この機能は最初の一致「ユーザおよびグループ」の条件に設定されているポリシーでのみサポートされます (「SYSTEM」アカウントを除く)。 ユーザレベルのブロックはアプリケーションの起動を許可した後に、タスクレベルでアプリケーションを停止します。ただし、一部のアプリケーションは起動後に停止させることができないことがあります。また、この機能では、信頼された送信元の機能とリンクライブラリ (DLL) および Java インタプリタアプリケーションのブロックはサポートされません。

ポリシーのログ

一致したユーザおよびエンドポイントについて次のポリシーを設定するには、[ログ] を展開します。

ポリシーの設定	詳細
次の処理を記録します	次のログ制限事項のいずれかを選択します。 • 処理をログに記録しない場合は、[なし] を選択します。 • 除外されたディレクトリ以外から発生したブロック済みアプリケーションの開始またはアクセスをログに記録する場合は、[ブロック] を選択します。 これは、新しいポリシーの初期設定です。 • 除外されたディレクトリ以外から発生した選択済みアプリケーションの開始またはアクセスをログに記録する場合は、[選択済み] を選択します。表示されたリストを使用して、一致するルールを選択します。 • 除外されたディレクトリ以外から発生した任意のアプリケーションの開始またはアクセスをログに記録する場合は、[任意] を選択します。 注意 このオプションを選択すると大容量のログファイルが生成され、ネットワークのデータ転送が大幅に増加する可能性があります。
次のディレクトリをログから除外	[次のディレクトリをログから除外] を選択して、除外するアプリケーションパスを入力します。各パスを改行で区切ります。 初期設定パスは%SYSTEMROOT%と%WINDIR%です。
集計ログの収集間隔	エンドポイントごとに集計されたログを収集する間隔を選択します。 初期設定は 2 時間です。提案される設定は、配信されたエージェントの数によって決まります。

ポリシーの配信

一致したユーザおよびエンドポイントについて次のポリシーを設定するには、[配信] を展開します。

ポリシーの設定	詳細
次の間隔でポリシーアップデートを送信	ポリシーアップデートを実行する時間間隔を選択します。 初期設定は 15 分です。提案される間隔は、配信されたエージェントの数によって決まります。 初期設定では、ネットワークのデータ転送とローカルストレージの必要量を削減するために、配信されたポリシーにはエンドポイントのインベントリで検出済みの一致したアプリケーションのみが含まれます。各ポリシー配信間隔で、Endpoint Application Control には、配信されたポリシーのルールに一致する、エンドポイント上に新しく追加されたアプリケーションが含まれます。
次の条件に該当する場合にポリシー全体を配信  注意 このオプションを選択すると、ネットワークのデータ転送が大幅に増加する可能性があります。	必要に応じて、「ポリシー全体」を配信できます。この場合、一致したアプリケーションがすべて含まれ、エンドポイントインベントリの一致は無視されます。 • 一致したエンドポイントが定期的にサーバに接続しない場合は、[エンドポイントの接続時間が次より短い] を選択し、週あたりの時間数を指定します。 • 一致したエンドポイントが、ロックダウンルールの適用後に許可ルールで指定されたアプリケーションをインストールして実行できるようにする必要がある場合は、[エンドポイントがロックダウンルールの適用を開始] を選択します。

ポリシーサーバ接続

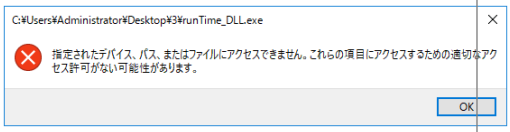
一致したユーザおよびエンドポイントについて次のポリシーを設定するには、[サーバ接続] を展開します。

ポリシーの設定	詳細
次のサーバに接続	ネットワークに複数の Endpoint Application Control サーバが存在するか、サーバが新しい IP アドレスに移動している可能性があります。 このポリシーが適用された後にエンドポイントが接続する必要があるサーバを指定します。 • 管理コンソールをホストしているサーバと同じサーバを使用するには、[初期設定] を選択します。これは、新しいポリシーの初期設定です。 • [指定済み] を選択し、サーバアドレスとポートを入力してサーバを指定します。
HTTPS を使用する	初期設定では、Endpoint Application Control は、サーバのインストール中に選択された HTTP または HTTPS の設定を使用します。 すべての一致したユーザまたはエンドポイントを、常に HTTPS を使用するように設定するには、[HTTPS を使用する] を選択します。 ヒント このオプションを使用するには、サーバ CA をクライアントエンドポイントにインポートする必要があります。 詳細な手順については、https://success.trendmicro.com/solution/1115573 を参照してください。

ポリシーユーザエクスペリエンス

一致したユーザおよびエンドポイントについて次のポリシーを設定するには、[ユーザエクスペリエンス] を展開します。

ポリシーの設定	詳細
システムトレイアイコンの表示	Endpoint Application Control システムトレイアイコン () は通知を表示できるため、ユーザはアプリケーションへのアクセスを要求できます。また、このアイコンを使用して、ユーザは Endpoint Application Control 設定とログを手動でアップデートできます。 • 一致したユーザの Windows システムトレイにアイコンを表示するには、[はい] を選択します。 • アイコンを非表示にするには、[いいえ] を選択します。

ポリシーの設定	詳細
通知ポップアップの表示	一部のユーザに対しては、通知を表示することが適切でない場合があります。たとえば、ATM、医療機器、キオスク、給油ポンプなど、特殊な用途のエンドポイントのユーザは、通知や関連する対話の要求によって混乱する可能性があります。 • Endpoint Application Control 通知を一致したユーザに表示するには、[はい] を選択します。 • 通知を抑止し、関連するユーザとの対話を無効にするには、[いいえ] を選択します。 **重要** Endpoint Application Control がカーネルレベル方式を使用してアプリケーションの開始をブロックしたり遅らせたりすると、Windows によって次の通知がエンドユーザに表示されることがあります。  図 26-1. Windows のブロック通知 Endpoint Application Control はこの通知を非表示にすることはできません。その代わりに、ユーザレベルのブロックを適用することでこの通知を回避できます。
新規インベントリの生成	エンドポイントは、インベントリを生成して、新規アプリケーションおよび削除されたアプリケーションを追跡します。Endpoint Application Control はアプリケーションインベントリをエンドポイントから定期的に収集します。 時間間隔 (毎日、毎週など) を選択します。

ポリシーの設定	詳細
開始時刻	インベントリ検索の開始時刻を選択します。

パート XI

Endpoint Encryption のウィジェットとポリシー

第 27 章

Endpoint Encryption ダッシュボードウィジェット

本章では、Apex Central ダッシュボードでサポートされる Endpoint Encryption のウィジェットについて説明します。

次のトピックがあります。

Endpoint Encryption ユーザ

Endpoint Encryption ユーザウィジェットを使用すると、Apex Central のダッシュボードからユーザを直接管理できます。Endpoint Encryption ユーザウィジェットでは、Apex Central のユーザアカウントの追加や削除、パスワードのリセット、権限の変更、ポリシーグループの優先度の設定、Active Directory からのインポート、特定のユーザアカウントの検索を実行できます。

項目	説明
表示	表示するユーザを選択します。エンタープライズのすべてのユーザか、特定のポリシー内のユーザを表示できます。
検索 ( )	アイコンをクリックすると、表内に表示する Apex Central ユーザをフィルタできます。検索フィールドを使用して検索するパラメータを指定します。

項目	説明
設定 ( ) ユーザを右クリック	アイコンをクリックすると、ユーザの属性を表示したり、選択したユーザに対して処理を実行したりできます。
ユーザの追加 ( )	アイコンをクリックすると、個別のユーザの追加、CSV ファイルからのユーザのインポート、または Active Directory LDAP からのユーザのインポートを実行できます。
ユーザ数	エンタープライズ全体、選択したポリシー、または指定した検索内の合計ユーザ数が表示されます。

ユーザ設定オプション

次の表は、設定アイコンで使用可能なオプションを示しています。

表 27-1. ユーザ設定オプション

オプション	説明
パスワードの変更	認証の種類として固定パスワードを使用して、ユーザの新しいパスワードを指定します。認証の種類がドメインの場合、ウィジェットではパスワードの変更をサポートしていません。
ユーザの削除	選択したユーザを削除します。
ユーザの変更	選択したユーザのプロパティを更新します。次のプロパティを変更できます。 • ユーザ名 • 名前 (名) • 名前 (姓) • 従業員 ID • メールアドレス • フリーズ • ユーザタイプ • 1 つのポリシー • 認証方法

オプション	説明
ポリシーの一覧表示	選択したユーザがメンバーになっているポリシーが表示されます。 選択したユーザの [インストールの許可] 列が [はい] の場合、選択したポリシーのインストールを許可/禁止するオプションと、最優先の順位を付与するポリシーの選択が有効になります。

新しいユーザオプションを追加する

次の表に、新しい Apex Central ユーザを追加するときに使用可能なオプションを示します。

表 27-2. 新しいユーザオプションを追加する

オプション	説明
ユーザ名	ユーザが認証に使用するアカウントのユーザ名を指定します。
名前 (名)	ユーザの名前 (名) を指定します。
名前 (姓)	ユーザの名前 (姓) を指定します。
従業員 ID	ユーザの従業員 ID を指定します (オプション)。
メールアドレス	ユーザの電子メールアドレスを指定します (オプション)。
フリーズ	[はい] を選択して、一時的にアカウントをロックします。ロックされたアカウントでは、Apex Central デバイスにログオンできません。
ユーザタイプ	[ユーザ]、[オーセンティケータ]、または [管理者] を選択します。
1 グループ	[はい] を選択すると、ユーザは一度に 1 つのポリシーにしか属することができなくなります。ユーザをその他のポリシーグループに追加することはできません。 このオプションを [はい] に設定し、[ユーザタイプ] を [オーセンティケータ] または [管理者] に設定した場合、ユーザはそれぞれ、グループオーセンティケータまたはグループ管理者になります。
認証方法	ユーザが利用可能な認証方法を選択します。

ポリシーメンバーシップ

次の表に、Apex Central ユーザポリシーメンバーシップの概要を示します。

注意

Apple FileVault および Microsoft BitLocker の暗号化管理は、認証を必要とせず、認証ポリシーによる影響を受けません。クライアント、ログイン、パスワード、および認証の各ポリシーや、ユーザへのセキュリティエージェントソフトウェアのアンインストールの許可は、ディスク全体の暗号化エージェントおよびファイル暗号化エージェントにのみ影響します。

ヘッダ	例	説明
優先順位	1、2、3	Apex Central がポリシーを適用する順序を示します。ユーザに影響のあるポリシーが適用されると、Apex Central が処理を実行します。その他のポリシーは当該イベントのユーザに影響を与えません。
ポリシー名	GP1	ユーザが現在割り当てられているすべてのポリシーの名前を示します。
説明	一時的な従業員ポリシー。	ポリシーの説明を示します。
インストールの許可	Yes、No	ユーザが新しいデバイスをインストールできるかどうかを示します。

CSV ファイルからユーザをインポートする

注意

CSV ファイルからのユーザのインポートは、固定パスワード認証を使用するユーザの場合のみサポートされます。

CSV ファイル内の各行の形式は次のようになります。

```
<ユーザ ID（必須）>，<名前（名）>，<名前（姓）>，<従業員 ID>，<メールアドレス>
```

データがないフィールドの場合は、プレースホルダとしてコンマを使用します。以下は CSV エントリの例です。

```
example_id, name,,, name@example.com
```

手順

1. Endpoint Encryption ユーザウィジェットから、[ユーザの追加] をクリックして、[ファイルからのユーザのインポート] を選択します。

   [ファイルからのユーザのインポート] 画面が表示されます。

2. CSV ファイルを選択するには、[ファイルの選択] をクリックします。

   [CSV ファイルを開く] ウィンドウが表示されます。

3. ファイルを選択して、[開く] をクリックします。

4. [追加] をクリックします。

   CSV ファイル内のユーザがインポートされます。

Active Directory ユーザをインポートする

PolicyServer では、Active Directory データベースとは別にユーザディレクトリを保持しています。これにより、すべての Apex Central デバイスへのアクセス、ユーザ権限、および認証方法に対してポリシーサーバの絶対的なセキュリティを確保できます。

Apex Central の Endpoint Encryption ユーザウィジェットを使用して、Active Directory ユーザをインポートします。

手順

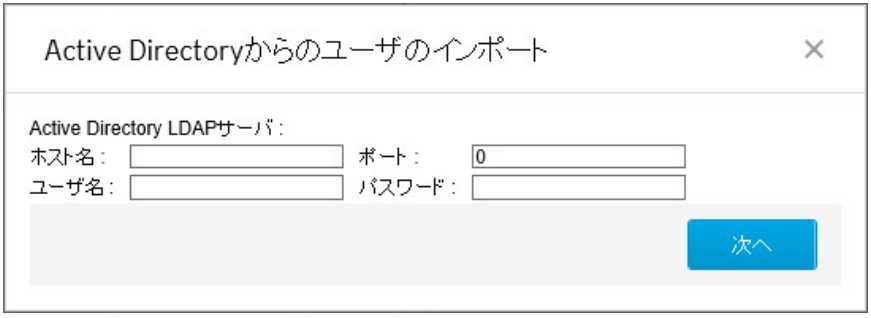
1. Apex Central にログオンします。

2. Endpoint Encryption ユーザウィジェットに移動します。

3. アイコンをクリックします。

4. [Active Directory からのユーザのインポート] を選択します。

[Active Directory からのユーザのインポート] 画面が表示されます。



5. Active Directory LDAP サーバの認証情報を指定します。

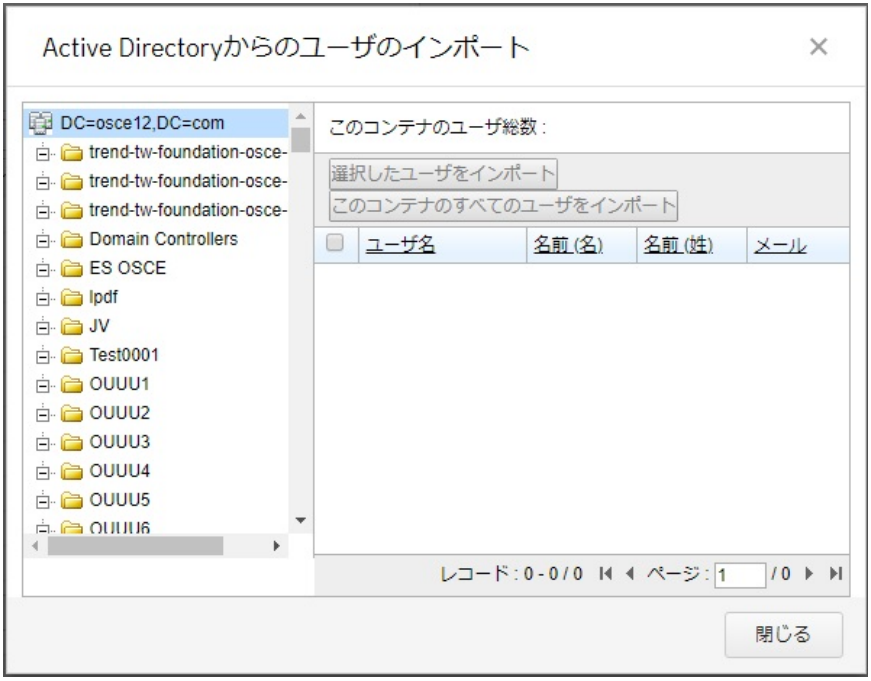
注意

[ポート] では、値「0」は初期設定のポートを示します。初期設定のポートは 389 です。

---

6. [次へ] をクリックします。
7. 指定された Active Directory ドメインにデータが入力されるのを待ちます。

指定されたドメインの Active Directory ツリーが左側のペインに表示されます。



8. 左側のペインから、ナビゲーションツリーを使用してユーザの追加元のコンテナを選択します。

   選択可能なユーザが右側のペインに表示されます。

9. 次のいずれかを実行します。

   - 個々のユーザを選択して、[選択したユーザをインポート] をクリックします。
   - [このコンテナのすべてのユーザをインポート] をクリックします。

10. ユーザを指定された場所に追加するには、[OK] をクリックします。

    確認ウィンドウが表示されます。

11. 確認して、[OK] をクリックします。

    インポートステータスメッセージが表示されます。

12. [閉じる] をクリックして終了するか、または手順を繰り返して、追加のユーザを選択してインポートします。

Endpoint Encryption デバイス

Endpoint Encryption バイスとは、PolicyServer に登録されている Endpoint Encryption エージェントです。Endpoint Encryption エージェントをインストールすると、エンドポイントは新しい Endpoint Encryption デバイスとして自動的に PolicyServer に登録されます。複数の Endpoint Encryption エージェントが指定された 1 つのエンドポイントを保護できるため、1 つのエンドポイントが PolicyServer 上に複数の Endpoint Encryption デバイスとして表示されることがあります。

Endpoint Encryption デバイスウィジェットを使用すると、Apex Central のダッシュボードから Endpoint Encryption デバイスを直接管理できます。Endpoint Encryption Devices ウィジェットでは、アクティビティの監視や、Endpoint Encryption デバイスの検索に加え、エンドポイントの紛失や盗難が

発生したときに lock または kill コマンドを実行してエンドポイントのデータを保護できます。

オプション	説明
表示	表示するデバイスを選択します。エンタープライズのすべてのデバイスか、特定のポリシー内のデバイスを表示できます。
検索 (🔍▼)	🔍▼アイコンをクリックしてセキュリティエージェントを選択し、表内に表示されるデバイスをフィルタします。検索フィールドを使用して検索するパラメータを指定します。デバイスの属性にリストされているすべての属性を検索できます。
設定 (⚙) デバイスを右クリック	デバイスを選択して⚙アイコンをクリックするか、デバイスを右クリックすると、デバイスの属性を表示したり、選択したデバイスへの処理を実行したりできます。

オプション	説明
デバイス数	エンタープライズ全体、選択したポリシー、または指定した検索内の合計デバイス数が表示されます。

デバイス処理

デバイスを選択して アイコンをクリックするか、デバイスを右クリックすると、以下の処理を実行できます。

処理	説明
デバイスの削除	エンタープライズから Apex Central デバイスを削除すると、そのデバイスはすべてのポリシーグループからも削除されます。削除された Apex Central デバイスは、そのデバイス上で接続およびパスワードポリシーが最新の状態である限り機能し続けます。エージェントは、PolicyServer とポリシーを同期できなくなります。 警告! ディスク全体の暗号化を実行したデバイスを削除する前に、ディスクを復号し、ディスク全体の暗号化エージェントをアンインストールしてください。エージェントを削除せずにディスク全体の暗号化を実行したデバイスを削除すると、PolicyServer でディスク全体の暗号化のプリブートを認証できず、データにアクセスできなくなる可能性があります。
ソフトトークン	「ソフトウェアトークン」を生成すると、一意の文字列が作成されます。この文字列は、Apex Central デバイスのロックを解除する場合、および Apex Central のユーザがパスワードを忘れたときにリセットする際にリモートでサポートする場合に使用できます。 ソフトウェアトークンは、製品版のディスク全体の暗号化でのみ使用できます。Apple FileVault または Microsoft BitLocker の暗号化管理では使用できません。

処理	説明
リカバリキー	「リカバリキー」を生成すると、ユーザは元のパスワードまたはキーを忘れてしまったときにハードディスクを復号できます。 リカバリキーは、ディスク全体の暗号化で利用可能な別のリカバリ手法を使用しないため、Apple FileVault および Microsoft BitLocker エージェントの暗号化管理でのみ使用できます。
デバイス属性	選択したデバイスの最新のスナップショットが表示されます。
デバイスの強制終了	「kill」コマンドを開始すると、Apex Central デバイスのすべてのデータが削除されます。削除されるデータは、関連付けられているセキュリティエージェントが管理するデータの範囲に応じて異なります。たとえば、ディスク全体の暗号化を実行したデバイスに対して kill コマンドを開始すると、エンドポイントからすべてのデータが削除されますが、ファイル暗号化を実行したデバイスに対して「kill」コマンドを開始すると、ファイル暗号化エージェントによって保護されているローカルのすべてのファイルとフォルダ、またはリムーバブルストレージが削除されます。「kill」コマンドは、セキュリティエージェントがポリシーサーバと通信するときに発行されます。 警告! デバイスの強制終了は取り消しできません。kill コマンドを開始する前にすべてのデータをバックアップしてください。
デバイスのロック	Apex Central デバイスに対して「lock」コマンドを開始すると、リモートヘルプ認証が成功するまで、Apex Central ユーザはデバイスにアクセスできなくなります。デバイスをロックすると、エンドポイントが再起動し、エンドポイントは強制的にリモートヘルプ認証が必要な状態に置かれます。lock コマンドは、セキュリティエージェントがポリシーサーバと通信するときに発行されます。
ソフトリセット	soft reset コマンドを開始するとエンドポイントが再起動します。このコマンドは、次回エージェントが PolicyServer と通信するときに発行されます。

デバイス属性

次の表は、Apex Central デバイスの属性を示しています。

属性名	例	説明
AD NetBIOS 名	エンタープライズ	AD NetBIOS に割り当てられている名前。
AD オブジェクト GUID	6629bdeb-99a8-456b-b7c5-dbbc50ad13d0	AD オブジェクトに割り当てられている GUID。
バッテリー数	2	装着されているバッテリー数。
.NET のバージョン	2.0.50727.3620	インストールされている.NET Framework のバージョンとビルド番号。
共通フレームワークビルド番号	5.0.0.84	セキュリティエージェントは暗号化のために共通フレームワークを使用します。ビルド番号は、エージェントが最新の状態かどうかを確認するために使用されます。
ディスクモデル	VMware Virtual IDE	ハードディスクのモデル。
ディスク名	¥¥.¥PHYSICALDRIVE0	ハードディスクの名前。
ディスクシリアル番号		ハードディスクのシリアル番号。
ディスクパーティション	1	エージェントがインストールされているディスク上のパーティション数。
ディスクサイズ	10733990400	ハードディスクの合計容量 (バイト)。
ドメイン名	WORKGROUP	エンドポイントがメンバーになっているドメイン。
エンドポイント ID	85b1e3e2a3c25d882540ef6e4818c3e4	Apex Central の統合に使用される、エンドポイントの一意の ID。
ファイル暗号化バージョン	6.0.0.1039	エンドポイントにインストールされているファイル暗号化のバージョン。
ホスト名	TREND-4136D2DB3	エンドポイントのホスト名。
IP アドレス	10.1.152.219	エンドポイントの IP アドレス。
言語	英語 (米国)	エンドポイントが使用する言語。

属性名	例	説明
ロケール	ja-JP	エンドポイントが使用する地域設定。
MAC アドレス	00-50-56-01-xx-xx	エンドポイントの MAC アドレス。
コンピュータ名	TREND-4136D2DB3	エンドポイントが使用するコンピュータ名。
製造元	VMware, Inc.	ハードディスクの製造元。
モデル	VMware Virtual Platform	ハードディスクのモデル
OS:	Microsoft Windows NT 5.1.2600 Service Pack 3	エージェントと同じハードディスクにインストールされている OS。
OS 名	Microsoft Windows XP Professional	エージェントと同じハードディスクにインストールされている OS の一般名。
OS Service Pack	Service Pack 3	エージェントと同じハードディスクにインストールされている OS の Service Pack の番号。
OS バージョン	5.1.2600.196608	エージェントと同じハードディスクにインストールされている OS のバージョン番号。
パーティションスキーム	Classical MBR	ハードディスクのパーティションスキーム。
プロセッサ	x86 Family 6 Model 30 Stepping 5, Genuine Intel	エンドポイントのプロセッサ製造元とモデル。
プロセッサ数	2	エンドポイントのプロセッサ数。
プロセッサリビジョン	1e05	プロセッサのリビジョン番号。
タイムゾーン	台湾標準時	エンドポイント所在地のタイムゾーン。
物理メモリ合計	2047MB	エンドポイントにインストール済み、または割り当てられている RAM の合計。
種類	X86 ベース PC	エンドポイントのプロセッサの種類。

属性名	例	説明
Windows ユーザ名	TREND-4136D2DB3\admin	エンドポイントに最後にログオンした Windows アカウントのユーザ名。
<エージェント> ユーザ	john_smith	最後のログオンに使用されたユーザ名。
<エージェント> バージョン	5.0.0.260	インストールされたエージェントのバージョンとビルド番号。

ディスク全体の暗号化ステータス

ディスク全体の暗号化ステータスウィジェットには、ネットワーク上のすべてのデバイスの現在の暗号化ステータスが表示されます。

列	説明
ステータス	エンドポイントのステータス。次のステータスがあります。 • 暗号化完了: エンドポイントはすべて暗号化されています。 • 暗号化中: エンドポイントは、現在ハードディスクを暗号化中です。暗号化が完了し、エンドポイントが再起動すると、ステータスは 「[暗号化完了]」 に変わります。 • 暗号化未完了: エンドポイントは全く暗号化されていません。 • 復号中: エンドポイントは、現在ハードディスクを復号中です。復号が完了し、エンドポイントが再起動すると、ステータスは [暗号化未完了] に変わります。 • 不明: エンドポイントは同期されましたが、ポリシーサーバは暗号化ステータスを確認できません。
比率	エンドポイントが暗号化されている割合。
デバイス	現在のステータスに該当するエンドポイントの数。数字をクリックすると、Endpoint Encryption デバイスレポートが表示されます。

注意

ウィジェットの下部の [合計] の隣の数字をクリックすると、ディスク全体の暗号化ステータスレポートが表示されます。

ディスク全体の暗号化ステータスレポート

次の表は、ディスク全体の暗号化ステータスレポートについて示しています。このレポートを詳しく理解するために使用してください。

表 27-3. ディスク全体の暗号化ステータスレポートの例

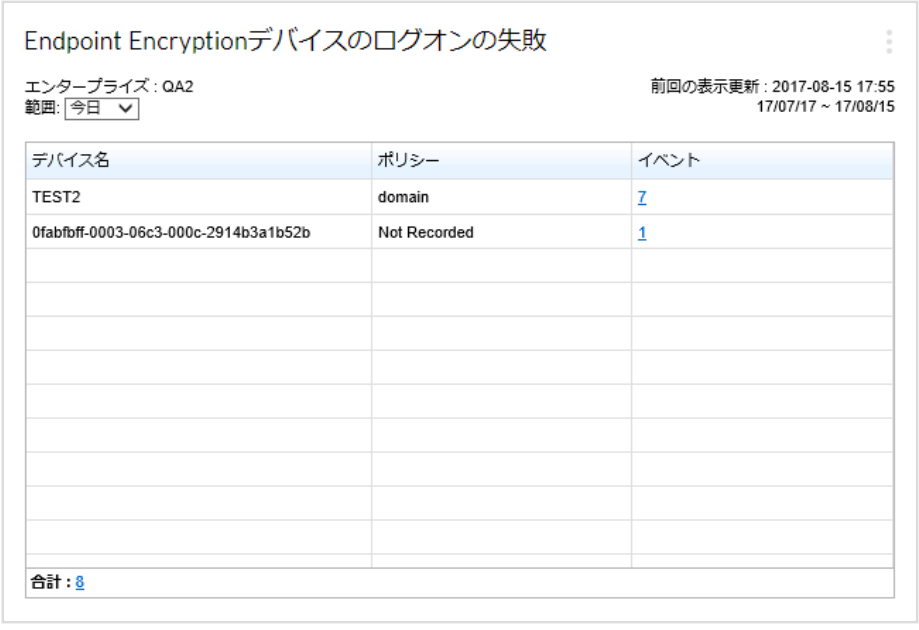
ヘッダ	例	説明
ポリシー	GP1	エンドポイントを制御しているポリシーのタイトル。
モバイルデバイス名	TREND-4136D2DB3	エンドポイントが使用するコンピュータ名。

ヘッダ	例	説明
デバイス ID	1fabfbff-0001-06e5-000c-297085710000	エンドポイントにセキュリティエージェントがインストールされ、新しいエンドポイントがポリシーサーバに登録された後に確立された一意の ID。
エージェント	ディスク全体の暗号化	現在インストールされているセキュリティエージェント。
ステータス	暗号化未完了	エンドポイントの現在のステータス。
前回の同期日	2013/10/07 11:05	エンドポイントが前回ポリシーサーバからポリシーを更新したときのタイムスタンプ。
前回のポリシー施行	2013/10/07 11:05	Apex Central が前回ポリシーサーバのポリシー変更を実施したときのタイムスタンプ。

Endpoint Encryption デバイスのログオンの失敗

Endpoint Encryption デバイスのログオンの失敗ウィジェットには、ユーザがログオン試行に失敗したデバイス (管理下のエンドポイント) がすべて表示さ

れます。デバイスのログオン失敗イベントはセキュリティ違反を表す場合があります。または、ユーザがログオン認証情報を忘れた可能性があります。



列	説明
モバイルデバイス名	エンドポイントのコンピュータ名。
ポリシー	エンドポイントを管理しているポリシー。
イベント	ログオン試行に失敗した回数。 Endpoint Encryption デバイスのログオンの失敗に関するレポートを表示するには、数字をクリックします。

ログオンに失敗したデバイスに関するレポート

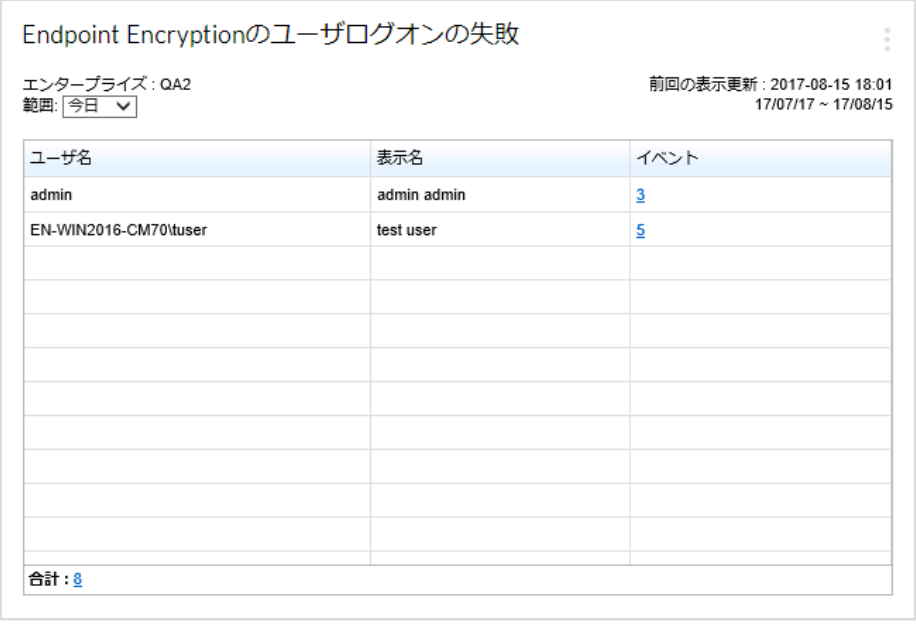
次の表は、ログオンに失敗した Endpoint Encryption デバイスに関するレポートについて示しています。このレポートを詳しく理解するために使用してください。

表 27-4. Endpoint Encryption デバイスのログオンの失敗例

ヘッダ	例	説明
イベントのタイムスタンプ	07/02/2012 01:56 pm	イベントの発生日時
ポリシー	GP1	エンドポイントを制御しているポリシーのタイトル。
モバイルデバイス名	TREND-4136D2DB3	エンドポイントが使用するコンピュータ名。
デバイス ID	1fabfbff-0001-06e5-000c-297085710000	エンドポイントにセキュリティエージェントがインストールされ、新しいエンドポイントがポリシーサーバに登録された後に確立された一意の ID。
IP アドレス	`10.1.152.219`	エンドポイントの IP アドレス。
エージェント	ディスク全体の暗号化	現在インストールされているセキュリティエージェント。
ユーザ名	user325	エンドポイントへのログオンの試行に使用されたユーザ名。
表示名	Mary Jones	Apex Central のユーザアカウントの氏名。指定されたユーザ名が有効な Apex Central ユーザ名でない場合、この列には「Not Recorded」と表示されます。
イベント	固定パスワードによるログインの失敗	記録されたイベントには認証方法が含まれます。

Endpoint Encryption のユーザログオンの失敗

Endpoint Encryption のユーザログオンの失敗ウィジェットには、Apex Central ネットワーク上の管理下のエンドポイントに対するユーザの失敗したログオン試行がすべて表示されます。



列	説明
ユーザ名	エンドポイントへのログオンの試行に使用されたユーザ名。
表示名	エンドポイントへのログオンを試行したユーザアカウントの表示名。
イベント	認証の試行回数。 数字をクリックすると、Endpoint Encryption のユーザログオンの失敗に関するレポートが表示されます。

ユーザログオンの失敗に関するレポート

次の表は、Endpoint Encryption のユーザログオンの失敗に関するレポートについて説明しています。このレポートを詳しく理解するために使用してください。

表 27-5. Endpoint Encryption のユーザログオンの失敗に関するレポートの例

ヘッダ	例	説明
イベントのタイムスタンプ	07/02/2012 01:56 pm	イベントの発生日時
ポリシー	GP1	エンドポイントを制御しているポリシーのタイトル。
モバイルデバイス名	TREND-4136D2DB3	エンドポイントが使用するコンピュータ名。
デバイス ID	1fabfbff-0001-06e5-000c-297085710000	エンドポイントにセキュリティエージェントがインストールされ、新しいエンドポイントがポリシーサーバに登録された後に確立された一意の ID。
IP アドレス	10.1.152.219	エンドポイントの IP アドレス。
エージェント	ディスク全体の暗号化	現在インストールされているセキュリティエージェント。
ユーザ名	user325	エンドポイントへのログオンの試行に使用されたユーザ名。
表示名	Mary Jones	Apex Central のユーザアカウントの氏名。指定されたユーザ名が有効な Apex Central ユーザ名でない場合、この列には「Not Recorded」と表示されます。
イベント	固定パスワードによるログインの失敗	記録されたイベントには認証方法が含まれます。

Endpoint Encryption デバイスのロックアウト

Endpoint Encryption デバイスのロックアウトウィジェットには、ポリシー制限によってロックアウトされている Apex Central デバイスが表示されます。

ヘッダ	説明
モバイルデバイス名	エンドポイントが使用するコンピュータ名。
ポリシー	エンドポイントを制御しているポリシーのタイトル。
ロックアウト日時	PolicyServer がデバイスの lock コマンドを発行したときのタイムスタンプ。実際には、エンドポイントは、Endpoint Encryption エージェントがポリシーサーバとポリシーを同期するまでロックされません。
詳細	詳細アイコンをクリックすると、Endpoint Encryption デバイスのロックアウトに関するレポートが表示されます。

ウィジェットの下部の [合計] の隣の数字をクリックすると、レポートが表示されます。

デバイスのロックアウトに関するレポート

次の表は、Endpoint Encryption デバイスのロックアウトに関するレポートについて示しています。このレポートを詳しく理解するために使用してください。

表 27-6. Endpoint Encryption デバイスのロックアウトに関するレポートの例

ヘッダ	例	説明
イベントのタイムスタンプ	07/02/2012 01:56 pm	イベントの発生日時
ポリシー	GP1	Endpoint Encryption デバイスを制御しているポリシーのタイトル。
モバイルデバイス名	TREND-4136D2DB3	Endpoint Encryption デバイスによって使用されたコンピュータ名
デバイス ID	1fabfbff-0001-06e5-000c-297085710000	エンドポイントに Endpoint Encryption エージェントがインストールされ、新しい Endpoint Encryptionr デバイスがポリシーサーバに登録された後に確立された一意の ID。
IP アドレス	10.1.152.219	Endpoint Encryption デバイスの IP アドレス。
エージェント	ディスク全体の暗号化	現在インストールされている Endpoint Encryption エージェント。
ユーザ名	user325	Endpoint Encryption デバイスへのログオンの試行に使用されたユーザ名。

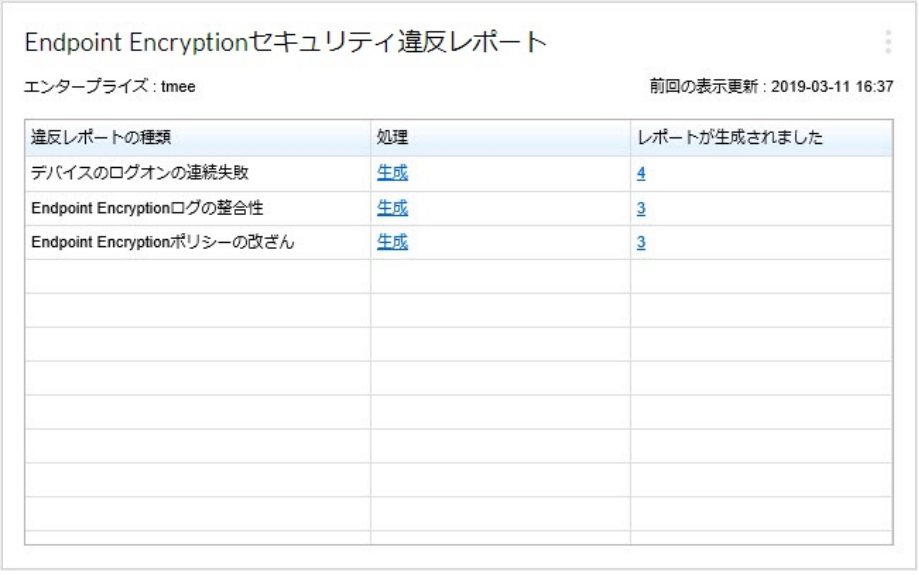
ヘッダ	例	説明
表示名	Mary Jones	Endpoint Encryption のユーザアカウントの氏名。指定されたユーザ名が有効な Endpoint Encryption ユーザ名でない場合、この列には「Not Recorded」と表示されます。
イベント	無効なログオンの試行違反のためにロックされたデバイス。	記録されたイベントには認証方法が含まれます。

Endpoint Encryption セキュリティ違反レポート

Endpoint Encryption セキュリティ違反レポートウィジェットには、次のレポートによって評価されたセキュリティ違反が表示されます。

- Endpoint Encryption デバイスのログオンの連続失敗
- Endpoint Encryption ポリシーの改ざん
- Endpoint Encryption ログの整合性

レポートを生成には、その時点で PolicyServer によって記録されているすべてのセキュリティ違反が収集されます。生成後、[レポート数] 列の数字をクリックすると、その違反について生成されたレポートが表示されます。



ヘッダ	説明
違反レポートの種類	さまざまな違反に使用可能なレポートの種類。
処理	[生成] をクリックして、新しいレポートを作成します。
レポート	当該違反について生成されたレポートの合計数。使用可能なレポートを表示するには、数をクリックします。

注意

セキュリティ違反と見なされる前のログオン試行失敗回数を指定するには、▼をクリックして [ウィジェット設定] ウィンドウを開き、[ログオンの連続失敗] テキストボックスに値を入力して、[保存] をクリックします。

デバイスのログオンの連続失敗レポート

次の表は、ログオンに連続失敗した Endpoint Encryption デバイスに関するレポートについて示しています。ログオン試行の発生時に、影響を受けた Endpoint Encryption デバイス、およびその Endpoint Encryption デバイスにユーザがログオンしようとした回数を確認するために使用します。

表 27-7. ログオンに連続失敗した Endpoint Encryption デバイスに関するレポートの例

入力	例	説明
イベントのタイムスタンプ	07/02/2012 01:56 pm	イベントの発生日時
モバイルデバイス名	TREND-4136D2DB3	Endpoint Encryption デバイスによって使用されたコンピュータ名
試行回数	5	Endpoint Encryption デバイスにユーザがログオンしようとした回数

ポリシーの改ざんレポート

次の表は、Endpoint Encryption ポリシーの改ざんレポートについて示しています。このレポートを詳しく理解するために使用してください。

表 27-8. Endpoint Encryption ポリシーの改ざんレポートの例

ヘッダ	例	説明
イベントのタイムスタンプ	07/02/2012 01:56 pm	イベントの発生日時
イベント	ポリシー値の整合性チェックに失敗しました	記録されたイベントには認証方法が含まれます。

ログ整合性レポート

次の表は、Endpoint Encryption ログの整合性レポートについて示しています。このレポートを詳しく理解するために使用してください。

表 27-9. Endpoint Encryption ログの整合性レポートの例

ヘッダ	例	説明
イベントのタイムスタンプ	07/02/2012 01:56 pm	イベントの発生日時
イベント	監査ログレコードが見つかりません	記録されたイベントには認証方法が含まれます。

第 28 章

Endpoint Encryption のポリシー設定

本章では、Apex Central コンソールで Endpoint Encryption のポリシーを設定する方法について説明します。

次のトピックがあります。

認証の概要

Endpoint Encryption によって提供される基本的な保護の形態は、暗号化されたエンドポイントやデバイスに対する不正なユーザアクセスを防ぐことです。Endpoint Encryption デバイス、ユーザ、およびポリシーグループを正しく設定することで、不慮の情報公開や意図的な妨害行為による情報漏えいのリスクを防ぐことができます。

468 ページの「デバイス」	Endpoint Encryption では、特定のデバイスに対するログオン連続試行回数と、一定期間に PolicyServer と行った最後の通信以降の時間がカウントされます。デバイスがポリシーの条件に違反した場合、そのディスクをリセット、ロック、または消去できます。
469 ページの「ユーザ」	Endpoint Encryption では、デバイスでの認証試行回数の確認に加え、特定のユーザアカウントによる連続ログオン試行回数もカウントされます。そのユーザがポリシーの条件に違反した場合、そのディスクをリセット、ロック、または消去できます。
470 ページの「グループ」	グループは、ポリシー管理のためのユーザのコンテナとして機能します。グループ内の管理者やオーセンティケータにはそのグループ内のみの特別な権限を持ちますが、割り当てられていない管理者やオーセンティケータには、エンタープライズ全体でその役割を担います。

デバイス

Endpoint Encryption バイスとは、ポリシーサーバに登録されている Endpoint Encryption エージェントです。Endpoint Encryption エージェントをインストールすると、エンドポイントは新しい Endpoint Encryption デバイスとして自動的に PolicyServer に登録されます。複数の Endpoint Encryption エージェントが指定された 1 つのエンドポイントを保護できるため、1 つのエンドポイントが PolicyServer 上に複数の Endpoint Encryption デバイスとして表示されることがあります。

ユーザがデバイスへのログインを連続して失敗すると、Endpoint Encryption はポリシー設定に応じて以下のいずれかの処理を実行します。

- 次回の認証の試行を遅らせる
- デバイスをロックする
- デバイス上のすべてのデータを消去する

注意

Endpoint Encryption デバイスを設定するには、Endpoint Encryption デバイスウィジェットを使用します。447 ページの「Endpoint Encryption デバイス」を参照してください。

ユーザ

Endpoint Encryption ユーザとは、ポリシーサーバに手動で追加されたユーザアカウント、または Active Directory と同期されたユーザアカウントです。

Endpoint Encryption には、ID に基づく包括的な認証と管理に使用される、いくつかの種類のアカウントの役割と認証方法があります。Endpoint Encryption またはポリシーサーバ MMC を使用して、ユーザアカウントの追加またはインポート、認証の制御、Active Directory との同期、ポリシーグループメンバーシップの管理を、必要に応じて実行できます。

次の表は、Endpoint Encryption ユーザの役割を示しています。

役割	説明
管理者	管理者は管理コンソールにアクセスして、ドメイン内のすべての設定を実行できます。管理者の役割が追加されたレベルに応じて、この役割にはさまざまな権限があります。 • エンタープライズ管理者: エンタープライズ内のすべてのポリシー、グループ、ユーザ、デバイスを制御できます。 • グループ管理者: 特定のグループ内で認証されたユーザおよびデバイスを制御できます。Endpoint Encryption ではポリシーごとにグループを作成するため、グループ管理者は「ポリシー管理者」とも呼ばれます。

役割	説明
オーセンティケータ	オーセンティケータは、ユーザが Endpoint Encryption のパスワードを忘れたり、技術的な問題が発生したりしたときにリモートアシスタントを提供します。オーセンティケータの役割が追加されたレベルに応じて、この役割にはさまざまな権限があります。 • エンタープライズオーセンティケータ: エンタープライズ内のすべてのユーザを支援できます。 • グループオーセンティケータ: 特定のグループ内のユーザを支援できます。Endpoint Encryption ではポリシーごとにグループが作成されるため、グループオーセンティケータは「ポリシーオーセンティケータ」とも呼ばれます。
ユーザ (アカウント)	基本的なエンドユーザには特殊な権限が付与されていません。このユーザの役割では、Endpoint Encryption 管理コンソールにログオンできない場合があります。PolicyServer で許可されていない場合、このユーザの役割ではリカバリユーティリティを使用できない可能性があります。

注意

Endpoint Encryption ユーザを設定するには、Endpoint Encryption ユーザウィジェットを使用します。440 ページの「Endpoint Encryption ユーザ」を参照してください。

グループ

Apex Central では、ポリシーはユーザグループごとに管理されます。グループの管理方法は、ポリシーサーバ MMC と Apex Central で異なります。ポリシーとグループを変更すると、PolicyServer は両方のコンソールでグループを同期します。

重要

Apex Central は、ポリシーとグループの割り当てにおいて、常にポリシーサーバ MMC より優先されます。ポリシーサーバ MMC でのグループ割り当ての変更は、Apex Central が次にポリシーサーバと同期するときに自動的に上書きされます。

コンソール	グループ管理
Apex Central	Apex Central では、特定の対象を持つポリシーが配信されるたびにグループが作成されます。配信後に、Endpoint Encryption ユーザウィジェットでユーザが含まれるグループを変更し、ポリシー管理画面でポリシー内のユーザを変更します。
PolicyServer MMC	PolicyServer MMC の左側のペインで、直接グループの追加と削除を実行します。PolicyServer MMC のグループは、次の方法で割り当てられます。 • 上位グループ: 上位グループはエンタープライズ下の最高レベルのグループです。各上位グループは、エンタープライズの下に一意のノードを持ちます。 • サブグループ: サブグループは上位グループ内に作成されます。サブグループは作成時に上位グループのポリシーを継承しますが、上位グループに加えられた変更は継承しません。サブグループに上位グループよりも多くの権限を持たせることはできません。  注意 各サブグループには、手動でデバイスとユーザを割り当てる必要があります。サブグループに Apex Central ユーザを追加しても、そのユーザは上位グループに自動的に追加されません。ただし、上位グループとサブグループの両方にユーザを追加することはできます。

 注意

Apex Central のポリシーグループ内のユーザを設定するには、Endpoint Encryption ユーザウィジェットを使用します。

PolicyServer MMC のポリシーグループ内のユーザを設定する方法については、『Endpoint Encryption PolicyServer MMC ガイド』を参照してください。

Endpoint Encryption ユーザルールを設定する

次の手順では、認証および Endpoint Encryption ユーザアカウントに影響する、ポリシールールで設定可能なオプションについて説明します。

手順

1. 新しい Endpoint Encryption ポリシーを作成します。
2. [ユーザ] をクリックします。

   ユーザポリシールールの設定画面が表示されます。

図 28-1. Endpoint Encryption ユーザポリシールール

3. ユーザがドメイン認証を必要とする場合は、[ドメインユーザ設定] の [ドメイン認証を有効にする] を選択します。

   [ドメイン認証を有効にする] を選択した場合は、Active Directory (AD) アカウントのサーバ情報を指定します。

   a. AD ドメイン名を設定します。

   b. AD サーバのホスト名を設定します。

   c. サーバの種類を次のように選択します。

      - LDAP
      - LDAP プロキシ

4. [ユーザ管理] で、ユーザアクセスを設定します。

オプション	説明
すべての Endpoint Encryption ユーザ	すべてのユーザ、ドメイン、およびローカルアカウントに、デバイスの認証を許可します。

オプション	説明
Active Directory ユーザ	AD 内の組織単位 (OU) のユーザにデバイスの認証を許可します。 **注意** [Active Directory ユーザ] オプションを有効にするには、[ドメイン認証を有効にする] を選択します。
特定ユーザの選択	すでに追加されているユーザのうち、管理対象のエンドポイントに対して認証できるユーザを指定します。 **注意** このオプションを使用して特定のユーザを選択するには、ユーザリストに入力する必要があります。[Active Directory ユーザ] オプションを使用して OU を追加するか、Endpoint Encryption ユーザウィジェットを使用してユーザを追加します。

5. [Active Directory ユーザ] を選択した場合は、識別名でポリシーに対して OU を追加します。

   [Active Directory ユーザ] を選択すると、次の追加オプションが表示されます。

オプション	説明
ユーザ名	Active Directory ユーザ名を指定します。
パスワード	Active Directory パスワードを指定します。

オプション	説明
識別名	コンマで区切られた一連の相対識別名 (RDN) によって各 OU を指定します。 例: OU=TW, DC=mycompany, DC=com OU の識別名を指定してから、[OK] をクリックします。 重要 Apex Central では、ポリシーごとに最大 12 の OU を指定できます。

ディスク全体の暗号化ルールを設定する

次の手順では、ディスク全体の暗号化デバイスに影響するポリシールールで設定可能なオプションについて説明します。

注意

Apple FileVault および Microsoft BitLocker の暗号化管理は、認証を必要とせず、認証ポリシーによる影響を受けません。クライアント、ログイン、パスワード、および認証の各ポリシーや、ユーザへの Endpoint Encryption エージェントソフトウェアのアンインストールの許可は、ディスク全体の暗号化エージェントおよびファイル暗号化エージェントにのみ影響します。

手順

1. 新しい Endpoint Encryption ポリシーを作成します。
2. [ディスク全体の暗号化] をクリックします。

ディスク全体の暗号化ポリシールールの設定画面が表示されます。

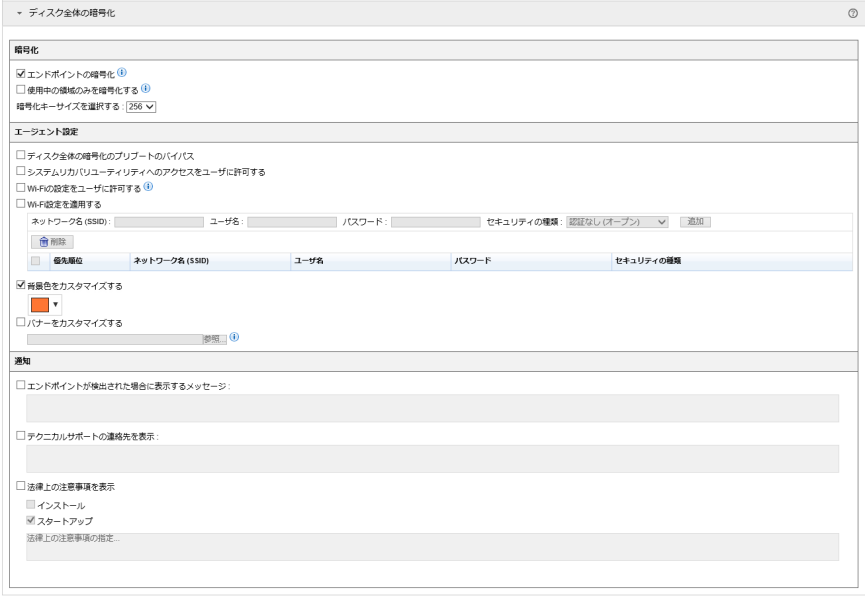


図 28-2. ディスク全体の暗号化ポリシールール

3. [暗号化] で、次のオプションを選択します。

   - [エンドポイントの暗号化] を選択して、Endpoint Encryption エージェントがポリシーサーバとポリシーを同期するときにディスク全体の暗号化を開始します。

     警告!

     ディスク全体の暗号化エージェントに暗号化を配置する前に、エンドポイントのハードドライブを準備してください。

     ハードドライブの準備の詳細については、Endpoint Encryption インストールガイドの「Full Disk Encryption Deployment Outline」を参照してください。

- [使用中の領域のみを暗号化する] を選択して、使用済みの領域のみを暗号化するようにします。
- [暗号化キーサイズを選択する] を選択して、デバイス暗号化キーサイズをビット単位で指定するようにします。

4. [エージェント設定] で、次のオプションを選択します。
   - [ディスク全体の暗号化のプリブートのバイパス] を選択して、ユーザがプリブート認証からの保護なしで直接 Windows に認証を行うことができるようにします。
   - [システムリカバリユーティリティへのアクセスをユーザに許可する] を選択して、ユーザがリカバリコンソールにアクセスできるようにします。
   - [Wi-Fi の設定をユーザに許可する] を選択して、ユーザがプリブート中にデバイスで Wi-Fi ポリシーを設定できるようにします。
   - [Wi-Fi 設定を適用する] を選択して、プリブート中にあらかじめ決められた Wi-Fi 設定を使用するようにします。次の詳細を指定します。
     - ネットワーク名 (SSID)
     - ユーザ名
     - パスワード
     - セキュリティの種類
   - [ログオン背景色の有効化] を選択して、ログオン中の背景色を指定します。
   - [ログオンバナーの有効化] を選択して、ログオンバナー画像を指定します。

     画像は 128 KB を超えないサイズで 512 x 64 ピクセルである必要があります。使用可能なファイル形式は、透過 PNG (推奨)、JPG、および GIF です。
5. [通知] で、次のオプションを設定します。

- [エンドポイントが検出された場合に表示するメッセージ] を選択して、If Found ポリシーがアクティブな場合にメッセージを表示するようにします。
- [テクニカルサポートの連絡先を表示] を選択して、ユーザがディスク全体の暗号化エージェントにログオンした後にメッセージを表示するようにします。
- [法律上の注意事項を表示] を選択して、スタートアップ時、またはディスク全体の暗号化エージェントのインストール後にのみ特定の法律上のメッセージを表示するようにします。

ファイル暗号化ルールを設定する

次の手順では、ファイル暗号化デバイスに影響するポリシールールで設定可能なオプションについて説明します。

手順

1. 新しい Endpoint Encryption ポリシーを作成します。
2. [ファイル暗号化] をクリックします。

ファイル暗号化ポリシールールの設定画面が表示されます。

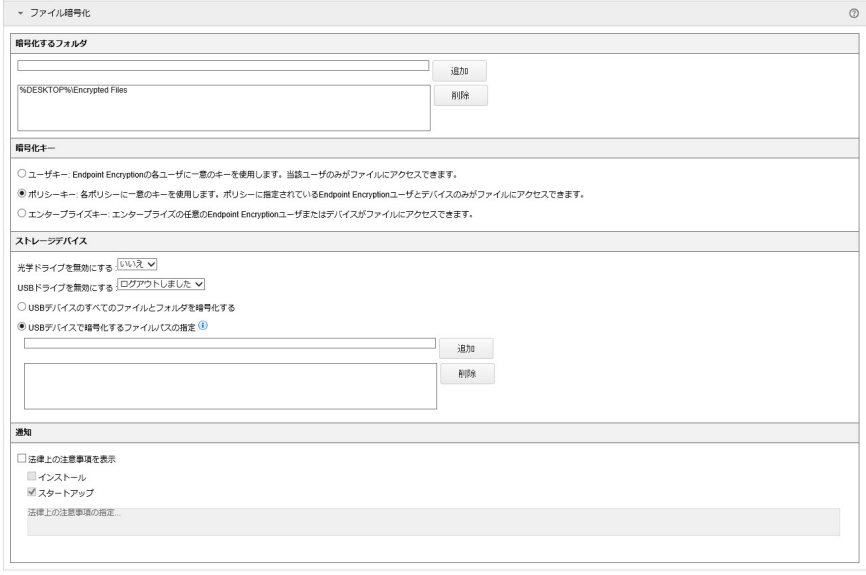


図 28-3. ファイル暗号化ポリシールール

3. [暗号化するフォルダ] で、ファイル暗号化エージェントがポリシーを同期したときに、エンドポイントで自動的に作成および暗号化されるフォルダを指定します。

4. [暗号キー] で、ファイル暗号化で暗号化されるフォルダの暗号化キーを選択します。

   - ユーザキー: Endpoint Encryption の各ユーザに一意のキーを使用します。Endpoint Encryption ユーザのみが、自身の暗号化したファイルを復号できます。
   - ポリシーキー: 各ポリシーに一意のキーを使用します。ポリシーに指定されている Endpoint Encryption ユーザとデバイスのみがファイルを復号できます。
   - エンタープライズキー: エンタープライズの任意の Endpoint Encryption ユーザまたはデバイスがファイルを復号できます。

注意

[ポリシーキー] または [エンタープライズキー] を選択すると、ファイル暗号化の共有キーの共有が制御されます。

5. [ストレージデバイス] で、次のオプションを設定します。
   - [光学ドライブを無効にする] を選択して、エンドポイントからリムーバブルメディアにアクセスできるようにするかどうかを制御します。
   - [USB ドライブを無効にする] を選択して、USB ポートを無効にするタイミングを制御します。オプションは次のとおりです。
     - 常時
     - ログアウトしました
     - 無期限
   - [USB デバイスのすべてのファイルとフォルダを暗号化する] を選択して、リムーバブルドライブがエンドポイントに接続されたときに、そのデバイス上のすべてのファイルとフォルダを自動的に暗号化するようにします。
   - [USB デバイスで暗号化するファイルパスの指定] を選択して、暗号化されるフォルダを USB ドライブに追加または USB ドライブから削除します。フォルダが存在しない場合は作成されます。ドライブ文字が指定されない場合、すべての USB デバイスが影響を受けます。
6. [通知] で、[法律上の注意事項を表示] を選択して、スタートアップ時、またはファイル暗号化エージェントのインストール後にのみ特定の法律上のメッセージを表示するようにします。

注意

通知は、Trend Micro ファイル暗号化エージェントのバージョン 3.1.3 以前でのみサポートされています。

共通ポリシールールの設定する

ここでは、すべての Endpoint Encryption デバイスに影響する、ポリシールールで設定可能なオプションについて説明します。

手順

1. 新しい Endpoint Encryption ポリシーを作成します。
2. [共通] をクリックします。

   共通ポリシールールの設定画面が表示されます。

図 28-4. 共通ポリシールール

3. [アンインストールをユーザに許可] で、[管理者以外のユーザアカウントにエージェントのアンインストールを許可] を選択して、すべての Endpoint Encryption ユーザがエージェントをアンインストールできるようにします。

注意

初期設定では、管理者アカウントのみが Endpoint Encryption エージェントをアンインストールできます。

4. [デバイスのロックアウトおよびロック処理] で、次のオプションを設定します。
   - [次の日数を経過したらアカウントをロックする <number> 日] を選択して、ポリシーが同期されない日数が何日経過したら Endpoint Encryption デバイスをロックするかを指定します。
     - [アカウントロックアウト処理] を使用して、ロックアウト時にリモート認証を行うか、消去処理を行うかを指定します。

注意

ロックオプションについては、482 ページの「ロックアウト処理」を参照してください。

   - [ログオン失敗回数の上限] を選択して、ユーザが認証を何回失敗したら Endpoint Encryption デバイスをロックするかを指定します。
   - ディスク全体の暗号化デバイスまたはファイル暗号化デバイスで、次のオプションを個別に設定します。
     - [デバイスロック処理] を使用して、ロックアウト時に「リモート認証」を行うか、「消去」処理を行うかを指定します。

注意

ロックオプションについては、482 ページの「ロックアウト処理」を参照してください。

     - [デバイスをロックする時間 (分)] を使用して、時間の遅れにより Endpoint Encryption デバイスが認証からロックされる時間を指定します。
5. [パスワード] で、次のオプションを設定します。
   - [ユーザによるパスワード変更が必要な回数 <number> 日] を選択して、ユーザにパスワードの更新を求めるタイミングを制御します。

- [ユーザの再使用不可 <number> パスワード] を選択して、ユーザが過去何回分のパスワードを再使用できないようにするかを指定します。
- [パスワードで許可される連続する文字数] を選択して、ユーザがパスワードに指定できる繰り返し文字の数を指定します。
- [パスワードで許可される最小文字数] を選択して、ユーザがパスワードに使用する必要のある文字数を指定します。

6. [パスワード文字の要件] で、パスワード文字の制限を指定します。
   - 文字
   - 小文字
   - 大文字
   - 数字
   - 記号

   重要
   文字、数字、および記号を合わせた最大数は 255 文字です。

7. [エージェント] で、[同期間隔] を分単位で指定します。

ロックアウト処理

一部のポリシーには、特定の条件に基づいてユーザアカウントをロックアウトしたり、デバイスをロックしたりする設定があります。アカウントロックアウト処理とデバイスロックアウト処理は、エージェントによってポリシーがポリシーサーバと同期されているかどうかに関係なく、Endpoint Encryption デバイスに影響します。たとえば、Endpoint Encryption エージェントが一定期間ポリシーサーバと通信していない場合、Endpoint Encryption エージェントは、Endpoint Encryption デバイスを自動的にロックします。次の表で、アカウントロックアウト処理とデバイスロック処理で使用できる処理について説明します。

次の表は、ロックアウト処理の実行時期について示しています。

種類	説明
アカウントロックアウト	Endpoint Encryption エージェントがポリシーで設定されている一定期間ポリシーサーバと通信していないと、アカウントロックアウト処理が有効になります。
ディスク全体の暗号化デバイスのロックアウト	Endpoint Encryption ユーザによるディスク全体の暗号化デバイスへのログオン試行の失敗回数が、ポリシーで指定されている上限回数を超えると、ディスク全体の暗号化デバイスのロックアウト処理が有効になります。
ファイル暗号化デバイスのロックアウト	Endpoint Encryption ユーザによるファイル暗号化デバイスへのログオン試行の失敗回数が、ポリシーで指定されている上限回数を超えると、ファイル暗号化デバイスのロックアウト処理が有効になります。

ロックアウト処理のオプションは次のとおりです。

処理	説明
消去	ポリシーサーバは、関連する Endpoint Encryption エージェントが制御するすべてのデータを消去します。 警告! Endpoint Encryption ユーザは、消去されたデータを復元できません。
リモート認証	Endpoint Encryption のユーザ担当者がオーセンティケータまたはサポートからリモートヘルプ認証を受信するまで、ポリシーサーバは Endpoint Encryption デバイスをロックします。
時間の遅れ	ポリシーサーバは Endpoint Encryption デバイスを一時的にロックし、Endpoint Encryption ユーザにデバイスがロックされていることを通知します。時間の遅れの間にパスワードの認証/リセット機能は無効になります。時間の遅れの期間はポリシーによって決定されます。時間の遅れの期間が終了すると、ユーザは認証を許可されます。

Apex Central にグループを移行する

次の手順を使用して、既存のグループをポリシーサーバ MMC から Apex Central に追加します。

手順

1. PolicyServer MMC にログオンします。
2. 次の情報を収集します。
   - グループの合計数、そのグループの名前、サブグループ
   - 各グループに割り当てられたすべてのユーザ
   - 各グループのポリシー設定
3. Apex Central にログオンします。
4. PolicyServer MMC のグループごとに、対応するグループポリシー設定に一致する新しいポリシーを設定します。

   注意

   サブグループは Apex Central ではサポートされていません。サブグループポリシー設定を複製するには、サブグループごとに個別のポリシーを作成します。

5. ユーザをそれぞれの対応する新しいポリシーに追加します。
6. 各ポリシーを配信します。

パート XII

Endpoint Sensor のウィジェットとポリシー

第 29 章

Trend Micro Endpoint Sensor のダッシュボードウィジェット

本章では、Apex Central でサポートされる Trend Micro Endpoint Sensor のダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

Endpoint Sensor の調査

Endpoint Sensor の調査ウィジェットは、リモートの Trend Micro Endpoint Sensor サーバに接続して調査を開始し、Apex Central ダッシュボードからこの調査の結果を直接表示します。

[新しい調査を開始] をクリックして新しい調査を開始し、次に調査方法を選択します。

- 履歴レコード: ユーザ定義の基準に基づいて履歴イベントを調査します。
- システムスナップショット: 選択したエンドポイントの現在の状態を調査します。

[新しい調査] 画面が表示されたら、必要な条件を入力します。次の調査の種類があります。

調査の種類	説明
履歴検索 - Retro Scan	ユーザ定義の基準に基づく履歴イベントの調査
履歴検索 - IOC ルール	IOC ルールを使用した履歴イベントの調査
システムスナップショット- レジストリ検索	Windows レジストリの調査
システムスナップショット - YARA ルール	YARA ルールを使用した、メモリ常駐型の脅威の調査
システムスナップショット - IOC ルール	IOC ルールを使用したイベントの調査
システムスナップショット - ディスク IOC ルール	IOC ルールを使用したファイルの調査
システムスナップショット - システム監査	現在実行中のすべてのプロセス、サービス、およびモジュールの調査

[調査] をクリックして調査を開始します。継続中の調査を停止するには、[キャンセル] をクリックします。

ウィジェットの表示が定期的に更新され、調査の進捗状況が表示されます。このウィジェットには、次のように分類された合計エンドポイント数を視覚的に表す円グラフが表示されます。

- 一致: 一致するオブジェクトが見つかったエンドポイント数を示します。
- 安全: 一致するオブジェクトが見つからなかったエンドポイント数を示します。
- 保留: まだ調査が完了していないエンドポイント数を示します。
- キャンセル: 次のいずれかの基準に合致するエンドポイント数を示します。
  - エンドポイントで実行された調査でエラーが発生した
  - エンドポイントがオフラインであるか、エンドポイント宛てに送信したすべてのコマンドがタイムアウトになった
  - エンドポイントの調査がユーザによって手動で中断された

円グラフの右側に総数の内訳が表示されます。各分類の数をクリックすると、[調査結果] 画面が表示されます。この画面には、Apex Central から開始された最新の調査結果に関する詳細が表示されます。

注意

- サーバが追加されたら、ウィジェットを更新し、新しいサーバからのデータ取得を開始します。
- 複数のサーバを追加した場合、すべてのサーバのデータの集計結果が表示されます。

インテリジェント監視概要 (ホスト別)

このウィジェットは、最新の監視ルールが実行されたエンドポイントの概要を表示します。データは、Trend Micro Endpoint Sensor サーバダッシュボードの[インテリジェント監視概要 (ホスト別)]ウィジェットから取得されます。

列名	説明
ホスト名	エンドポイントのホスト名
ヒット数	エンドポイントで実行された一致するルールの数 クリックすると、エンドポイントで実行されたルールの詳細が表示されます。
ルールのカテゴリ	標的型攻撃の 6 つのステージに基づく分類
検出時刻	ルールが最後にエンドポイントで実行された日時

この時間の初期設定は過去 24 時間です。必要に応じて期間を変更してください。

注意

- このウィジェットを使用するには、Trend Micro Endpoint Sensor サーバへの接続を確立する必要があります。サーバが追加されたら、ウィジェットを更新し、新しいサーバからのデータ取得を開始します。
- 複数のサーバを追加した場合、すべてのサーバのデータの集計結果が表示されます。

Dwell Time で報告された重大な脅威ウィジェット

このウィジェットには、影響を受けたユーザのエンドポイント上に脅威が存在していた期間に基づく重大な脅威の概要が表示されます。

重要

このウィジェットを使用するには、登録済みの Trend Micro Endpoint Sensor サーバが必要です。ウィジェットには、重大な脅威と見なされるファイルの SHA-1 値に基づいて、Trend Micro Endpoint Sensor サーバによって実行された影響診断の結果が表示されます。

[緩和されていない脅威のみを表示します] を選択すると、修復が必要な重大な脅威だけを表示できます。

列の見出しをクリックすると、表内のデータが並べ替えられます。

列	説明
ファイル名	重大な脅威が検出されたファイル名を表示します。 追加の脅威情報を表示したり、追加の調査を実行したりするには、ファイル名をクリックします。
影響を受けたユーザ	影響を受けたユーザの名前が表示されます。
修復	トレンドマイクロ製品によって実行された修復処理が表示されます。
Dwell Time	影響を受けたユーザのエンドポイントに脅威が存在していた時間の長さが表示されます。

[消去済みのアラートの表示] をクリックすると [アラート消去] 画面が開き、Apex Central ユーザアカウントによって手動で消去された重大な脅威アラートのみに関する情報が表示されます。

列	説明
消去	重大な脅威アラートが消去された時間が表示されます。
ファイル名	重大な脅威が検出されたファイル名を表示します。 追加の脅威情報を表示したり、追加の調査を実行したりするには、ファイル名をクリックします。

列	説明
影響を受けたユーザ	影響を受けたユーザの名前が表示されます。
Dwell Time	影響を受けたユーザのエンドポイントに脅威が存在していた時間の長さが表示されます。
消去したユーザ	重大な脅威アラートを消去した Apex Central ユーザアカウントが表示されます。

第 30 章

Trend Micro Endpoint Sensor の統合とポリシー設定

本章では、Apex Central と Trend Micro Endpoint Sensor を統合し、Apex Central のコンソールでポリシーを管理する方法について説明します。

次のトピックがあります。

Endpoint Sensor の統合

Apex Central をスタンドアロンの Endpoint Sensor サーバと統合すると、次の機能を使用できます。

- アップロードされた Apex Central の IOC ファイルを使用して、Apex Central 管理コンソールから Endpoint Sensor に対する直接の調査を開始します。
- 複数の Endpoint Sensor サーバを登録します。複数の Endpoint Sensor サーバで同時に調査を開始できます。
- Endpoint Sensor の調査結果からデータを取得します。データは Apex Central ウィジェットに表示されます。
- ポリシーを作成し、Apex Central に登録された Endpoint Sensor サーバに配信します。
- Apex Central の監視ルールを管理します。
- 送信設定を実行し、Apex Central に登録された Endpoint Sensor サーバに配信します。

Apex Central に登録する

手順

1. Apex Central 管理コンソールを開きます。

   ネットワーク上の任意のエンドポイントで Apex Central 管理コンソールを開くには、Web ブラウザを起動して次を入力します。

   ```
   https:// <Apex Central サーバ名> /Webapp/index.html
   ```

   <Apex Central サーバ名>には、Apex Central サーバの IP アドレスまたはホスト名を入力します。

2. [運用管理] > [管理下のサーバ] > [サーバの登録] に移動します。
3. 表示される画面の [サーバの種類] で [Trend Micro Endpoint Sensor] を選択し、次に [追加] をクリックします。
4. [サーバの追加] 画面で、次の情報を入力します。

- サーバ
- 表示名
- ユーザ名
- パスワード

5. [保存] をクリックするとサーバがリストに追加されます。サーバごとにこの手順を繰り返します。

Endpoint Sensor ウィジェットを追加する

手順

1. Apex Central 管理コンソールを開きます。

   ネットワーク上の任意のエンドポイントで Apex Central 管理コンソールコンソールを開くには、Web ブラウザを起動して次を入力します。

   ```
   https:// <Apex Central サーバ名> /Webapp/index.html
   ```

   <Apex Central サーバ名>には、Apex Central サーバの IP アドレスまたはホスト名を入力します。

2. [運用管理] > [管理下のサーバ] > [サーバの登録] に移動します。
3. 表示される画面の [サーバの種類] で [Trend Micro Endpoint Sensor] を選択し、次に [追加] をクリックします。
4. 追加するサーバの詳細を指定し、[保存] をクリックします。
5. [ダッシュボード] に移動します。
6. 既存のタブを選択するか、または新規のタブを作成します。
7. タブ表示の右にある [設定] ボタンをクリックします。
8. [ウィジェットの追加] をクリックします。
9. 表示された画面で、リストから [Endpoint Sensor] カテゴリを選択します。

   次のウィジェットがあります。

表 30-1. Endpoint Sensor のウィジェット

ウィジェット名	説明
インテリジェント監視概要 (ホスト別)	監視ルールがトリガされたエンドポイントを表示します。最新データを表示するには、ウィジェットを手動で更新します。ウィジェットを設定するには、[▾] をクリックします。
Endpoint Sensor の調査	調査を実行し、Apex Central から開始された最新の Trend Micro Endpoint Sensor の調査の概要を表示します。初期設定では、ウィジェットは自動的に 2 分ごとに更新されます。ウィジェットを設定するには、[▾] をクリックします。 詳細については、『Trend Micro Endpoint Sensor サーバの管理者ガイド』を参照してください。

10. 一方または両方のウィジェットを選択し、[追加] をクリックします。

    追加したウィジェットが [ダッシュボード] に表示されます。これらのウィジェットには、最新の調査の概要と、すべての登録済みサーバの監視結果が表示されます。

注意

新しい Endpoint Sensor サーバを登録した後で、[Endpoint Sensor の調査] ウィジェットと [インテリジェント監視概要 (ホスト別)] ウィジェットを更新し、新しいサーバのデータを使用してウィジェットのコンテンツをアップデートします。

Apex Central を使用してステータスを確認する

製品の接続ステータスウィジェットとエージェントの接続ステータスウィジェットを使用して、登録済みの Endpoint Sensor サーバまたはエージェントのステータスを確認できます。これらのウィジェットには、[運用管理] > [管理下のサーバ] > [サーバの登録] 画面で追加された Endpoint Sensor サーバの情報が表示されます。

手順

1. [ダッシュボード] に移動します。

2. [コンプライアンス] タブをクリックして以下のウィジェットを確認します。

   注意

   製品の接続ステータスは、[概要] タブにも表示されます。

   - 製品の接続ステータス: [ステータス] 列にサーバのステータスが表示されます。

     [詳細の表示] をクリックすると、サーバについての詳細情報を確認できます。

   - エージェントの接続ステータス: 各サーバのエージェント、オンラインのエージェント、オフラインのエージェントの総数が表示されます。

     [オンライン] 列、[オフライン] 列、または [合計] 列の値をクリックすると、エージェントについての詳細情報が表示されます。

3. 以下の手順でウィジェットをタブに追加します。

   a. 既存のタブに移動するか、または新規のタブを作成します。

   b. タブ表示の右にある [設定] ボタンをクリックします。

   c. [ウィジェットの追加] をクリックします。

   d. [ウィジェットの追加] 画面で、[コンプライアンス] カテゴリを選択します。

   e. [エージェントの接続ステータス] または [製品の接続ステータス] を選択して、

   f. [追加] をクリックします。

      これで追加したウィジェットが現在のタブに表示されます。

Endpoint Sensor の調査ウィジェットを使用する

手順

1. Apex Central 管理コンソールを開きます。
2. Endpoint Sensor の調査ウィジェットが追加されたタブに移動します。
3. Endpoint Sensor の調査ウィジェットで、[新しい調査を開始] をクリックし、実行する予定の調査の種類に応じて [履歴レコード] か [システムスナップショット] をクリックします。
4. 表示される画面で、必要な情報を指定します。

   また、Endpoint Sensor の調査ウィジェットでは、調査条件として C&C コールバックイベントのインポートをサポートします。

   a. Endpoint Sensor の調査ウィジェットで、[新しい調査を開始] > [履歴レコード] をクリックします。

   b. 調査方法として [Retro Scan] を選択します。

   c. [C&C コールバックイベントからインポート] をクリックします。

   d. 表示される画面で、調査する必要がある C&C コールバックイベントを選択して、[OK] をクリックします。イベントが調査条件として追加されます。
5. [調査] をクリックします。

   画面の表示が更新され、調査の進行状況が表示されます。

   注意

   継続中の調査を停止するには、[キャンセル] をクリックします。
6. 調査が終了すると、調査中に [一致]、[安全]、[保留中]、または [キャンセル] に分類されたエンドポイントの数がウィジェットに表示されます。詳細を表示するには、各調査の結果をクリックします。

自動アップデートを使用する

Apex Central を Endpoint Sensor のローカルアップデートサーバとして使用するには、次の手順を実行します。

手順

1. Apex Central で自動アップデートを設定します。
   a. Apex Central 管理コンソールを開きます。
   b. [運用管理] > [アップデート] > [予約アップデート] に移動します。
   c. 次のパターンファイルを探します。
      - Endpoint Sensor 除外パターンファイル
      - Endpoint Sensor 信頼済みパターンファイル
      - Attack Discovery パターンファイル
   d. パターンファイルごとに、パターンファイル名をクリックして、[予約ダウンロードを有効にする] を選択します。それ以外はすべて初期設定のままにします。

      注意

      Endpoint Sensor integration については、[自動配信設定] はサポートされていません。

   e. [保存] をクリックします。
2. Apex Central をアップデート元として使用するように Endpoint Sensor を設定します。
   a. Endpoint Sensor サーバの管理コンソールを開きます。
   b. [運用管理] > [アップデート] の順にクリックします。
   c. [次のアップデート元から監視ルールをダウンロードします] を有効にします。
   d. [その他のアップデート元] を選択して、下のテキストボックスに次のように入力します。

```
http://<Apex Central サーバ名>/TVCSDownload/Activeupdate
```

e. [保存] をクリックします。

次の予約アップデート時に、Apex Central には Endpoint Sensor パターンファイルが含まれます。その後、Endpoint Sensor は、次の予約アップデート時にこれらのパターンファイルを Apex Central からダウンロードします。

Trend Micro Endpoint Sensor ポリシー

Apex Central には、管理者がリモートで登録済みサーバの監視ルールを更新したり送信設定を行ったりできるようにするポリシー管理機能が用意されています。

注意

複数の Endpoint Sensor ポリシーを作成できますが、各サーバが一度に発行できるポリシーは 1 つに限られます。

詳細については、以下の Web サイトにアクセスして、Apex Central のドキュメントを参照してください。

http://docs.trendmicro.com/ja-jp/enterprise/apex-central.aspx

---

ポリシーを配信するためにサーバを準備する

初期設定では、追加された最新の Endpoint Sensor サーバは [新規エンティティ] フォルダに配置されます。ポリシーの配信用にサーバを表示するには、別のフォルダに移動する必要があります。

手順

1. Apex Central 管理コンソールを開きます。
2. [ディレクトリ] > [製品] に移動して、[ディレクトリ管理] をクリックします。
3. ディレクトリツリーで、[新規エンティティ] フォルダを展開して対象サーバを見つけます。

4. 次のいずれかを実行します。
   - サーバを別のフォルダにドラッグアンドドロップします。
   - [フォルダの追加] をクリックして新しいフォルダを作成し、サーバを新しいフォルダにドラッグアンドドロップします。

ポリシーを作成して配信する

手順

1. Apex Central 管理コンソールを開きます。
2. [ポリシー] > [ポリシー管理] に移動します。
3. [製品] ドロップダウンリストで [Trend Micro Endpoint Sensor] を選択します。
4. [作成] をクリックします。
5. [対象の指定] をクリックして、配信先となる Endpoint Sensor サーバを選択します。
6. [監視設定] セクションで監視ルールを設定し、新しいポリシーの送信設定を行います。
7. ポリシーの配信をただちに開始するには、[配信] をクリックします。

   その後、対象の Endpoint Sensor サーバでは、24 時間ごとに Apex Central によってポリシーに対する以降のアップデートが適用されます。

   詳細については、以下の Web サイトにアクセスして、Apex Central のドキュメントを参照してください。

   http://docs.trendmicro.com/ja-jp/enterprise/apex-central.aspx

監視ルールを管理する

次の留意点について確認してください。

- 監視ルールの管理:

  [Monitoring Rules] タブにはユーザ指定のルールのみが表示されます。監視ルールが複数のポリシーで共有されている場合、監視ルールのステ

ータス (有効/無効/削除) はポリシーごとに異なります。管理者は、有効化、無効化、または削除する監視ルールをポリシーごとに選択することでポリシーをカスタマイズできます。新しい監視ルールは初期設定で無効になっています。

Apex Central では、監視ルールが Endpoint Sensor ポリシーに含まれる Endpoint Sensor サーバでその監視ルールをリモートからのみ制御できます。

新しい Endpoint Sensor サーバが登録されると、Apex Central では、その Endpoint Sensor サーバがルール配信スケジュールに自動的に組み込まれます。次回の配信スケジュールの実行時、アクティブな監視ルールがすべて、Apex Central から新規登録サーバにアップロードされます。

- 監視ルールのアップロード:

  監視ルールをアップロードするには、[ポリシー] > [ポリシー管理] の順にクリックして、[製品] に [Trend Micro Endpoint Sensor] を選択します。[作成] をクリックして新しいポリシーを作成するか、既存のポリシーをクリックして [ポリシーの作成] または [ポリシーの編集] 画面を表示します。[監視設定] を展開し、[IOC ルールをアップロードする] > [ファイルを選択] の順にクリックして、監視ルールの場所に移動します。[開く] をクリックして監視ルールを自動的にアップロードします。アップロードが完了したら、[保存] または [配信] をクリックします。

  注意

  - ルールをアップロードする前に、アップロード先の Endpoint Sensor サーバを指定することをお勧めします。
  - [IOC ルールをアップロードする] 機能は、Endpoint Sensor サーバが少なくとも 1 つ Apex Central に登録されている場合にのみ有効になります。

  Apex Central と、Apex Central に登録された Endpoint Sensor サーバの両方に同じ監視ルールをアップロードすると競合が発生することがあります。アップロードした監視ルールを [監視設定] 画面で定期的に追跡することで重複を回避できます。

監視ルールが重複している場合は、次のメッセージが表示されます。「ファイルをアップロードできません。このファイルは Endpoint Sensor サーバにすでに存在します。Endpoint Sensor 管理コンソールでファイルを削除してから、再度実行してください。」

- 監視ルールのステータスの変更:

  監視ルールのステータスを変更するには、[Toggle Status] をクリックして [Enable] または [Disable] を選択します。その後、このポリシーに対象として指定されている Endpoint Sensor サーバのリモートルールをアップデートします。

  監視ルールのステータスはポリシーごとに異なります。

- 監視ルールの削除:

  ルールを削除するには、ルールを選択して [Remove] をクリックします。削除したルールのステータスが [remove] に変更されます。[保存] または [配信] をクリックして操作を完了します。

警告!

- 削除した監視ルールは、他のすべての Endpoint Sensor ポリシーからも削除されます。
- 新しいポリシーで同じルールを再度アップロードすると、予約実行時に古いポリシーによってそのルールが再度削除されます。

問題が解決しない場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。

送信設定を管理する

[送信設定] タブでは、収集されたファイルをユーザが指定した UNC パス上にあるファイルサーバに送信する設定や、さらなる調査のために Deep Discovery Analyzer に送信する設定ができます。

Apex Central は、Endpoint Sensor エンドポイントと Deep Discovery Analyzer の間のプロキシ接続を設定できません。Endpoint Sensor エンドポイントと Deep Discovery Analyzer の間のプロキシ接続を設定するには、Endpoint Sensor サーバコンピュータの [プロキシ] 画面を使用します。

パート XIII

InterScan のセキュリティポリシー

第 31 章

InterScan Messaging Security Suite ポリシー設定

本章では、Apex Central で InterScan Messaging Security Suite ポリシーを設定する方法について説明します。

次のトピックがあります。

IMSS ルール

InterScan Messaging Security Suite (IMSS) は、定義されたルールセットに基づいてメールメッセージのデータを評価します。 ルールによって、不正な転送から保護する必要があるデータが判別され、転送の検出時に IMSS が実行する処理が決定されます。

IMSS ルールには、次のコンポーネントがあります。

- メールルート:送信者および受信者の一連のメールアドレスまたはグループ、あるいはポリシーの適用先の LDAP ユーザまたはグループ。アスタリスク (*) を使用して、ワイルドカード表現を作成し、ルート設定を簡素化できます。
- フィルタ:特定のルートに適用するルールまたはルールのセット。In Apex Central では、テンプレートを使用してデータ損失を保護するルールを設定できます。
- 処理:フィルタ条件が満たされた場合に IMSS が実行する処理。

IMSS ルールを追加する

ルールを作成するには、次の手順に従ってください。

- 手順 1: ルール名を設定
- 手順 2: 受信者と送信者を選択
- 手順 3: テンプレートを選択
- 手順 4: 処理を選択

手順

1. [設定] で [追加] をクリックします。

   [ルールの追加] 画面が表示されます。

手順 1: ルール名を設定

手順

1. ルールの名前を入力します。名前の長さは、122 バイト以下でなければなりません。
2. ルールの階層内の位置を表す優先順位を割り当てます。
3. [次へ] をクリックします。

   [受信者と送信者を選択する] 画面が表示されます。

手順 2: 受信者と送信者を選択

送信者および受信者のメールアドレスまたはグループ、あるいはルールの適用先の LDAP ユーザまたはグループを設定します。メールルートの除外も設定できます。

手順

1. [宛先:] または [送信元:] の横のリンクをクリックします。

   [受信者の設定] 画面または [送信者の設定] 画面が表示されます。
2. 次のいずれかを選択してください。
   - すべてのユーザ:このオプションを選択すると、受信者または送信者に関するあらゆる制限が解除されます。
   - 選択したアドレス
3. [選択したアドレス] を選択した場合、リストボックスから次のいずれかを選択します。
   - メールアドレスを入力:追加するメールアドレスを入力します。
   - LDAP ユーザまたはグループの検索:LDAP ユーザ名またはグループ名を入力し、[検索] をクリックします。リストボックスに結果が表示されます。
   - アドレスグループの選択: 既存のすべてのアドレスグループがリストに表示されます。

Microsoft Active Directory または Sun iPlanet Directory を LDAP サーバとして指定している場合、LDAP グループを受信者または送信者として選択するときに、LDAP グループの先頭と末尾のいずれかまたは両方でワイルドカードを使用できます。

詳細については、「アスタリスクワイルドカードの使用」を参照してください。511 ページの

4. メールアドレスを追加する場合、[追加 >] をクリックします。LDAP ユーザまたはグループ、あるいはアドレスグループを追加する場合、リストボックスでこれをクリックしてから [追加 >] をクリックします。
5. [保存] をクリックします。
6. [次へ] をクリックします。

   [手順 3: テンプレートを選択する] 画面が表示されます。

除外を設定する

送信者または受信者の大人数のグループに適用するルートの設定では、ルールを適用しない特定のユーザを例外として指定できます。

手順

1. [除外] の横の [送信者と受信者] をクリックします。

   [除外の設定] 画面が表示されます。
2. [アドレスの選択] で、[差出人（送信者）] と [宛先（受信者）] の両方に対して次のいずれかを選択します。
   - メールアドレスを入力:追加するメールアドレスを入力します。
   - LDAP ユーザまたはグループの検索: LDAP ユーザ名またはグループ名を入力し、[検索] をクリックします。リストボックスに結果が表示されます。
   - アドレスグループの選択: 既存のすべてのアドレスグループがリストに表示されます。

3. メールアドレスを追加する場合、[追加 >] をクリックします。LDAP ユーザまたはグループ、あるいはアドレスグループを追加する場合、リストボックスでこれをクリックしてから [追加 >] をクリックします。
4. [保存] をクリックします。

アスタリスクワイルドカードを使用する

ルートを定義するときに、メールアドレスでワイルドカードとしてアスタリスク (*) を使用できます。

ワイルドカードは、メールアドレスの名前またはドメインのセクションで使用できます。次に有効な例を示します。

- *@*: すべてのメールアドレスを表す例。
- *@domain.tld、name@*.tld: 名前全体またはドメインを表す例 (トップレベルドメイン (TLD) ではない)。
- *@*.tld: 名前とドメインの両方を表す例 (TLD ではない)。

ワイルドカードは、サブドメインまたはトップレベルドメインでは使用できません。またワイルドカードは、他の文字とともに使用することはできません。単独で使用する必要があります。次に無効な例を示します。

- name@domain.*.tld: サブドメインで使用されるため無効。
- name@domain.*: TLD で使用されるため無効。
- *name@domain.tld: 名前とともに使用しているため無効。

手順 3: テンプレートを選択

テンプレートを使用すると、デジタル資産 (社会保障番号、クレジットカード番号など) が会社のネットワークに残らないようになります。プライバシーに関する政府の規制を遵守するようにもなります。

手順

1. [利用可能なテンプレート] リストからテンプレートを選択し、[>>] をクリックします。

ヒント

複数のテンプレートを選択するには、<Ctrl> キーを押しながらテンプレートを選択します。

2. [次へ] をクリックします。

   [手順 4: 処理を選択する] 画面が表示されます。

手順 4: 処理を選択

IMSS は、デジタル資産を送信しようとしたことを検出すると、1 つ以上の処理を実行します。

手順

1. 次の処理のいずれかを選択します。
   - 隔離先:メッセージがインターセプトされ、受信者に到達しないようにします。
   - 通知の送信:1 人以上の受信者にメール通知を送信します。
2. [通知の送信] を選択した場合、ドロップダウンリストから使用する通知メッセージの種類を選択します。使用できる通知メッセージは、選択した対象によって異なります。
3. [完了] をクリックします。

既存の IMSS ルールを変更する

手順

1. 編集するルールの名前をクリックします。

   ルールの [概要] 画面が表示されます。

2. [ルール] タブで、[受信者と送信者] の [編集] をクリックします。
3. ルートを設定します。

詳細については、509 ページの「手順 2: 受信者と送信者を選択する」を参照してください。

4. [検索条件] の [編集] をクリックします。
5. テンプレートを設定します。
6. [処理] の [編集] をクリックします。
7. 処理を設定します。

注意

Apex Central が、選択済みの対象に接続できない場合、一部の処理オプションは使用できなくなります。

8. [保存] をクリックします。

IMSS ルールを削除する

手順

1. 削除するルールの横のチェックボックスをオンにします。
2. [削除] をクリックします。

第 32 章

InterScan Messaging Security Virtual Appliance ポリシー設定

本章では、Apex Central で InterScan Messaging Security Virtual Appliance ポリシーを設定する方法について説明します。

次のトピックがあります。

IMSVA 情報漏えい対策のポリシー

InterScan Messaging Security Virtual Appliance (IMSVA) は、定義されたルールセットに基づいてメールメッセージのデータを評価します。ルールによって、不正な転送から保護する必要があるデータが判別され、転送の検出時に IMSVA が実行する処理が決定されます。

IMSVA 情報漏えい対策のポリシーには、次のコンポーネントがあります。

- メールルート:送信者および受信者の一連のメールアドレスまたはグループ、あるいはポリシーの適用先の LDAP ユーザまたはグループ。アスタリスク (*) を使用して、ワイルドカード表現を作成し、ルート設定を簡素化できます。
- フィルタ:特定のルートに適用するルールまたはルールのセット。Apex Central では、テンプレートを使用してデータ損失を保護するルールを設定できます。
- 処理:フィルタ条件が満たされた場合に IMSVA が実行する処理。

ルールを追加する

ルールを作成するには、次の手順に従ってください。

- 手順 1: ルール名を設定
- 手順 2: 受信者と送信者を選択
- 手順 3: テンプレートを選択
- 手順 4: 処理を選択

手順

1. [設定] で [追加] をクリックします。

   [ルールの追加] 画面が表示されます。

手順 1: ルール名を設定

手順

1. ルールの名前を入力します。名前の長さは、122 バイト以下でなければなりません。
2. ルールの階層内の位置を表す優先順位を割り当てます。
3. [次へ] をクリックします。

   [受信者と送信者を選択する] 画面が表示されます。

手順 2: 受信者と送信者を選択

送信者および受信者のメールアドレスまたはグループ、あるいはルールの適用先の LDAP ユーザまたはグループを設定します。メールルートの除外も設定できます。

手順

1. [宛先:] または [送信元:] の横のリンクをクリックします。

   [受信者の設定] 画面または [送信者の設定] 画面が表示されます。
2. 次のいずれかを選択してください。
   - すべてのユーザ:このオプションを選択すると、受信者または送信者に関するあらゆる制限が解除されます。
   - 選択したアドレス
3. [選択したアドレス] を選択した場合、リストボックスから次のいずれかを選択します。
   - メールアドレスを入力:追加するメールアドレスを入力します。
   - LDAP ユーザまたはグループの検索:LDAP ユーザ名またはグループ名を入力し、[検索] をクリックします。リストボックスに結果が表示されます。
   - アドレスグループの選択: 既存のすべてのアドレスグループがリストに表示されます。

Microsoft Active Directory または Sun iPlanet Directory を LDAP サーバとして指定している場合、LDAP グループを受信者または送信者として選択するときに、LDAP グループの先頭と末尾のいずれかまたは両方でワイルドカードを使用できます。詳細については、「アスタリスクワイルドカードの使用」を参照してください。

4. メールアドレスを追加する場合、[追加 >] をクリックします。LDAP ユーザまたはグループ、あるいはアドレスグループを追加する場合、リストボックスでこれをクリックしてから [追加 >] をクリックします。
5. [保存] をクリックします。
6. [次へ] をクリックします。

   [手順 3: テンプレートを選択する] 画面が表示されます。

除外を設定する

送信者または受信者の大人数のグループに適用するルートの設定では、ルールを適用しない特定のユーザを例外として指定できます。

手順

1. [除外] の横のリンクをクリックします。

   [除外の設定] 画面が表示されます。
2. [アドレスの選択] で、送信元アドレスと送信先アドレスの両方に対して次のいずれかを選択します。
   - メールアドレスを入力:追加するメールアドレスを入力します。
   - LDAP ユーザまたはグループの検索: LDAP ユーザ名またはグループ名を入力し、[検索] をクリックします。リストボックスに結果が表示されます。
   - アドレスグループの選択: 既存のすべてのアドレスグループがリストに表示されます。
3. メールアドレスを追加する場合、[追加 >] をクリックします。LDAP またはアドレスグループを追加する場合、リストボックスでこれをクリックしてから [追加 >] をクリックします。

4. [保存] をクリックします。

アスタリスクワイルドカードを使用する

ルートを定義するときに、メールアドレスでワイルドカードとしてアスタリスク (*) を使用できます。

ワイルドカードは、メールアドレスの名前またはドメインのセクションで使用できます。次に有効な例を示します。

- *@*: すべてのメールアドレスを表す例。
- *@domain.tld、name@*.tld: 名前全体またはドメインを表す例 (トップレベルドメイン (TLD) ではない)。
- *@*.tld: 名前とドメインの両方を表す例 (TLD ではない)。

ワイルドカードは、サブドメインまたはトップレベルドメインでは使用できません。またワイルドカードは、他の文字とともに使用することはできません。単独で使用する必要があります。次に無効な例を示します。

- name@domain.*.tld: サブドメインで使用されるため無効。
- name@domain.*: TLD で使用されるため無効。
- *name@domain.tld: 名前とともに使用しているため無効。

手順 3: テンプレートを選択

テンプレートを使用すると、デジタル資産 (社会保障番号、クレジットカード番号など) が不正な転送から保護されます。また、プライバシーに関する政府の規制を遵守するように設定することもできます。

手順

1. [利用可能なテンプレート] リストからテンプレートを選択し、[>>] をクリックします。

   [Ctrl] キーを押しながらテンプレートを選択することで複数のテンプレートを選択できます。

2. [次へ] をクリックします。

[手順 4: 処理を選択する] 画面が表示されます。

手順 4: 処理を選択

IMSVA は、デジタル資産を送信しようとしたことを検出すると、1 つ以上の処理を実行します。

手順

1. 次の処理のいずれかを選択します。
   - 隔離先:メッセージがインターセプトされ、受信者に到達しないようにします。
   - 通知の送信:1 人以上の受信者にメール通知を送信します。
2. [通知の送信] を選択した場合、ドロップダウンリストから使用する通知メッセージの種類を選択します。

   使用できる通知メッセージは、選択した対象によって異なります。
3. [完了] をクリックします。

既存の IMSVA ルールを変更する

手順

1. 編集するルールの名前をクリックします。

   ルールの [概要] 画面が表示されます。
2. [ルール] タブで、[受信者と送信者] の [編集] をクリックします。
3. ルートを設定します。

   詳細については、517 ページの「手順 2: 受信者と送信者を選択する」を参照してください。
4. [検索条件] の [編集] をクリックします。
5. テンプレートを設定します。

6. [処理] の [編集] をクリックします。
7. 処理を設定します。

注意

Trend Micro Apex Central が、選択済みの対象に接続できない場合、一部の処理オプションは使用できなくなります。

8. [保存] をクリックします。

ルールを削除する

手順

1. 削除するルールの横のチェックボックスをオンにします。
2. [削除] をクリックします。

第 33 章

InterScan Web Security Suite ポリシー設定

本章では、Apex Central で InterScan Web Security Suite ポリシーを設定する方法について説明します。

次のトピックがあります。

情報漏えい対策ルールリスト

情報漏えい対策オプションを有効にする場合、個別の情報漏えい対策ルールを有効または無効にすることもできます。緑のチェックアイコンは、ルールが有効であることを示します。赤の [x] アイコンは、ルールが無効であることを示します。アイコンをクリックして、有効と無効の状態を切り替えることができます。

この画面には次のオプションがあります。

ルール: クリックすると、ルールを編集できます。

追加: [ルールの追加] 画面が開き、そこで新しいルールを設定できます。

コピー: リストからルールを選択してコピーできます。

削除: リストからルールを削除しできます。

優先順位: 矢印をクリックして、ルールの優先順位を変更します。

ステータス: アイコンをクリックすると、ルールが有効または無効になります。

保存: クリックすると、ルールを保存できます。

手順 1: ルール名を設定

以下は、この画面で使用可能なオプションの簡単な説明です。

- 有効にする: 選択すると、ルールが有効になります。
- ルール名: このルールの表示名を入力します。
- 次へ>: クリックすると続行されます。

手順 2: アカウントを選択する

以下は、この画面で使用可能なオプションの簡単な説明です。

注意

ドラフトルール作成時には、すべてのオプションが使用可能なわけではありません。すべてのオプションを有効にするには、サーバを指定してください。

- ルールの適用先のアカウントの IP アドレスを指定します。
  - [開始] と [終了] に IP 範囲を入力します。特定のアカウントの IP アドレスまたはホスト名を [IP/ホスト名] に、または IP サブネットを [アドレス] および [プレフィックス長] に入力します。
  - 1 つまたは複数のアカウントを右の表に作成するには、[追加] をクリックします。
  - 1 つまたは複数のアカウントを右の表から削除するには、[削除] をクリックします。
- < 戻る: クリックすると、前のページに戻ります。
- 次へ>: クリックすると続行されます。

手順 3: ブロックするコンプライアンステンプレートを選択する

以下は、この画面で使用可能なオプションの簡単な説明です。

- このルールを使用してブロックするコンプライアンステンプレートを指定します。
  - 使用可能なテンプレート: このリストのテンプレートは、ルールで使用可能です。
  - 選択されたブロックするテンプレート: このリストのテンプレートに、ブロックするルールが適用されます。

ヒント

<Shift> キーまたは <Ctrl> キーを押したままアカウント名をクリックすると、複数のテンプレートを選択できます。

  - >>: クリックすると、選択されたテンプレートのリストに使用可能なテンプレートが追加されます。
  - <<: クリックすると、選択されたテンプレートのリストからテンプレートが削除されます。
- < 戻る: クリックすると、前のページに戻ります。

- 次へ>: クリックすると続行されます。

手順 4: 監視するコンプライアンステンプレートを選択する

以下は、この画面で使用可能なオプションの簡単な説明です。

- このルールを使用して監視するコンプライアンステンプレートを指定します。
  - 使用可能なテンプレート: このリストのテンプレートは、ルールで使用可能です。
  - 選択された監視するテンプレート: このリストのテンプレートに、監視するルールが適用されます。

    ヒント

    <Shift> キーまたは <Ctrl> キーを押したままアカウント名をクリックすると、複数のテンプレートを選択できます。

  - >>: クリックすると、選択されたテンプレートのリストに使用可能なテンプレートが追加されます。
  - <<: クリックすると、選択されたテンプレートのリストからテンプレートが削除されます。
- < 戻る: クリックすると、前のページに戻ります。
- 完了: クリックすると、ルールのリストに戻ります。

第 34 章

InterScan Web Security Virtual Appliance ポリシー設定

本章では、Apex Central で InterScan Web Security Virtual Appliance ポリシーを設定する方法について説明します。

次のトピックがあります。

情報漏えい対策ルールリスト

情報漏えい対策オプションを有効にする場合、個別の情報漏えい対策ルールを有効または無効にすることもできます。緑のチェックアイコンは、ルールが有効であることを示します。赤の [x] アイコンは、ルールが無効であることを示します。アイコンをクリックして、有効と無効の状態を切り替えることができます。

この画面には次のオプションがあります。

ルール: クリックすると、ルールを編集できます。

追加: [ルールの追加] 画面が開き、そこで新しいルールを設定できます。

コピー: リストからルールを選択してコピーできます。

削除: リストからルールを削除しできます。

優先順位: 矢印をクリックして、ルールの優先順位を変更します。

ステータス: アイコンをクリックすると、ルールが有効または無効になります。

保存: クリックすると、ルールを保存できます。

手順 1: ルール名を設定

以下は、この画面で使用可能なオプションの簡単な説明です。

- 有効にする: 選択すると、ルールが有効になります。
- ルール名: このルールの表示名を入力します。
- 次へ>: クリックすると続行されます。

手順 2: アカウントを選択する

以下は、この画面で使用可能なオプションの簡単な説明です。

注意

ドラフトルール作成時には、すべてのオプションが使用可能なわけではありません。すべてのオプションを有効にするには、サーバを指定してください。

- ルールの適用先のアカウントの IP アドレスを指定します。
  - [開始] と [終了] に IP 範囲を入力します。特定のアカウントの IP アドレスまたはホスト名を [IP/ホスト名] に、または IP サブネットを [アドレス] および [プレフィックス長] に入力します。
  - 1 つまたは複数のアカウントを右の表に作成するには、[追加] をクリックします。
  - 1 つまたは複数のアカウントを右の表から削除するには、[削除] をクリックします。
- < 戻る: クリックすると、前のページに戻ります。
- 次へ>: クリックすると続行されます。

手順 3: ブロックするコンプライアンステンプレートを選択する

以下は、この画面で使用可能なオプションの簡単な説明です。

- このルールを使用してブロックするコンプライアンステンプレートを指定します。
  - 使用可能なテンプレート: このリストのテンプレートは、ルールで使用可能です。
  - 選択されたブロックするテンプレート: このリストのテンプレートに、ブロックするルールが適用されます。

ヒント

<Shift> キーまたは <Ctrl> キーを押したままアカウント名をクリックすると、複数のテンプレートを選択できます。

  - >>: クリックすると、選択されたテンプレートのリストに使用可能なテンプレートが追加されます。
  - <<: クリックすると、選択されたテンプレートのリストからテンプレートが削除されます。
- < 戻る: クリックすると、前のページに戻ります。

- 次へ>: クリックすると続行されます。

手順 4: 監視するコンプライアンステンプレートを選択する

以下は、この画面で使用可能なオプションの簡単な説明です。

- このルールを使用して監視するコンプライアンステンプレートを指定します。
  - 使用可能なテンプレート: このリストのテンプレートは、ルールで使用可能です。
  - 選択された監視するテンプレート: このリストのテンプレートに、監視するルールが適用されます。

    ヒント

    <Shift> キーまたは <Ctrl> キーを押したままアカウント名をクリックすると、複数のテンプレートを選択できます。

  - >>: クリックすると、選択されたテンプレートのリストに使用可能なテンプレートが追加されます。
  - <<: クリックすると、選択されたテンプレートのリストからテンプレートが削除されます。
- < 戻る: クリックすると、前のページに戻ります。
- 完了: クリックすると、ルールのリストに戻ります。

パート XIV

InterScan for Microsoft Exchange のポリシー

第 35 章

InterScan for Microsoft Exchange のポリシー設定

本章では、Apex Central コンソールで InterScan for Microsoft Exchange のポリシーを設定する方法について説明します。

次のトピックがあります。

情報漏えい対策ポリシーの設定

情報漏えい対策ポリシーは、メールに機密情報が見つかったときに Apex Central で実行する処理を定義します。

新規ポリシーを作成する場合は、[情報漏えい対策] > [情報漏えい対策ポリシー] > [追加] を順にクリックします。

既存のポリシーを変更する場合は、[情報漏えい対策] > [情報漏えい対策ポリシー] > [情報漏えい対策ポリシー名] を順にクリックします。

情報漏えい対策ポリシーを設定するには、次の 5 つの手順を実行します。

1. 534 ページの「アカウントの選択」
2. 535 ページの「情報漏えい対策対象の設定」
3. 536 ページの「情報漏えい対策処理の設定」
4. 537 ページの「情報漏えい対策通知の設定」
5. 538 ページの「情報漏えい対策ポリシーの有効化」

アカウントの選択

手順

1. [情報漏えい対策] > [情報漏えい対策ポリシー] を順に選択して、[情報漏えい対策ポリシー] 画面に移動します。
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:

     [追加] をクリックします。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。
     b. [アカウント] タブをクリックします。
3. 次のいずれかを選択します。
   - すべて — このポリシーまたは除外をすべてのユーザに適用します。

- 特定のアカウント — Active Directory グループまたは Apex Central 特定グループから選択します。

4. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。
5. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。

情報漏えい対策対象の設定

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:
     a. [追加] をクリックします。
     b. [ルールの指定] 画面に移動します。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。
     b. [対象] タブをクリックします。
3. 検索対象に含めるメール領域のチェックボックスをオンにします。

   選択可能な対象は次のとおりです。
   - ヘッダ ([送信者]、[送信先]、および [Cc])

- 件名
- 本文
- 添付ファイル

4. 利用可能なテンプレートのリストからテンプレートを選択し、[追加 >>] をクリックしてテンプレートをポリシーに適用します。

注意

情報漏えい対策ポリシーを有効にするには、テンプレートを少なくとも 1 つは選択する必要があります。

5. 新しいテンプレートを作成するには、[使用可能な情報漏えい対策テンプレート] ツールバーで [追加] をクリックします。テンプレートファイルをインポートするには、[インポート] をクリックします。

情報漏えい対策処理の設定

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:
     a. [追加] をクリックします。
     b. [処理の指定] 画面に移動します。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。

b. [処理] タブをクリックします。

3. 望ましくないコンテンツを検出したときに Apex Central が実行する処理を選択します。
4. 指定したユーザに通知するには、次の操作を行います。
   - [送信者の管理者に転送する] チェックボックスをオンにします。
   - [特定のメールアドレスに転送する] チェックボックスをオンにし、受信者のメールアドレスを入力します。
5. 処理が実行されたときの動作として、[通知する] または [通知しない] を選択します。
6. 必要に応じて [詳細オプション] を設定します。

情報漏えい対策通知の設定

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:
     a. [追加] をクリックします。
     b. [通知の指定] 画面に移動します。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。
     b. [通知] タブをクリックします。

3. Apex Central で通知するユーザに対応するチェックボックスをオンにします。
4. [詳細の表示] をクリックして、その受信者の通知をカスタマイズします。
5. 通知オプションの中から選択します。
6. [Windows イベントログに書き込む] チェックボックスをオンにして、Windows のイベントログに通知が記録されるように設定します。

情報漏えい対策ポリシーの有効化

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーを有効にする前に、追加または編集します。
   - 新規ポリシーの場合:
     a. [追加] をクリックします。
     b. [名前と優先度] 画面に移動します。
   - 既存のポリシーの場合:

     ポリシー名をクリックします。
3. このポリシーまたは除外を有効にします。
4. このポリシーの名前を [ポリシー名] に入力します。
5. 優先度を指定します。
   - 新規ポリシーの場合:

     このポリシーの優先度を [優先度] に入力します。

- 既存のポリシーの場合:
  a. リスト内のポリシー名または除外名の横にあるチェックボックスをオンにします。
  b. [優先度の再設定] をクリックします。
  c. [優先度] フィールドに、優先度を数字で入力します。
  d. [優先度を保存] をクリックします。

6. [保存] をクリックします。

パート XV

Smart Protection Server

第 36 章

Smart Protection Server のダッシュボードウィジェット

本章では、Apex Central でサポートされる Smart Protection Server のダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

ファイルレピュテーションを使用中のユーザ

このウィジェットは、Smart Protection Server にファイルレピュテーションクエリを送信するユーザの数を追跡するために使用します。各エンドポイントコンピュータは、それぞれがアクティブなユーザと見なされます。

注意

このウィジェットには情報が 2 次元のグラフで表示され、1 時間ごとに更新されます。また、いつでも更新アイコン ( ) をクリックしてデータを更新できます。

表 36-1. ウィジェットのデータ

データ	説明
ユーザ	Smart Protection Server のコンピュータにクエリを送信したユーザ数
日付	クエリの日付

Web レピュテーションを使用中のユーザ

このウィジェットは、Smart Protection Server に Web レピュテーションクエリを送信するユーザの数を追跡するために使用します。各エンドポイントコンピュータは、それぞれがアクティブなユーザと見なされます。

注意

このウィジェットには情報が 2 次元のグラフで表示され、5 分ごとに更新されます。また、いつでも更新アイコン ( ) をクリックしてデータを更新できます。

表 36-2. ウィジェットのデータ

データ	説明
ユーザ	Smart Protection Server コンピュータにクエリを送信したユーザ数
日付	クエリの日付

ファイルレピュテーションの HTTP トラフィックレポート

HTTP トラフィックレポートウィジェットには、クライアントで生成されたファイルレピュテーションクエリによって、Smart Protection Server に送信されたネットワークトラフィックの総容量がキロバイト (KB) 単位で表示されます。このウィジェットの情報は、1 時間ごとに更新されます。また、更新アイコン ( ) をクリックすると、いつでもデータを更新できます。

表 36-3. ウィジェットのデータ

データ	説明
トラフィック (KB)	クエリによって生成されたネットワークトラフィック
日付	クエリの日付

Web レピュテーションの HTTP トラフィックレポート

この HTTP トラフィックレポートウィジェットには、クライアントで生成された Web レピュテーションクエリによって、Smart Protection Server に送信されたネットワークトラフィックの総容量がキロバイト (KB) 単位で表示されます。このウィジェットの情報は、1 時間ごとに更新されます。また、更新アイコン ( ) をクリックすると、いつでもデータを更新できます。

表 36-4. ウィジェットのデータ

データ	説明
トラフィック (KB)	クエリによって生成されたネットワークトラフィック
日付	クエリの日付

Smart Protection Server のステータス

このウィジェットは、Smart Protection Server のステータスを監視するために使用します。

注意

このウィジェットが [概要] 画面に表示されている場合、製品コンソールセッションは終了しません。コンピュータのステータスは 1 分間隔で更新されます。したがって、サーバへの要求の送信によってセッションが終了することはありません。ただし、現在表示されているタブにこのウィジェットが含まれない場合、セッションは終了します。

表 36-5. ウィジェットのデータ

データ	説明
サービス	Smart Protection Server によって提供されるサービス。
プロトコル	各種サービスによってサポートされているプロトコルが表示されます。ファイルレピュテーションでは、HTTP と HTTPS プロトコルの両方がサポートされます。Web レピュテーションでは HTTP がサポートされます。HTTPS では接続の安全性が高くなる一方、HTTP では使用する帯域幅が少なくなります。
ホスト	ファイルレピュテーションおよび Web レピュテーションサービスのアドレスです。これらのアドレスは、Smart Protection Server コンピュータをサポートするトレンドマイクロ製品で使用します。Smart Protection Server コンピュータへの接続の設定に使用されるアドレスです。

データ	説明
コンピュータステータス	次の項目がシステムヘルスステータスに表示されます。 • ファイルレピュテーションクエリ: ファイルレピュテーションが機能しているかどうかを表示します。 • Web レピュテーションクエリ: Web レピュテーションが機能しているかどうかを表示します。 • ActiveUpdate: ActiveUpdate が機能しているかどうかを表示します。 • 平均 CPU 負荷: カーネルで生成された、過去 1 分間、5 分間、15 分間のコンピュータの平均負荷を表示します。 • 空きメモリ: コンピュータの使用可能物理メモリを表示します。 • スワップディスク使用率: スワップディスク使用率を表示します。 • 空き容量: コンピュータの使用可能なディスク空き容量を表示します。

ファイルレピュテーションの感染コンピュータトップ 10

Smart Protection Server が既知のウイルスをファイルレピュテーションクエリで受信した後に、感染コンピュータに分類された上位 10 個のコンピュータの IP アドレスが表示されます。このウィジェットに表示される情報には、コンピュータの IP アドレスや各コンピュータの検出総数などがあり、表形式で表示されます。このウィジェットの情報は、1 時間ごとに更新されます。更新アイコン ( ) をクリックすると、ウィジェットの表示データをいつでも更新できます。

このウィジェットを使用して、ネットワーク上の感染数が最も多いコンピュータを追跡します。

注意

このウィジェットで複数の Smart Protection Server を有効にすると、選択した Smart Protection Server の検出総数が計算され、リストで選択した Smart Protection Server コンピュータの上位 10 個のコンピュータが表示されます。

表 36-6. ウィジェットのデータ

データ	説明
IP	コンピュータの IP アドレス
検出	このコンピュータで検出されたセキュリティ脅威の数

Web レピュテーションでブロックされたコンピュータトップ 10

Smart Protection Server が URL を Web レピュテーションクエリで受信した後に、ブロックされたコンピュータに分類された上位 10 個のコンピュータの IP アドレスが表示されます。このウィジェットに表示される情報には、コンピュータの IP アドレスや各コンピュータのブロックされた URL 総数などがあり、表形式で表示されます。このウィジェットの情報は、毎日更新されます。更新アイコン ( ) をクリックすると、ウィジェットの表示データをいつでも更新できます。

このウィジェットを使用して、ネットワーク上のブロックされた回数が最も多いサイトにアクセスしているコンピュータを追跡します。

注意

このウィジェットで複数の Smart Protection Server を有効にすると、選択した Smart Protection Server の検出総数が計算され、リストで選択した Smart Protection Server コンピュータの上位 10 個のブロックされたコンピュータが表示されます。

表 36-7. ウィジェットのデータ

データ	説明
IP	コンピュータの IP アドレス
検出	このコンピュータでブロックされた URL の数

パート XVI

Trend Micro Mobile Security のウィジェットとポリシー

第 37 章

Trend Micro Mobile Security ダッシュボードウィジェット

本章では、Apex Central でサポートされる Trend Micro Mobile Security ダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

Android デバイスのステータス

登録されている Android デバイスのステータス情報を表示します。

ステータスが最新の場合、Android モバイルデバイスが Mobile Security マネージメントサーバに登録されており、その Android モバイルデバイス上のすべてのコンポーネントとポリシーが最新であることを示します。

ステータス	説明
最新	最新の Android モバイルデバイスの数
期限切れ	期限切れの Android モバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android デバイスの暗号化ステータス情報ウィジェット

登録されている Android デバイスの暗号化ステータス情報を表示します。

ステータス	説明
暗号化完了	暗号化されている Android モバイルデバイスの数
暗号化未完了	暗号化されていない Android モバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android デバイス OS バージョン情報ウィジェット

登録されている Android モバイルデバイスにインストールされた OS のバージョン情報を表示します。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android デバイスの root 化ステータス情報ウィジェット

登録されている Android デバイスの root 化ステータス情報を表示します。

ステータス	説明
root 化完了	root 化されているモバイルデバイスの数
root 化未完了	root 化されていないモバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android デバイスのセキュリティステータスウィジェット

登録されている Android デバイスのセキュリティステータス情報を表示します。

- 検索されていません
- 保護されていません
- 保護されています
- 警告

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android 不正プログラム検索情報ウィジェット

インストールされているすべての Android アプリについて、不正プログラム検索の結果を表示します。

このウィジェットは、結果を次のカテゴリにグループ化します。

- 不明
- 潜在的に不要なオブジェクト

- 標準
- 不正プログラム

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android 改ざんアプリ検索情報ウィジェット

インストールされているすべての Android アプリについて、改ざんアプリ検索の結果を表示します。

このウィジェットは、結果を次のカテゴリにグループ化します。

- 不明
- 改ざんあり
- 改ざんなし

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android プライバシーデータ漏えい検索情報ウィジェット

インストールされているすべての Android アプリについて、アプリ権限チェックの結果を表示します。

このウィジェットは、結果を次のカテゴリにグループ化します。

- 不明
- 潜在的に不要なオブジェクト
- 標準
- 不正プログラム

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Android 脆弱性検索情報ウィジェット

インストールされているすべての Android アプリについて、脆弱性検索の結果を表示します。

このウィジェットは、結果を次のカテゴリにグループ化します。

- 不明
- 標準
- 高
- 中

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

コンポーネントのアップデートステータスウィジェット

登録されているモバイルデバイスのアップデートステータス情報を表示します。

列	説明
現在のバージョン	モバイルデバイスエージェントまたは Mobile Security マネージメントサーバ上のコンポーネントの現在のバージョン番号
最新バージョン	最新のモバイルデバイスエージェントのバージョンまたはコンポーネントを使用しているモバイルデバイスの数
古いバージョン	古いコンポーネントを使用しているモバイルデバイスの数
アップデート率	最新のコンポーネントバージョンを使用しているモバイルデバイスの割合
アップグレード完了	最新のモバイルデバイスエージェントのバージョンを使用しているモバイルデバイスの数
アップグレード未完了	最新のモバイルデバイスエージェントのバージョンを使用するようにアップグレードされていないモバイルデバイスの数

列	説明
アップグレード率	最新のモバイルデバイスエージェントを使用しているモバイルデバイスの割合

モバイル向けサイバーセキュリティニュースウィジェット

このウィジェットには、トレンドマイクロが公開した、モバイルデバイスに関連するサイバーセキュリティニュースが表示されます。

iOS デバイスの暗号化ステータス情報ウィジェット

登録されている iOS デバイスの暗号化ステータス情報を表示します。

ステータス	説明
暗号化完了	暗号化されている iOS モバイルデバイスの数
暗号化未完了	暗号化されていない iOS モバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

iOS デバイスのステータスウィジェット

登録されている iOS デバイスのステータス情報を表示します。

ステータスが最新の場合、iOS モバイルデバイスが Mobile Security マネージメントサーバに登録されており、その iOS モバイルデバイス上のすべてのコンポーネントとポリシーが最新であることを示します。

ステータス	説明
最新	最新の iOS モバイルデバイスの数
期限切れ	期限切れの iOS モバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

iOS デバイスのセキュリティステータスウィジェット

登録されている iOS デバイスのセキュリティステータス情報を表示します。

- 検索されていません
- 保護されていません
- 保護されています
- 警告

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

iOS デバイスの Jailbreak ステータス情報ウィジェット

登録されている iOS デバイスの Jailbreak ステータス情報を表示します。

ステータス	説明
Jailbreak あり	Jailbreak ありのモバイルデバイスの数
Jailbreak なし	Jailbreak なしのモバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

iOS デバイス OS バージョン情報ウィジェット

登録されている iOS モバイルデバイスにインストールされた OS のバージョン情報を表示します。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

iOS 不正プログラム検索情報ウィジェット

インストールされているすべての iOS アプリについて、不正プログラム検索の結果を表示します。

このウィジェットは、結果を次のカテゴリにグループ化します。

- 不明
- 不正プログラム
- 標準

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイスのアプリ制御ステータス情報ウィジェット

登録されているモバイルデバイスのアプリケーション制御ステータス情報を表示します。

ステータス	説明
コンプライアンス準拠	Mobile Security のコンプライアンスとアプリケーション制御ポリシーに準拠するモバイルデバイスの数
コンプライアンス違反	Mobile Security のコンプライアンスとアプリケーション制御ポリシーに準拠しないモバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイスの暗号化ステータス情報ウィジェット

登録されているモバイルデバイスの暗号化ステータス情報を表示します。

ステータス	説明
暗号化完了	暗号化されているモバイルデバイスの数

ステータス	説明
暗号化未完了	暗号化されていないモバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイスのステータスウィジェット

登録されているモバイルデバイスのステータス情報を表示します。

ステータス	説明
最新	デバイスは Mobile Security マネージメントサーバに登録されており、そのモバイルデバイス上のコンポーネントとポリシーは最新です。
コンプライアンス違反	デバイスは Mobile Security マネージメントサーバに登録されていますが、サーバポリシーに準拠していません。
非同期	デバイスは Mobile Security マネージメントサーバに登録されていますが、コンポーネントかポリシーのいずれかは最新ではありません。
非アクティブ	デバイスはまだ Mobile Security マネージメントサーバに登録されていません。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイスの Jailbreak ステータス情報ウィジェット

登録されているモバイルデバイスの Jailbreak ステータス情報を表示します。

ステータス	説明
Jailbreak あり	Jailbreak ありのモバイルデバイスの数
Jailbreak なし	Jailbreak なしのモバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイス OS バージョン情報ウィジェット

登録されているモバイルデバイスにインストールされた OS のバージョン情報を表示します。

OS:	説明
Android	登録された Android モバイルデバイスの数
iOS	登録された iOS モバイルデバイスの数
Windows Phone	登録された Windows Phone モバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイスのランサムウェア検索の概要ウィジェット

インストールされているすべてのアプリについて、ランサムウェア検索の結果を表示します。

モバイル OS 別に結果がグループ分けされます。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイスのセキュリティステータスウィジェット

登録されているモバイルデバイスのセキュリティステータス情報を表示します。

- 検索されていません
- 保護されていません

- 保護されています
- 警告

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

モバイルデバイスのベンダー情報ウィジェット

登録されているモバイルデバイスのモバイルデバイスベンダー情報を表示します。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

ポリシーのアップデートステータス情報ウィジェット

登録されているモバイルデバイスのポリシーのアップデートステータス情報を表示します。

ステータス	説明
最新バージョン	アップデートされたモバイルデバイスエージェントのバージョンまたはコンポーネントで実行しているモバイルデバイスの数
古いバージョン	最新のコンポーネントで実行しているモバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

サーバコンポーネントのステータス情報ウィジェット

サーバコンポーネントのアップデートステータスとバージョン番号を表示します。

列	説明
サーバ	モジュールの名前

列	説明
アドレス	モジュールをホストしているマシンのドメイン名または IP アドレス
現在のバージョン	インストールされた Mobile Security マネージメントサーバモジュールのバージョン番号
最終更新日	最終更新の日時

携帯電話キャリア情報ウィジェット

このウィジェットには、登録されている Android モバイルデバイスで使用される携帯電話キャリア情報が表示されます。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

インストールされた上位 10 個のアプリウィジェット

登録されているモバイルデバイスにインストールされた上位 10 個のアプリをリストで表示します。[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

検出された上位 5 個の Android ランサムウェアウィジェット

このウィジェットには、指定されたランサムウェアの検出回数に基づいて、Mobile Security で検出された上位 5 個の Android ランサムウェアがリストで表示されます。[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

ブロックされた上位 5 個の Web サイトウィジェット

このウィジェットには、各サイトへのアクセス回数に基づいて、Mobile Security でブロックされた上位 5 個の Web サイトがリストで表示されます。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

検出された上位 5 個の iOS ランサムウェア

このウィジェットには、指定されたランサムウェアの検出回数に基づいて、Mobile Security で検出された上位 5 個の iOS ランサムウェアがリストで表示されます。[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

検出された上位 5 個の不正プログラムウィジェット

このウィジェットには、指定された不正プログラムの検出回数に基づいて、Mobile Security で検出された上位 5 個の不正プログラムがリストで表示されます。[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Windows Phone デバイスの暗号化ステータス情報ウィジェット

登録されている Windows Phone デバイスの暗号化ステータス情報を表示します。

ステータス	説明
暗号化完了	暗号化されている Windows Phone モバイルデバイスの数
暗号化未完了	暗号化されていない Windows Phone モバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Windows Phone デバイスのステータスウィジェット

このウィジェットには、登録されている Windows Phone モバイルデバイスのステータス情報が表示されます。

ステータスが最新の場合、Windows Phone モバイルデバイスが Mobile Security マネージメントサーバに登録されており、その Windows Phone モバイルデバイス上のすべてのコンポーネントとポリシーが最新であることを示します。

ステータス	説明
最新	最新の Windows Phone モバイルデバイスの数
期限切れ	期限切れの Windows Phone モバイルデバイスの数

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

Windows Phone デバイス OS バージョン情報ウィジェット

このウィジェットには、登録されている Windows Phone モバイルデバイスにインストールされた OS のバージョン情報が表示されます。

[すべて] を選択するか、またはドロップダウンリストからグループ名を選択して、関連するデバイスの情報を表示します。

第 38 章

Trend Micro Mobile Security のポリシー設定

本章では、Apex Central 管理コンソールで Mobile Security のセキュリティポリシーを設定する方法について説明します。

ポリシーを使用してデバイスを保護する

管理サーバの Mobile Security グループに対してセキュリティポリシーを設定できます。これらのポリシーは、グループ内のすべてのモバイルデバイスに適用されます。モバイルデバイスグループ (ルートグループ) を選択することで、セキュリティポリシーをすべての Mobile Security グループに適用できます。次の表は、Mobile Security で利用できるセキュリティポリシーを示しています。

表 38-1. Mobile Security のセキュリティポリシー

ポリシーグループ	ポリシー	レファレンス/参照情報
一般	共通ポリシー	製品版配信モードについては、568 ページの「製品版配信モードの共通ポリシー」を参照してください。 セキュリティ検索配信モードについては、569 ページの「セキュリティ検索配信モードの共通ポリシー」を参照してください。
プロビジョニング	Wi-Fi ポリシー	569 ページの「Wi-Fi ポリシー」を参照してください。
	Exchange ActiveSync ポリシー	570 ページの「Exchange ActiveSync ポリシー」を参照してください。
	証明書ポリシー	570 ページの「証明書ポリシー」を参照してください。
	VPN ポリシー	570 ページの「VPN ポリシー」を参照してください。
	グローバル HTTP プロキシポリシー	570 ページの「グローバル HTTP プロキシポリシー」を参照してください。
	シングルサインオンポリシー	570 ページの「シングルサインオンポリシー」を参照してください。

ポリシーグループ	ポリシー	レファレンス/参照情報
	モバイルデータ通信ネットワークポリシー	「572 ページのモバイルデータ通信ネットワークポリシー」を参照してください。
	AirPlay/AirPrint ポリシー	「572 ページの AirPlay/AirPrint ポリシー」を参照してください。
	テーマポリシー	「572 ページのテーマポリシー」を参照してください。
	管理対象ドメインポリシー	572 ページの「管理対象ドメインポリシー」を参照してください。
デバイスセキュリティ	セキュリティポリシー	製品版配信モードのセキュリティポリシーについては、573 ページの「製品版配信モードのセキュリティポリシー」を参照してください。 セキュリティ検索配信モードのセキュリティポリシーについては、575 ページの「セキュリティ検索配信モードのセキュリティポリシー」を参照してください。
	迷惑メール対策ポリシー	577 ページの「迷惑メール対策ポリシー」を参照してください。
	着信フィルタポリシー	580 ページの「着信フィルタポリシー」を参照してください。
	Web 脅威検出ポリシー	582 ページの「Web 脅威検出ポリシー」を参照してください。
デバイス	パスワードポリシー	585 ページの「パスワードポリシー」を参照してください。
	機能ロックポリシー	586 ページの「機能ロックポリシー」を参照してください。

ポリシーグループ	ポリシー	レファレンス/参照情報
	コンプライアンスポリシー	595 ページの「コンプライアンスポリシー」を参照してください。
アプリケーション管理	アプリの監視および制御ポリシー	596 ページの「アプリの監視および制御ポリシー」を参照してください。
	Volume Purchasing Program ポリシー	599 ページの「Volume Purchasing Program ポリシー」を参照してください。
Samsung KNOX	コンテナポリシー	「601 ページのコンテナポリシー」を参照してください。

製品版配信モードの共通ポリシー

共通ポリシーは、モバイルデバイス向けの共通セキュリティポリシーを提供します。共通セキュリティポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[共通ポリシー] をクリックします。

- ユーザ権限: ユーザによるモバイルデバイスエージェントのアンインストールを許可する機能を有効または無効にできます。さらに、ユーザによる Mobile Security デバイスエージェントの設定を許可するかどうかを選択できます。

  アンインストールの保護に関連付けられている機能は次のとおりです。

  - アンインストールの保護は管理コンソールからオンまたはオフにします。
  - パスワードの長さは 6〜12 文字で、数字、文字、または記号を使用できます。
  - パスワードは管理コンソールからグループごとに設定できます。

  [ユーザによる Mobile Security クライアントの設定を許可する] チェックボックスをオンにしない場合、ユーザはモバイルデバイスエージェント設定を変更できません。ただし、このオプションが選択されていても、スパムメール対策ポリシー、着信フィルタポリシー、および Web 脅威検出ポリシーのフィルタリストは影響を受けません。詳細については、

577 ページの「迷惑メール対策ポリシー」、580 ページの「着信フィルタポリシー」、および 582 ページの「Web 脅威検出ポリシー」を参照してください。

- アップデート設定: 更新で新しいコンポーネントを使用できるようになった場合に、Mobile Security マネージメントサーバからモバイルデバイスエージェントに通知が送信されるように選択できます。または、自動チェックオプションを選択して、モバイルデバイスエージェントが定期的に Mobile Security マネージメントサーバ上のコンポーネントまたは設定の更新を確認するようにすることができます。
- ログ設定: モバイルデバイスエージェントが Android OS 上のマルウェアなどのセキュリティリスクを検出すると、モバイルデバイス上でログが生成されます。

セキュリティ検索配信モードの共通ポリシー

共通ポリシーは、モバイルデバイス向けの共通セキュリティポリシーを提供します。共通セキュリティポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[共通ポリシー] をクリックします。

- ユーザ権限:
  - ユーザによる Mobile Security デバイスエージェントの設定を許可するかどうかを選択できます。

    [ユーザによる Mobile Security クライアントの設定を許可する] チェックボックスをオンにしない場合、ユーザはモバイルデバイスエージェント設定を変更できません。ただし、このオプションが選択されていても、Web 脅威検出ポリシーのフィルタリストは影響を受けません。詳細については、582 ページの「Web 脅威検出ポリシー」を参照してください。
  - 自動チェックオプションを選択して、モバイルデバイスエージェントが定期的に Mobile Security マネージメントサーバ上のコンポーネントまたは設定の更新を確認するようにすることができます。

Wi-Fi ポリシー

Wi-Fi ポリシーにより、ネットワーク名、セキュリティの種類、およびパスワードを含む、組織の Wi-Fi ネットワーク情報を、Android および iOS モバイルデバイスに配信できます。

Wi-Fi ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[Wi-Fi ポリシー] をクリックします。

Exchange ActiveSync ポリシー

Exchange ActiveSync ポリシーにより、組織のための Exchange ActiveSync ポリシーを作成し、それを iOS モバイルデバイスに配信できます。

Exchange ActiveSync ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[Exchange ActiveSync ポリシー] をクリックします。

証明書ポリシー

証明書ポリシーにより、iOS モバイルデバイスに配信する必要のある証明書をインポートできます。

証明書ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[証明書ポリシー] をクリックします。

VPN ポリシー

VPN ポリシー設定により、組織のための VPN ポリシーを作成し、それを iOS モバイルデバイスに配信できます。

VPN ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[VPN ポリシー] をクリックします。

グローバル HTTP プロキシポリシー

グローバル HTTP プロキシポリシーにより、組織のプロキシ情報をモバイルデバイスに配信できます。このポリシーは、監視モードである iOS モバイルデバイスにのみ適用されます。

グローバル HTTP プロキシポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[グローバル HTTP プロキシポリシー] をクリックします。

シングルサインオンポリシー

シングルサインオン (SSO) ポリシーを使用すると、ユーザは Mobile Security およびアプリストアを含む複数のアプリケーション間で同じアカウント情報

を使用できます。SSO 証明書で設定された新しいアプリケーションはそれぞれ、エンタープライズリソースのユーザ権限を検証し、ユーザにパスワードの再入力を要求することなく、ユーザをログインします。

シングルサインオンポリシーには、次の情報が含まれます。

- 名前: Kerberos プリンシパル名。
- レルム:Kerberos レルム名。

  Kerberos レルム名は、大文字と小文字が適切に設定されている必要があります。
- URL プレフィックス (オプション): HTTP 経由の Kerberos 認証にアカウントを使用するために一致する必要のある URL のリスト。このフィールドが空白の場合、アカウントはすべての HTTP および HTTPS の URL に一致できます。URL 一致パターンは、http または https で始まる必要があります。

  このリストの各エントリには、URL プレフィックスが含まれている必要があります。アカウント内の文字列の 1 つで始まる URL のみが、Kerberos チケットへのアクセスを許可されます。URL 一致パターンには、スキームが含まれている必要があります。たとえば、「http://www.example.com/」のようになります。一致パターンが/で終了しない場合、URL に自動的に/が追加されます。
- アプリケーション ID (オプション): アカウントの使用を許可されるアプリケーション ID のリスト。このフィールドが空白の場合、このアカウントはすべてのアプリケーション ID に一致します。

  アプリケーション ID の配列には、アプリケーションバンドル ID に一致する文字列が含まれている必要があります。これらの文字列は、完全一致 (「com.mycompany.myapp」など) にすることも、また*ワイルドカード文字を使用して、バンドル ID 上のプレフィックス一致を指定することもできます。ワイルドカード文字は、ピリオド文字 (.) の後か、または文字列の最後 (「com.mycompany.*」など) に付ける必要があります。ワイルドカード文字を使用すると、バンドル ID がプレフィックスで始まるアプリケーションに、アカウントに対するアクセス権が付与されます。

iOS 設定のシングルサインオンポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[シングルサインオンポリシー] をクリックします。

モバイルデータ通信ネットワークポリシー

モバイルデータ通信ネットワークポリシー設定により、組織のためのモバイルデータ通信ネットワークを設定し、それを iOS モバイルデバイスに配信できます。

モバイルデータ通信ネットワークポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[モバイルデータ通信ネットワークポリシー] をクリックします。

AirPlay/AirPrint ポリシー

AirPlay/AirPrint ポリシー設定により、組織のための AirPlay および AirPrint ポリシーを作成し、それを iOS モバイルデバイスに配信できます。

AirPlay/AirPrint ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[AirPlay/AirPrint ポリシー] をクリックします。

テーマポリシー

テーマポリシーを設定すると、フォントをプッシュし、iOS モバイルデバイスのホーム画面とロック画面の壁紙を設定できます。このポリシーは、監視モードである iOS モバイルデバイスにのみ適用されます。

テーマポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[テーマポリシー] をクリックします。

管理対象ドメインポリシー

管理対象ドメインポリシーを使用すると、組織が管理する電子メールや Web ドメインを設定できます。

- マークされていないメールドメイン: ユーザがシステムのメールクライアントを使用して電子メールを作成している場合、設定済みのドメインに一致しないメールアドレスを入力すると、赤で強調表示 (マーク) されます。管理者は、ユーザが信頼されていないメールアドレスに対して不注意に機密情報を送信しようした場合に警告できるよう、この機能の使用を検討する必要があります。

- 管理対象の Safari Web ドメイン: Safari を使用して特定のドメインからダウンロードされたファイルは、管理対象のアプリでしか開けないように指定できます。たとえば、internal.example.com からダウンロードされた PDF は Adobe Reader (管理対象アプリ) で開くことはできますが、Dropbox (非管理対象アプリ) で開くことはできません。これにより、Safari を使用した場合の機能性が向上し、企業向けブラウザとしての用途を広げることができます。

  重要

  機能ロックポリシーで次の iOS 機能を無効にする必要があります。そうしないと、ダウンロードされたファイルを他の (非管理対象の) アプリで開くことができるため、管理対象の Safari Web ドメインの設定は効果がなくなります。

  - その他のアプリ内の管理対象アプリからドキュメントを開く (7.0 以上)
  - 管理対象アプリ内のその他のアプリからドキュメントを開く (7.0 以上)

管理対象ドメインポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[管理対象ドメインポリシー] をクリックします。

製品版配信モードのセキュリティポリシー

[セキュリティポリシー] 画面から、セキュリティ設定ができます。

セキュリティ保護ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[セキュリティポリシー] をクリックします。

次の表は、このポリシーに対して利用可能な設定を示しています。

表 38-2. セキュリティポリシー設定

セクション	項目	説明	サポートされるモバイルデバイスの OS
セキュリティ設定	インストールされているアプリのみを検索する	インストールされているアプリのみを検索するには、このオプションを選択します。	
	インストールされているアプリとファイルを検索する	インストールされているアプリケーションと、モバイルデバイスに保存されているその他のファイルを検索するには、このオプションを選択します。 このオプションを選択する場合、APK ファイルのみを検索するか、またはすべてのファイルを検索するかを指定します。	
	パターンファイルのアップデート後に検索する	パターンファイルのアップデート後に毎回不正プログラムを検索する場合は、このオプションを有効にします。 Android モバイルデバイスのアップデートが正常に完了すると、Mobile Security によって自動的に検索が実行されます。	
	Facebook 検索を有効にする	Facebook プライバシー設定を検索する場合は、このオプシ	

セクション	項目	説明	サポートされるモバイルデバイスの OS
		ョンを有効にします。 注意 Facebook 検索を有効にすると、ユーザは情報を保護し、確実に信頼する人とのみデータを共有できます。	
検索スケジュール	日次	検索は、指定した曜日の [開始時刻] に日ごとに実行されます。	
	週次	検索は、指定した曜日の [開始時刻] に 1 週間に 1 回実行されます。	
	月次	検索は、指定した曜日の [開始時刻] に 1 か月に 1 回実行されます。	

セキュリティ検索配信モードのセキュリティポリシー

[セキュリティポリシー] 画面から、セキュリティ設定ができます。

セキュリティ保護ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[セキュリティポリシー] をクリックします。

次の表は、このポリシーに対して利用可能な設定を示しています。

表 38-3. セキュリティポリシー設定

セクション	項目	説明	サポートされるモバイルデバイスの OS
セキュリティ設定	インストールされているアプリのみを検索する	インストールされているアプリのみを検索するには、このオプションを選択します。	
	インストールされているアプリとファイルを検索する	インストールされているアプリケーションと、モバイルデバイスに保存されているその他のファイルを検索するには、このオプションを選択します。 このオプションを選択する場合、APK ファイルのみを検索するか、またはすべてのファイルを検索するかを指定します。	
	パターンファイルのアップデート後に検索する	パターンファイルのアップデート後に毎回不正プログラムを検索する場合は、このオプションを有効にします。 Android モバイルデバイスのアップデートが正常に完了すると、Mobile Security によって自動的に検索が実行されます。	
検索スケジュール	日次	検索は、指定した曜日の [開始時刻] に日ごとに実行されます。	

セクション	項目	説明	サポートされるモバイルデバイスの OS
	週次	検索は、指定した曜日の [開始時刻] に 1 週間に 1 回実行されます。	
	月次	検索は、指定した曜日の [開始時刻] に 1 か月に 1 回実行されます。	

迷惑メール対策ポリシー

Mobile Security のスパムメール対策ポリシーは、スパムメールである WAP プッシュおよび SMS テキストメッセージからの保護を提供します。

スパムメール対策ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[迷惑メール対策ポリシー] をクリックします。

迷惑 SMS 対策ポリシー

この機能により、サーバ側で SMS スパムメール対策ポリシーを制御できるようになります。SMS スパムメール対策ポリシーの設定時、次のことを実行できます。

- モバイルデバイスでスパムメール SMS 対策を有効または無効にする
- モバイルデバイスでブロックリスト、承認済みリストを使用するよう設定するか、またはモバイルデバイスで SMS スパムメール対策機能を無効にする
- 管理コンソールから承認済みリストを設定する
- 管理コンソールからブロックリストを設定する

承認済みまたはブロックフィルタリスト設定の詳細については、次の表を参照してください。

表 38-4. スパムメール SMS 対策ポリシーのフィルタリスト設定

一括管理	ユーザ管理	説明
無効	有効	ユーザは、モバイルデバイスエージェント上の承認済み/ブロックリストを編集できます。 Mobile Security は、次の優先順位に従ってメッセージを許可またはブロックします。 1. モバイルデバイスエージェント上の承認済みリスト 2. モバイルデバイスエージェント上のブロックリスト
有効	無効	ユーザは、モバイルデバイスエージェント上の承認済み/ブロックリストの編集のみ実行できます。 Mobile Security は、次の優先順位に従ってメッセージを許可またはブロックします。 1. サーバ上の承認済みリストまたはブロックリスト 2. モバイルデバイスエージェント上の承認済みリスト 3. モバイルデバイスエージェント上のブロックリスト

一括管理	ユーザ管理	説明
有効	有効	ユーザは、管理者によって定義された承認済み/ブロックリストを表示または編集できます。また、モバイルデバイスエージェント上の承認済み/ブロックリストを使用することもできます。 セキュリティポリシーがモバイルデバイスエージェントと同期される際、フィルタリストは同期されず、ポリシーに従って他のすべての設定が更新されます。 Mobile Security は、次の優先順位に従ってメッセージを許可またはブロックします。 1. モバイルデバイスエージェント上の承認済みリスト 2. モバイルデバイスエージェント上のブロックリスト 3. サーバ上の承認済みリストまたはブロックリスト

注意

SMS の承認済みおよびブロックリストでは、「[name1:]number1; [name2:]number2;...」という形式を使用する必要があります。

「name」の長さは、30 文字以内にする必要があります。さらに、電話番号は、4〜20 文字で指定する必要があり、0〜9、+、-、#、(、)、および空白を使用できます。エントリの最大数は 200 以内にする必要があります。

迷惑 WAP プッシュ対策ポリシー

この機能により、サーバ側で WAP プッシュ対策を制御できるようになります。この機能が有効にされている場合、WAP 承認済みリストを使用するかどうかを選択できます。

注意

WAP 承認済みリストでは、「[name1:]number1;[name2:]number2;...」という形式を使用する必要があります。

「name」の長さは、30 文字以内にする必要があります。さらに、電話番号は、4〜20 文字で指定する必要があり、0〜9、+、-、#、(,)、および空白を使用できます。エントリの最大数は 200 以内にする必要があります。

WAP プッシュ対策ポリシーの設定時、次のことを実行できます。

- モバイルデバイスで WAP プッシュ対策を有効または無効にする
- モバイルデバイスで承認済みリストを使用するよう設定するか、またはモバイルデバイスで WAP プッシュ対策を無効にする
- 管理コンソールから承認済みリストを設定する
- 管理者がサーバ側の制御を有効にしている場合は、ユーザは管理者によって定義された WAP プッシュ対策のタイプを変更することはできません。
- 管理者がサーバ側の制御を無効にしており、ユーザがモバイルデバイス上で Mobile Security を設定できるようにしている場合は、ユーザは管理者により設定された WAP プッシュ対策を表示または編集できませんが、モバイルデバイス側で個人の WAP プッシュ対策を編集できます。

注意

スパムメールメッセージのユーザの個人設定は、スパムメール対策ポリシーがモバイルデバイスエージェントに適用された後にクリアされます。

着信フィルタポリシー

この機能は、着信フィルタポリシーのサーバ側の制御を提供します。着信フィルタポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[着信フィルタポリシー] をクリックします。

着信フィルタポリシーの設定時、次のことを実行できます。

- モバイルデバイスの着信フィルタを有効または無効にする

- ブロックリストまたは承認済みリストを使用するようにモバイルデバイスを設定する
- 管理コンソールから承認済みリストを設定する
- 管理コンソールからブロックリストを設定する

承認済みまたはブロックフィルタリスト設定の詳細については、次の表を参照してください。

表 38-5. 着信フィルタポリシーのフィルタリスト設定

一括管理	ユーザ管理	説明
無効	有効	ユーザは、モバイルデバイスエージェント上の承認済み/ブロックリストを編集できます。 Mobile Security は、次の優先順位に従って URL を許可またはブロックします。 1. モバイルデバイスエージェント上の承認済みリスト 2. モバイルデバイスエージェント上のブロックリスト
有効	無効	ユーザは、モバイルデバイスエージェント上の承認済み/ブロックリストの編集のみを行えます。 Mobile Security は、次の優先順位に従って着信を許可またはブロックします。 1. サーバ上のブロックリスト 2. モバイルデバイスエージェント上の承認済みリスト 3. モバイルデバイスエージェント上のブロックリスト Android モバイルデバイス上の発信に対してサーバ側の制御を設定することもできます。

一括管理	ユーザ管理	説明
有効	有効	ユーザは、管理者によって定義された承認済み/ブロックリストを表示または編集できます。また、モバイルデバイスエージェント上の承認済み/ブロックリストを使用することもできます。 セキュリティポリシーがモバイルデバイスエージェントと同期される際、フィルタリストは同期されず、ポリシーに従って他のすべての設定が更新されます。 Mobile Security は、次の優先順位に従って着信を許可またはブロックします。 1. モバイルデバイスエージェント上の承認済みリスト 2. モバイルデバイスエージェント上のブロックリスト 3. サーバ上のブロックリスト Android モバイルデバイス上の発信に対してサーバ側の制御を設定することもできます。

注意

着信フィルタの承認済みおよびブロックリストでは、「[name1:]number1; [name2:]number2;...」という形式を使用する必要があります。

「name」の長さは、30 文字以内にする必要があります。さらに、電話番号は、4〜20 文字で指定する必要があり、0〜9、+、-、#、(,)、および空白を使用できます。エントリの最大数は 200 以内にする必要があります。

Web 脅威検出ポリシー

Mobile Security マネージメントサーバから Web 脅威検出ポリシーを管理できるようにし、それを Android モバイルデバイスに配信します。また、Android モバイルデバイスから Web 脅威検出ログをサーバに返せるようにします。

注意

Mobile Security Web 脅威検出は、初期設定の Android ブラウザおよび Google Chrome のみをサポートします。

Web 脅威検出ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[Web 脅威検出ポリシー] をクリックします。

Android モバイルデバイスのための Web 脅威検出

Web 脅威検出機能は、Android モバイルデバイス上での Web 脅威検出ポリシーのサーバ側の制御と、[低]、[中]、および [高] の 3 種類の事前定義されたセキュリティレベルを提供します。また、特定の URL をブロックまたは許可するための、ブロックリストと承認済みリストも提供します。Mobile Security は、ブロックリストに追加されたすべての URL をブロックし、承認済みリストに含まれるすべての URL を許可します。

注意

Web 脅威検出ポリシーは、モバイルデバイス上で Google Chrome および Android の初期設定の Web ブラウザのみをサポートします。

承認済みまたはブロックフィルタリスト設定の詳細については、次の表を参照してください。

表 38-6. Web 脅威検出ポリシーのフィルタリスト設定

サーバ制御	ユーザ管理	説明
無効	有効	ユーザは、モバイルデバイスエージェント上の承認済み/ブロックリストを編集できます。 Mobile Security は、次の優先順位に従って URL を許可またはブロックします。 1. モバイルデバイスエージェント上の承認済みリスト 2. モバイルデバイスエージェント上のブロックリスト

サーバ制御	ユーザ管理	説明
有効	無効	ユーザは、モバイルデバイスエージェント上の承認済み/ブロックリストの編集のみを行えます。 Mobile Security は、次の優先順位に従って URL を許可またはブロックします。 1. サーバ上の承認済みリスト 2. サーバ上のブロックリスト 3. モバイルデバイスエージェント上の承認済みリスト 4. モバイルデバイスエージェント上のブロックリスト
有効	有効	ユーザは、管理者によって定義された承認済み/ブロックリストを表示または編集できます。また、モバイルデバイスエージェント上の承認済み/ブロックリストを使用することもできます。 セキュリティポリシーがモバイルデバイスエージェントと同期される際、フィルタリストは同期されず、ポリシーに従って他のすべての設定が更新されます。 Mobile Security は、次の優先順位に従って URL を許可またはブロックします。 1. モバイルデバイスエージェント上の承認済みリスト 2. モバイルデバイスエージェント上のブロックリスト 3. サーバ上の承認済みリスト 4. サーバ上のブロックリスト

注意

Web 脅威フィルタの承認済みおよびブロックリストでは、[URL1] [URL2] [URL3] の形式を使用する必要があります。URL の間には、スペースまたは改行を挿入してください。

iOS モバイルデバイスのための Web 脅威検出

Web 脅威検出は、監視された iOS モバイルデバイスに、以下に対するアクセスを許可することによって、サーバ側の制御を提供します。

- 特定の Web サイトのみ
- 制限されたアダルトコンテンツ

機能の詳細については、次の表を参照してください。

表 38-7. Web 脅威検出ポリシーのフィルタリスト設定

機能	説明
特定の Web サイトのみ	このオプションを使用すると、サーバ上で設定した Web サイトにのみアクセスが制限されます。 Web 脅威検出ポリシーの [iOS] タブで、許可する URL を追加できます。これらの URL は、ユーザの iOS モバイルデバイスの Safari Web ブラウザに追加されます。
制限されたアダルトコンテンツ	このオプションは、フィルタリストを使用して、iOS モバイルデバイス上で許可またはブロックする Web サイトのサーバ側の制御を提供します。これらのフィルタは、iOS モバイルデバイスの初期設定のフィルタ設定とは関係なく、Web サイトへのアクセスをブロックまたは許可します。

注意

Web 脅威フィルタの承認済みおよびブロックリストでは、[URL1] [URL2] [URL3] の形式を使用する必要があります。URL の間には、スペースまたは改行を挿入してください。

パスワードポリシー

パスワードポリシーは、モバイルデバイス上のデータへの不正なアクセスを防止します。

パスワードポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、左側のメニューの [パスワードポリシー] をクリックします。

機能ロックポリシー

この機能を使用して、モバイルデバイスの特定の機能/コンポーネントの使用を制限 (無効化) または許可 (有効化) することができます。たとえば、特定グループのすべてのモバイルデバイスのカメラ機能を無効にすることができます。

機能ロックポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、左側のメニューの [機能ロックポリシー] をクリックします。

サポートされている機能/コンポーネントのリストについては、586 ページの「サポートされるモバイルデバイスの OS 機能」を参照してください。

警告!

WLAN/WIFI や Microsoft ActiveSync を無効にしている場合は注意が必要です。これらのオプションが両方とも使用できない場合、モバイルデバイスがサーバと通信できないことがあります。

Android モバイルデバイスでは、アクセスポイントを追加して、それらのアクセスポイントの範囲内のデバイスコンポーネントの可用性を制御することもできます。

サポートされるモバイルデバイスの OS 機能

次の表は、Mobile Security でプラットフォームごとにサポートされる機能の一覧を示しています。

表 38-8. Trend Micro Mobile Security 9.7 機能のマトリックス

ポリシー	機能	設定			
プロビジョニング	Wi-Fi	標準の Wi-Fi 設定	●	●	
		旧バージョンのホットスポット設定	●		
		Hotspot 2.0 の設定	●		
	Exchange ActiveSync	Exchange ActiveSync 設定	●		

ポリシー	機能	設定			
	VPN	VPN 設定	●		
	グローバル HTTP プロキシ	グローバル HTTP プロキシ設定	●		
	シングルサインオン	シングルサインオン設定	●		
	証明書	証明書設定	●		
	モバイルデータ通信ネットワーク	モバイルデータ通信ネットワーク設定	●		
	AirPlay/AirPrint	AirPlay/AirPrint 設定	●		
	テーマ (監視モードの場合のみ)	壁紙設定	●		
		フォント設定	●		
	管理対象ドメイン	マークされていないメールドメイン	●		
		管理対象の Safari Web ドメイン	●		
デバイスセキュリティ	セキュリティ設定	リアルタイム検索		●	
		パターンファイルのアップデート後に検索する		●	
		手動検索	●	●	
		Facebook 検索	●	●	
データ保護	スパム SMS 対策	サーバ側制御		●	
		ブロックリストを使用する		●	
		承認済みリストを使用する		●	
	スパムメール WAP プッシュ対策	サーバ側制御		●	
		承認済みリストを使用する		●	

ポリシー	機能	設定			
	着信フィルタ	サーバ側制御		●	
		ブロックリストを使用する		●	
		承認済みリストを使用する		●	
	Web 脅威検出	サーバ側制御		●	
		ブロックリストを使用する		●	
		承認済みリストを使用する		●	
		特定の Web サイトのみを許可する	●		
		制限されたアダルトコンテンツを許可する	●		
データ保護	パスワード設定	ログインにパスワードを使用する	●	●	●
		単純なパスワードを許可する	●	●	●
		英数字のパスワードが必要	●	●	●
		パスワードの最小文字数	●	●	●
		パスワードの有効期限	●	●	●
		パスワードの履歴	●	●	●
		自動ロック	●	●	●
		パスワードの失敗時の処理	●	●	●
	機能ロック	カメラ	●	●	
		FaceTime	●		
		画面キャプチャ	●		
		アプリのインストール	●		

ポリシー	機能	設定			
		ローミング中の同期	●		
		音声ダイヤル	●		
		アプリ内課金	●		
		マルチプレイヤーゲーム	●		
		ゲームセンター関係の友人の追加	●		
		ゲームセンター (監視モードの場合のみ)	●		
		暗号化バックアップの実行	●		
		音楽、ポッドキャスト、および iTunes U の明示化	●		
		デバイスのロック中の Passbook	●		
		Bluetooth および Bluetooth 検出		●	
		WLAN/Wi-Fi		●	
		3G データネットワーク		●	
		テザリング		●	
		開発者モード		●	
		スピーカー/スピーカーフォン/マイク			
		メモリカードの制限		●	
		Siri	●		
		デバイスのロック中の Siri	●		

ポリシー	機能	設定			
		不適切な言葉に対するフィルタを有効にする	●		
		iCloud サービスへのアクセスを有効にする	●		
		クラウドバックアップ	●		
		クラウドでのドキュメント同期	●		
		フォトストリーム	●		
		共有フォトストリーム	●		
		診断データ	●		
		信頼されていない Transport Layer Security (TLS) の受け入れ	●		
		iTunes Store パスワードの要求	●		
		YouTube	●		
		その他のアプリ内の管理対象アプリからドキュメントを開く	●		
		管理対象アプリ内のその他のアプリからドキュメントを開く	●		
		iTunes	●		
		Safari Web ブラウザ	●		
		オートフィル	●		
		JavaScript	●		
		ポップアップ	●		
		不正行為に関する警告の表示	●		

ポリシー	機能	設定			
		Cookie の許可	●		
		アプリの削除 (監視モードの場合のみ)	●		
		ブックストア (監視モードの場合のみ)	●		
		性描写を含む書籍 (監視モードの場合のみ)	●		
		設定プロファイルのインストール (監視モードの場合のみ)	●		
		iMessage (監視モードの場合のみ)	●		
		評価区分	●		
		ムービー	●		
		テレビ番組	●		
		アプリ	●		
		アカウントの変更 (監視モードの場合のみ)	●		
		AirDrop (監視モードの場合のみ)	●		
		アプリでのモバイルデータ通信の変更 (監視モードの場合のみ)	●		
		アシスタント (Siri) ユーザが生成したコンテンツ (監視モードの場合のみ)	●		
		クラウドキーチェーンの同期	●		
		「友達を探す」の変更 (監視モードの場合のみ)	●		

ポリシー	機能	設定			
		デバイスのロック解除のための指紋認証	●		
		ホストペアリング (監視モードの場合のみ)	●		
		ロック画面のコントロールセンター	●		
		ロック画面の通知の表示	●		
		ロック画面の今日の表示	●		
		Over the Air Public Key Infrastructure (OTAPKI) のアップデート	●		
		追跡型広告の制限の適用	●		
		AirPlay の発信でのペアリングパスワードの要求	●		
		管理対象アプリが iCloud にデータを保存することを許可	●		
		エンタープライズブックのバックアップを許可	●		
		制限の構成を許可	●		
		[すべてのコンテンツと設定の消去] を許可	●		
		Handoff を許可	●		
		Spotlight でインターネット検索結果を許可	●		
		エンタープライズブックのメモとハイライトの同期を許可	●		
		管理対象のドキュメントを AirDrop で共有することを許可	●		

ポリシー	機能	設定			
		iCloud フォトライブラリを許可	●		
		デバイスからのアプリのインストールを許可する	●		
		キーボードショートカットを許可	●		
		Apple Watch のペアリングを許可	●		
		パスコードの変更を許可	●		
		デバイス名の変更を許可	●		
		壁紙の変更を許可	●		
		アプリの自動ダウンロードを許可	●		
		エンタープライズアプリの信頼を許可	●		
	コンプライアンス設定	root 化/Jailbreak	●	●	
		暗号化なし	●	●	
		OS バージョンチェック	●	●	
アプリケーション管理	アプリの監視および制御	必須アプリ	●	●	
		許可するアプリ	●	●	
		アプリのロック (監視モードの場合のみ)	●		
	Volume Purchasing Program	Volume Purchasing Program	●		
リモートコントロール	登録		●	●	
	アップデート		●	●	

ポリシー	機能	設定			
	盗難対策	リモートの探索		●	
		リモートロック	●	●	
		リモートワイプ	●	●	●
		パスワードのリセット	●	●	
	Samsung KNOX ワークスペース	コンテナの作成		●	
		コンテナの削除		●	
		コンテナのロック		●	
		コンテナのロック解除		●	
		コンテナのパスワードのリセット		●	
Samsung KNOX ワークスペースポリシー	コンテナのアカウント設定	ブロックリスト		●	
		承認済みリスト		●	
	制約の設定	ユーザによるカメラの使用を許可する		●	
		アプリケーションのリストで共有の表示を許可		●	
	ブラウザの設定	[オートフィルを有効にする] の設定		●	
		[Cookie を有効にする] の設定		●	
		[ポップアップを有効にする] の設定		●	
		[不正行為に関する警告の表示] の設定		●	
		[JavaScript を有効にする] の設定		●	

ポリシー	機能	設定			
		Web プロキシを有効にする		●	
Samsung KNOX ワークスペースポリシー	コンテナのパスワード設定	パスワードの可視化を有効にする		●	
		パスワードの最小変更文字数		●	
		パスワードの最小文字数		●	
		自動ロックするまでの待ち時間		●	
		パスコードの最大入力回数		●	
		パスワードの履歴		●	
		パスワードの最長有効期間		●	
		パスワードに必要な特殊文字の最小数		●	
		パスワードの複雑さ		●	
	アプリの設定	インストールの承認済みリスト		●	
		インストールのブロックリスト		●	
		必須アプリ		●	
		無効化されたアプリ		●	
デバイス登録プログラム			●		

コンプライアンスポリシー

コンプライアンスポリシーにより、モバイルデバイスのコンプライアンス条件を設定できます。モバイルデバイスが条件に一致しない場合、Mobile Security は、サーバ UI 上にその非準拠の状態を表示します。Mobile Security はまた、非準拠の iOS モバイルデバイスにメールを送信し、非準拠の Android

モバイルデバイスに通知を表示します。コンプライアンスチェックリストには次のものが含まれます。

- root 化/Jailbreak — モバイルデバイスが root 化またはジェイルブレイクされていないかどうかをチェックします。
- 暗号化なし — モバイルデバイスで暗号化が有効かどうかをチェックします。
- OS バージョンチェック — OS のバージョンが、定義されている条件に一致するかどうかをチェックします。

コンプライアンスポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[コンプライアンスポリシー] をクリックします。

アプリの監視および制御ポリシー

アプリの監視および制御ポリシーにより、モバイルデバイスにインストールされているアプリのサーバ側の制御が可能になり、必須アプリがモバイルデバイスにプッシュされるようになります。

アプリの監視および制御ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[アプリの監視および制御ポリシー] をクリックします。

- 必須アプリ — リストに追加したすべてのアプリがモバイルデバイスにプッシュされます。VPN をアプリにリンクすることもできます。これにより、アプリは常にこの VPN を使用してネットワークに接続するようになります。
- 許可するアプリ — 承認済みリストおよびブロックリストを使用して、モバイルデバイスにインストールするアプリを制御します。

  iOS モバイルデバイスの場合、ポリシーに準拠していないアプリがあると、Mobile Security は管理者およびユーザに通知を送信します。

  Android モバイルデバイスの場合、Mobile Security はポリシーに準拠していないアプリをブロックし、他のすべてのアプリを許可します。

  - システムアプリのブロックを有効にする (Android のみ):

    Mobile Security は、Android モバイルデバイス上のすべてのシステムアプリをブロックします。

- 指定されたカテゴリのアプリを管理: モバイルデバイス上で有効または無効にするアプリケーションカテゴリを選択します。それらのカテゴリに属するアプリを承認済みリストまたはブロックリストに追加することで、例外を設定することもできます。たとえば、「ゲーム」というカテゴリタイプを無効にした場合、Mobile Security は、そのカテゴリに属するすべてのアプリをブロックします。ただし、そのアプリが承認済みリストに記載されている場合はブロックされません。

  Mobile Security は、次の優先順位に従ってアプリを許可またはブロックします。

  1. 承認済みリスト — Mobile Security は、無効にしたカテゴリに属しているアプリであっても、承認済みリストに指定されているアプリを許可します。
  2. ブロックリスト — Mobile Security は、有効にしたカテゴリに属しているアプリであっても、ブロックリストに指定されているアプリをブロックします。
  3. アプリの許可 — Mobile Security は、アプリが属しているカテゴリの、ユーザが選択した許可の状況に従ってアプリを許可またはブロックします。

- アプリの許可を有効にする (Android のみ): Android モバイルデバイス上で有効または無効にするアプリケーションサービスを選択します。それらのサービスを使用するアプリを承認済みリストまたはブロックリストに追加することで、例外を設定することもできます。たとえば、「データの読み取り」というサービスタイプを無効にした場合、Mobile Security は、データの読み取りサービスを使用するすべてのアプリをブロックします。ただし、そのアプリが承認済みリストに記載されている場合はブロックされません。

  Mobile Security は、次の優先順位に従ってアプリを許可またはブロックします。

  1. 承認済みリスト — Mobile Security は、無効にしたサービスを使用するアプリであっても、承認済みリストに指定されているアプリを許可します。

2. ブロックリスト — Mobile Security は、有効にしたサービスを使用するアプリであっても、ブロックリストに指定されているアプリをブロックします。

3. アプリの許可 — Mobile Security は、アプリが使用するサービスの、ユーザが選択した許可の状況に従ってアプリを許可またはブロックします。

- 次のアプリのみを許可する: ユーザがモバイルデバイスで使用することを許可するアプリを承認済みリストに追加します。有効な場合は、次のようになります。
  - Mobile Security は、承認済みリストに記載されていないアプリを検出すると、Android モバイルデバイス上に警告のポップアップメッセージを表示します。
  - iOS デバイスでは、Mobile Security は、承認済みリストに記載されていないアプリを検出すると、ユーザにメール通知を送信します。
- 次のアプリのみをブロックする: ユーザがモバイルデバイスで使用することを許可しないアプリをブロックリストに追加します。有効な場合は、次のようになります。
  - Mobile Security は、ブロックリストに記載されているアプリを検出すると、Android モバイルデバイス上に警告のポップアップメッセージを表示します。
  - iOS デバイスでは、Mobile Security は、ブロックリストに記載されているアプリを検出すると、ユーザにメール通知を送信します。
- アプリのロック (監視モードの場合のみ) — iOS モバイルデバイスで、指定されたアプリのみを使用できるように制限します。

Mobile Security は、制限されたアプリの有無を調べ、次のいずれかの方法でユーザにメールアラートを送信します。

- [管理] > [コミュニケーションサーバの設定] > [共通設定] (タブ) の [情報を収集する頻度] の設定に従って自動的に送信します。
- [管理] > [コミュニケーションサーバの設定] > [共通設定] (タブ) の [情報を収集する頻度] の設定を更新したときに送信します。

Volume Purchasing Program ポリシー

このポリシーは、Apple の Volume Purchase Program から購入された iOS アプリケーションを、管理者が Mobile Security 管理 Web コンソールにインポートできるようにします。Mobile Security は、Volume Purchasing Program リストにあるすべてのアプリケーションをグループ内のモバイルデバイスに配信します。

Volume Purchasing Program ポリシーを設定するには、次の手順を実行します。

1. エンタープライズアプリストアにアプリケーションを追加します。手順については、599 ページの「アプリケーションを追加する」を参照してください。
2. [ポリシー] をクリックし、ポリシー名をクリックして、[Volume Purchasing Program ポリシー] をクリックします。
3. [インポート] をクリックして、エンタープライズアプリストアからインポートするアプリケーションを選択します。
4. [保存] をクリックして、iOS モバイルデバイスにすべてのアプリケーションを配信します。

アプリケーションを追加する

手順

1. Mobile Security 管理 Web コンソールで、[アプリケーション] > [エンタープライズアプリストア] の順に選択します。

   [エンタープライズアプリストア] 画面が表示されます。
2. [Android] または [iOS] タブをクリックします。
3. [追加] をクリックします。

   [アプリの追加] 画面が表示されます。
4. これで、次のオプションのいずれかを使用して、リストにアプリケーションを追加できます。

   - ローカルコンピュータから追加 — Android または iOS モバイルデバイスのインストールファイルを選択します。

- Web クリップを追加 – アプリケーションの URL を入力すると、アプリケーションのアイコンがユーザのモバイルデバイスの [ホーム] 画面に表示され、モバイルデバイスの初期設定の Web ブラウザでリンクが開きます。
- (Android) 外部のアプリストアから追加 – 外部アプリストア内のアプリケーションへのリンクを入力します。アプリケーションのアイコンがユーザのモバイルデバイスの [ホーム] 画面に表示され、モバイルデバイスの初期設定の Web ブラウザでリンクが開きます。
- (iOS) iTunes Store のアプリへのリンクを追加 – 検索する VPP アプリケーションの名前を入力し、Apple アプリストアでアプリケーションを検索する国を選択し、検索結果から追加するアプリケーションを選択します。追加後は、VPP アプリケーションは Mobile Security の管理 Web コンソールのアプリストアでのみ利用できるようになります。モバイルデバイスにアプリケーションをプッシュするには、アプリケーションを Volume Purchasing Program ポリシーに追加する必要があります。手順については、599 ページの「Volume Purchasing Program ポリシー」を参照してください。

5. [続行] をクリックします。

   [アプリの編集] 画面が表示されます。

6. 次の項目を設定します。

   - アプリ名: アプリケーションの名前を入力します。
   - アプリのアイコン: アプリケーションのアイコンが表示されない場合、[アプリのアイコンのアップロード] アイコンをクリックして、アプリケーションアイコンを選択してアップロードします。
   - パッケージ名: アプリケーション ID が表示されない場合、アプリケーション ID を入力します。
   - VPP コードのファイル: iOS VPP アプリケーションの場合は、Apple から送信された Volume Purchase Code のファイルをアップロードします。
   - カテゴリ: アプリケーションのカテゴリを選択します。

注意

ドロップダウンからカテゴリを選択する必要があります。カテゴリを追加または削除するには、[カテゴリ] ボタンをクリックします。

- 説明: アプリケーションの説明を入力します。
- 公開方法: 次のいずれかを選択します。
  - 公開しない – サーバにアプリケーションをアップロードしますが、モバイルデバイスからは非表示のままにします。
  - 製品版として公開 – サーバにアプリケーションをアップロードし、モバイルデバイスに公開してダウンロードできるようにします。
  - ベータ版として公開 – サーバにアプリケーションをアップロードし、ベータ版としてモバイルデバイスに公開してダウンロードできるようにします。
- スクリーンショット: アプリケーションのスクリーンショットを選択してアップロードします。

7. [続行] をクリックします。

   そのアプリケーションがアプリケーションリストに表示されます。

コンテナポリシー

このポリシーを使用すると、Samsung KNOX コンテナのセキュリティ設定を管理できます。アカウントの承認済みリストまたはブロックリストを設定したり、制限を適用したり、ブラウザ、パスワード、およびアプリケーションを設定したりできます。

注意

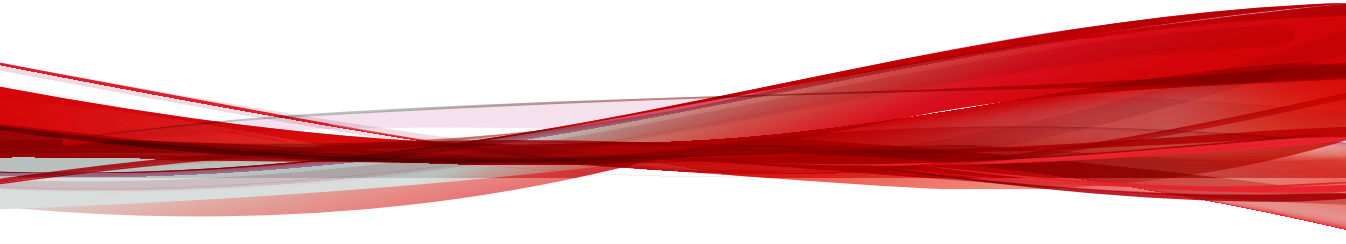
このポリシーを有効にする前に、Mobile Security で KNOX のライセンスを設定する必要があります。KNOX のライセンスを設定するには、管理 Web コンソールで、[運用管理] > [製品ライセンス] に移動します。

- アカウントの設定: 承認済みリストやブロックリストを使用して、Samsung KNOX コンテナにて追加または制限できるアカウントを指定します。
- 制約の設定: Samsung KNOX コンテナでカメラやファイル共有を無効にします。
- ブラウザの設定: Samsung KNOX コンテナのネイティブの Android Web ブラウザに対してセキュリティを設定します。
- パスワード設定: Samsung KNOX コンテナのパスワードセキュリティを設定します。
- アプリの設定: 次のリストを設定します。
  - フィルタアプリリスト: Samsung KNOX コンテナでアプリケーションのインストールを制限するための承認済みリストまたはブロックリストを設定します。
  - 必須アプリ: Samsung KNOX にインストールする必要があるアプリを指定する必須アプリリストを設定します。
  - アプリの無効化: 無効にするアプリリストを設定して、モバイルデバイスで特定のアプリを無効にします。このリストのアプリがモバイルデバイスにインストールされている場合、アプリは削除されませんが、ユーザが使用することはできなくなります。

コンテナポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、[コンテナポリシー] をクリックします。

パート XVII

Virtual Mobile Infrastructure



第 39 章

Virtual Mobile Infrastructure のダッシュボードウィジェット

本章では、Apex Central でサポートされる Virtual Mobile Infrastructure のウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

Trend Micro Virtual Mobile Infrastructure の起動回数の多いアプリケーションのトップ 5 ウィジェット

このウィジェットには、Trend Micro Virtual Mobile Infrastructure サーバによって報告された、起動回数の多い上位 5 個のアプリケーションが表示されます。

データは棒グラフで表示されます。Y 軸にはアプリケーション名が表示され、X 軸にはアプリケーションの起動回数が表示されます。

ドロップダウンメニューをクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。ドロップダウンメニューオプションで、ソースとして使用する管理下のサーバの IP アドレスを選択します。

Trend Micro Virtual Mobile Infrastructure の起動回数の多い Web アプリケーションのトップ 5 ウィジェット

このウィジェットには、Trend Micro Virtual Mobile Infrastructure サーバによって報告された、起動回数の多い上位 5 個の Web アプリケーションが表示されます。

データは棒グラフで表示されます。Y 軸にはアプリケーション名が表示され、X 軸にはアプリケーションの起動回数が表示されます。

ドロップダウンメニューをクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。ドロップダウンメニューオプションで、ソースとして使用する管理下のサーバの IP アドレスを選択します。

Trend Micro Virtual Mobile Infrastructure - オンラインユーザトップ 5 ウィジェット

このウィジェットには、Trend Micro Virtual Mobile Infrastructure サーバによって報告された、ワークスペースに最も長期間アクセスした上位 5 個のアクティブなユーザが表示されます。

データは棒グラフで表示されます。Y 軸にはユーザ名が表示され、X 軸にはユーザがワークスペースにアクセスした時間 (分) が表示されます。

ドロップダウンメニューをクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。ドロップダウンメニューオプションで、ソースとして使用する管理下のサーバの IP アドレスを選択します。

Trend Micro Virtual Mobile Infrastructure サーバの CPU の使用ステータスウィジェット

このウィジェットには、Trend Micro Virtual Mobile Infrastructure サーバの CPU 使用率が表示されます。

データはグラフで表示されます。Y 軸は CPU 使用率を割合で表し、X 軸は CPU 使用率が記録された時間を表します。

ドロップダウンメニューをクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。ドロップダウンメニューオプションで、ソースとして使用する管理下のサーバの IP アドレスを選択します。

Trend Micro Virtual Mobile Infrastructure サーバのディスクの使用状況ウィジェット

このウィジェットには、Trend Micro Virtual Mobile Infrastructure サーバのディスクの使用状況が表示されます。

次のデータが円グラフで表示されます。

- 空き: 管理下のサーバ上の使用可能なディスクストレージの量。
- 使用済み: 管理下のサーバ上の使用済みディスクストレージの量。
- 合計: 管理下のサーバ上の合計ディスクストレージの量。

ドロップダウンメニューをクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。ドロップダウンメニューオプションで、ソースとして使用する管理下のサーバの IP アドレスを選択します。

Trend Micro Virtual Mobile Infrastructure サーバのメモリの使用ステータス

このウィジェットには、Trend Micro Virtual Mobile Infrastructure サーバのメモリ使用量が表示されます。

次のデータが円グラフで表示されます。

- 空き: 管理下のサーバ上の使用可能なメモリの容量。
- 使用済み: 管理下のサーバ上の使用済みメモリの容量。
- 合計: 管理下のサーバ上の合計メモリの容量。

ドロップダウンメニューをクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。ドロップダウンメニューオプションで、ソースとして使用する管理下のサーバの IP アドレスを選択します。

Trend Micro Virtual Mobile Infrastructure のユーザのステータスウィジェット

このウィジェットには、Trend Micro Virtual Mobile Infrastructure サーバによって報告された、現在のユーザのステータスが表示されます。

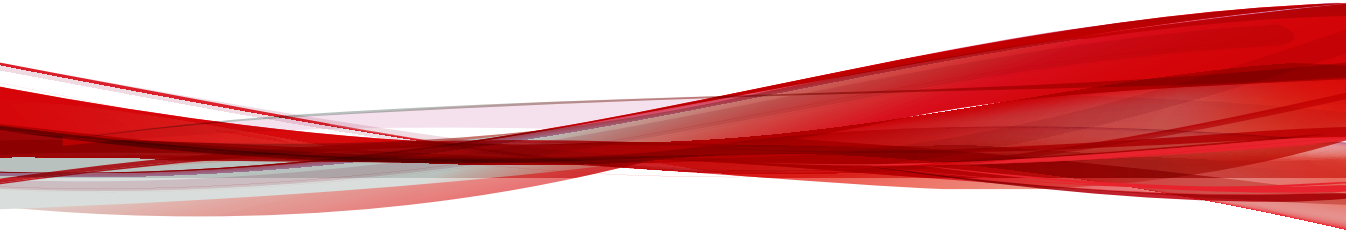
次のユーザステータスが円グラフで表示されます。

- 有効: ユーザは現在サーバに接続されており、ワークスペースにアクセスしています。
- アイドル: ユーザはサーバに接続されていますが、現在はワークスペースにアクセスしていません。
- オフライン: ユーザはサーバから切断されています。
- 無効: ユーザアカウントは無効化されており、ユーザはサーバにアクセスできません。

ドロップダウンメニューをクリックして、ウィジェットがソースとして使用する管理下のサーバを変更します。ドロップダウンメニューオプションで、ソースとして使用する管理下のサーバの IP アドレスを選択します。

パート XVIII

Vulnerability Protection



第 40 章

Vulnerability Protection のダッシュボードウィジェット

本章では、Apex Central でサポートされる Vulnerability Protection のダッシュボードウィジェットのヘルプトピックについて説明します。

次のトピックがあります。

Vulnerability Protection アプリケーションの種類のアクティビティ (検出) ウィジェット

このウィジェットでは、IPS (検出) イベントに関連付けられているアプリケーションの種類をエンドポイント上で追跡します。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

ヒント

このウィジェットには、単一の Vulnerability Protection サーバのデータのみが表示されます。複数の Vulnerability Protection サーバを監視するには、サーバごとにウィジェットを作成します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、特定のアプリケーションの種類に関連付けられている IPS (検出) イベントをフィルタして表示するには、[合計] 列の値をクリックします。

データ	説明
アプリケーションの種類名	アプリケーションの種類の名前
合計	時間範囲内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の時間範囲におけるイベント数

データ	説明
Trend	前回の期間から今回の期間への割合の変化

Vulnerability Protection アプリケーションの種類のアクティビティ (防御) ウィジェット

このウィジェットでは、IPS (防御) イベントに関連付けられているアプリケーションの種類をエンドポイント上で追跡します。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

ヒント

このウィジェットには、単一の Vulnerability Protection サーバのデータのみが表示されます。複数の Vulnerability Protection サーバを監視するには、サーバごとにウィジェットを作成します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、特定のアプリケーションの種類に関連付けられている IPS (防御) イベントをフィルタして表示するには、[合計] 列の値をクリックします。

データ	説明
アプリケーションの種類名	アプリケーションの種類の名前
合計	時間範囲内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の時間範囲におけるイベント数
Trend	前回の期間から今回の期間への割合の変化

Vulnerability Protection 機能の概要ウィジェット

このウィジェットは、Vulnerability Protection モジュールそれぞれの最新アクティビティを表示します。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

ヒント

このウィジェットには、複数の Vulnerability Protection インストールから集計されたデータが表示されます。このウィジェットに表示される Vulnerability Protection インストールは、[サーバの登録] 画面で定義します。複数の Vulnerability Protection インストールを監視するには、インストールごとにウィジェットを作成します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

データ	説明
モジュール	Vulnerability Protection モジュールの名前
保護されているコンピュータ	モジュールで現在保護されている管理対象コンピュータの数と、その数が示すすべての管理対象コンピュータの割合
イベント数	指定された期間にモジュールによって生成されたイベント数
Trend	前回の期間から今回の期間への割合の変化

Vulnerability Protection のファイアウォールイベント履歴ウィジェット

このウィジェットには、指定された時間範囲内に発生するファイアウォールイベントの件数が表示されます。グラフには、検出モードと防御モードの両方のファイアウォールルールによって実行されたイベントが表示されます。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、選択した時間範囲内に発生したファイアウォールイベント (検出または防御) をフィルタして表示するには、棒グラフのセクションをクリックします。

Vulnerability Protection の IPS イベント履歴ウィジェット

このウィジェットは、指定された時間範囲内に発生した IPS イベントの件数を表示します。グラフには、検出モードと防御モードの両方の IPS ルールによって実行されたイベントが表示されます。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、特定の時間範囲内に発生した IPS イベント (検出または防御) をフィルタして表示するには、棒グラフのセクションをクリックします。

Vulnerability Protection の侵入防御のアクティビティ (検出) ウィジェット

このウィジェットは、検出モードで動作中に、イベントを実行した件数が最も多かった 5 つの IPS ルールを表示します。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サ

ーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、特定のルールによって実行された IPS (検出) イベントをフィルタして表示するには、[合計] 列の値をクリックします。

データ	説明
理由	ルールの名前
合計	時間範囲内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の時間範囲におけるイベント数
Trend	前回の期間から今回の期間への割合の変化

Vulnerability Protection の侵入防御のアクティビティ (防御) ウィジェット

このウィジェットには、防御モードで動作中に、イベントを実行した件数が最も多かった 5 つの IPS ルールが表示されます。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意
ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、特定のルールによって実行された IPS (防御) イベントをフィルタして表示するには、[合計] 列の値をクリックします。

データ	説明
理由	ルールの名前
合計	時間範囲内のイベント数と、その種類のイベント総数の割合
前回の合計	前回の時間範囲におけるイベント数
Trend	前回の期間から今回の期間への割合の変化

Vulnerability Protection のキーパフォーマンスインジケータウィジェット

このウィジェットは、指定された時間範囲内に、攻撃の予兆の検出の設定によって実行されたイベントの件数を表示します。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意
ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、特定の時間範囲内に発生した攻撃の予兆の検出イベントをフィルタして表示するには、棒グラフのセクションをクリックします。

Vulnerability Protection の攻撃の予兆検索イベント履歴ウィジェット

このウィジェットは、指定された時間範囲内に、攻撃の予兆の検出の設定によって実行されたイベントの件数を表示します。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager の [イベント] ページを表示して、特定の時間範囲内に発生した攻撃の予兆の検出イベントをフィルタして表示するには、棒グラフのセクションをクリックします。

Vulnerability Protection のステータスの概要ウィジェット

このウィジェットには、重大なアラートと警告アラートの件数、および特定のステータスのエンドポイントの割合を示す円グラフが表示されます。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

ヒント

このウィジェットには、複数の Vulnerability Protection インストールから集計されたデータが表示されます。このウィジェットに表示される Vulnerability Protection インストールは、[サーバの登録] 画面で定義します。複数の Vulnerability Protection インストールを監視するには、インストールごとにウィジェットを作成します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

コンピュータステータス	説明
管理 (緑)	保護されており、エラーや警告はありません。
未管理 (青)	保護されていません。
ロック (灰色)	ロックされています。コンピュータがロック状態の間、Vulnerability Protection Manager は Agent/Appliance とは通信せず、コンピュータ関連のアラートは発令されません。
重大 (赤)	エラー状態です。
警告 (黄)	警告状態です。

Vulnerability Protection 脆弱なエンドポイントウィジェット

このウィジェットは、脆弱なエンドポイントを追跡するために使用します。

このウィジェットのデータソースとして使用する Vulnerability Protection インストールを選択できます。データソースを選択するには、設定アイコン (>) をクリックして、表示されたリストからソースを選択します。

ヒント

このウィジェットには、単一の Vulnerability Protection サーバのデータのみが表示されます。複数の Vulnerability Protection サーバを監視するには、サーバごとにウィジェットを作成します。

Vulnerability Protection のウィジェットで選択可能な Vulnerability Protection インストールを定義するには、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択し、新しい Vulnerability Protection サーバを追加します。

注意

ユーザアカウントの権限によって許可されているデータのみがウィジェットに表示されます。

Vulnerability Protection Manager のルールプロパティページを表示して、仮想パッチが適用済みのエンドポイントや保護されていないエンドポイントを表示するには、[仮想パッチ適用済み] または [保護なし] 列の値をクリックします。

データ	説明
名前	IPS ルールの名前
重大度	IPS ルールの重大度レベル
CVE	CVE (Common Vulnerabilities and Exposure) 番号
CVSS スコア	National Vulnerability Database に登録されている脆弱性の重大度
MS ID	Microsoft のセキュリティパッチ ID
仮想パッチ適用済み	検索後に推奨されるルールが割り当てられたエンドポイントの数

データ	説明
保護なし	検索後に推奨されるルールが割り当てられていないエンドポイントの数

索引

さ

た