Trend Micro Apex Central™

Patch 4

管理者ガイド

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/jp/solution/000207383

法人向け製品のサポートについて

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

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

商標について

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

P/N: APEM09683/230207_JP (2023/03)

プライバシーと個人データの収集に関する規定

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

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

https://www.go-tm.jp/data-collection-disclosure

重要

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

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

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

目次

第 8 章：管理下の製品の登録

第 9 章：セキュリティエージェントのインストール

第 10 章：製品ディレクトリ

第 11 章：コンポーネントアップデート

第 12 章：コマンド追跡と製品通信

パート IV：ポリシー

第 13 章：ポリシー管理

第 14 章：ポリシーリソース

パート V：検出

第 15 章：ログ

第 16 章：通知

付録 C：トークン変数

付録 D：IPv6 のサポート

付録 E：MIB ファイル

付録 F：Syslog コンテンツマッピング - CEF

索引

はじめに

このドキュメントでは、Trend Micro Apex Central™について説明し、概要、管理下の製品の統合、およびセキュリティ監視の詳細を示します。

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。
インストールおよびアップグレードガイド	Apex Central をインストールするための要件や手順を説明する PDF ドキュメント **注意** マイナーリリースバージョン、Service Pack、またはパッチでは、インストールおよびアップグレードガイドを利用できない場合があります。
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。
ウィジェットおよびポリシー管理ガイド	Apex Central でのダッシュボードウィジェットおよびポリシー管理の設定方法の説明 このガイドを参照するには、https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-apex-central-2019-widget-and-policy-management-guide/preface-(wpg)_001.aspx にアクセスしてください。
Automation Center	Apex Central のオートメーション API の使用方法を説明したオンラインユーザガイドとレファレンス: https://automation.trendmicro.com/apex-central/home
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/jp/technical-support を参照してください。

PDF ドキュメントおよび Readme の最新バージョンをダウンロードするには、次の Web サイトにアクセスしてください。

http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

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

表記	説明
 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
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

用語	説明
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

Apex Central の概要

本章では、Trend Micro Apex Central™について説明し、その機能の概要を示します。

次のトピックがあります。

Apex Central について

Trend Micro Apex Central™は、トレンドマイクロの製品およびサービスを、ゲートウェイ、メールサーバ、ファイルサーバ、およびデスクトップの各レベルで集中管理するための Web ベースのコンソールです。管理者は、ポリシー管理機能を使用して製品設定を行い、管理下の製品やエンドポイントに配信できます。Apex Central の Web ベースの管理コンソールにより、ネットワーク全体のウイルス対策およびコンテンツセキュリティ 製品やサービスを 1 か所で監視できます。

Apex Central により、システム管理者は感染、セキュリティ違反、ウイルス/不正プログラムの検出ポイントなどの活動を監視し、報告できるようになります。システム管理者は、パターンファイル、検索エンジン、スパムメール判定ルールなどのコンポーネントをダウンロードし、ネットワーク全体に配信することにより、最新の保護を確実に行うことができます。Apex Central では、手動アップデートと予約アップデートの両方が可能です。また、さらに柔軟性を高めるため、グループまたは個人として製品の設定や管理ができるようになっています。

新機能

このバージョンの Apex Central には、次の新機能と拡張機能が含まれています。

機能	説明
新しいプラットフォーム	Apex Central では、Windows Server 2022 へのインストールがサポートされます。

表 1-1. これまでのアップデート

機能	説明
イベント通知	不要な通知が大量に受信者に送信されないように、次のイベント通知設定は無効になりました ([レポート] > [通知] > [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 • 相関関係のあるイベントの検出
高度な脅威アクティビティの通知の追加	Apex Central は、挙動監視違反と機械学習型検索の検出に対して高度な脅威アクティビティのイベント 通知をサポートします。
詳細ログポリシーの最適化	Apex One 仮想パッチの詳細ログポリシー ([ポリシー] > [ポリシー管理] > [Apex One セキュリティエージェント] > [仮想パッチの設定] > [ネットワークエンジンの設定]) では、初期設定として「ステートフル, フラグおよび確認の抑制」が使用され、フラグと確認機能に関連するイベントが除外されます。
同時セッションの制限	Apex Central では、1 つのユーザアカウントに対して複数の管理コンソールセッションが実行されないよう管理者が制限できます。
重大イベントの監査	Apex One サーバとセキュリティエージェントは、重大なシステムイベント (セキュリティエージェントの移動、セキュリティエージェントのアンインストール、パスワードのリセット) に関連する Windows イベントログを収集し、そのログを Apex Central 製品監査イベントログに送信します。
ダッシュボードの拡張機能	• [オペレーションセンター] タブの名称は [セキュリティ状態]、[脅威の検出] タブの名称は [脅威の統計] に、それぞれ変更になりました。また、以前の [情報漏えい対策イベントの調査] タブにあったウィジェットは [情報漏えい対策] タブに移動されました。 • ダッシュボードの [セキュリティ状態] タブを [表データ] 表示に切り替えることで、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できます。

機能	説明
強化された API 統合	Apex Central には、CEF 形式の検出ログ、製品監査イベント、セキュリティエージェントのパターンファイルのアップデートステータス、セキュリティエージェントのエンジンのアップデートステータスを SIEM サーバに転送するための API が用意されます。 詳細については、https://automation.trendmicro.com/apex-central/home を参照してください。
影響分析の機能強化	影響分析を実行したときに 60 秒ごとに自動的に、[影響を受けたユーザ] 画面の表示が更新されるようになりました。
新しいダッシュボードウィジェット	• クイック調査ウィジェットを使用すると、履歴調査をダッシュボードから直接開始できます。 • Attack Discovery による検出ウィジェットを使用すると、Endpoint Sensor の Attack Discovery 機能により生成された検出ログを表示できます。 Attack Discovery のログに、MITRE™による攻撃手法と技術の分析情報と Windows Antimalware Scan Interface (AMSI) のデータが含まれます。 • IPS イベントの影響を受ける上位のエンドポイント、上位の IPS 攻撃元、および上位の IPS イベントの 3 つのウィジェットで、ネットワークで発生した IPS イベントの可視性が高まりました。
パスワードの複雑さの強化	• Apex Central のユーザアカウントのパスワードの複雑さの要件が強化されました。 • セキュリティ向上のため、セキュリティエージェントのアンロードおよびアンインストール機能のパスワードの複雑さの要件が強化されました。
ポリシーの継承	挙動監視、機械学習型検索、および信頼済みプログラムリストのポリシーが強化され、ポリシーの継承がサポートされるようになりました。
SQL Server のサポート	Apex Central では、Microsoft SQL Server 2019 の累積アップデート 4 (CU4) と SQL Server Express CU4 をサポートします。
Syslog の強化	• Apex Central では、IPS および製品監査イベントログを Syslog サーバに送信できます。 • Common Event Format (CEF) の Syslog に、検出された重大な脅威の種類が示されます。

機能	説明
脆弱性に対する Patch	Apex Central では、クロスサイトスクリプティング (XSS) および SQL インジェクションの脆弱性に対する Patch を適用済みです。
Web ブラウザのサポート	Apex Central は Microsoft Edge (Chromium) をサポートします。

主な機能と利点

Apex Central には、次の機能と利点があります。

機能	利点
Active Directory の統合	Apex Central では複数の Active Directory フォレストとの統合がサポートされ、ユーザだけでなく Active Directory グループもインポートできます。さらに、Active Directory 認証を有効にすることで、エクストラネット全体でフェデレーションビジネスパートナーのユーザまたはグループが Apex Central コンソールに安全にログオンできるようになります。
ダッシュボード	[ダッシュボード] タブとウィジェットを使用すると、脅威の検出、コンポーネントのステータス、ポリシー違反などに関する、管理下の製品と Apex Central の情報を幅広く確認できます。
セキュリティ状態	[セキュリティ状態] タブを使用すると、パターンファイルと情報漏えい対策のコンプライアンスのステータス、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に関する情報をすぐに確認できます。
ユーザ/エンドポイントディレクトリ	Apex Central ネットワーク内のすべてのユーザとエンドポイント、およびセキュリティの脅威の検出に関する詳細情報が表示されます。
製品ディレクトリ	システム管理者は、管理下の製品に対して設定の変更を即座に配信したり、ウイルス/不正プログラムの大規模感染発生時であっても Apex Central 管理コンソールから手動検索を実行したりできます。

機能	利点
ポリシー管理	システム管理者は、ポリシーを使用して単一の管理コンソールから管理下の製品とエンドポイントに製品を設定および配信し、組織内で一貫したウイルス/不正プログラム対策ポリシーおよびコンテンツセキュリティポリシーを実施できます。
ログ	単一の管理コンソールを使用して、個々の製品コンソールにログオンすることなく、登録済みのすべての管理下の製品の統合されたログを確認できます。
イベント通知	メール、Windows の Syslog、SNMP トラップ、アプリケーションによって通知が送信されるように Apex Central を設定することで、管理者はネットワークイベントを常に把握できます。
レポート	カスタムテンプレートまたはデフォルトテンプレートから包括的なレポートを作成すると、ネットワーク保護とセキュリティコンプライアンスの実現に必要な実用的な情報を入手できます。
コンポーネントアップデート	パターンファイル、スパムメール判定ルール、検索エンジン、およびその他のウイルス対策/コンテンツセキュリティコンポーネントを安全にダウンロードおよび配信して、すべての管理下の製品を最新の状態にします。
Connected Threat Defense	Apex Central では、トレンドマイクロのさまざまな製品やソリューションを統合することで、標的型攻撃や高度な脅威を検出して分析し、被害が拡大する前に対処することができます。
安全な通信インフラストラクチャ	Apex Central には、SSL (Secure Socket Layer) プロトコルに基づいた通信インフラストラクチャが使用されており、認証を使用してメッセージを暗号化することもできます。
役割ベースの管理	特定の Web コンソール権限を管理者に割り当て、特定のタスクを実行するために必要なツールと権限だけを提供することにより、Apex Central 管理コンソールへのアクセス権の付与と管理を実行します。
コマンド追跡	コマンド追跡を使用すると、Apex Central 管理コンソールを使用して実行されたコマンド (パターンファイルの更新やコンポーネントの配信など) が正常に完了したかどうかを継続的に監視できます。
ライセンス管理	新しいアクティベーションコードを配信するか、管理下の製品の既存のアクティベーションコードを再アクティベートします。

機能	利点
セキュリティエージェントのインストール	Apex One または Apex One (Mac) 向けのセキュリティエージェントのインストールパッケージを、Apex Central 管理コンソールから直接ダウンロードします。
2 要素認証	2 要素認証はユーザアカウントの安全性を強化します。そのためには、ユーザは Apex Central にログオンするために、Google Authenticator アプリで生成された認証コードを入力する必要があります。
ブラウザのサポート	このバージョンの Apex Central では、以下がサポートされています。 • Microsoft™ Internet Explorer™ • Microsoft™ Edge™ • Microsoft™ Edge™ (Chromium) • Google™ Chrome™

Apex Central アーキテクチャ

Trend Micro Apex Central™は、トレンドマイクロの製品やサービスを 1 か所から集中管理する機能を提供します。Apex Central を使用することにより、企業におけるウイルス/不正プログラム対策ポリシーやコンテンツセキュリティポリシーを一貫して実施できます。

次の表は、Apex Central が使用するコンポーネントについて説明しています。

コンポーネント	説明
Apex Central サーバ	エージェントから収集したすべてのデータを保存する格納先として機能します。Apex Central サーバでは次の機能が提供されます。 • 管理下の製品の設定やログを保存する SQL データベース Apex Central は、ログ、管理下の製品の情報、ユーザアカウント、ネットワーク環境、通知設定などのデータの保存に Microsoft SQL Server データベース (`db_ApexCentral.mdf`) を使用します。 • Apex Central の Web コンソールをホストする Web サーバ • メールメッセージでイベントに関する通知を送信するメールクライアント Apex Central は、個々の受信者または受信者グループに Apex Central システム内で発生したイベントに関する通知を送信します。メール、SNMP トラップ、Syslog、または組織が通知の送信に使用する組織内のアプリケーションまたは業界標準のアプリケーションを使用して、イベントに関する通知を送信します。 • ウイルス対策/コンテンツセキュリティ製品に関するレポートを生成するレポートサーバ Apex Central レポートは、Apex Central ネットワークで発生したセキュリティの脅威およびコンテンツセキュリティ関連イベントのデータをオンラインで収集します。
Trend Micro Management Communication Protocol (MCP)	MCP は、Apex Central サーバと次世代エージェントをサポートする管理下の製品間の通信を処理します。 MCP は管理下の製品と共にインストールされ、一方向または双方向通信を使用して Apex Central と通信します。MCP エージェントは、Apex Central に対して、指示とアップデートをポーリングします。
Web サービスの統合通信	Apex Central と管理下の製品との通信を可能にするエージェントレスの統合モデル

コンポーネント	説明
Web ベースの管理コンソール	このコンソールにより、管理者はインターネット接続と Web ブラウザを利用して、すべてのコンピュータから Apex Central を管理できるようになります。 Apex Central 管理コンソールは、Microsoft Internet Information Server (IIS) を経由してインターネット上に公開され、Apex Central サーバのサービスを提供する Web ベースのコンソールです。管理者は、対応する Web ブラウザがインストールされた任意のコンピュータから、Apex Central システムを管理できるようになります。
ウィジェットフレームワーク	管理者はウィジェットフレームワークを使用して、Apex Central システムを監視するためにカスタマイズしたダッシュボードを作成できます。

パート II

はじめに

第 2 章

管理コンソール

このセクションでは、Apex Central の Web ベース管理コンソールにアクセスして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。

管理コンソールについて

Apex Central の管理コンソールは、Apex Central サーバに登録されたトレンドマイクロ製品によって保護されているすべてのエンドポイントおよびユーザに対して、集中管理、監視、セキュリティの可視性を提供します。コンソールには、セキュリティ要件と仕様に基づいて設定できる一連の初期設定と値が含まれています。管理コンソールを使用すると、対応する Web ブラウザがインストールされた任意のコンピュータから、Apex Central システムを管理できます。

注意

管理コンソールは、画面解像度 1366×768 ピクセルで表示してください。

Apex Central では、次の Web ブラウザがサポートされます。

- Microsoft Internet Explorer™ 11
- Microsoft Edge™
- Microsoft Edge™ (Chromium)
- Google Chrome™

管理コンソールの要件

リソース	要件
プロセッサ	300 MHz Intel™ Pentium™プロセッサまたは同等の CPU
RAM	128 MB 以上
使用可能な空きディスク容量	30 MB 以上

リソース	要件
ブラウザ	Microsoft Internet Explorer™ 11、Microsoft Edge™、Microsoft Edge™ (Chromium)、または Google Chrome™ **重要** Internet Explorer を使用して Apex Central 管理コンソールにアクセスするときは、[互換表示] をオフにしてください。
その他	解像度が 1366 x 768、256 色以上をサポートするモニタ

管理コンソールへの HTTPS アクセスの設定

Apex Central のインストールの際には、管理コンソールにアクセスするときのセキュリティレベルを選択できます。最も低いセキュリティレベルでは、HTTP 接続のみが要求されます。最も高いセキュリティレベルでは、HTTPS 接続が要求されます。インストール時に最も低いセキュリティレベルの接続を選択した場合でも、インストール後にアクセスレベルを最も高いセキュリティレベルの接続に変更できます。

重要

- Apex Central サーバとの間で暗号化された情報やデジタル署名付きの情報を送受信するには、証明書を取得して、Apex Central 仮想ディレクトリをセットアップしておく必要があります。
- 以下の手順では、Apex Central のインストールが済んでいる Windows Server 2012 R2 における証明書の設定方法について説明します。

  異なるバージョンの Windows Server を実行している場合は、その Windows Server に関する Microsoft のドキュメントを参照してください。

手順

1. 証明書発行機関から「SSL サーバ証明書」を取得します。
2. Apex Central サーバにログオンします。

3. [スタート] > [管理ツール] > [インターネット インフォメーション サービス (IIS) マネージャー] に移動します。

   [インターネット インフォメーション サービス (IIS) マネージャー] 画面が表示されます。

4. 左側の [接続] ペインで、サーバを選択します。

5. 中央の [機能の表示] ペインで、[サーバ証明書] をダブルクリックします。

6. 右側の [処理] ペインで、[インポート...] をクリックします。

   [証明書のインポート] 画面が表示されます。

7. 手順 1 で取得した Web サイト証明書をインポートします。

   a. 証明書ファイルをアップロードします。

   b. 証明書のパスワードを指定します。

   c. 証明書ストアを選択します。

   d. [OK] をクリックします。

      Windows Server から証明書ファイルがインポートされ、[証明書のインポート] 画面が閉じます。

8. 右側の [接続] ペインで [サイト] フォルダを展開し、Apex Central のインストール中に作成された [<Web サイト>] を選択します。

   注意

   Apex Central のインストール時に [<Web サイト>] のカスタム名を指定しなかった場合、初期設定の [<Web サイト>] の名前は [既定の Web サイト] になります。

9. [<Web サイト>] を右クリックして [バインドの編集] を選択します。

   [サイトのバインド] 画面が表示されます。

10. サイトのバインドを設定します。

    a. [https] タイプを選択して [編集] をクリックします。

ヒント

[サイトのバインド] リストに [https] タイプが表示されなかった場合は、[追加] をクリックして手動で [https] タイプを追加します。

b. [SSL 証明書] ドロップダウンリストから、インポートされた証明書ファイルを選択します。

c. [OK] をクリックします。

d. [閉じる] をクリックします。

11. SSL を設定します。

a. [<Web サイト>] を展開し、[WebApp] 仮想ディレクトリを選択します。

b. 中央の [機能の表示] ペインで、[SSL 設定] をダブルクリックします。

c. [SSL が必要] を選択します。

d. 右側の [処理] ペインで、[適用] をクリックします。

[アラート] ペインが表示され、変更が正常に保存されたことが示されます。

12. 次の場所で HTTPS ポート番号を指定します。

- レジストリキー:

  ```
  HKLM\Software\Wow6432Node\TrendMicro\TVCS\WebPort
  ```

- システム設定ファイル:

  `<Apex Central のインストールフォルダ>\systemconfiguration.xml` ファイルで `m_uiWebServer_Https_Port` を探し、値を HTTPS ポート番号に設定します。

13. 次のサービスを再起動します。

- Trend Micro Apex Central
- Trend Micro Management Infrastructure

- World Wide Web Publishing Service

管理コンソールにアクセスする

Apex Central サーバ、またはインターネットにアクセス可能な、サポート対象の Web ブラウザが備わった任意のエンドポイントから Apex Central 管理コンソールにログオンします。

注意

- 同じエンドポイントの複数のブラウザから、同じユーザアカウントを使用して Apex Central 管理コンソールにログオンすることはできません。
- 異なるエンドポイントから、同じユーザアカウントを使用して Apex Central 管理コンソールにログオンすることはできます。

手順

1. Apex Central 管理コンソールにローカルまたはリモートでアクセスします。
   - コンソールにローカルでアクセスするには、Apex Central サーバで、[スタート] > [プログラム] > [Trend Micro Apex Central] > [Trend Micro Apex Central] の順に選択します。
   - コンソールにリモートでアクセスするには、Web ブラウザを開き、次のアドレスに移動します。

     `http(s)://<ホスト名>/WebApp/login.html`

     <ホスト名> には、Apex Central サーバの完全修飾ドメイン名 (FQDN)、IP アドレス、またはサーバ名を指定します。

   [ログオン] 画面が表示されます。
2. ログオン情報を入力します。
   - Apex Central アカウントのログオン情報を使用してログオンするには、ユーザ名とパスワードを入力します。

- ドメインのログオン情報でログオンするには、ドメインとユーザ名を次の形式で入力し、パスワードを入力します。

  ドメイン\ユーザ名

  注意

  ドメインのログオン情報でログオンするには、Active Directory 構造が統合されている必要があります。

  詳細については、Active Directory 管理者にお問い合わせください。

3. [ログオン] をクリックします。

   注意

   管理者が 2 要素認証を有効にしている場合は、次の画面の指示に従います。

   2 要素認証の設定の詳細については、管理者に問い合わせてください。

4. (オプション) ドメインのログオン情報でログオンする場合、[ドメインのログオン情報でログオンする] ボタンをクリックすることで、ログオン情報を保存して再利用できます。

   注意

   [ドメインのログオン情報でログオンする] ボタンは、管理者が Apex Central サーバを Active Directory サーバ上の Active Directory ドメインに追加した場合にのみ表示されます。

   Apex Central では、ドメインのログオン情報を入力し、自動ログオンを確認するよう求めるメッセージが表示されます。次回コンソールにアクセスしたときは、[ドメインのログオン情報でログオンする] をクリックすると自動的にログオンします。

5. 管理コンソールからログオフするには、管理コンソールの右上にある<アカウント名> > [ログオフ]をクリックします。

管理コンソールの設定

Apex Central の管理コンソールの設定では、管理コンソールへのアクセス方法と画面の更新の間隔を設定できます。

手順

1. [運用管理] > [設定] > [管理コンソールの設定] に移動します。

   [管理コンソールの設定] 画面が表示されます。

2. 必要に応じて設定します。

セクション	設定
管理コンソールの自動更新	[自動更新を有効にする] を選択すると、指定した間隔で Apex Central サーバの画面のデータが更新されるようになります。 • 管理コンソールの更新間隔: 管理コンソールの画面のデータが更新される間隔 (秒数) を選択します。
管理コンソールのタイムアウト	[管理コンソールからの自動ログアウトを有効にする] を選択すると、指定した間隔でユーザがログオフされます。 • 管理コンソールから自動ログアウトするまでの経過時間: 操作がなく、管理コンソールから自動ログアウトするまでの時間を選択します。
セキュリティ設定	[ログオン試行の失敗後、ユーザアカウントを自動的にロックします] を選択すると、指定したログオンの失敗回数に達するとユーザアカウントがロックされます。 • ログオンの連続失敗: ログオンの連続失敗回数を指定します。 • アカウントのロック時間: ユーザアカウントをロックする時間 (分数) を指定します。
同時セッションの制限	同じユーザアカウントに対して複数の管理コンソールログオンセッションを実行しないようにするには、[アカウントごとに 1 つのセッションを適用] を選択します。

3. [保存] をクリックします。

第 3 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

  詳細については、186 ページの「サーバの登録」を参照してください。
- Trend Micro Smart Protection Network

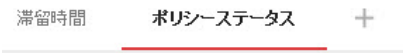
タブはウィジェット用のコンテナを用意します。[ダッシュボード] では、最大 30 のタブがサポートされます。

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。

詳細については、123 ページの Active Directory とコンプライアンスの設定を参照してください。

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。

詳細については、55 ページの「セキュリティ 状態のグラフ」を参照してください。

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 **注意** Apex Central では、次の管理下の製品のセキュリティエージェントをサポートしています。 • Apex One • ウイルスバスタービジネスセキュリティサービス コンプライアンスインジケータの設定の詳細については、130 ページの「パターンファイルのコンプライアンスインジケータを設定する」を参照してください。 • 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。 詳細については、142 ページの「ユーザ/エンドポイントディレクトリ」を参照してください。

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 コンプライアンスインジケータの設定の詳細については、132 ページの「情報漏えい対策のコンプライアンスインジケータを設定する」を参照してください。 • 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。 詳細については、142 ページの「ユーザ/エンドポイントディレクトリ」を参照してください。

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。

重要なユーザまたはエンドポイントの定義の詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

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。

詳細については、142 ページの「ユーザ/エンドポイントディレクトリ」を参照してください。

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
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

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。

詳細については、141 ページのユーザ/エンドポイントディレクトリを参照してください。

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。

詳細については、123 ページの Active Directory とコンプライアンスの設定を参照してください。

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。

  詳細については、134 ページの「エンドポイントおよびユーザのグループ設定」を参照してください。

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。

  詳細については、51 ページの「コンプライアンスインジケータ」を参照してください。

- 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。

  詳細については、57 ページの「セキュリティ状態の詳細ペイン」を参照してください。

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。

  詳細については、51 ページの「コンプライアンスインジケータ」を参照してください。

- 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。

  詳細については、55 ページの「セキュリティ状態のグラフ」を参照してください。

- 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 3-1. 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。
	
	詳細については、次のトピックを参照してください。
	
	• 130 ページの「パターンファイルのコンプライアンスインジケータを設定する」
	• 141 ページのユーザ/エンドポイントディレクトリ

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。
	
	詳細については、次のトピックを参照してください。
	
	• 132 ページの「情報漏えい対策のコンプライアンスインジケータを設定する」
	• 141 ページのユーザ/エンドポイントディレクトリ

表 3-2. 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。 詳細については、161 ページの「影響を受けたユーザ」を参照してください。
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。 詳細については、147 ページの「ユーザのセキュリティの脅威」を参照してください。
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。 詳細については、154 ページの「エンドポイントのセキュリティの脅威」を参照してください。

表 3-3. 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。

データ	説明
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。 詳細については、141 ページのユーザ/エンドポイントディレクトリを参照してください。

[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 3-1. [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。

  詳細については、147 ページの「ユーザのセキュリティの脅威」を参照してください。

- [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。

  詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

図 3-2. [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。

  詳細については、161 ページの「影響を受けたユーザ」を参照してください。

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。

脅威の種類	説明
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
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。

- 重要なユーザまたはエンドポイントの定義の詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

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。

  詳細については、147 ページの「ユーザのセキュリティの 脅威」を参照してください。

[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

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。

- 重要なユーザまたはエンドポイントの定義の詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

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。

  詳細については、154 ページの「エンドポイントのセキュリティの脅威」を参照してください。

[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。

- 詳細については、318 ページの「ログクエリを使用する」を参照してください。

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。

チャネル	説明
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。
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。

重要

このウィジェットには、情報漏えい対策 (DLP) のユーザの役割を割り当てられた Apex Central のユーザアカウントのデータのみが表示されます。

情報漏えい対策イベントのレビューと DLP ユーザの役割の設定の詳細については、https://docs.trendmicro.com/ja-jp/enterprise/apex-central-online-help/detections/data-loss-prevention_005.aspx を参照してください。

[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。

重要

このウィジェットには、情報漏えい対策 (DLP) のユーザの役割を割り当てられた Apex Central のユーザアカウントのデータのみが表示されます。

情報漏えい対策イベントのレビューと DLP ユーザの役割の設定の詳細については、https://docs.trendmicro.com/ja-jp/enterprise/apex-central-online-help/detections/data-loss-prevention_005.aspx を参照してください。

[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。

設定	説明
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。

重要

このウィジェットには、情報漏えい対策 (DLP) のユーザの役割を割り当てられた Apex Central のユーザアカウントのデータのみが表示されます。

情報漏えい対策イベントのレビューと DLP ユーザの役割の設定の詳細については、https://docs.trendmicro.com/ja-jp/enterprise/apex-central-online-help/detections/data-loss-prevention_005.aspx を参照してください。

[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。
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。
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。
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。

- 詳細については、318 ページの「ログクエリを使用する」を参照してください。

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。
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。

データ	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。

データ	説明
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 3-4. 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
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。

データ	説明
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 4 章

アカウント管理

このセクションでは、Apex Central ユーザアカウントと役割を作成して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。

ユーザアカウント

[ユーザアカウント] 画面には、Apex Central 管理コンソール用にそれまでに設定されたすべてのユーザアカウントのリストが表示されます。この画面を使用して、ユーザアカウントを設定したり、各ユーザに役割を設定したりできます。

ユーザの役割の詳細については、107 ページの「ユーザの役割」を参照してください。

次の表は、[ユーザアカウント] 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
ユーザアカウントの追加	新しいユーザアカウントを設定したり、統合された Active Directory 構造からユーザまたはグループをインポートしたりするには、[追加] をクリックします。 詳細については、97 ページの「ユーザアカウントの追加」を参照してください。 **注意** Apex Central では、統合された Active Directory 構造からのユーザおよびグループのユーザアカウントを作成できます。 詳細については、124 ページの「Active Directory 統合」を参照してください。
ユーザアカウントの削除	既存アカウントのユーザ名/グループ名の横にあるチェックボックスをオンにし、[削除] をクリックすると、アカウントが完全に削除されます。 **警告!** アカウントを完全に削除すると、それまでに設定したアカウント情報が Apex Central サーバから完全に削除されます。

タスク	説明
2 要素認証の有効化	[2 要素認証を有効にする] リンクをクリックすると、ユーザは Apex Central にログオンするために Google Authenticator アプリで生成される認証コードの入力が必要になります。 詳細については、104 ページの「2 要素認証を有効または無効にする」を参照してください。
2 要素認証の無効化	[2 要素認証を無効にする] リンクをクリックすると、Apex Central には有効なユーザアカウントとパスワードだけでログオンできるようになります。 詳細については、104 ページの「2 要素認証を有効または無効にする」を参照してください。
ユーザアカウントの編集	ユーザ情報を編集するユーザアカウントのユーザ名/グループ名をクリックします。 詳細については、102 ページの「ユーザアカウントの編集」を参照してください。
ユーザアカウントのロック解除	指定したログオンの連続失敗回数を超えたアカウントのロックを解除するには、[ロック済み] 列の [ロック解除] ボタンをクリックします。 詳細については、44 ページの「管理コンソールの設定」を参照してください。
ユーザアカウントの有効化	Apex Central 管理コンソールにログオンするために無効なアカウントを有効にするには、[有効] 列の  アイコンをクリックします。 注意 無効なアカウントを有効にするには、アカウントを編集する方法もあります。 詳細については、102 ページの「ユーザアカウントの編集」を参照してください。

タスク	説明
ユーザアカウントの無効化	ユーザが Apex Central 管理コンソールに一時的にログオンできないようにするには、[有効] 列の  アイコンをクリックします。 **注意** • ユーザアカウントを無効にするには、アカウントを編集する方法もあります。 詳細については、102 ページの「ユーザアカウントの編集」を参照してください。 • Apex Central では、Active Directory ユーザまたはグループ用のアカウントを無効にできません。Active Directory アカウントを無効にするには、Active Directory サーバからアカウントを無効にする必要があります。 詳細については、Active Directory 管理者にお問い合わせください。

root アカウント

Apex Central のインストール時に、<root>アカウントの名前を指定できます。<root>権限のアカウントでは、メニュー内のすべての機能を表示し、使用可能なすべてのサービスを使用できます。また、エージェントをインストールできます。<root>アカウントは削除できません。

<root>アカウントには、他にも次の権限があります。

- <root>アカウントは、他のユーザが使用している機能によるロックを解除して、強制的にログオフさせることができます。
- <root>アカウントは 2 要素認証をバイパスできます。

注意

Apex Central のアカウントは、Apex Central にログオンするためのもので、ネットワーク全体にログオンするためのものではありません。Apex Central のユーザアカウントは、ネットワークのドメインアカウントとは異なります。

ユーザアカウントの追加

Apex Central 管理者用の新しいユーザアカウントを作成したり、統合された Active Directory 構造からユーザまたはグループをインポートしたりするには、[ユーザアカウント] 画面を使用します。

重要

- インストール時に作成した<root>アカウントと「管理者」または「管理者および情報漏えい対策コンプライアンス責任者」のユーザの役割を割り当てられたユーザアカウントのみが、Apex Central の新しいユーザアカウントを作成できます。
- Active Directory 構造からユーザまたはグループをインポートするには、統合された Active Directory 構造が必要です。

  詳細については、124 ページの「Active Directory 統合」を参照してください。
- Active Directory 構造を統合すると、Active Directory ユーザまたはグループは [ドメインのログオン情報でログオンする] ボタンを使用して、ユーザ名とパスワードを入力することなく Apex Central にログオンできます。

  詳細については、42 ページの「管理コンソールにアクセスする」を参照してください。

手順

1. [運用管理] > [アカウント管理] > [ユーザアカウント] に移動します。

   [ユーザアカウント] 画面が表示されます。
2. [追加] をクリックします。

   [ユーザアカウント] の [手順 1: ユーザ情報] 画面が表示されます。

3. [このアカウントを有効にする] チェックボックスをオンにして、作成時にアカウントを有効にします。

注意

Apex Central では、Active Directory ユーザまたはグループ用のアカウントを無効にできません。Active Directory アカウントを無効にするには、Active Directory サーバからアカウントを無効にする必要があります。

詳細については、Active Directory 管理者にお問い合わせください。

---

4. アカウントの種類を選択します。

- 新しい Apex Central ユーザアカウントを作成するには、次の手順を実行します。

  a. [カスタムアカウント] を選択します。

  b. 次の情報を設定してください。

情報	説明
ユーザ名	ユーザが Apex Central 管理コンソールにログオンするために指定するアカウント名を入力します。
名前	ユーザのフルネームを入力します。
パスワード	ユーザが Apex Central 管理コンソールにログオンするために指定するパスワードを入力します。 **注意** ユーザは [マイアカウント] 画面で各自のパスワードを変更できます。 詳細については、105 ページの「ユーザアカウント情報を表示または編集する」を参照してください。
パスワードの確認入力	[パスワード] フィールドと同じパスワードを入力します。

情報	説明
メールアドレス	通知の受信に使用するメールアドレスを入力します。 注意 • Apex Central からレポートやイベント通知をメールで送信する場合や 2 要素認証が有効な場合、このフィールドは必須項目です。 • また、2 要素認証が正常に機能し、Apex Central がレポートと通知を E メールで送信できるように SMTP サーバを設定する必要があります。 詳細については、342 ページの「SMTP サーバを設定する」を参照してください。

- 統合された Active Directory 構造からユーザまたはグループをインポートするには、次の手順を実行します。

  a. [Active Directory ユーザまたはグループ] を選択します。

  b. 次の項目を使用して Active Directory ユーザまたはグループを検索します。

     - ユーザ名/グループ名

       注意
       - このフィールドは必須項目です。
       - 部分一致を使用して検索するときはアスタリスクワイルドカード (*) を使用できます。

         たとえば「tom*」と入力すると、名前が「tom」で始まるすべてのユーザやグループが検索されます。

     - 基本識別名

  c. [検索] をクリックします。

指定された条件に一致する Active Directory アカウントが [検索結果] リストに表示されます。

d. [検索結果] リストから Active Directory ユーザまたはグループを選択し、[>] をクリックします。

選択した Active Directory ユーザまたはグループが [選択されたユーザ/グループ] リストに表示されます。

重要

- Apex Central では、インポートしたユーザまたはグループが各自の Active Directory ドメインのログオン情報を使用して Apex Central にログオンする前に、Active Directory のデータを手動で同期する必要があります。

  詳細については、124 ページの「Active Directory 統合」を参照してください。

- 旧バージョンの Control Manager から移行した Active Directory 構造から Active Directory のデータを手動で同期する必要はありません。移行した Active Directory 構造のユーザおよびグループは、移行が完了するとすぐに Apex Central にログオンできます。

5. [次へ] をクリックします。

[ユーザアカウント] の [手順 2: アクセス管理] 画面が表示されます。

6. [役割の選択] ドロップダウンからユーザの役割を選択します。

注意

- ユーザの役割に定義されたアクセス権は、個々のユーザアカウントに設定された管理下の製品/フォルダのアクセス権より優先されます。
- 情報漏えい対策コンプライアンス責任者および情報漏えい対策イベントレビューアの役割は、Active Directory ユーザまたはグループにのみ割り当てることができます。

  詳細については、107 ページの「ユーザの役割」を参照してください。

7. [アクセスを許可する製品/フォルダ] ツリーで、ユーザがアクセスできる製品ディレクトリ構造内の製品またはフォルダを選択します。

注意

個別の管理下の製品を選択してアクセス権を与えると、選択した製品に対するアクセス権のみが与えられます。製品ディレクトリ全体にアクセス権を与えることもできます。フォルダにアクセス権を割り当てると、ユーザは、フォルダ内のすべてのサブフォルダおよび管理下の製品にアクセスできるようになります。

詳細については、101 ページの「管理下の製品のアクセス管理」を参照してください。

8. ユーザアカウントに管理下の製品/フォルダのアクセス権を指定します。

注意

アクセス権により、製品に対してユーザアカウントが実行できる処理が決まります。権限を設定するアカウントよりも上位の権限を設定することはできません。

詳細については、101 ページの「管理下の製品のアクセス管理」を参照してください。

9. [保存] をクリックします。

新しいユーザアカウントが [ユーザアカウント] 画面に表示されます。

管理下の製品のアクセス管理

選択した管理下の製品/フォルダに指定するアクセス権によって、[製品ディレクトリ] 画面でユーザが使用できるコントロールが決まります。たとえば、選択した管理下の製品/フォルダに実行のアクセス権のみを指定した場合、ユーザは [製品ディレクトリ] 画面の [タスク] ボタンだけを使用できます。

注意

[製品ディレクトリ] 画面のボタンで利用できる処理は、ユーザの役割、管理下の製品/フォルダのアクセス権、および製品ディレクトリ構造で選択する管理下の製品/フォルダに基づいて動的に変化します。

詳細については、210 ページの「製品ディレクトリ」を参照してください。

アクセス可能な管理下の製品/フォルダに次のアクセス権 (複数可) を指定できます。

アクセス権	説明
実行	ユーザアカウントは、[製品ディレクトリ] 画面の [タスク] ボタンを使用して、アクセス可能なフォルダにある管理下の製品に対してタスクを実行できます。 詳細については、216 ページの「管理下の製品のタスクを実行する」を参照してください。
設定	ユーザアカウントは、[製品ディレクトリ] 画面の [設定] ボタンを使用して、管理下の製品の設定を実行したり、Apex Central から管理下の製品の管理コンソールにログオンしたりできます。 詳細については、217 ページの「管理下の製品を設定する」を参照してください。
ディレクトリ編集	ユーザアカウントは、[ディレクトリ管理] ボタンを使用して、アクセス可能な管理下の製品またはフォルダを製品ディレクトリ構造で編成できます。 詳細については、219 ページの「ディレクトリ管理」を参照してください。

注意

管理者がユーザアクセス可能な製品を指定すると、ユーザアクセス可能な Apex Central の情報も指定されることになります。この情報には、コンポーネントに関する情報、ログ、製品の概要情報、セキュリティ情報、レポートおよびクエリ対象として使用できる情報などが該当します。

ユーザアカウントの編集

[ユーザアカウント] 画面を使用して、編集する権限を持つユーザアカウントのユーザ情報、ユーザの役割、または管理下の製品/フォルダのアクセス権を編集します。

重要

- インストール時に作成した<root>アカウントは、Apex Central ネットワークのすべてのユーザアカウントを編集できます。「管理者」または「管理者および情報漏えい対策コンプライアンス 責任者」のユーザの役割が割り当てられているユーザアカウントは、Apex Central ネットワークの<root>アカウントを除く他のすべてのユーザアカウントを編集できます。
- ユーザアカウントのアクセス権を変更すると、変更されたアカウントのすべての Apex Central セッションと、変更されたアカウントによって作成されたすべてのアカウントが終了します。
- 既存のアカウントのユーザ名を変更できません。

手順

1. [運用管理] > [アカウント管理] > [ユーザアカウント] に移動します。

   [ユーザアカウント] 画面が表示されます。

2. 変更するアカウントのユーザ名/グループ名をクリックします。

   [ユーザアカウント] の [手順 1: ユーザ情報] 画面が表示されます。

3. アカウントを有効または無効にするには、[このアカウントを有効にする] チェックボックスをオンまたはオフにします。

4. ユーザ情報を変更します。

5. [次へ] をクリックします。

   [ユーザアカウント] の [手順 2: アクセス管理] 画面が表示されます。

6. ユーザの役割、アクセス可能な製品/フォルダ、またはアクセス権を変更します。

7. [保存] をクリックして変更を適用します。

2 要素認証を有効または無効にする

2 要素認証はユーザアカウントの安全性を強化します。そのためには、ユーザは Apex Central にログオンするために、Google Authenticator アプリで生成された認証コードを入力する必要があります。

重要

Apex Central の 2 要素認証では、次の作業を実行する必要があります。

- 各ユーザアカウントのメールアドレスを設定

  詳細については、105 ページの「ユーザアカウント情報を表示または編集する」を参照してください。

- メール通知を送信するように SMTP サーバを設定

  詳細については、342 ページの「SMTP サーバを設定する」を参照してください。

- 各ユーザのモバイルデバイスに Google Authenticator アプリをダウンロードしてインストールしておきます。

注意

- <root>アカウントは、常に 2 要素認証をバイパスできます。
- Google Authenticator システムアプリによって生成される認証コードは 30 秒ごとに変更されますが、生成されてから 5 分以内のコードまでは Apex Central のログインに使用できます。

手順

1. [運用管理] > [アカウント管理] > [ユーザアカウント] に移動します。

   [ユーザアカウント] 画面が表示されます。

2. 2 要素認証を有効にするには、次の手順を実行します。

   a. [2 要素認証を有効にする] をクリックします。

      確認ダイアログボックスが表示されます。

b. [有効にする] をクリックします。

- [ユーザアカウント] 画面の上部に、すべてのユーザアカウントのメールアドレスを設定するよう指示する警告メッセージが表示されます。

  リンクをクリックすると、メールアドレスが設定されていないユーザが表示されます。

- [ユーザアカウントの追加] 画面のメールアドレスは必須フィールドです。

- Apex Central では、ログオンするために、有効なユーザ名とパスワードに加えて、Google Authenticator アプリで生成された認証コードを入力する必要があります。

3. 2 要素認証を無効にするには、次の手順を実行します。

   a. [2 要素認証を無効にする] をクリックします。

      確認ダイアログボックスが表示されます。

   b. [無効にする] をクリックします。

      Apex Central 管理コンソールへのログオンに必要なのは、有効なユーザアカウントとパスワードだけです。

ユーザアカウント情報を表示または編集する

[マイアカウント] 画面を使用して、自分自身のユーザアカウントまたは自分が作成したユーザアカウントのアカウント情報を表示したり変更したりできます。

特定のユーザアカウントに割り当てられているユーザの役割の編集については、102 ページの「ユーザアカウントの編集」を参照してください。

手順

1. [運用管理] > [アカウント管理] > [マイアカウント] に移動します。

   [マイアカウント] 画面が表示されます。

2. 次のアカウント情報を設定します。

情報	説明
名前	ユーザのフルネームを入力します。 注意 このフィールドは必須項目です。
パスワード	ユーザが Apex Central 管理コンソールにログオンするために指定するパスワードを入力します。 注意 このフィールドは必須項目です。
パスワードの確認入力	[パスワード] フィールドと同じパスワードを入力します。 注意 このフィールドは必須項目です。
メールアドレス	通知の受信に使用するメールアドレスを入力します。 注意 • Apex Central からレポートやイベント通知をメールで送信する場合や 2 要素認証を使用する場合、このフィールドは必須項目です。 2 要素認証の詳細については、104 ページの「2 要素認証を有効または無効にする」を参照してください。 • Apex Central からレポートやイベント通知をメールで送信するには、SMTP サーバを設定する必要もあります。 詳細については、342 ページの「SMTP サーバを設定する」を参照してください。

情報	説明
電話番号	ユーザアカウントに関連付けられている固定電話番号を入力します。
携帯電話番号	ユーザアカウントに関連付けられている携帯電話番号を入力します。

3. [保存] をクリックして変更を適用します。

ユーザの役割

[ユーザの役割] 画面には、ユーザアカウントに割り当て可能な、すべての初期設定のユーザの役割とすべてのカスタムのユーザの役割のリストが表示されます。ユーザの役割により、ユーザがアクセスおよびコントロール可能な Apex Central 管理コンソールの領域が定義されます。この画面を使用して、カスタムの Apex Central ユーザの役割を作成および編集できます。

重要

旧バージョンの Control Manager でカスタマイズしたユーザの役割にポリシー管理のメニュー項目に対する権限が割り当てられている場合、現在のリリースにアップグレード後、その役割にはフルコントロールが付与されます。これらの権限は、「メンテナンス」または「読み取り専用」に変更可能です。ポリシー管理を含まないバージョンの Control Manager からアップグレードする場合、役割の設定を変更するまで、カスタムのユーザの役割にはポリシー管理機能を管理または表示する権限がありません。

注意

- インストール時に作成した<root>アカウントと「管理者」または「管理者および情報漏えい対策コンプライアンス責任者」のユーザの役割を割り当てられたユーザアカウントのみが、新しいユーザアカウントを作成したり、ユーザの役割を割り当てたりできます。
- ユーザの役割に定義されたアクセス権は、個々のユーザアカウントに設定された管理下の製品/フォルダのアクセス権より優先されます。

  詳細については、101 ページの「管理下の製品のアクセス管理」を参照してください。

次の表は、[ユーザの役割] 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
ユーザの役割の追加	新しいカスタムのユーザの役割を作成するには、[追加] をクリックします。 詳細については、111 ページの「ユーザの役割の追加」を参照してください。
ユーザの役割の削除	役割を完全に削除するには、カスタムのユーザの役割の [名前] の横にあるチェックボックスをオンにして、[削除] をクリックします。 注意 Trend Micro Apex Central™が提供する初期設定のユーザの役割は削除できません。
ユーザの役割の編集	割り当てられたアクセス権を編集または表示するには、ユーザの役割の [名前] をクリックします。 詳細については、113 ページの「ユーザの役割の編集」を参照してください。 注意 Trend Micro Apex Central™が提供する初期設定のユーザの役割は編集できません。 初期設定のユーザの役割の詳細については、108 ページの「初期設定のユーザの役割」を参照してください。

初期設定のユーザの役割

Apex Central では、初期設定のユーザの役割が用意されており、それをユーザアカウントに割り当てることができます。ユーザの役割により、ユーザがアクセスおよびコントロール可能な Apex Central 管理コンソールの領域が定義されます。初期設定のユーザの役割にアクセス権を追加することはできますが、初期設定のユーザの役割から事前定義済みのアクセス権を削除することはできません。

注意

インストール時に作成した<root>アカウントと「管理者」または「管理者および情報漏えい対策コンプライアンス責任者」のユーザの役割を割り当てられたユーザアカウントのみが、新しいユーザアカウントを作成したり、ユーザの役割を割り当てたりできます。

カスタマイズしたユーザの役割の追加または編集の詳細については、次のトピックを参照してください。

- 111 ページの「ユーザの役割の追加」
- 113 ページの「ユーザの役割の編集」

次の表は、[ユーザの役割] 画面で使用可能な初期設定の役割について示しています。

役割	説明
Administrator_and_DLP Compliance_Officer	• すべてのメニュー項目のすべてのアクションを 実行できます。 • すべての Active Directory ユーザによって開始された情報漏えい対策イベントを監視、レビュー、および調査できます。
Administrator	• すべてのメニュー項目のすべてのアクションを 実行できます。 • すべての Active Directory ユーザによって開始された情報漏えい対策イベントを監視、レビュー、または調査できません。
DLP_Compliance_Officer	• [ダッシュボード] のすべてのアクションを 実行できます。 • すべての Active Directory ユーザによって開始された情報漏えい対策イベントを監視、レビュー、および調査できます。 **注意** このユーザの役割は Active Directory ユーザまたはグループにのみ割り当てることができます。

役割	説明
DLP_Incident_Reviewer	• [ダッシュボード] のすべてのアクションを 実行できます。 • 情報漏えい対策イベントレビューアにレポートを送信する Active Directory ユーザによって開始された情報漏えい対策イベントの監視、レビュー、および調査のみが可能です。 **注意** このユーザの役割は Active Directory ユーザまたはグループにのみ割り当てることができます。 詳細については、次のトピックを参照してください。 • 137 ページの「レポートライン」 • 97 ページの「ユーザアカウントの追加」
Operator	• すべての [ダッシュボード] および [ディレクトリ] メニュー項目のすべてのアクションを 実行できます。 • ログクエリの実行、他のユーザによって生成および送信されたレポートの表示、[マイアカウント] 画面でユーザアカウント情報の更新が可能です。 • [ポリシー管理] 画面でのみ情報を表示できます。 • すべての Active Directory ユーザによって開始された情報漏えい対策イベントを監視、レビュー、または調査できません。
Power_User	• すべての [ダッシュボード] および [ディレクトリ] メニュー項目のすべてのアクションを 実行できます。 • ログクエリの実行、ログの管理、レポートの生成および管理を実行できます。 • [ポリシー管理] 画面でのみ情報を表示できます。 • すべての Active Directory ユーザによって開始された情報漏えい対策イベントを監視、レビュー、または調査できません。

役割	説明
Read-only_User	• すべてのメニュー項目の情報を表示し、ユーザアカウント情報を更新できます。 • [ダッシュボード] のすべてのアクションを 実行できます。 • ログクエリの実行、レポートの生成、カスタムレポートテンプレートの作成、ディレクトリの検索、ユーザ/エンドポイントディレクトリツリーを管理するためのカスタムタグ/フィルタの作成および使用が可能です。 • 他のユーザによって生成されたレポートを表示できません。
SSO_User	• すべてのメニュー項目のすべてのアクションを 実行できます。 • すべての Active Directory ユーザによって開始された情報漏えい対策イベントを監視、レビュー、または調査できません。 **注意** このユーザの役割は初期設定で非表示です。
Threat_Investigator	• 管理下のエンドポイント/サーバのセキュリティ 脅威イベントを調査できます。

注意

旧バージョンの Operator と Power_Users の役割には、[ポリシー管理]のメニュー項目で処理を実行する権限はありません。このバージョンにアップグレードすると、これら 2 つの役割には読み取り専用権限が付与されます。この設定は変更できません。

ユーザの役割の追加

[ユーザの役割] 画面を使用して、カスタムのユーザの役割を作成できます。

手順

1. [運用管理] > [アカウント管理] > [ユーザの役割] に移動します。

   [ユーザの役割] 画面が表示されます。

2. [追加] をクリックします。

   [役割の追加] 画面が表示されます。

3. [役割の情報] セクションで次のように実行します。

   a. [名前] フィールドに一意のユーザの役割名を入力します。

   b. [説明] にユーザの役割の説明を入力します。

   > **注意**
   >
   > この説明は [ユーザの役割] リストに表示されます。ユーザの役割名が、対象とするユーザの役割を完全には表していない場合、意味がわかるような説明を入力することによって、ユーザの役割の識別に役立てることができます。

4. [メニューのアクセス管理] セクションで、対象のユーザの役割でアクセス可能なメニュー項目を選択します。

5. 選択したメニュー項目のアクセス権を指定します。

   - フルコントロール、次を除く:: ユーザに対して、アクセス可能なメニュー項目で選択可能なすべてのアクションの実行を許可する場合に選択します。
     - ポリシーの作成、コピー、インポート: ユーザが [ポリシー管理] 画面でポリシーを作成、コピー、またはインポートできないようにする場合に選択します。

       詳細については、248 ページの「ポリシー管理」を参照してください。

     - すべてのユーザによって実行された情報漏えい対策イベントの監視、レビュー、および調査: ユーザがすべての Active Directory ユーザによって実行された情報漏えい対策イベントを調査できないようにする場合に選択します。
   - 読み取りのみ: ユーザに [メニューのアクセス管理] セクションで選択されたメニュー項目に関する情報の表示のみを許可する場合に選択します。

6. [保存] をクリックします。

   新しいユーザの役割が [ユーザの役割] 画面に表示されます。

ユーザの役割の編集

Apex Central では、カスタマイズしたユーザの役割のアクセス権を変更できます。

特定のユーザアカウントに割り当てられているユーザの役割の編集については、102 ページの「ユーザアカウントの編集」を参照してください。

注意

アクセス可能なメニュー項目に表示される管理下の製品に関する情報は、Apex Central 管理者が個々のユーザアカウントに対して指定した管理下の製品/ディレクトリ権限によって決まります。

手順

1. [運用管理] > [アカウント管理] > [ユーザの役割] に移動します。

   [ユーザの役割] 画面が表示されます。

2. 編集するユーザの役割の名前をクリックします。

   [役割の編集] 画面が表示されます。

3. ユーザの役割の情報を編集します。

4. [保存] をクリックして変更を適用します。

第 5 章

ライセンス管理

このセクションでは、Apex Central および管理下の製品の製品ライセンスをアクティベーションまたは更新を実行する方法について説明します。

次のトピックがあります。

Apex Central のアクティベーションおよびライセンス情報

アクティベーションコードによって Apex Central の機能が有効化されます。

Apex Central のアクティベーションを実行する

トレンドマイクロの営業担当者や法人カスタマーサイトなどからアクティベーションコードを入手したら、[ライセンス管理] 画面で Apex Central をアクティベートできます。

Apex One Sandbox as a Service のライセンスを購入した場合、[ライセンス管理] 画面からライセンスをアクティベートすることもできます。

重要

Apex Central のアクティベーション後、変更を有効にするには、Apex Central 管理コンソールからログオフして再びログオンしてください。

手順

1. [運用管理] > [ライセンス管理] > [Apex Central] に移動します。

   [ライセンス情報] 画面が表示され、現在のライセンス情報が示されます。

2. [新しいアクティベーションコードを 入力してください] リンクをクリックします。

3. アクティベーションコードを 入力します。

4. [アクティベート] をクリックします。

5. Apex Central 管理コンソールからログオフして再びログオンすると、変更が有効になります。

Apex Central ライセンス情報を確認および更新する

[ライセンス管理] 画面に、最新の Apex Central ライセンス情報とアクティベーションステータスが表示されます。

Apex One Sandbox as a Service のライセンスを購入済みの場合は、[ライセンス管理] 画面にそのライセンス情報とアクティベーションステータスも 表示されます。

手順

1. [運用管理] > [ライセンス管理] > [Apex Central] に移動します。

   [ライセンス情報] 画面が表示され、現在のライセンス情報が示されます。

2. 画面を更新して最新のライセンス情報を表示するには、次の手順を実行します。

   a. [ライセンス情報の更新] をクリックします。

   b. Apex Central 管理コンソールからログオフして再びログオンすると、変更が有効になります。

3. ライセンスを更新するには、次の手順を実行します。

   a. [新しいアクティベーションコードを 入力してください] リンクをクリックします。

   b. アクティベーションコードを 入力します。

   c. [アクティベート] をクリックします。

   d. Apex Central 管理コンソールからログオフして再びログオンすると、変更が有効になります。

4. 現在のライセンスに関する情報を確認するには [ライセンス情報をオンラインで確認] をクリックします。

管理下の製品のアクティベーションと登録

Apex Central、管理下の製品 (Apex One、InterScan for Microsoft Exchange など)、およびその他のサービスを使用するには、アクティベーションコードを取得して、ソフトウェアやサービスのアクティベーションを実行する必要があります。

管理下の製品を Apex Central に登録すると、最新コンポーネントのダウンロードをはじめ、各製品の機能をすべて利用できるようになります。各製品パッケージに付属するアクティベーションコードを使用して、管理下の製品のアクティベーションを実行できます (一部本機能がサポートされない製品もあります)。

ライセンス管理の詳細

次の表は、[ライセンス管理] 画面に表示される管理下の製品のライセンス情報を示しています ([運用管理] > [ライセンス管理] > [管理下の製品])。

ヒント

[期限切れのアクティベーションコードを隠す] チェックボックスをオフにすると、すべての管理下の製品のライセンスの詳細を確認できます。

列名	説明
アクティベーションコード	管理下の製品のアクティベーションコードが表示されます。
注意	アクティベーションコードに関する追加情報が表示されます。
アクティベート済み製品	アクティベーションコードの配信先の管理下の製品の数が表示されます。
ライセンスステータス	アクティベーションコードのステータスを示します。 • 有効 • サポート契約終了

列名	説明
種類	アクティベーションコードの種類を示します。 • 製品版: サポート契約期間 (通常は 1 年間) の間、製品のすべての機能を使用できます。 • 体験版: 試用期間 (通常は 3 か月) の間、製品のすべての機能を使用できます。
有効期限	アクティベーションコードが期限切れになる日付が表示されます。
ライセンス数	このアクティベーションコードで使用できるライセンス数が表示されます。

管理下の製品のライセンス情報

[ライセンス管理] 画面 ([運用管理] > [ライセンス管理] > [管理下の製品]) でアクティベーションコードをクリックすると、管理下の製品/サービスに関する次のライセンス情報が表示されます。

フィールド	説明
アクティベーションコード	製品/サービスのアクティベーションに使用されたコードを示します。
ステータス	ライセンスステータスを示します。 (「[有効]」 など)
種類	製品/サービスのライセンスの種類を示します。 (「[製品版]」 や「[体験版]」 など)
有効期限	製品/サービスのライセンスの有効期限を示します。
説明	ユーザが定義したアクティベーションコードの説明です。 • テキストボックスに説明を入力し、[完了] をクリックして、変更を保存します。

管理下の製品のアクティベーション

[ライセンス管理] 画面を使用すると、管理下の製品ライセンスのアクティベーションを実行できます。管理下の製品のインストール時にアクティベーショ

ンを実行しなかった場合は、管理コンソールからアクティベーションを 実行できます (一部本機能がサポートされない製品があります。詳しくは管理下の製品サポート窓口にお問い合わせください)。製品パッケージに付属するアクティベーションコードを使用し、管理下の製品のアクティベーションを実行して、アップデートファイルのダウンロードなどのサポートサービスを含む全機能を使用できるようにします。

手順

1. [運用管理] > [ライセンス管理] > [管理下の製品] に移動します。

   [ライセンス管理] 画面が表示されます。

2. [追加と配信] をクリックします。

   [新しいライセンスの追加と配信]>[手順 1 :アクティベーションコードの入力] 画面が表示されます。

3. アクティベートする製品のアクティベーションコードを [新しいアクティベーションコード] フィールドに入力します。

4. [次へ] をクリックします。

   [新しいライセンスの追加と配信]>[手順 2 :対象の選択] 画面が表示されます。

   注意

   製品がリストに表示されていない場合、選択されたアクティベーションコードでは、Apex Central に現在登録されている製品はサポートされていません。つまり、管理下の製品は Apex Central サーバのアクティベーションコードを受信できません。

5. アクティベーションコードの配信先となる管理下の製品を選択します。

6. [配信] をクリックします。

   [ライセンス管理] 画面が表示され、表に新しいアクティベーションコードの一覧が表示されます。

注意

アクティベーションコードの配信ステータスが、[ライセンス管理] 画面の上でトーストメッセージとして表示されます。

[コマンド追跡] 画面で配信ステータスの詳細を表示するには、メッセージ内のリンクをクリックします。

管理下の製品のライセンスの更新

Apex Central では、[ライセンス管理] 画面で、登録された製品にアクティベーションコードを配信または再配信できます。

手順

1. [運用管理] > [ライセンス管理] > [管理下の製品] に移動します。

   [ライセンス管理] 画面が表示されます。

2. リストからアクティベーションコードを選択します。

3. [再配信] をクリックします。

   [ライセンスの再配信] 画面が表示されます。

4. アクティベーションコードを配信する製品を選択します。

   注意

   - 製品がリストに表示されていない場合、選択されたアクティベーションコードでは、Apex Central に現在登録されている製品はサポートされていません。
   - アクティベーションコードを配信するには、製品を少なくとも 1 つ選択する必要があります。

5. [配信] をクリックします。

   選択した製品に Apex Central からアクティベーションコードが配信されます。

第 6 章

Active Directory とコンプライアンスの設定

このセクションでは、Apex Central で Active Directory 統合とコンプライアンスインジケータの設定を実行する方法について説明します。

次のトピックがあります。

Active Directory 統合

Apex Central を Microsoft Active Directory サーバと統合すると、以下を実行できます。

- 管理者は、Active Directory のユーザまたはグループに基づいて、管理コンソールへのアクセス用のユーザアカウントを作成できます。

  詳細については、97 ページの「ユーザアカウントの追加」を参照してください。

- 既存の組織構造に基づいてユーザ/エンドポイントディレクトリをマップし、エンドポイント情報 (脅威の検出やポリシーステータスなど) を Active Directory のユーザ情報 (ログイン履歴や連絡先の詳細など) と統合できます。

  詳細については、142 ページの「ユーザ/エンドポイントディレクトリ」を参照してください。

- Active Directory のサイトの場所およびレポートライン情報を使用して、[セキュリティ状態] ダッシュボードタブのネットワーク保護ステータスをより詳細に確認できます。

  詳細については、128 ページの「コンプライアンスインジケータ」を参照してください。

Active Directory 接続を設定する

Apex Central が Active Directory サーバからのエンドポイントおよびユーザの情報を同期できるように接続設定を指定します。

注意

Apex Central は、複数の Active Directory フォレストとの同期をサポートしています。Active Directory ドメインを追加すると、同じフォレストのすべてのドメインが自動的に同期されます。

フォレストの信頼の詳細については、Active Directory 管理者にお問い合わせください。

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの設定] に移動します。
2. [Active Directory の設定] タブをクリックします。
3. [Active Directory との同期と認証を有効にする] を選択します。
4. Active Directory サーバにアクセスするための接続を設定します。

フィールド	説明
サーバアドレス	Active Directory サーバの FQDN または IP アドレス (IPv4 または IPv6) を入力します。
ユーザ名	Active Directory サーバへのアクセスに必要なドメイン名とユーザ名を入力します。 形式の例: ドメイン\ユーザ名
パスワード	Active Directory サーバへのアクセスに必要なパスワードを入力します。

   - 他の Active Directory サーバを追加するには、追加アイコン (+) をクリックします。
   - Active Directory サーバを削除するには、削除アイコン (−) をクリックします。

5. [同期の頻度 (時間単位)] ドロップダウンリストから、Apex Central が Active Directory サーバとデータを同期する頻度を選択します。

   注意

   Active Directory の同期時間は、Active Directory データベースのサイズと複雑さに応じて異なります。同期が完了するまでに 1 時間以上かかる場合もあります。

6. (オプション) [詳細設定] を展開して、[同期元] または [接続モード] を設定します。
   a. 同期元として次のいずれかを選択します。

- [ドメインコントローラ]: 信頼関係で結ばれた複数のフォレストのすべてのドメインを同期します。
- [グローバルカタログ]: 単一のフォレストのすべてのドメインを同期します。

重要

初期設定のグローバルカタログを同期元とした場合、グローバルグループまたはドメインローカルグループでの 地理的な位置やユーザのメンバーシップなど、Apex Central が使用する一部の情報を同期できません。グローバルカタログを同期元に選択するのは、ネットワークポリシーによって Apex Central がすべてのドメインコントローラに接続できない場合のみにしてください。

b. 接続モードとして次のいずれかを選択します。

- SSL

重要

SSL 接続を使用するには、Active Directory 証明書を Apex Central サーバにインポートします。

- 非 SSL

7. (オプション) [接続テスト] をクリックして、サーバ接続をテストします。

注意

接続をテストしても、Active Directory サーバの設定は保存されません。

サーバアドレスの前に、Active Directory サーバの接続ステータスアイコン (または) が表示されます。

8. [保存] をクリックします。

Apex Central が、同期の頻度に従って Active Directory サーバからエンドポイントとユーザ情報を同期します。

9. (オプション) 次の場所にある ADSyncOUList.config 設定ファイルを変更して、Apex Central の同期対象になる Active Directory ドメインと OU を設定します。

   <Apex Central インストールディレクトリ>\ADSyncOUList.config

10. (オプション) [今すぐ同期]をクリックして、Active Directory のデータを手動で同期します。

    サーバアドレスの前に、Active Directory サーバの接続ステータスアイコン (または) が表示されます。

11. 同期した Active Directory サーバを削除するには、次の手順を行います。

    a. [Active Directory との同期を有効にする] チェックボックスをオフにします。

    b. [データのクリア] をクリックして、削除された Active Directory サーバのデータを Apex Central サーバから削除します。

       Apex Central によって、同期された Active Directory サーバが削除されます。

       注意

       [データのクリア] をクリックすると、2 分ごとに実行されるようにスケジュールされたタスクがトリガされ、削除された Active Directory サーバのすべてのデータが Apex Central のデータベースから削除されます。

Active Directory との同期をトラブルシューティングする

Active Directory との同期では、Apex Central は Active Directory サーバからユーザ情報 (サイトやレポートラインなどの情報) を取得できます。

Active Directory 関連のエラーが [ダッシュボード] 画面に表示される場合は、次の表でトラブルシューティングの 解決策を参照してください。

問題	解決策
ユーザ名またはパスワードが正しくない	• 正しいアカウント情報が指定されていることを確認します。 • ユーザアカウントに Active Directory サーバにアクセスするための権限があることを確認します。 Active Directory 管理者にお問い合わせください。
Active Directory サーバに接続できない	• 正しい Active Directory 接続が設定されていることを確認します。 詳細については、124 ページの「Active Directory 接続を設定する」を参照してください。 • Active Directory サーバが使用可能であることを確認します。 • ネットワーク接続とファイアウォール設定を確認します。 • Apex Central サーバと Active Directory サーバの両方から相互に通信を確立できることを確認します。 Apex Central から Active Directory サーバへの接続をテストするには、[Active Directory とコンプライアンスの設定] 画面の [接続テスト] をクリックします。
Apex Central データベースにアクセスできない	Apex Central データベースに接続できることを確認します。 詳細については、606 ページの「Apex Central データベースについて」を参照してください。

接続の問題が解決しない場合は、テクニカルサポートに問い合わせてください。

詳細については、619 ページのテクニカルサポートを参照してください。

コンプライアンスインジケータ

Apex Central には次のコンプライアンスインジケータがあり 、これらのインジケータの設定と Active Directory サーバから同期したユーザおよびエンドポイントの情報に基づいてコンプライアンスの計算が実行されます。コンプライアンスインジケータの 情報は、[セキュリティ状態] ダッシュボードタブで確認できます。

- ウイルスパターンファイルのコンプライアンス : 対応するパターンファイル (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ている管理下の Apex One セキュリティエージェント の割合
- 情報漏えい対策のコンプライアンス : データ検出が有効な管理下の Apex One および Cloud App Security のエージェントのうち、機密データ検出イベント数が許容範囲内のエージェントの割合

Apex Central でコンプライアンスの計算を実行し、[セキュリティ状態] ダッシュボードタブでコンプライアンス情報を表示する大まかな手順は次のとおりです。

手順

1. Active Directory サーバに接続してユーザおよびエンドポイントの情報を同期します。

   詳細については、124 ページの「Active Directory 接続を設定する」を参照してください。

2. コンプライアンスインジケータを 設定します。

   詳細については、次のトピックを参照してください。

   - 130 ページの「パターンファイルのコンプライアンスインジケータを設定する」
   - 132 ページの「情報漏えい対策のコンプライアンスインジケータを 設定する」

3. (オプション) Active Directory サイトおよびレポートラインに基づいてエンドポイントおよびユーザのグループ設定をカスタマイズします。

   詳細については、134 ページの「エンドポイントおよびユーザのグループ設定」を参照してください。

4. [ダッシュボード] に進み、コンプライアンス情報を確認します。

注意

Active Directory グループ設定を変更したり、管理下のエージェントのデータ検出コンプライアンスを確認したりするには、[セキュリティ状態] タブの設定を編集します。

詳細については、次のトピックを参照してください。

- 50 ページの「[セキュリティ状態] タブ」
- 48 ページの「ウィジェットを使用する」

パターンファイルのコンプライアンスインジケータを 設定する

受け入れ可能なパターンファイル (ウイルス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) のバージョンを使用して、管理下のセキュリティエージェントの 割合を表示するために、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 設定値と除外を [セキュリティ状態] タブで設定できます。

注意

Apex Central では、次の管理下の製品のセキュリティエージェント をサポートしています。

- Apex One
- ウイルスバスタービジネスセキュリティサービス

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの 設定]に移動します。
2. [コンプライアンスインジケータ] タブをクリックします。
3. [ウイルスパターンファイルのコンプライアンス] をクリックします。
4. 次の表は、利用可能な設定オプションを示しています。

列	説明
許容されるパターンファイルのバージョン	準拠しているとみなされるエンドポイントのパターンファイルのバージョンを指定します。
アラートインジケータ	スライダを調整して、さまざまなアラートレベルのしきい値 (準拠するセキュリティエージェントの割合) を設定します。

5. [除外リスト] では、カスタムタグとカスタムフィルタを選択して、コンプライアンスの計算からユーザまたはエンドポイントを除外します。

注意

- 除外リストはすべての Apex Central ユーザに適用されます。除外リストへの追加と削除、および対応するタグとフィルタの変更は、ユーザの権限に従ってのみ実行できます。
- タグまたはフィルタの作成の詳細については、171 ページの「カスタムタグおよびカスタムフィルタ」を参照してください。

a. [追加] をクリックします。

[除外設定の追加] 画面が表示されます。

b. [種類] ドロップダウンリストで、[ユーザ] または [エンドポイント] を選択して、利用可能なカスタムフィルタとカスタムタグを種類別に表示します。それ以外の場合は、[すべて] を選択してすべてのエントリを表示します。

注意

カスタムフィルタまたはカスタムタグを検索するには、テキストフィールドに名前を入力して、<Enter> キーを押します。

カスタムタグおよびフィルタの詳細については、171 ページの「カスタムタグおよびカスタムフィルタ」を参照してください。

c. 1 つ以上のカスタムタグまたはカスタムフィルタを選択して、[追加] をクリックします。

選択した項目が除外リストに表示されます。

d. [閉じる] をクリックします。

e. [保存] をクリックします。

f. 追加したタグまたはフィルタの 対象範囲を [次のユーザが追加した例外を適用] ドロップダウンリストから指定します。

- すべてのユーザアカウント: ユーザアカウントによって追加されたカスタムフィルタとカスタムタグに指定されているすべてのユーザとエンドポイントを除外します。
- ログオンしたアカウントのみ: 現在ログオンしているユーザアカウントによって追加されたカスタムフィルタとカスタムタグに指定されているユーザとエンドポイントのみ除外します。

6. [保存] をクリックします。

情報漏えい対策のコンプライアンスインジケータを設定する

[セキュリティ 状態] タブで、情報漏えい対策のコンプライアンスインジケータの設定値と除外を設定して、情報漏えい対策が有効にされ、許容される数の機密データ検出イベントが発生した、セキュリティエージェントの割合を表示できます。

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの 設定]に移動します。
2. [コンプライアンスインジケータ] タブをクリックします。
3. [情報漏えい対策のコンプライアンス] をクリックします。
4. 次の表は、利用可能な設定オプションを示しています。

列	説明
期間	表示されるデータの時間範囲を指定します。

列	説明
許容される脅威の検出数	許容される機密データ検出イベント数を入力します。
アラートインジケータ	スライダを調整して、さまざまなアラートレベルのしきい値 (準拠するセキュリティエージェントの割合) を設定します。

5. [除外リスト] では、カスタムタグとカスタムフィルタを選択して、コンプライアンスの計算からユーザまたはエンドポイントを除外します。

注意

- 除外リストはすべての Apex Central ユーザに適用されます。除外リストへの追加と削除、および対応するタグとフィルタの変更は、ユーザの権限に従ってのみ実行できます。
- タグまたはフィルタの作成の詳細については、171 ページの「カスタムタグおよびカスタムフィルタ」を参照してください。

a. [追加] をクリックします。

[除外設定の追加] 画面が表示されます。

b. [種類] ドロップダウンリストで、[ユーザ] または [エンドポイント] を選択して、利用可能なカスタムフィルタとカスタムタグを種類別に表示します。それ以外の場合は、[すべて] を選択してすべてのエントリを表示します。

ヒント

カスタムフィルタまたはカスタムタグを検索するには、テキストフィールドに名前を入力して、<Enter> キーを押します。

カスタムタグおよびフィルタの詳細については、171 ページの「カスタムタグおよびカスタムフィルタ」を参照してください。

c. 1 つ以上のカスタムタグまたはカスタムフィルタを選択して、[追加] をクリックします。

選択した項目が除外リストに表示されます。

d. [閉じる] をクリックします。

e. [保存] をクリックします。

f. 追加したタグまたはフィルタの対象範囲を [次のユーザが追加した例外を適用] ドロップダウンリストから指定します。

- すべてのユーザアカウント: ユーザアカウントによって追加されたカスタムフィルタとカスタムタグに指定されているすべてのユーザとエンドポイントを除外します。
- ログオンしたアカウントのみ: 現在ログオンしているユーザアカウントによって追加されたカスタムフィルタとカスタムタグに指定されているユーザとエンドポイントのみ除外します。

6. [保存] をクリックします。

エンドポイントおよびユーザのグループ設定

Apex Central では、次の情報に基づいて [セキュリティ状態] タブでエンドポイントまたはユーザをグループ化できます。

- サイトの場所
- レポートラインのマネージャ

初期設定では、Apex Central は、Active Directory からのユーザまたはエンドポイントのサイトとレポートラインに関する情報を同期します。コンプライアンス情報を表示するように、カスタムサイトおよびレポートラインのグループを設定できます。

サイト

次の表は、[運用管理] > [設定] > [Active Directory とコンプライアンスの設定] > [サイト] タブに表示されるサイト情報を示しています。

表 6-1. サイト

列	説明
表示名	[セキュリティ状態] ウィジェット/タブに表示される名前を入力します。 注意 初期設定では、[その他] グループにはサイトに所属していないすべてのエンドポイントが含まれます。
サイト	Active Directory から同期されたサイト名を示します。

カスタムサイトを作成する

カスタムサイトグループを 作成して、指定された IP アドレス範囲のエンドポイントまたはユーザを含めることができます。

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの 設定]に移動します。
2. [サイト] タブをクリックします。
3. [カスタム設定の追加] をクリックします。

   [カスタムサイトの追加] 画面が表示されます。
4. [セキュリティ 状態] ウィジェット/タブでグループを識別するための [表示名] を指定します。
5. [セキュリティ 状態] ウィジェット/タブでグループを識別するための [ノードの色] を選択します。
6. カスタムサイトに含めるエンドポイントの IPv4 または IPv6 アドレス範囲を指定します。
7. [保存] をクリックします。

   カスタムサイトを作成した後、次のようにします。

- 選択したカスタムサイトを削除するには、[カスタム設定の削除] をクリックします。
- 設定を変更するには、カスタムサイト名をクリックします。

サイトをマージする

2 つ以上のサイトをマージして、カスタムサイトを作成できます。既存のサイトをマージすると、Apex Central によって元のサイトがリストから削除されます。

ヒント

Apex Central では、マージしたグループを塗りつぶした点のアイコン ( ) で示します。

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの 設定]に移動します。
2. [サイト] タブをクリックします。
3. 2 つ以上のサイトを選択します。
4. [マージ] をクリックします。

   [サイトのマージ] 画面が表示されます。
5. [セキュリティ状態] ウィジェット/タブでグループを識別するための [表示名] を指定します。
6. [セキュリティ状態] ウィジェット/タブでグループを識別するための [ノードの色] を選択します。
7. [保存] をクリックします。

   サイトをマージした後は、[分割] をクリックするとマージ済みのサイトを分割できます。

レポートライン

次の表は、[レポートライン] タブに表示される情報を示しています。

表 6-2. レポートライン

データ	説明
レポートラインのレベル	レポートラインのレベルは、Active Directory 内でユーザの管理階層レベルを示します。 [レポートラインのレベル] ドロップダウンリストからレベル番号を選択し、[適用] をクリックしてリストを更新します。
表示名	[セキュリティ状態] タブに表示される名前 ヒント 初期設定では、[その他] グループにはレポートラインのレベルが選択したレベルよりも高いすべてのマネージャが含まれます。
マネージャ	レポートラインのマネージャを示します。 この情報は Active Directory サーバから同期されます。

カスタムレポートラインを作成する

カスタムレポートラインを作成して、選択したマネージャに直接的または間接的にレポートするユーザを含めることができます。

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの設定]に移動します。
2. [レポートライン] タブをクリックします。
3. (オプション) [レポートラインのレベル] の設定を変更し、[適用] をクリックしてリストを更新します。

レポートラインのレベルは、Active Directory 内でユーザの管理階層レベルを示します。

4. [カスタム設定の追加] をクリックします。

   [カスタムレポートラインの追加] 画面が表示されます。

5. [セキュリティ状態] ウィジェット/タブでグループを識別するための [表示名] を指定します。

6. [ユーザ] リストからユーザを選択し、[選択したユーザ] リストに追加するアイコンをクリックします。

   注意

   複数のユーザを選択するには、<Ctrl> キーを押して、ユーザ名をクリックします。

7. [保存] をクリックします。

   カスタムレポートラインを作成した後、次のようにします。

   - 選択したカスタムレポートラインを削除するには、[カスタム設定の削除] をクリックします。
   - 設定を変更するには、カスタムグループ名をクリックします。

レポートラインをマージする

2 つ以上のレポートラインをマージして、カスタムレポートラインを作成できます。既存のレポートラインをマージすると、Apex Central によって元のレポートラインがリストから削除されます。

ヒント

Apex Central では、マージしたグループを塗りつぶした点のアイコン ( ) で示します。

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの設定]に移動します。
2. [レポートライン] タブをクリックします。
3. 2 つ以上のレポートラインを選択します。
4. [マージ] をクリックします。

   [レポートラインのマージ] 画面が表示されます。
5. [セキュリティ状態] ウィジェット/タブでグループを識別するための [表示名] を指定します。
6. [保存] をクリックします。

   レポートラインをマージした後は、[分割] をクリックするとマージ済みのレポートラインを分割できます。

第 7 章

ユーザ/エンドポイントディレクトリ

このセクションでは、Apex Central ネットワーク内のすべてのユーザとエンドポイントに関する情報を確認する方法について説明します。

次のトピックがあります。

ユーザ/エンドポイントディレクトリ

[ユーザ/エンドポイントディレクトリ] 画面には、指定された時間範囲の、Apex Central ネットワーク内のすべてのユーザおよびエンドポイントに関する情報が表示されます。

- [エンドポイント] タブまたは [ユーザ] タブにあるドロップダウンコントロールを使用して、表示するデータの時間範囲を指定したり、[表形式] と [タイムライン表示] を切り替えたりできます。
- [エクスポート] をクリックして、データを*.csv ファイルまたは*.png 画像でエクスポートします。

注意

[表形式] では、データを*.csv ファイルでエクスポートできます。[タイムライン表示] では、データを*.csv ファイルまたは*.png 画像でエクスポートできます。エクスポートした*.png のタイムライン画像には、最大で 30 件のユーザまたはエンドポイントの情報のみが表示されます。

ユーザ/エンドポイントツリーでは、データを次のカテゴリに編成します。

- ユーザ: エンドポイントにログオンするユーザ、または統合された Active Directory 構造の一部であるユーザに関する情報が含まれます。

  詳細については、143 ページの「ユーザの詳細情報」を参照してください。

- エンドポイント: Apex Central にログを送信するエンドポイント、または統合された Active Directory 構造の一部であるエンドポイントに関する情報が含まれます。

  詳細については、151 ページの「エンドポイントの詳細」を参照してください。

- Active Directory: 統合された Active Directory サーバの組織単位が表示されます。

注意

Apex Central は、複数の Active Directory フォレストとの同期をサポートしています。Active Directory ドメインを追加すると、同じフォレストのすべてのドメインが自動的に同期されます。

フォレストの信頼の詳細については、Active Directory 管理者にお問い合わせください。

詳細検索、タグ、およびフィルタを使用して [ユーザ] および [エンドポイント] ノードに表示される初期設定データを変更できます。

詳細については、166 ページの「詳細検索の使用」および 171 ページの「カスタムタグおよびカスタムフィルタ」を参照してください。

ユーザの詳細情報

[ユーザ/エンドポイントディレクトリ] 画面には、指定された時間範囲のユーザ情報が表示されます。

- [エンドポイント] タブまたは [ユーザ] タブにあるドロップダウンコントロールを使用して、表示するデータの時間範囲を指定したり、[表形式] と [タイムライン表示] を切り替えたりできます。
- [エクスポート] をクリックして、データを*.csv ファイルまたは*.png 画像でエクスポートします。

注意

[表形式] では、データを*.csv ファイルでエクスポートできます。[タイムライン表示] では、データを*.csv ファイルまたは*.png 画像でエクスポートできます。エクスポートした*.png のタイムライン画像には、最大で 30 件のユーザまたはエンドポイントの情報のみが表示されます。

次の表は、[ユーザ/エンドポイントディレクトリ] 画面の [表形式] に表示されるユーザ情報を示しています。

表 7-1. 表形式でのユーザの詳細情報

列	説明
	エンドポイントまたはユーザに重要度タグが割り当てられている場合、Apex Central に黄色の星アイコン () が表示され、重要度が示されます。 詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

ユーザ (アカウント)	Apex Central は、エンドポイントの種類に基づいて、または Active Directory との統合により、ユーザを識別してエンドポイントと関連付けます。
	
	• サーバおよびデスクトッププラットフォーム: Apex Central によって、最後にログオンしたユーザがエンドポイントに関連付けられます。
	• モバイルデバイス:
	  • Active Directory と同期できる場合、Apex Central によって関連付けられた Active Directory アカウントのあるモバイルデバイスの登録済みメールアドレスが解決されます。
	  • Active Directory と同期できない場合、Apex Central にモバイルデバイスの登録済みメールアドレスが表示されます。
	
	ユーザ名をクリックすると、連絡先の詳細が表示されます。
	
	詳細については、150 ページの「連絡先情報」を参照してください。
	
	  注意
	
	[ユーザ] > [すべて] ノードには、重複に関係なく各種エンドポイントのすべてのローカルユーザがリストされます。管理下の製品のエンドポイントに同じ名前を持つ複数のローカルユーザが存在する場合、同じユーザ名が重複して表示されることがあります。

列	説明
ドメイン	• Active Directory と同期できる場合、Apex Central にユーザが所属するドメイン名が表示されます。 • Active Directory と同期できない場合、Apex Central にユーザが最後にログオンしたエンドポイント/ホスト名が表示されます。
マネージャ	Active Directory と同期できる場合、Apex Central にユーザのマネージャが表示されます。 マネージャ列の名前をクリックすると、マネージャの連絡先の詳細が表示されます。 詳細については、150 ページの「連絡先情報」を参照してください。
エンドポイント	エンドポイントからの最後のログオン情報に基づいた、ユーザに現在関連付けられているエンドポイントの数を示します。 数字をクリックすると、関連するエンドポイントの情報が表に示されます。 詳細については、151 ページの「エンドポイントの詳細」を参照してください。
ポリシー	エンドポイントからの最後のログオン情報に基づいた、ユーザに現在関連付けられているポリシーの数を示します。 [ポリシー] の数字をクリックすると、ユーザに関連するポリシーの情報が表示されます。 詳細については、149 ページの「ポリシーステータス」を参照してください。

列	説明
脅威	ユーザに関連付けられたエンドポイントで発生したセキュリティの脅威の総数を示します。 [脅威] の数字をクリックすると、ユーザに関連する脅威の情報が表示されます。 詳細については、147 ページの「ユーザのセキュリティの脅威」を参照してください。 たとえば、エンドポイント「us-mkt-dev1」に最後にログオンしたユーザが Henry で、そのエンドポイントで 10 件のウイルス/不正プログラムの検出と 2 件の Web 違反が報告された場合、Henry の [脅威] の数は 12 と表示されます。 **注意** • ネットワーク環境で Active Directory を使用していない場合、ゲートウェイ製品に対するコンテンツ違反、フィッシング、およびスパムといった検出/違反は表示されません。 • Apex One などのエンドポイント製品によって検出されたセキュリティの脅威は、エンドポイントに最後にログオンしたユーザに関連付けられます。IWSVA などのゲートウェイ製品によって検出されたセキュリティの脅威は、検出を実行したユーザに関連付けられます。

次の表は、[ユーザ/エンドポイントディレクトリ] 画面の [タイムライン表示] に表示されるユーザ情報を示しています。

表 7-2. タイムライン表示でのユーザの詳細情報

列	説明
ユーザ (アカウント)	Apex Central は、エンドポイントの種類に基づいて、または Active Directory との統合により、ユーザを識別してエンドポイントと関連付けます。

列	説明
脅威	ユーザに関連付けられたエンドポイントで発生したセキュリティの脅威の総数を示します。 [脅威] の数字をクリックすると、ユーザに関連する脅威の情報が表示されます。 詳細については、147 ページの「ユーザのセキュリティの脅威」を参照してください。
<タイムライン>	タイムラインには、各ユーザのセキュリティの脅威がいつ発生したかが示されます。 • 赤色の警告点 () にマウスを重ねると、特定の日付のユーザの重大な脅威の数とすべてのセキュリティの 脅威検出の総数が表示されます。 • 赤色の無地の点 () にマウスを重ねると、特定の日付のユーザの重大な脅威以外の検出数が表示されます。 • 赤色の点をクリックすると、特定の日付の関連する脅威情報が表示されます。 詳細については、147 ページの「ユーザのセキュリティの脅威」を参照してください。

ユーザのセキュリティの脅威

[ユーザ] 情報画面の [脅威] タブでは、選択したユーザに割り当てられているエンドポイントで検出されたすべてのセキュリティの 脅威を確認できます。

この画面は、Apex Central 管理コンソールの [ダッシュボード] > [概要] タブの次のウィジェットからアクセスできます。

- 重大な脅威: [重要なエンドポイント] 列または [その他のエンドポイント] 列の数字をクリックしてから、表示するユーザをクリックします。
- 脅威にさらされているユーザ: 表示するユーザの [脅威] 列の数字をクリックします。
- 脅威にさらされているエンドポイント: 表示するエンドポイントの [脅威] 列の数字をクリックします。[エンドポイント] 情報画面で、[一般情報] タブをクリックし、ユーザ名をクリックします。

- セキュリティの脅威の時間別推移: 検出時刻、および割り当てエンドポイントとユーザのアカウントのどちらで検出されたかに基づいて、脅威に関する情報がグラフィカルに表示されます。
  - 脅威のアイコン (など) にマウスを重ねると、検出の詳細を確認できます。
  - 表示される時間間隔を変更するには、[ズーム] の値を変更します。
  - 終了日を変更するには、グラフの下に表示される日付をスクロールします。
  - フィルタを適用するには、漏斗アイコン ( ) をクリックし、以下の条件を選択します。詳細フィルタを作成するには [OR] または [AND] 演算子を使用します。
    - 脅威の種類: 2 番目のドロップダウンリストから脅威のカテゴリを選択します。
    - セキュリティの脅威: 不正プログラム名または不審な URL、IP アドレス、または送信者のメールアドレスを入力します。
    - 脅威のステータス: [製品による解決]、[処理が必要です]、または [手動による解決] を選択します。
- セキュリティの脅威の詳細: [セキュリティの脅威の時間別推移] グラフに表示された脅威に関する詳細情報が示されます。
  - [セキュリティの脅威] 列の値をクリックすると、[影響を受けたユーザ] 画面が表示されます。

- [詳細] 列の [表示] リンクをクリックすると、詳細を確認できます。
- [脅威のステータス] 列のフラグアイコン ( ) をクリックすると、脅威のステータスが変更されます。

注意

脅威のステータスを変更しても、その脅威は実際には解決していません。脅威のステータスは、識別された脅威を管理者が追跡したり、他の管理者に脅威が解決したことを示したりするためのものです。

脅威のステータス	説明
製品による解決 ( )	脅威が管理下の製品によって解決されたことを示します。 **注意** この脅威のステータスは変更できません。
処理が必要です ( )	修復が必要であることを示します。 [処理が必要です] アイコン ( ) をクリックすると、脅威のステータスが [手動による解決] ( ) に変化します。
手動による解決 ( )	管理者によって修復されたことを示します。 [製品による解決] アイコン ( ) をクリックすると、脅威のステータスが [処理が必要です] ( ) に変化します。

ポリシーステータス

[ポリシーステータス] タブには、対象エンドポイントにインストールされているすべての製品、割り当てられている Apex Central ポリシー、およびインストールされている製品ごとの現在のポリシーステータスが表示されます。

注意

Apex Central は、エンドポイントの種類に基づいて、または Active Directory との統合により、ユーザを識別してエンドポイントと関連付けます。

ポリシーを確認または編集するには、割り当てられたポリシーの名前をクリックします。

連絡先情報

[連絡先情報] 画面には、Active Directory のエントリと同様のユーザの詳細情報が表示されます。

連絡先情報を Active Directory と同期する

Apex Central では、Active Directory のグローバルカタログ (GC) からデータが同期されます。

手順

1. Microsoft 管理コンソール (mmc) を開きます。
2. スナップイン (Active Directory スキーマ) を追加します。
3. 左側のパネルで、[属性] に移動します。
4. 次のそれぞれについて、[グローバル カタログにこの属性をレプリケートする] をオンにします。
   - proxyAddresses
   - department
   - homephone
   - PhysicalDeliveryOfficeName
   - telephoneNumber
   - title
5. Active Directory の複製が実行されるまで待ちます。

エンドポイントの詳細

[ユーザ/エンドポイントディレクトリ] 画面には、指定された時間範囲のエンドポイント情報が表示されます。

- [エンドポイント] タブまたは [ユーザ] タブにあるドロップダウンコントロールを使用して、表示するデータの時間範囲を指定したり、[表形式] と [タイムライン表示] を切り替えたりできます。
- [エクスポート] をクリックして、データを*.csv ファイルまたは*.png 画像でエクスポートします。

> **注意**
>
> [表形式] では、データを*.csv ファイルでエクスポートできます。[タイムライン表示] では、データを*.csv ファイルまたは*.png 画像でエクスポートできます。エクスポートした*.png のタイムライン画像には、最大で 30 件のユーザまたはエンドポイントの情報のみが表示されます。

次の表は、[ユーザ/エンドポイントディレクトリ] 画面の [表形式] に表示されるユーザ情報を示しています。

列	説明
	エンドポイントまたはユーザに重要度タグが割り当てられている場合、Apex Central に黄色の星アイコン ( ) が表示され、重要度が示されます。 詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。
エンドポイント	ホスト名またはデバイス名を示します。 エンドポイント名をクリックすると、[エンドポイント] 画面が表示され、[ポリシーステータス] タブが開きます。 詳細については、157 ページの「ポリシーステータス」を参照してください。
IP アドレス	エンドポイントの静的または動的な IP アドレスを示します。
種類	マシンまたはデバイスの種類を示します: サーバ、デスクトップ、ノートパソコン、モバイルデバイスなど

列	説明
OS	マシンまたはデバイスで稼働している OS を示します。
エンドポイントサーバ	エンドポイントを管理しているサーバの名前とインストールされている製品を示します。
ユーザ (アカウント)	最後にエンドポイントにログオンまたはエンドポイントを使用したユーザの名前またはメールアドレスを示します。 詳細については、150 ページの「連絡先情報」を参照してください。
脅威	エンドポイントで発生したセキュリティの脅威の総数を示します。 [脅威] の数字をクリックすると、エンドポイントに関連する脅威の情報が表示されます。 詳細については、154 ページの「エンドポイントのセキュリティの脅威」を参照してください。

次の表は、[ユーザ/エンドポイントディレクトリ] 画面の [タイムライン表示] に表示されるエンドポイント情報を示しています。

表 7-3. タイムライン表示でのエンドポイントの詳細

列	説明
エンドポイント	ホスト名またはデバイス名を示します。 エンドポイント名をクリックすると、[エンドポイント] 画面が表示され、[ポリシーステータス] タブが開きます。 詳細については、157 ページの「ポリシーステータス」を参照してください。 **注意** Apex Central では、エンドポイントに重要なタグが割り当てられている場合、エンドポイント名の前に黄色の星アイコン ( ) が表示されます。 詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

列	説明
脅威	エンドポイントで発生したセキュリティの脅威の総数を示します。 [脅威] の数字をクリックすると、エンドポイントに関連する脅威の情報が表示されます。 詳細については、154 ページの「エンドポイントのセキュリティの脅威」を参照してください。
<タイムライン>	タイムラインには、各エンドポイントのセキュリティの脅威がいつ発生したかが示されます。 • 赤色の警告点 () にマウスを重ねると、特定の日付のエンドポイントの重大な脅威の数とすべてのセキュリティの 脅威検出の総数が表示されます。 • 赤色の無地の点 () にマウスを重ねると、特定の日付のエンドポイントの重大な脅威以外の検出数が表示されます。 詳細については、154 ページの「エンドポイントのセキュリティの脅威」を参照してください。

エンドポイントの情報

[エンドポイント] 情報画面には、選択したエンドポイントに関する詳細情報が表示されます。[エンドポイント] 情報画面のタイトルには、エンドポイントのアイコン () に続いてエンドポイント名が表示されます。

関連情報を表示するには、次のいずれかのタブをクリックします。

- 脅威: 選択したエンドポイントで検出されたすべてのセキュリティの 脅威が表示されます。

  詳細については、154 ページの「エンドポイントのセキュリティの 脅威」を参照してください。

- ポリシーステータス: 選択したエンドポイントに関連するポリシーのリストが表示されます。

  詳細については、157 ページの「ポリシーステータス」を参照してください。

- メモ: 選択したエンドポイントに関する手動で追加されたメモが表示されます。

  詳細については、157 ページの「エンドポイントのメモ」を参照してください。

- 一般情報: 選択したエンドポイントに関する基本情報が表示されます。

  詳細については、158 ページの「エンドポイントの一般情報」を参照してください。

また、[エンドポイント] 情報画面では、[タスク] メニューを使用して、選択したエンドポイントに対する特定のアクションを実行できます。

- タグの割り当て: 検索のために、タグと選択したエンドポイントを関連付けます。

  詳細については、173 ページの「カスタムタグ」を参照してください。

- 隔離: ネットワークおよびインターネットへのエンドポイントのアクセスを制限します。

  詳細については、508 ページの「エンドポイントを隔離する」を参照してください。

- 復元: 隔離されたエンドポイントに対するネットワークアクセスを復元します。

  詳細については、508 ページの「エンドポイントを隔離する」を参照してください。

エンドポイントのセキュリティの脅威

[エンドポイント] 情報画面の [脅威] タブでは、特定のエンドポイントで検出されたすべてのセキュリティの脅威を確認できます。

[エンドポイント] 情報画面の [脅威] タブには次の場所からアクセスできます。

- 脅威にさらされているエンドポイントウィジェット: [脅威] 列の数字をクリックします。

詳細については、67 ページの「脅威にさらされているエンドポイントウィジェット」を参照してください。

- [エンドポイントの詳細] 画面: [脅威] 列の数字をクリックします。

  詳細については、151 ページの「エンドポイントの詳細」を参照してください。

- [セキュリティの脅威] 画面の [影響を受けたユーザ] タブ: [ホスト名] 列のエンドポイント名をクリックします。

  詳細については、161 ページの「影響を受けたユーザ」を参照してください。

- タスク: [タグの割り当て] を実行したり、エンドポイントへの接続に対して [隔離] または [復元] を実行したりできます。

  詳細については、508 ページの「エンドポイントを隔離する」を参照してください。

- セキュリティの脅威の時間別推移: 検出時刻、および割り当てエンドポイントとユーザのアカウントのどちらで検出されたかに基づいて、脅威に関する情報がグラフィカルに表示されます。

  - 脅威のアイコン (など) にマウスを重ねると、検出の詳細を確認できます。
  - 表示される時間間隔を変更するには、[ズーム] の値を変更します。
  - 終了日を変更するには、グラフの下に表示される日付をスクロールします。

- フィルタを適用するには、漏斗アイコン () をクリックし、以下の条件を選択します。詳細フィルタを作成するには [OR] または [AND] 演算子を使用します。
  - 脅威の種類: 2 番目のドロップダウンリストから脅威のカテゴリを選択します。
  - セキュリティの脅威: 不正プログラム名または不審な URL、IP アドレス、または送信者のメールアドレスを入力します。
  - 脅威のステータス: [製品による解決]、[処理が必要です]、または [手動による解決] を選択します。

- セキュリティの脅威の詳細: [セキュリティの脅威の時間別推移] グラフに表示された脅威に関する詳細情報が示されます。
  - [セキュリティの脅威] 列の値をクリックすると、[影響を受けたユーザ] 画面が表示されます。
  - [詳細] 列の [表示] リンクをクリックすると、詳細を確認できます。
  - [脅威のステータス] 列のフラグアイコン () をクリックすると、脅威のステータスが変更されます。

注意

脅威のステータスを変更しても、その脅威は実際には解決していません。脅威のステータスは、識別された脅威を管理者が追跡したり、他の管理者に脅威が解決したことを示したりするためのものです。

脅威のステータス	説明
製品による解決 ()	脅威が管理下の製品によって解決されたことを示します。 **注意** この脅威のステータスは変更できません。

脅威のステータス	説明
処理が必要です ()	修復が必要であることを示します。 [処理が必要です] アイコン () をクリックすると、脅威のステータスが [手動による解決] () に変化します。
手動による解決 ()	管理者によって修復されたことを示します。 [製品による解決] アイコン () をクリックすると、脅威のステータスが [処理が必要です] () に変化します。

ポリシーステータス

[ポリシーステータス] タブには、対象エンドポイントにインストールされているすべての製品、割り当てられている Apex Central ポリシー、およびインストールされている製品ごとの現在のポリシーステータスが表示されます。

ポリシーを確認または編集するには、割り当てられたポリシーの名前をクリックします。

エンドポイントのメモ

エンドポイントに手動でメモを追加すると、特定のエンドポイントで問題や解決策を追跡するのに便利です。たとえば、隔離したエンドポイントについて、調査を行って脅威を解決するときや、すべての脅威を解決してネットワーク接続を復元する前など、状況に応じて追加のメモを入力します。

Apex Central では、特定の処理に対応する次のメモが自動で追加されます。

- 隔離
- 復元
- タグの割り当て: {タグ名}
- タグの削除: {タグ名}

詳細については、175 ページの「ユーザ/エンドポイントにカスタムタグを割り当てる」および 508 ページの「エンドポイントを隔離する」を参照してください。

エンドポイントの一般情報

エンドポイントに関する次の情報を表示できます。

情報	説明
IP アドレス	エンドポイントの IP アドレスを示します。
種類	エンドポイントの種類を示します。(例:「ノートパソコン」)
OS	エンドポイントの OS を示します。
ユーザ	エンドポイントに関連付けられているユーザアカウントを示します。 注意 Apex Central は、エンドポイントの種類に基づいて、または Active Directory との統合により、ユーザを識別してエンドポイントと関連付けます。
ドメイン	エンドポイントに関連付けられている Active Directory ドメインを示します。

エンドポイントを隔離する

危険性の高いエンドポイントを隔離して調査を実行し、セキュリティの問題を解決します。すべての問題を解決したら、すぐに接続を復元します。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。
2. エンドポイントの表示を選択します。
3. リスト内のエンドポイントの名前をクリックします。

4. 表示される [エンドポイント] 情報画面で [タスク] > [隔離] をクリックします。

   Apex Central では、次の理由により、エンドポイント上で [隔離] オプションが無効になります。

   - エンドポイントのエージェントでサポート対象外のバージョンが実行されている
   - Apex Central へのログオンに使用されているユーザアカウントに必要な権限がない

5. [エンドポイント] 情報画面の上部にメッセージが表示され、その画面で隔離ステータスを監視できます。隔離が終了すると、メッセージが閉じられ、対象エンドポイントにユーザへの通知が表示されます。

   隔離プロセス中に問題が発生した場合、[エンドポイント - <名前>] 画面の上部に問題を通知するメッセージが表示されます。

6. Apex Central ネットワーク上の隔離されたエンドポイントをすべて表示するには、[ユーザ/エンドポイントディレクトリ] ツリーで [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み] ノードを順にクリックします。

7. (オプション) 隔離されたすべてのエンドポイントに許可する送受信トラフィックを設定するには、次の手順を実行します。

   トレンドマイクロの初期設定の通信ポートの一覧については、202 ページの「セキュリティエージェントのインストールパッケージをダウンロードする」を参照してください。

   a. 表示された画面のメモにある [コントロール] ハイパーリンクをクリックします。

b. [隔離されたエンドポイント上のトラフィック制御] を選択します。

c. [受信トラフィック] または [送信トラフィック] セクションを展開します。

d. [プロトコル]、[IP アドレス]、および [送信先ポート] を指定して、許可するトラフィックを指定します。

   コンマを使用して複数の送信先ポートを区切ります。

e. [送信先ポート] 情報の右側の - コントロールをクリックして、複数の送受信エントリを追加します。

注意

許可するトラフィックの設定を変更した後、以前に隔離されたエンドポイントと後で隔離されるエンドポイントはすべて、送受信トラフィックの設定が適用されます。

---

8. 隔離されたエンドポイントでセキュリティの脅威が解決したら、次の場所からネットワーク接続を復元します。

- [エンドポイント] 情報画面: [タスク] > [復元]をクリックします。
- [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み]: 表内のエンドポイントの行を選択して、[タスク] > [ネットワーク接続の復元] をクリックします。

9. 画面の上部にメッセージが表示され、その画面で復元ステータスを監視できます。復元が終了すると、メッセージが閉じられ、対象エンドポイントにユーザへの通知が表示されます。

   復元プロセス中に問題が発生した場合、画面の上部に問題を通知するメッセージが表示されます。

Active Directory の詳細

Active Directory ノードには、統合された Active Directory 構造が表示されます。Active Directory ノードの組織単位を表示すると、リストには次の 2 つのタブがあります。

- ユーザ: 詳細については、143 ページの「ユーザの詳細情報」を参照してください。
- エンドポイント: 詳細については、151 ページの「エンドポイントの詳細」を参照してください。

影響を受けたユーザ

[セキュリティの脅威] 画面の [影響を受けたユーザ] タブを使用すると、ネットワーク全体で特定の脅威の対象となったユーザを確認できます。

[影響を受けたユーザ] タブには、[ユーザ] または [エンドポイント] 情報画面から表内のセキュリティの脅威名をクリックするとアクセスできます。

- 影響を受けた一意のユーザ数の時間別推移: 脅威の影響を受けたユーザと検出時間がグラフィカルに表示されます。
  - [影響の分析] をクリックして Root Cause Analysis を開始し、脅威がネットワーク上の他のエンドポイントに影響しているかどうかを診断します。

    重要

    [脅威情報] 画面から影響分析を実行するには、有効な Apex One Endpoint Sensor ライセンスが必要です。また、適切な [Apex One セキュリティエージェント] ポリシーまたは [Apex One (Mac)] ポリシーに対して Endpoint Sensor 機能を有効にする必要があります。

    詳細については、163 ページの「影響を受けたユーザに対する影響を分析する」を参照してください。

  - [Retro Scan 開始] をクリックして、C&C サーバへのコールバックの試行やネットワークでのその他の関連するアクティビティについての過去の Web アクセスのログを検索します。

重要

[脅威情報] 画面から Retro Scan を実行するには、Apex Central の [サーバの登録] 画面で Deep Discovery Inspector サーバを少なくとも 1 つ追加し、登録した Deep Discovery Inspector サーバで Retro Scan を有効にする必要があります。

詳細については、164 ページの「影響を受けたユーザに対する Retro Scan を実行する」を参照してください。

- ユーザアイコンにマウスを重ねて、この特定の脅威の影響を受けるすべてのユーザと、環境内でのその脅威の検出履歴を確認します。
  - 最近の検出: 検索中に行われた脅威の検出
  - 前回未検出: ログデータの影響分析中に行われた脅威の検出
- 表示される時間間隔を変更するには、[ズーム] の値を変更します。
- 終了日を変更するには、グラフの下に表示される日付をスクロールします。

- 詳細: [影響を受けた一意のユーザ数の時間別推移] グラフに表示された脅威に関する詳細情報が示されます。
  - [ユーザ名] 列または [ホスト名] 列の値をクリックすると、詳細情報が表示されます。

    詳細については、「ユーザのセキュリティの脅威」または「エンドポイントのセキュリティの脅威」を参照してください。

セキュリティの脅威の一般情報

表示される情報は、管理下の製品から受け取った脅威の種類および脅威関連の情報によって異なります。

影響を受けたユーザに対する影響を分析する

Apex Central の [セキュリティの脅威] 画面の [影響を受けたユーザ] タブで環境内のセキュリティの脅威の過去の影響分析を実行できます。

Apex One Endpoint Sensor は、エージェントと通信し、エージェントログの履歴検索を実行して、不審オブジェクトが検出されずに一定期間にわたって環境に影響を与えているかどうか判断します。このようにして、環境内の不審なファイル、IP アドレス、およびドメインの影響を分析します。

重要

影響分析には、有効な Apex One Endpoint Sensor ライセンスが必要です。有効な Apex One Endpoint Sensor ライセンスがあることを確認し、適切な [Apex One セキュリティエージェント] ポリシーまたは [Apex One (Mac)] ポリシーに対して Endpoint Sensor 機能を有効にしてください。

詳細については、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. Apex Central 管理コンソールで、[ダッシュボード] に移動します。
2. 脅威にさらされているユーザウィジェットまたは脅威にさらされているエンドポイントウィジェットで、数字をクリックします。
3. 表示される画面で、[セキュリティの脅威の詳細] 表にある [セキュリティの脅威] の名前を選択します。

   [影響を受けたユーザ] 画面が表示されます。
4. [影響の分析] をクリックします。

   Endpoint Sensor で、過去のネットワークトラフィックおよび検出された不審オブジェクトのログが検索されます。

   詳細については、490 ページの「Endpoint Sensor での履歴調査」を参照してください。

影響を受けたユーザに対する Retro Scan を実行する

Apex Central の [セキュリティの脅威] 画面の [影響を受けたユーザ] タブで Retro Scan を実行して、C&C サーバへのコールバックの試行やネットワークでのその他の関連するアクティビティについての 過去の Web アクセスのログを検索できます。

Deep Discovery Inspector は、トレンドマイクロの Retro Scan で収集された過去のネットワークトラフィック情報に基づいて、不審な URL の影響を分析します。

重要

[脅威情報] 画面から Retro Scan を実行するには、Apex Central の [サーバの登録] 画面で Deep Discovery Inspector サーバを少なくとも 1 つ追加し、登録した Deep Discovery Inspector サーバで Retro Scan を有効にする必要があります。

詳細については、Deep Discovery Inspector 管理者ガイドを参照してください。

手順

1. Apex Central 管理コンソールで、[ダッシュボード] に移動します。
2. 脅威にさらされているユーザウィジェットまたは脅威にさらされているエンドポイントウィジェットで、数字をクリックします。
3. 表示される画面で、[セキュリティの脅威の詳細] 表にある [セキュリティの脅威] の名前を選択します。

   [影響を受けたユーザ] 画面が表示されます。
4. [Retro Scan 開始] をクリックします。

   Deep Discovery Inspector で、C&C サーバへのコールバックの試行やネットワークでのその他の関連するアクティビティについての 過去の Web アクセスのログが検索されます。

   詳細については、165 ページの「Deep Discovery Inspector の Retro Scan」を参照してください。

Deep Discovery Inspector の Retro Scan

Retro Scan は、C&C サーバへのコールバックやネットワークでのその 他の関連アクティビティについて 、過去の Web アクセスログを検索するクラウドベースのサービスです。Web アクセスログには、ごく最近検出された C&C サーバへの接続 （検出もブロックもされてない）が記録されていることがあります。フォレンジックス調査においては、ネットワークが攻撃の影響を受

けていないかどうかを確認するために、このようなログを調べることが重要です。

Retro Scan では、次のログ情報を Smart Protection Network に保存します。

- Deep Discovery Inspector で監視しているエンドポイントの IP アドレス
- エンドポイントがアクセスした URL
- Deep Discovery Inspector の GUID

その後、保存したログエントリを定期的に検索し、次のリストに含まれる C&C サーバへのコールバック試行がないかを確認します。

- トレンドマイクログローバルインテリジェンスリスト : トレンドマイクロでは、複数のソースからの情報をリストにまとめ、各 C&C コールバックアドレスのリスクレベルを評価しています。C&C リストは毎日更新され、有効化されている製品に配信されます。
- ユーザ指定リスト: Retro Scan では、ログを独自の C&C サーバリストと照合することもできます。リストを指定するには、テキストファイルにアドレスを保存します。

重要

Deep Discovery Inspector の Retro Scan 画面には、トレンドマイクログローバルインテリジェンスリストを使用した検索の情報だけが表示されます。

詳細検索の使用

Apex Central では、部分一致検索を使用してユーザまたはエンドポイントを検索できます。ブール演算子を使用してリストに表示されるユーザまたはエンドポイントをフィルタすることもできます。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。

   [ユーザ/エンドポイントディレクトリ] 画面が表示されます。

2. 表の上にある [詳細] リンクをクリックします。
3. [検索] ドロップダウンで、[ユーザ] または [エンドポイント] を選択します。

   2 番目のドロップダウンコントロールの検索条件は選択内容に基づいて動的に変化します。

   詳細については、168 ページの「詳細検索のカテゴリ」を参照してください。
4. フィルタの右にあるブール演算子を使用して、複数の検索条件を追加します。
5. フィルタの右にあるブール演算子を使用して、複数の検索条件を追加します。

   - OR: 指定した条件で複数の値を検索できます。いずれかの値と一致するレコードがすべて表示されます。
   - AND: 新しい検索条件を選択できます。この条件に指定した値と選択したその他すべての条件の値と一致するレコードのみが表示されます。

   Active Directory ドメインが「HR」で、直属の上司が「Mary」または「Bill」、部署が「Finance」、ユーザ名に「ja」が含まれるすべてのユーザをフィルタするには、次の条件を指定します。

6. 次のいずれかをクリックして結果を表示します。

   - 検索: 検索結果がリストに表示されますが、検索条件は保存されません。

- 新規カスタムフィルタとして保存: 検索結果がリストに表示され、検索条件をカスタムフィルタに保存するかどうかメッセージが表示されます。カスタムフィルタは、ユーザ/エンドポイントディレクトリツリーの [ユーザ] または [エンドポイント] ノードに表示されます。

  詳細については、176 ページの「フィルタ」を参照してください。

7. (オプション) [エンドポイント] タブまたは [ユーザ] タブのドロップダウンコントロールを使用して、表示するデータの時間範囲を指定したり、[表形式] と [タイムライン表示] を切り替えたりします。

8. (オプション) [エクスポート] をクリックして、データを*.csv ファイルまたは*.png 画像でエクスポートします。

注意

- [表形式] では、データを*.csv ファイルでエクスポートできます。
- [タイムライン表示] では、データを*.csv ファイルまたは*.png 画像でエクスポートできます。

詳細検索のカテゴリ

詳細検索時には、[ユーザ] および [エンドポイント] に次の検索条件オプションを使用します。

表 7-4. ユーザのカテゴリ

カテゴリ	説明
ユーザ名	ローカルユーザまたは Active Directory 構造に属するユーザのアカウント名を示します。
直属の上司	ユーザに割り当てられているレポート先ユーザのアカウント名を示します。
Active Directory 内の場所	検索を開始する部署を示します。
部署	職務 (経理など) や他の条件に基づいてユーザをグループ化する社内の部署名を示します。

カテゴリ	説明
Active Directory グループ	Active Directory のユーザやコンピュータのアカウント、連絡先などをまとめて管理できるように 1 つにしたグループを示します。
脅威の種類	3 番目のドロップダウンリストからセキュリティの脅威の種類を選択します。
セキュリティの脅威	不正プログラム名、URL、IP アドレス、または送信者のメールアドレスを入力して特定のセキュリティの脅威を検索します。
脅威のステータス	[セキュリティの脅威] 画面の最初の列に、フラグアイコンで示されている修復ステータスです ([製品で解決されました]、[処理が必要です]、または [手動で解決されました])。 詳細については、147 ページの「ユーザのセキュリティの脅威」を参照してください。
重要度	割り当てられた重要度レベルを示します。 詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。
Active Directory サイト	Active Directory から同期されたサイト名を示します。 詳細については、134 ページの「エンドポイントおよびユーザのグループ設定」を参照してください。
レポートライン	Active Directory から同期されたレポートラインの表示名を示します。 詳細については、134 ページの「エンドポイントおよびユーザのグループ設定」を参照してください。

表 7-5. エンドポイントのカテゴリ

カテゴリ	説明
エンドポイント名	エンドポイントのホスト名またはデバイス名を示します。

カテゴリ	説明
IP アドレス	IPv4 アドレス範囲を示します。 **注意** IPv4 セグメントによる検索では、第 1 オクテットから始まる特定の範囲が必要です。IP アドレスに指定した値を含むエンドポイントがすべて返されます。
エンドポイントの種類	コンピュータまたはデバイスの種類を示します: サーバ、デスクトップ、ノートパソコン、モバイルデバイスなど
OS	エンドポイントの OS の種類を示します。
Active Directory 内の場所	検索を開始する部署を示します。
脅威の種類	3 番目のドロップダウンリストからセキュリティの脅威の種類を選択します。
セキュリティの脅威	不正プログラム名、URL、IP アドレス、または送信者のメールアドレスを入力して特定のセキュリティの脅威を検索します。
脅威のステータス	[セキュリティの脅威] 画面の最初の列に、フラグアイコンで示されている修復ステータスです ([製品で解決されました]、[処理が必要です]、または [手動で解決されました])。 詳細については、154 ページの「エンドポイントのセキュリティの脅威」を参照してください。
コンプライアンス	パターンファイルのコンプライアンスまたは 情報漏えい対策のコンプライアンスのステータスを示します。 詳細については、128 ページの「コンプライアンスインジケータ」を参照してください。
重要度	割り当てられた重要度レベルを示します。 詳細については、179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。
Active Directory サイト	Active Directory から同期されたサイト名を示します。 詳細については、134 ページの「エンドポイントおよびユーザのグループ設定」を参照してください。

カテゴリ	説明
レポートライン	Active Directory から同期されたレポートラインの表示名を示します。 詳細については、134 ページの「エンドポイントおよびユーザのグループ設定」を参照してください。
インストールモード	セキュリティエージェントのインストールモードを示します。 詳細については、202 ページの「セキュリティエージェントのインストールパッケージをダウンロードする」を参照してください。
サービス	セキュリティエージェントのサービスを示します。 詳細については、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 ドメイン階層	Apex One ドメイン階層におけるエンドポイントの場所

カスタムタグおよびカスタムフィルタ

ネットワークおよび管理要件に基づいて、タグおよびフィルタを使用します。タグおよびフィルタを使用する際は、次の点を考慮することをお勧めします。

- Active Directory の組織に基づいてユーザをグループ化
- 場所に基づいてエンドポイントをグループ化
- 類似のプロパティや特性に基づいてユーザまたはエンドポイントをグループ化

  例:

  - 同じ直属上司の配下のユーザをグループ化
  - 同じ OS を使用してエンドポイントをグループ化

注意

- ユーザ/エンドポイントディレクトリでカスタムタグ、フィルタ、または重要度ラベルを作成/変更する権限のある Apex Central ユーザアカウントは、他のすべてのユーザアカウントが作成したカスタムタグ、フィルタ、または重要なラベルを表示/変更できます。
- [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。
- Apex Central は、Active Directory との同期後に、「ドメイン管理者」(ユーザ) および「ドメインコントローラ」(エンドポイント) に自動的に重要度を割り当てます。
  - 現在のバージョンの Apex Central では、統合された Active Directory ドメインごとに重要な「ドメイン管理者」が 1 つ、重要な「ドメインコントローラ」が 1 つサポートされます。個々のユーザアカウントが同じ「ドメイン管理者」および「ドメインコントローラ」に別々に「重要」タグを割り当てることはできなくなりました。
  - 旧バージョンの Apex Central で「ドメイン管理者」および「ドメインコントローラ」に個別のユーザアカウントによって作成された既存の「重要」タグがある場合は、既存の「ドメイン管理者」および「ドメインコントローラ」が削除され、統合された Active Directory ドメインごとに 1 つの重要な「ドメイン管理者」と 1 つの重要な「ドメインコントローラ」に置き換えられます。

ヒント

- [ユーザのアクセス] ログクエリデータビューに、使用可能なカスタムタグやカスタムフィルタに関するユーザ変更の詳細が表示されます。

  詳細については、次のトピックを参照してください。

  - 318 ページの「ログクエリを使用する」
  - 732 ページの「ユーザアクセス情報」

- 関連付けられたタグ、フィルタ、または重要度ラベルをレポート対象として指定して、タグ付けされたユーザとエンドポイントのカスタムレポートを生成できます。

  詳細については、次のトピックを参照してください。

  - 442 ページの「1 回限りのレポートを作成する」
  - 447 ページの「予約レポートの追加」
  - 451 ページの「予約レポートを編集する」

カスタムタグ

カスタムタグは、グループ化のために 1 つ以上のユーザ/エンドポイントに手動で関連付けることができるラベルです。

- 初期設定では、ユーザまたはエンドポイントにタグは割り当てられていません。
- 複数のカスタムタグを複数のユーザ/エンドポイントに適用できます。
- ユーザ/エンドポイントディレクトリでカスタムタグ、フィルタ、または重要度ラベルを作成/変更する権限のある Apex Central ユーザアカウントは、他のすべてのユーザアカウントが作成したカスタムタグ、フィルタ、または重要なラベルを表示/変更できます。

カスタムタグの作成

注意

- ユーザ/エンドポイントディレクトリでカスタムタグ、フィルタ、または重要度ラベルを作成/変更する権限のある Apex Central ユーザアカウントは、他のすべてのユーザアカウントが作成したカスタムタグ、フィルタ、または重要なラベルを表示/変更できます。
- [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。
2. ツリーの [ユーザ] または [エンドポイント] の下の [カスタムタグ] ノードを展開します。
3. [新規カスタムタグの追加] をクリックします。
4. タグにわかりやすい名前を入力し、<Enter> キーを押すか、 をクリックして新しいタグを保存します。

   タグが [ユーザ] タグまたは [エンドポイント] タグのリストに表示されます。

   カスタムタグを作成した後、次のようにします。

   - タグ名を編集するには、カスタムタグの横の アイコンをクリックします。
   - タグを削除するには、カスタムタグの横の アイコンをクリックします。

ユーザ/エンドポイントにカスタムタグを割り当てる

注意

- ユーザ/エンドポイントディレクトリでカスタムタグ、フィルタ、または重要度ラベルを作成/変更する権限のある Apex Central ユーザアカウントは、他のすべてのユーザアカウントが作成したカスタムタグ、フィルタ、または重要なラベルを表示/変更できます。
- [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。
2. 確認する [ユーザ] または [エンドポイント] を選択するか、特定のユーザ/エンドポイントを検索します。
3. カスタムタグをユーザ/エンドポイントに関連付けるには、次の手順を実行します。
   - ユーザ/エンドポイント行をクリックし、[タスク] > [カスタムタグの割り当て/削除] をクリックします。
   - ユーザ/エンドポイント行を右クリックし、[カスタムタグの割り当て/削除] をクリックします。
4. [カスタムタグの割り当て/削除] 画面で、必要なタグをリストから選択またはクリアして、[保存] をクリックします。

   [カスタムタグ] リストからタグを選択し、選択したユーザまたはエンドポイントが正しく表示されていることを確認することにより、選択したユーザまたはエンドポイントにタグが適切に関連付けられていることを確認できます。

フィルタ

フィルタを使用すると、同じ条件のユーザまたはエンドポイントを自動的にグループ化できます。

- カスタムタグおよびカスタムフィルタに基づいて [ユーザ] および [エンドポイント] をグループ化したり、重要度を割り当てたりできます。

  詳細については、178 ページの「カスタムフィルタの作成」および 179 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

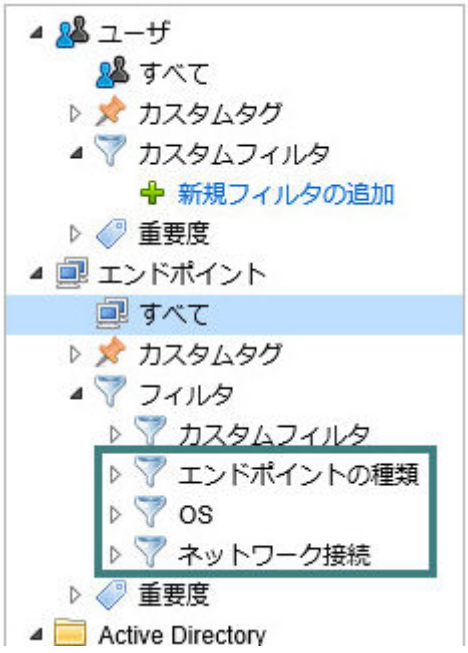
- さらに、[エンドポイント] ツリーでは、初期設定のフィルタに基づいてエンドポイントをグループ化することもできます。

  詳細については、177 ページの「初期設定のエンドポイントフィルタ」を参照してください。

- ユーザ/エンドポイントディレクトリでカスタムタグ、フィルタ、または重要度ラベルを作成/変更する権限のある Apex Central ユーザアカウントは、他のすべてのユーザアカウントが作成したカスタムタグ、フィルタ、または重要なラベルを表示/変更できます。

初期設定のエンドポイントフィルタ

[エンドポイント] ツリーには、典型的なエンドポイントのグループ分けに基づいて、初期設定のフィルタが用意されています。



初期設定のフィルタのいずれかを展開し、表示するエンドポイントのタイプを選択します。

表の列とそのデータに関する詳細については、143 ページの「ユーザの詳細情報」を参照してください。

初期設定のフィルタは次のとおりです。

- エンドポイントの種類: サーバ、デスクトップ、ノートパソコン、モバイルデバイスなど
- OS: Windows、Mac OS、iOS、Android など、エンドポイントにインストールされる一般的な OS

- ネットワーク接続: 隔離されたエンドポイント

注意

[隔離済み] のエンドポイントを表示した後、[タスク] > [ネットワーク接続の復元] をクリックして隔離を停止できます。

カスタムフィルタの作成

注意

- ユーザ/エンドポイントディレクトリでカスタムタグ、フィルタ、または重要度ラベルを作成/変更する権限のある Apex Central ユーザアカウントは、他のすべてのユーザアカウントが作成したカスタムタグ、フィルタ、または重要なラベルを表示/変更できます。
- [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。
2. ツリーの [カスタムフィルタ] ノードを展開します。
   - [ユーザ] の場合、[カスタムフィルタ] を展開します。
   - [エンドポイント] の場合、[フィルタ] を展開してから [カスタムフィルタ] を展開します。
3. [新規フィルタの追加] をクリックします。

   表の上の [検索] エリアに変更が加えられ、フィルタ条件を選択できるようになります。
4. 任意の条件に基づいてユーザまたはエンドポイントをフィルタします。

次の例では、Active Directory ドメインが「HR」で、直属の上司が「Mary」または「Bill」、部署が「Finance」、ユーザ名に「ja」が含まれるすべてのユーザをフィルタします。

詳細については、168 ページの「詳細検索のカテゴリ」を参照してください。

カスタムフィルタを作成した後、次のようにします。

- フィルタ名を編集するには、カスタムフィルタの横の アイコンをクリックします。
- ブール式を更新するには、カスタムフィルタの横の アイコンをクリックします。
- フィルタ名を削除するには、カスタムフィルタの横の アイコンをクリックします。

ユーザまたはエンドポイントの重要度

ユーザやエンドポイントのグループに重要度を割り当てると、[ダッシュボード] 画面からこれらの対象に対する脅威をすばやく監視して対応できます。Apex Central には、「重要な」ユーザやエンドポイントの脅威イベントを強調表示するウィジェットがいくつか用意されています。重要なユーザやエンドポイントにはより厳しいポリシーを適用して、保護ステータスを継続的に監視できます。

あらかじめカスタムタグを割り当てたりカスタムフィルタを作成したりして、重要なユーザやエンドポイントを識別する必要があります。ネットワー

ク上の重要なユーザやエンドポイントを識別したら、「重要」タグを割り当てて、[ダッシュボード] で見やすくすることができます。

詳細については、171 ページの「カスタムタグおよびカスタムフィルタ」を参照してください。

注意

- カスタムタグおよびカスタムフィルタを使用してグループ化したユーザ/エンドポイントに、重要度を手動で割り当てます。
- ユーザ/エンドポイントディレクトリでカスタムタグ、フィルタ、または重要度ラベルを作成/変更する権限のある Apex Central ユーザアカウントは、他のすべてのユーザアカウントが作成したカスタムタグ、フィルタ、または重要なラベルを表示/変更できます。
- [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。
- Apex Central は、Active Directory との同期後に、「ドメイン管理者」(ユーザ) および「ドメインコントローラ」(エンドポイント) に自動的に重要度を割り当てます。
  - 現在のバージョンの Apex Central では、統合された Active Directory ドメインごとに重要な「ドメイン管理者」が 1 つ、重要な「ドメインコントローラ」が 1 つサポートされます。個々のユーザアカウントが同じ「ドメイン管理者」および「ドメインコントローラ」に別々に「重要」タグを割り当てることはできなくなりました。
  - 旧バージョンの Apex Central で「ドメイン管理者」および「ドメインコントローラ」に個別のユーザアカウントによって作成された既存の「重要」タグがある場合は、既存の「ドメイン管理者」および「ドメインコントローラ」が削除され、統合された Active Directory ドメインごとに 1 つの重要な「ドメイン管理者」と 1 つの重要な「ドメインコントローラ」に置き換えられます。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。

2. ツリーの [ユーザ] または [エンドポイント] の下の [重要度] ノードを展開します。
3. [重要度] をクリックし、編集アイコン ( ) をクリックします。
4. 表示される画面で、次の手順を実行します。
   - 重要度を割り当てるには、カスタムタグまたはカスタムフィルタを選択し、[保存] をクリックします。
   - 重要度の割り当てを解除するには、カスタムタグまたはカスタムフィルタを選択解除し、[保存] をクリックします。

   メイン画面の表が更新され、カスタムタグまたはカスタムフィルタに一致するエンドポイントまたはユーザのリストが表示されます。

   表の列とそのデータに関する詳細については、143 ページの「ユーザの詳細情報」を参照してください。

パート III

管理下の製品の統合

第 8 章

管理下の製品の登録

このセクションでは、管理下の製品とサーバを Apex Central サーバに登録する方法について説明します。

次のトピックがあります。

管理下の製品の登録方法

Apex Central では、以下のいずれかの方法を使用して、管理下の製品を Apex Central サーバに登録する必要があります。

- Apex Central 管理コンソールの [サーバの登録] 画面
- 管理下の製品の管理コンソール (Apex Central MCP エージェント経由)

サーバの登録

[サーバの登録] 画面 ([運用管理] > [管理下のサーバ] > [サーバの登録]) では、Apex Central 管理コンソールを使用して Apex Central に登録される管理下の製品の登録、設定、登録解除を実行できます。

管理下の製品の Web コンソールを使用して Apex Central に登録される製品の詳細については、511 ページの「Connected Threat Defense 製品の統合」を参照してください。

次のタスクを実行するには、[サーバの登録] 画面を使用します。

タスク	説明
管理下のサーバの追加	管理下の製品を Apex Central サーバに追加するには、[追加] をクリックします。 詳細については、189 ページの「管理下のサーバを追加する」を参照してください。 **注意** [追加] アイコンが無効な場合、管理下の製品コンソールを使用して管理下の製品を Apex Central に登録します。
管理下のサーバ設定の編集	管理下のサーバの設定を変更するには、[処理] 列の [編集] アイコンをクリックします。 詳細については、191 ページの「管理下のサーバを編集する」を参照してください。

タスク	説明
管理下のサーバの削除	管理下のサーバを Apex Central サーバから登録解除するには、[処理] 列の [削除] アイコンをクリックします。 詳細については、192 ページの「管理下のサーバを削除する」を参照してください。
プロキシの設定	管理下の製品のプロキシを設定するには、[プロキシの設定] をクリックします。 詳細については、193 ページの「管理下の製品のプロキシ設定」を参照してください。
クラウドサービスの設定	クラウドサービスを登録、編集、または登録解除するには、[クラウドサービスの設定] をクリックします。 詳細については、194 ページの「クラウドサービスを設定する」を参照してください。
製品ディレクトリ構造での管理下のサーバの編成	製品ディレクトリ構造で管理下の製品をグループ化したり新しい場所に移動したりするには、[ディレクトリ管理] をクリックします。 詳細については、221 ページの「製品ディレクトリの管理」を参照してください。
管理下の製品のコンソールへのシングルサインオン	[サーバ] 列のリンクをクリックし、管理下の製品のコンソールへシングルサインオンします。 **ヒント** 一部の製品では、[製品ディレクトリ] 画面から、管理下の製品のコンソールにシングルサインオンすることもできます。 詳細については、210 ページの「製品ディレクトリ」を参照してください。

注意

[サーバの登録] 画面に表示される詳細については、188 ページの「管理下のサーバの詳細」を参照してください。

管理下のサーバの詳細

次の表は、[サーバの登録] 画面に表示される情報を示しています。

列名	説明
サーバ	管理下の製品のサーバ名が表示されます。 **注意** MCP エージェントを使用して Apex Central に登録されている管理下の製品のサーバ名をクリックすると、管理下の製品コンソールにリダイレクトします。
表示名	管理下の製品のサーバ表示名が表示されます。
製品	管理下の製品の名前が表示されます。
接続タイプ	管理下の製品の Apex Central への登録方法が表示されます。 • 自動 –管理下の製品は Apex Central に MCP エージェントを使用して登録されました。 詳細については、511 ページの「Connected Threat Defense 製品の統合」を参照してください。 • 手動 -管理者は [サーバの登録] 画面を使用して管理下の製品を登録しました。 詳細については、189 ページの「管理下のサーバを追加する」を参照してください。 • クラウドサービス -管理下の製品は [クラウドサービスの設定] を使用して登録されました。 詳細については、194 ページの「クラウドサービスを設定する」を参照してください。
最新のレポート	Apex Central で管理下の製品からの応答が受信された最新の日時が表示されます。
仮想アナライザ	管理下の製品からサンプルが送信される登録済みの仮想アナライザが表示されます。

列名	説明
処理	• 編集 –サーバ情報をアップデートするには、このアイコンをクリックします。 詳細については、191 ページの「管理下のサーバを編集する」を参照してください。 • 削除 –管理下のサーバを登録解除するには、このアイコンをクリックします。 詳細については、192 ページの「管理下のサーバを削除する」を参照してください。

管理下のサーバを追加する

[サーバの登録] 画面を使用して、管理下のサーバを Apex Central サーバに登録します。

注意

- [追加] ボタンが無効な場合、管理下の製品コンソールを使用して管理下の製品を Apex Central に登録します。

  詳細については、511 ページの「Connected Threat Defense 製品の統合」を参照してください。

- 新しく追加された管理下のサーバでポリシー管理を実行する前に、[ディレクトリ管理] をクリックして、管理下の製品を [新規エンティティ] フォルダから別の場所に移動します。

  詳細については、221 ページの「製品ディレクトリの管理」を参照してください。

手順

1. [運用管理] > [管理下のサーバ] > [サーバの登録]に移動します。

   サーバの登録 画面が表示されます。

2. [サーバの種類] ドロップダウンリストから製品を選択します。

   登録された管理下のサーバのリストが表示されます。

3. [追加] ボタンまたは表の [製品の追加] リンクをクリックします。

   [サーバの追加] 画面が表示されます。

4. 次のサーバ情報を指定します。

   - サーバ: <管理下の製品> のサーバ名、FQDN、または IPv4/IPv6 アドレスとポート番号 (ある場合) を入力します。

     重要

     サーバのアドレスは、`HTTP` または `HTTPS` で始まる必要があります。

   - 表示名: Apex Central に表示されている <管理下の製品> サーバの名前を指定します。

5. 管理下のサーバへのログオンに認証が必要な場合、次の認証情報を指定します。

   - ユーザ名: 管理者権限のある <管理下の製品> アカウントの名前を指定します。
   - パスワード: 指定したアカウントのパスワードを入力します。

     重要

     Apex Central では、ポリシー設定を配信するために管理者権限のあるアカウントが必要です。

6. (オプション) プロキシサーバを使用するには、[接続にプロキシサーバを使用する] チェックボックスをオンにします。

   詳細については、193 ページの「管理下の製品のプロキシ設定」を参照してください。

7. サンプル送信を有効にするには、[仮想アナライザ] ドロップダウンリストから仮想アナライザ製品/サービスを選択します。

重要

- Deep Security と Trend Micro Endpoint Sensor では、まず管理下のサーバを追加してから、仮想アナライザを選択するようそのサーバを編集する必要があります。
- その他すべての管理下の製品では、初めて管理下のサーバを追加したときに仮想アナライザを選択できます。
- 詳細については、511 ページの「Connected Threat Defense 製品の統合」を参照してください。

8. [保存] をクリックします。

   新しく追加されたサーバが、登録された管理下のサーバのリストに表示されます。

管理下のサーバを編集する

[サーバの登録] 画面を使用して、Apex Central サーバに登録された管理下のサーバに関する情報を編集します。

手順

1. [運用管理] > [管理下のサーバ] > [サーバの登録]に移動します。

   サーバの登録 画面が表示されます。

2. [サーバの種類] ドロップダウンリストから製品を選択します。

   登録された管理下のサーバのリストが表示されます。

3. 編集する管理下のサーバで [処理] 列の [編集] アイコンをクリックします。

   [サーバの編集] 画面が表示されます。

4. サーバ情報を編集します。

   - 認証: サーバがログオンに認証情報を必要とする場合、ユーザ名とパスワードを入力します。

- 接続: 設定されたプロキシサーバを使用するために、[接続にプロキシサーバを使用する] チェックボックスをオンにします。

  詳細については、193 ページの「管理下の製品のプロキシ設定」を参照してください。

- サンプル送信: [仮想アナライザ] ドロップダウンリストから仮想アナライザ製品/サービスを選択します。

  重要

  - [仮想アナライザ] ドロップダウンリストに [サポートなし] と表示される場合は、Apex Central ではなく管理下の製品サーバのコンソール (Deep Discovery Inspector コンソールなど) で仮想アナライザ製品/サービスを設定する必要があります。
  - ノード Apex Central の管理下の Apex One サーバでは、ブ Apex Central に登録されている Deep Discovery Analyzer を仮想アナライザ製品/サービスとして選択できます。

  詳細については、511 ページの「Connected Threat Defense 製品の統合」を参照してください。

5. [保存] をクリックします。

管理下のサーバを削除する

[サーバの登録] 画面を使用して、Apex Central から管理下のサーバを登録解除します。

手順

1. [運用管理] > [管理下のサーバ] > [サーバの登録]に移動します。

   サーバの登録 画面が表示されます。

2. [ディレクトリ管理] をクリックします。
3. 製品ツリーを展開して、削除するサーバを選択します。

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。

   選択されたサーバが製品ツリーから削除されます。

   注意

   [サーバの登録] 画面で管理下のサーバを削除しても、サーバプログラムまたは関連するエージェントはアンインストールされません。

6. サーバの管理コンソールで製品登録画面に移動し、Apex Central からサーバの登録を解除します。

7. [OK] をクリックします。

管理下の製品のプロキシ設定

Apex Central では、プロキシサーバを使用して内部ネットワークで管理下の製品に接続できます。管理下の製品にプロキシサーバを設定した後、特定の管理下のサーバに対してプロキシサーバ接続を有効にします。

詳細については、191 ページの「管理下のサーバを編集する」を参照してください。

重要

同じタイプの管理下の製品のすべての管理下のサーバに対して、1 つのプロキシサーバのみ使用できます。

手順

1. [運用管理] > [管理下のサーバ] > [サーバの登録]に移動します。

   サーバの登録 画面が表示されます。

2. [サーバの種類] ドロップダウンリストから製品を選択します。

   登録された管理下のサーバのリストが表示されます。

3. [プロキシの設定] をクリックします。

   [プロキシの設定] 画面が表示されます。

4. 次のプロトコルのいずれかを選択します。

   - HTTP
   - SOCKS 4
   - SOCKS 5

5. 次のフィールドを指定します。

   - サーバ: プロキシサーバのサーバ名、FQDN、または IPv4 アドレスを入力します。
   - ポート: プロキシサーバがクライアント接続に使用するポート番号を入力します。

6. プロキシサーバで認証が必要な場合、次の認証情報を指定します。

   - ユーザ名
   - パスワード

7. [保存] をクリックします。

8. プロキシサーバの接続を有効にするには、次の手順を実行します。

   a. 編集する管理下のサーバで [処理] 列の [編集] アイコンをクリックします。

      [サーバの編集] 画面が表示されます。

   b. [接続] セクションで [接続にプロキシサーバを使用する] チェックボックスをオンにします。

   c. [保存] をクリックします。

クラウドサービスを設定する

[サーバの登録] 画面を使用して、Apex Central から管理下のクラウドサービスを登録または登録解除します。

手順

1. [運用管理] > [管理下のサーバ] > [サーバの登録]に移動します。

   サーバの登録 画面が表示されます。

2. [クラウドサービスの設定] をクリックします。

   [クラウドサービスの設定] 画面が表示されます。

3. クラウドサービスを登録するには、次の認証情報を入力します。

   - アカウント: Trend Micro Customer Licensing Portal (https://clp.trendmicro.com/) でクラウドサービス契約を有効化したときに使用したユーザ名を入力します。
   - パスワード: クラウドサービスアカウントのパスワードを入力します。

4. クラウドサービスを登録解除するには、[Apex Central でのサービスの管理を停止します。] をクリックし、表示される確認メッセージに同意します。

5. [OK] をクリックします。

管理下の製品との通信

Apex Central では管理下のサーバにインストールされた Management Communication Protocol (MCP) エージェントを使用して、Apex Central サーバと通信します。

MCP エージェントは、管理下の製品が正常に動作していることを通知するために接続ステータスを定期的に送信することで、Apex Central サーバと通信します。

管理者は、エージェントの通信スケジュールを設定して、エージェントが Apex Central サーバに接続ステータスを送信するタイミングを決定できます。

重要

Apex Central では、Apex Central サーバに登録された管理下の製品に対して Apex Central 管理コンソールを介してエージェントの通信スケジュールを設定することのみ可能です。

エージェントの通信スケジュールの初期設定の変更

Apex Central は、初期設定のエージェントの通信スケジュールを使用して、カスタマイズされたエージェントの通信スケジュールが設定されていないすべての管理下の製品と通信します。

[コミュニケータスケジュールの設定] 画面を使用し、時間枠をクリックして通信のステータスを変更することで初期設定のスケジュールを変更します。

手順

1. [運用管理] > [管理下のサーバ] > [エージェントの通信スケジュール] に移動します。

   [エージェントの通信スケジュール] 画面が表示されます。

2. [コミュニケータ] 列で [初期設定のスケジュール] をクリックします。

   [コミュニケータスケジュールの設定] が表示されます。

3. 時間枠をクリックしてエージェントの通信のステータスを変更します。

   - 時間枠を [アイドル] に設定すると、エージェントが接続ステータスを Apex Central サーバに送信している間に、連続時間が作成されます。

     たとえば、時間枠 09 と 13 を [アイドル] に設定すると、2 つの連続時間枠が作成されます。

   - エージェントが接続ステータスを Apex Central サーバに送信している間に、[自動 (予約)] の時間枠に指定できる連続時間は 3 つまでです。

4. [保存] をクリックします。

エージェント通信スケジュールの設定

[コミュニケータスケジュールの設定] 画面で時間枠をクリックして通信ステータスを変更することにより、管理下の製品のエージェント通信スケジュールをカスタマイズします。

重要

エージェントの通信スケジュールは管理下の製品ごとに 1 つだけ設定できます。

手順

1. [運用管理] > [管理下のサーバ] > [エージェントの通信スケジュール] に移動します。

   [エージェントの通信スケジュール] 画面が表示されます。

2. [コミュニケータ] 列で、変更する管理下の製品をクリックします。

   [コミュニケータスケジュールの設定] 画面が表示されます。

3. 通信ステータスを変更する時間枠をクリックします。

   - 時間枠を [アイドル] に設定すると、エージェントが接続ステータスを Apex Central サーバに送信している間に、連続時間が作成されます。

     たとえば、時間枠 09 と 13 を [アイドル] に設定すると、2 つの連続時間枠が作成されます。

   - エージェントが接続ステータスを Apex Central サーバに送信している間に、[自動 (予約)] の時間枠に指定できる連続時間は 3 つまでです。

4. [保存] をクリックします。

管理対象製品の接続ステータスの間隔を設定する

[管理対象製品の接続ステータスの間隔] の設定は、エージェントが Apex Central サーバに接続ステータスを送信する頻度を決定します。

[通信タイムアウトの設定] 画面を使用して、管理対象製品の接続ステータスの間隔を分単位で定義します。

管理対象製品の接続ステータスの間隔を設定する際に、次の点を考慮してください。

- [管理対象製品の接続ステータスの間隔] の設定は、Apex Central 管理コンソールを使用して Apex Central サーバに登録されている管理対象製品にのみ適用されます。
- 接続ステータスの間隔が長いと、消費する帯域幅は減少しますが、Apex Central が通信ステータスをアップデートする 前に発生するネットワークイベントが増加します。
- 接続ステータスの実行間隔を短く設定すると、消費する帯域幅は増加しますが、より新しいネットワークステータスが表示されるようになります。

手順

1. [運用管理] > [管理下のサーバ] > [通信タイムアウトの設定] に移動します。

   [通信タイムアウトの設定] 画面が表示されます。

2. [管理対象製品の接続ステータスの間隔] セクションで、次の項目を設定します。

   - 管理対象製品のステータスをレポートする間隔: エージェントの通信接続ステータスの間隔を定義します。

     値は 5～480 分の範囲で指定します。

- 無通信状態が次の時間続いた場合はステータスを異常として設定する: エージェントの通信タイムアウトの間隔を定義します。

  値は 15～1440 分の範囲で指定します。

重要

[無通信状態が次の時間続いた場合はステータスを異常として設定する] には、[管理対象製品のステータスをレポートする間隔] の 3 倍以上の値を指定してください。

3. [保存] をクリックします。

第 9 章

セキュリティエージェントのインストール

この章では、セキュリティクライアントのインストール要件およびインストール方法について説明します。

次のトピックがあります。

セキュリティエージェントのインストールパッケージをダウンロードする

[セキュリティエージェントのダウンロード] 画面を使用して、Apex One または Apex One (Mac) のセキュリティエージェント インストールパッケージを作成し、ダウンロードします。セキュリティエージェント インストールパッケージをローカルにダウンロードしてインストールするか、セキュリティエージェントインストールパッケージを 対象エンドポイントに直接ダウンロードできる URL を入手し、ユーザに送ることができます。

表 9-1. インストール前の設定

セキュリティエージェント	設定
Apex One	Apex One セキュリティエージェントをインストールする前に、次の操作を行います。 • 初期設定の Apex One セキュリティエージェントのアンロードおよびアンインストールパスワードを変更します。 • エンドポイントがポート 80～443 経由で通信できるようにします。 • エンドポイントが*.trendmicro.com にアクセスできるようにします。 • 必要に応じて、Apex One セキュリティエージェントのプロキシサーバ設定を行います。
Apex One (Mac)	Apex One (Mac) セキュリティエージェントをインストールする前に、次の操作を行います。 • エンドポイントがポート 61617 経由で通信できるようにします。 • エンドポイントが*.trendmicro.com にアクセスできるようにします。 • 必要に応じて、Apex One セキュリティエージェントのプロキシサーバ設定を行います。

エンドポイントにセキュリティエージェントをインストールするためのシステム要件の詳細については、次のトピックを参照してください。

- 204 ページの「Apex One セキュリティエージェントのインストール」
- 207 ページの「Apex One (Mac) セキュリティエージェントのシステム 要件」

手順

1. [運用管理] > [セキュリティエージェントのダウンロード] に移動します。
2. オペレーティングシステムを 選択します。
   - Windows 64 ビット: Apex One セキュリティエージェント 用の 64 ビット MSI インストールパッケージを 作成する場合に選択します。
   - Windows 32 ビット: Apex One セキュリティエージェント 用の 32 ビット MSI インストールパッケージを 作成する場合に選択します。
   - Mac: Apex One (Mac) セキュリティエージェント 用の ZIP インストールパッケージを 作成する場合に選択します。
3. 選択したインストールパッケージの 種類に対応する管理下の製品のサーバが複数ある場合は、[サーバ] ドロップダウンを使用して、セキュリティエージェントから報告を受けるサーバを選択します。

   注意

   管理下の製品のサーバが 1 つしかない場合は、管理下の製品のサーバ名のみが表示されます。

4. 次のいずれかの配信オプションをクリックします。
   - ダウンロード: セキュリティエージェント のインストールパッケージをダウンロードします。これを使用して、ローカルでインストールしたり、後から対象エンドポイントに配信したりできます。
   - ダウンロードリンクの取得: 対象エンドポイントでセキュリティエージェントを直接インストールするためにユーザに送信できる URL を表示します。

注意

Apex One サーバの場合、Apex One セキュリティエージェント パッケージでは、セキュリティエージェント パッケージツールが最後に実行されたときに生成された設定が適用されます。

詳細については、Apex One 管理者ガイドを参照してください。

Apex One セキュリティエージェントのインストール

このセクションでは、サポートされている Windows プラットフォームに新規インストールする際の、Apex One セキュリティエージェント のシステム要件について説明します。

Windows エンドポイントプラットフォーム

Windows 7 (32 ビット/64 ビット) Service Pack 1 の要件

Apex One セキュリティエージェントのインストール 方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム 要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows Server 8.1 (32 ビット/64 ビット) の要件

Apex One セキュリティエージェントのインストール 方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム 要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows Server 10 (32 ビット/64 ビット) の要件

Apex One セキュリティエージェントのインストール方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows Server プラットフォーム

Windows Server 2008 R2 (64 ビット) プラットフォーム

Apex One セキュリティエージェントのインストール方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows MultiPoint Server 2010 (64 ビット) プラットフォーム

Apex One セキュリティエージェントのインストール方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows MultiPoint Server 2011 (64 ビット) プラットフォーム

Apex One セキュリティエージェントのインストール方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows Server 2012 (64 ビット) プラットフォーム

Apex One セキュリティエージェントのインストール方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows Server 2016 (64 ビット) プラットフォーム

Apex One セキュリティエージェントのインストール方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Windows Server 2019 (64 ビット) プラットフォーム

Apex One セキュリティエージェントのインストール方法については、Apex One のドキュメントを参照してください。

Apex One セキュリティエージェントのシステム要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Apex One (Mac) セキュリティエージェントのインストール

このセクションでは、Apex One (Mac) セキュリティエージェントのインストール要件とその方法について説明します。

詳細については、Apex One (Mac) のドキュメントを参照してください。

Apex One (Mac) セキュリティエージェントのシステム要件

エージェントのインストール要件のリストについては、次の Web サイトを参照してください。

http://www.go-tm.jp/corp-tmsm/req

第 10 章

製品ディレクトリ

このセクションでは、Apex Central サーバに登録されているすべての管理下の製品に関する情報を確認する方法、および [製品ディレクトリ] 画面で使用可能なタスクについて説明します。

次のトピックがあります。

製品ディレクトリ

[製品ディレクトリ] 画面 ([ディレクトリ] > [製品]) 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サーバに関する情報が表示されます。この画面を使用して、管理下の製品の特定のエンティティを検索したり、管理下のサーバのステータス概要を表示したり、管理下の製品のタスクを実行したり、管理下の製品を設定したり、管理下の製品のログをクエリしたりできます。

ヒント

また、[ログクエリ] 画面を使用して管理下の製品のログをクエリすることもできます。

詳細については、318 ページの「ログクエリを使用する」を参照してください。

[製品ディレクトリ] ツリーでは、管理下の製品を以下の初期設定のフォルダに編成します。

- <ルート>: Apex Central サーバの名前が表示され、以下のサブフォルダがすべて含まれます。
- ローカルフォルダ: [新規エンティティ] フォルダと、作成したカスタムフォルダが含まれます。
- 新規エンティティ: Apex Central サーバに新しく登録されたすべての管理下の製品が含まれます。(MCP を使用して登録した製品のみが表示されます。[運用管理] > [管理下のサーバ] > [サーバの登録] から登録した製品は表示されません)
- 検索結果: 基本検索または詳細検索の条件に一致するすべての管理下の製品が含まれます。

注意

Apex Central では、[新規エンティティ] フォルダを除くすべてのフォルダを、特殊文字 (!、#、$、%、(、)、*、+、-、コンマ (,)、ピリオド (.)、+、?、@、[、]、^、_、{、|、}、および~)、数字 (0〜9)、またはアルファベット順 (a/A〜z/Z) に昇順に並べます。

[製品ディレクトリ] 画面では、管理下の製品、および管理下の製品の接続ステータスを表すためにアイコンが使用されます。

[製品ディレクトリ] の接続ステータスアイコンの詳細については、212 ページの「接続ステータスアイコン」を参照してください。

次の表は、[製品ディレクトリ] 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
ステータス概要の表示	[製品ディレクトリ] で管理下の製品のエンティティを選択してステータス概要を表示します。 詳細については、213 ページの「管理下の製品のステータス概要を確認する」を参照してください。
管理下の製品のエンティティの検索	[エンティティの検索] 検索ボックスで、部分一致検索を使用して管理下の製品のエンティティを検索し、[検索] をクリックします。検索条件に一致する管理下の製品のエンティティが [検索結果] フォルダに表示されます。 詳細検索の実行の詳細については、216 ページの「管理下の製品のタスクを実行する」を参照してください。
管理下の製品の設定	[製品ディレクトリ] ツリーで管理下の製品のエンティティを選択し、[設定] ドロップダウンからオプションを選択します。 詳細については、217 ページの「管理下の製品を設定する」を参照してください。
管理下の製品のタスクの実行	[製品ディレクトリ] ツリーで管理下の製品のエンティティを選択し、[タスクリスト] ドロップダウンからオプションを選択します。 詳細については、216 ページの「管理下の製品のタスクを実行する」を参照してください。
管理下の製品のログのクエリ	[製品ディレクトリ] で管理下の製品のエンティティを選択し、[ログ] をクリックします。 詳細については、218 ページの「製品ディレクトリからログをクエリする」を参照してください。

タスク	説明
製品ディレクトリ構造の編成	[ディレクトリ管理] をクリックして、新しいフォルダを作成したり、[製品ディレクトリ] ツリー内で管理下の製品のエンティティを移動またはグループ化したりします。 詳細については、219 ページの「ディレクトリ管理」を参照してください。
管理下の製品のコンソールへのシングルサインオン	製品ディレクトリツリーの該当するフォルダにある管理下の製品サーバのアイコンを選択し、[設定] > [<管理下の製品> シングルサインオン] をクリックします。 **ヒント** 一部の製品では、[サーバの登録] 画面から、管理下の製品のコンソールにシングルサインオンすることもできます。 詳細については、186 ページの「サーバの登録」を参照してください。

接続ステータスアイコン

製品ディレクトリでは次のアイコンを使用して、Apex Central サーバと登録済みの管理下の製品との間の通信のステータスを示します。

アイコン	MCP エージェントのステータス	製品サービスのステータス
	実行中	実行中
	実行中	停止中

アイコン	MCP エージェントのステータス	製品サービスのステータス
	通信タイムアウト 注意 Apex Central サーバが、[通信タイムアウトの設定] 画面で設定された接続ステータスの間隔の時間内に、管理下の製品サーバ上の MCP エージェントとの通信を確立できませんでした。	不明
	停止中 注意 Apex Central サーバが、[通信タイムアウトの設定] 画面で設定された条件に基づく試行失敗回数の後も、管理下の製品サーバ上の MCP エージェントとの通信を確立できませんでした。	停止中

管理下の製品のステータス概要を確認する

Apex Central では、[製品ディレクトリ] 画面を使用して管理下の製品およびフォルダのステータス概要を確認できます。

ヒント

[ダッシュボード] の脅威の検出結果ウィジェットを使用して、管理下の製品のステータス概要を確認することもできます。

手順

1. [ディレクトリ] > [製品] に移動します。

[製品ディレクトリ] 画面が表示されます。

2. 製品ディレクトリツリーで次の項目を選択し、作業領域にステータス概要を表示します。

項目	説明
管理下の製品	選択すると、システム情報および製品ライセンス情報が表示されます。
管理下の製品フォルダ	選択すると、ウイルス対策、スパイウェア/グレーウェア、コンテンツセキュリティ、Web セキュリティ、ネットワークウイルス、違反ステータス、およびコンポーネントステータスの概要が表示されます。
管理下の製品サーバ	製品ディレクトリツリーで管理下の製品サーバを選択し、[フォルダ] > [製品表示] をクリックして、管理下の製品サーバ上のすべてのドメインを表示します。
製品ディレクトリツリー内のドメイン	選択すると、管理下の製品サーバでこのドメインに属しているすべてのクライアントを表示されます。

注意

初期設定では、最後に問い合わせた日付からさかのぼって 7 日間分の情報が Apex Central に表示されます。

[期間] ドロップダウンリストから [今日]、[過去 7 日間]、[過去 14 日間]、または [過去 30 日間] を選択して、概要の期間を変更できます。

製品ディレクトリの詳細検索を実行する

Apex Central では、部分一致検索を使用して、製品ディレクトリで管理下の製品のエンティティ名、ドメイン、およびエンドポイントを検索できます。また、フォルダオブジェクトで詳細検索を実行し、ブール演算子を使用して特定のオブジェクトを探すこともできます。

注意

検索すると、一致するものが製品ディレクトリツリーの [検索結果] ノードで新しいフォルダに表示されます。

手順

1. [ディレクトリ] > [製品] に移動します。

   [製品ディレクトリ] 画面が表示されます。

2. 製品ディレクトリツリーでフォルダを 選択し、検索します。

   重要

   詳細検索機能では、選択したフォルダとすべてのサブフォルダ 内だけを検索します。[検索結果] フォルダ内は検索できません。

3. [詳細検索] をクリックします。

   [詳細検索] 画面が表示されます。

4. [一致] ドロップダウンで、次から選択します。

   - すべての条件
   - いずれかの条件

5. フィルタ条件を指定します。

   注意

   - 使用可能な条件、演算子、および値は、Apex Central に登録された製品およびそれまでのフィルタ 選択によって変化します。
   - Apex Central では、検索用に最大 20 個の条件を指定できます。

6. 検索条件を追加または削除するには、検索条件の右側にあるボタンをクリックします。

7. [検索] をクリックします。

検索条件に一致する管理下の製品が、製品ディレクトリツリーの [検索結果] フォルダに表示されます。

管理下の製品のタスクを実行する

[タスク] ドロップダウンメニューを使用して、特定の管理下の製品または管理下の製品のグループに対してタスクを実行します。

表示されるコマンドの種類は、選択した管理下の製品に応じて異なります。

ヒント

特定またはグループ単位の管理下の製品にアップデートを配信する前に、トレンドマイクロのアップデートサーバから Apex Central サーバに最新コンポーネントをダウンロードします。

詳細については、233 ページの「手動アップデートを設定する」を参照してください。

手順

1. [ディレクトリ] > [製品] に移動します。

   [製品ディレクトリ] 画面が表示されます。

2. 製品ディレクトリツリーで管理下の製品またはフォルダを選択します。

   注意

   フォルダを選択すると、Apex Central は、選択したフォルダ内に含まれる該当するすべての管理下の製品に選択したコマンドを送信しようとします。

3. [タスク] ドロップダウンメニューから、実行するタスクを選択します。

4. コマンドを管理下の製品に送信するには、次の手順を実行します。

   - 配信コマンドの場合: [配信開始] をクリックします。

- 検索コマンドの場合:
  a. 検索コマンドを選択します。
  b. 管理下の製品を選択します。
  c. [要求の送信] をクリックします。

5. [コマンド詳細] をクリックしてタスクの進行状況を監視するか、[OK] をクリックして他のタスクに進みます。

管理下の製品を設定する

Apex Central を使用すると、管理下の製品の Web コンソールにログオンするか、または Apex Central 管理コンソールを使用して設定を対象コンピュータに複製することにより、管理下の製品を設定できます。

注意

管理下の製品の設定に関する詳細については、各製品に付属するドキュメントを参照してください。

手順

1. [ディレクトリ] > [製品] に移動します。

   [製品ディレクトリ] 画面が表示されます。

2. 製品ディレクトリツリーで管理下の製品を選択します。
3. [設定] ドロップダウンから、次のいずれかを選択します。

   注意

   [設定] ドロップダウンメニューのオプションは、選択した管理下の製品に応じて異なります。

   - 設定の複製: 選択した管理下の製品から対象コンピュータに設定を複製します。

- フォルダ全体に対する設定の複製: 選択した管理下の製品と同じフォルダに含まれる他のすべての管理下の製品に設定を複製します。
- <管理下の製品>シングルサインオン : Apex Central の認証情報を使用して管理下の製品の Web コンソールにログオンします。
- <管理下の製品>の設定: 管理下の製品の Web コンソールにログインします。
  - メッセージが表示されたら、ユーザ名とパスワードを入力して、管理下の製品の Web コンソールにログオンします。
  - [はい] をクリックして、管理下の製品の Web コンソールに進みます。

製品ディレクトリからログをクエリする

Apex Central では、[製品ディレクトリ] ツリーから管理下の製品またはフォルダを情報元として選択して、[製品ディレクトリ] 画面からログクエリを実行できます。

注意

[製品ディレクトリ] からログをクエリする際は、Apex Central により、[製品ディレクトリ] 画面で選択する管理下の製品サーバまたはフォルダに基づいて、製品の範囲があらかじめ選択されます。

[ログクエリ] 画面からのログクエリの実行の詳細については、318 ページの「ログクエリを使用する」を参照してください。

手順

1. [ディレクトリ] > [製品] に移動します。

   [製品ディレクトリ] 画面が表示されます。

2. 製品ディレクトリツリーで管理下の製品またはフォルダを選択します。

注意

選択した管理下の製品またはフォルダによって、ログクエリの製品の範囲が決まります。

3. [ログ] ボタンをクリックします。

   [ログクエリ] 画面が表示されます。

4. ログの種類を選択し、[OK] をクリックします。

5. 期間を選択するか、日付のカスタム範囲を指定します。

6. カスタムフィルタ条件を指定するには、次の手順を実行します。

   a. [詳細フィルタを表示する] をクリックします。

   b. 条件一致ルールとして [すべての条件] または [いずれかの条件] を選択します。

   c. [条件の選択] ドロップダウンからフィルタオプションを 選択します。

   d. 演算子を選択し、条件を指定します。

   注意

   Apex Central では、ログクエリごとに最大 20 個のカスタムフィルタ条件を指定できます。

7. [検索] をクリックします。

ディレクトリ管理

[ディレクトリ管理] 画面を使用して、管理ニーズに合うように、製品ディレクトリ構造をカスタマイズできます。[ディレクトリ管理] 画面を開くには、[製品ディレクトリ] 画面 ([ディレクトリ] > [製品]) の [ディレクトリ管理] ボタンをクリックします。

管理下の製品は、配置場所別、管理部門別、製品別などで分類してグループ化します。次の表では、ディレクトリにある管理下の製品またはフォルダへ

のアクセスに使用される各種アクセス権と組み合わせる場合に、推奨されるグループ化の種類と、その利点と欠点を示しています。

表 10-1. 管理下の製品のグループ化の比較

グループ化の種類	利点	欠点
配置場所別または管理部門別	構造が明確	同一製品に対するグループ設定がない
製品の種類別	グループ設定とステータスが使用できる	アクセス権が一致しないことがある
上記の組み合わせ	グループ設定とアクセス権の管理が可能	構造が複雑になり、管理が難しいことがある

製品ディレクトリ構成は、次の点を考慮して慎重に計画してください。

表 10-2. 構造に関する注意点

注意点	影響
ユーザのアクセス	ユーザのアクセス権は、アカウントの作成時に設定します。アクセス権を複数のセグメントに付与できます。例: root ディレクトリを選択すると、製品ディレクトリ全体へのアクセス権を付与することになります。管理下の特定の製品を選択した場合には、その製品へのアクセス権だけが付与されます。
配信計画	配信計画に基づいて、最新のパターンファイル、検索エンジン、スパムメール判定ルールなどのコンポーネントが、製品に対して配信されます。配信計画は、個々の製品ではなく製品グループに対して配信されます。このため、構造が適切なディレクトリでは、受信者の指定が簡単になります。

詳細については、221 ページの「製品ディレクトリの管理」を参照してください。

重要

ユーザアカウントには、製品ディレクトリフォルダに 基づいて割り当てられた特定のアクセス権限が設定されます。

- 製品ディレクトリ構造を変更すると、Apex Central ユーザが管理下の製品にアクセスする方法に影響する場合があります。
- [管理下の製品/フォルダを移動する場合は、現在のユーザのアクセス権限を維持します。] チェックボックスをオンにして、製品ディレクトリ構造を変更するときにユーザのアクセス範囲が変更されないようにできます。

詳細については、94 ページの「ユーザアカウント」を参照してください。

製品ディレクトリの管理

[ディレクトリ管理] 画面を使用すると、製品ディレクトリ構造を編成できます。

詳細については、219 ページの「ディレクトリ管理」を参照してください。

重要

- Apex Central では、ロックのメカニズムを利用して、複数のユーザが互いに認識せず同時に変更を加えることができないようにしています。別のユーザがすでに [ディレクトリ管理] 画面を使用している場合は、Apex Central によりユーザに通知されます。それでも製品ディレクトリに変更を加える必要があり、その結果、別のユーザの変更に影響を与える可能性がある場合は、[解除] をクリックして、すぐに画面にアクセスします。
- 製品ディレクトリ構造を変更すると、Apex Central ユーザが管理下の製品にアクセスする方法に影響する場合があります。ユーザアカウントには、製品ディレクトリフォルダに 基づいて割り当てられた特定のアクセス権限が設定されます。

  詳細については、94 ページの「ユーザアカウント」を参照してください。

手順

1. [ディレクトリ] > [製品] に移動します。

   [製品ディレクトリ] 画面が表示されます。

2. [ディレクトリ管理] ボタンをクリックします。

   [ディレクトリ管理] 画面が表示されます。

3. すべての管理下の製品について現在のユーザのアクセス権限を維持する場合は、[管理下の製品/フォルダを移動する場合は、現在のユーザのアクセス権限を維持します。] チェックボックスをオンにします。

   注意

   このオプションを無効にし、管理下の製品を新しい場所に移動すると、管理下の製品は新しいフォルダの場所における権限を継承します。

4. 製品ディレクトリを編成するには、次のタスクを実行します。

   - フォルダの追加: [ローカルフォルダ] ノード内に新しいカスタムフォルダを作成します。
   - 名前変更: 既存のカスタムフォルダの名前を変更します。
   - 削除: 既存のカスタムフォルダを削除します。

     注意

     Apex Central では、登録されている管理下の製品が含まれるカスタムフォルダを削除できません。

   - 管理下の製品またはフォルダの移動: 管理下の製品またはフォルダを新しい場所にドラッグしてドロップします。

     重要

     「root」、[階層フォルダ]、[新規エンティティ] の各フォルダは、名前の変更、削除、新しい製品やフォルダの追加ができません。

5. [戻る] をクリックすると、変更が適用され、[製品ディレクトリ] 画面に戻ります。

管理下の製品を再登録する

警告!

次の処理によって、管理下の製品が製品ディレクトリから削除されることがあります。

- Apex Central サーバを再インストールし、[既存のレコードを削除して新しいデータベースを作成] を選択した場合
- 破損した Apex Central データベースを、同名の別のデータベースで置き換えた場合

次の 3 つの方法のいずれかを使用して、製品ディレクトリから誤って削除された管理下の製品を再登録できます。

手順

- 管理下の製品のサーバで Apex Central MCP エージェントサービスを手動で再起動します。
- MCP エージェントが 8 時間後に自動で Apex Central サーバに再登録されるのを待ちます。
- 管理下の製品コンソールから、MCP エージェントを Apex Central サーバに手動で再登録します。

第 11 章

コンポーネントアップデート

このセクションでは、Apex Central でコンポーネントアップデート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。

コンポーネントアップデート

Apex Central サーバは、最新のセキュリティの脅威からネットワークを保護するために管理下の製品が使用するコンポーネントファイルを提供する機能を持ちます。

手動アップデートまたは予約アップデートを実行して、コンポーネントを最新の状態に保ってください。Apex Central を使用すると、次のタスクを実行できます。

- アップデート元から最新コンポーネントをダウンロードする
- アップデートしたコンポーネントを管理下の製品に配信する

コンポーネントリスト

Apex Central サーバで利用可能なコンポーネントのリストを [予約アップデート] 画面と [手動アップデート] 画面で確認できます。

次の表は、[予約アップデート] 画面と [手動アップデート] 画面に表示されるコンポーネント情報を示しています。

フィールド	説明
カテゴリ	コンポーネントのカテゴリの名前が表示されます。 ▸ をクリックして、カテゴリ内のコンポーネントのリストを表示します。
種類	コンポーネントの種類が表示されます。
現在のバージョン	Apex Central によって正常にダウンロードされたコンポーネントの最新バージョンが表示されます。
最終ダウンロード	Apex Central がコンポーネントの [現在のバージョン] をダウンロードした時間が表示されます。

フィールド	説明
関連付けられた製品	コンポーネントを使用している管理下の製品の名前または管理下の製品の数が表示されます。 複数の管理下の製品がコンポーネントを使用している場合、テキストの上にマウスのカーソルを移動して、関連付けられた管理下の製品のリストを表示します。

アップデート元

トレンドマイクロのアップデートサーバまたはその 他のアップデート元からコンポーネントをダウンロードするように Apex Central サーバを設定します。Apex Central サーバがトレンドマイクロのアップデートサーバに 直接接続できない場合、またはアップデートサーバをネットワーク内でホストしている場合は、その他のアップデート元を指定できます。

初期設定では、Apex Central はトレンドマイクロのアップデートサーバからコンポーネントをダウンロードするために、より安全な HTTPS 接続方法を使用します。

他のダウンロード元にアクセスできるように、Apex Central ではリモート環境の UNC 認証をサポートしています。この認証では、最新コンポーネントがダウンロードされるフォルダを共有する、コンポーネントのダウンロード元のサーバから取得したユーザアカウントを使用します。

配信計画

配信計画を使用すると、アップデートされたコンポーネントを 管理下の製品に配信する対象範囲とスケジュールを指定できます。

Apex Central サーバがアップデート 元から新規のコンポーネントをダウンロードした後、指定された時間、または保留時間が経過した後のいずれかに、アップデートされたコンポーネントを 管理下の製品に即座に配信するように Apex Central を設定できます。

アップデートされたコンポーネントを、別の配信スケジュールに基づいて、選択した管理下の製品に配信するように、Apex Central を設定できます。

配信スケジュールを作成するときは、次の点に注意してください。

- 1 つの配信スケジュールにつき、1 つフォルダまたは管理下の製品を選択できます。ただし、1 つの配信計画に複数のスケジュールを指定することができます。
- Apex Central での保留付きの配信は、ダウンロードの終了時間を基準に、それぞれ独立して実行されます。

  たとえば、5 分間隔でアップデートする 3 つのフォルダがある場合、最初のフォルダを 5 分後、2 番目のフォルダを 10 分後、3 番目のフォルダを 15 分後にそれぞれ配信することができます。

注意

配信スケジュールを配信計画で指定しない場合、Apex Central では、アップデートはダウンロードされますが、アップデートされたコンポーネントは管理下の製品に配信されません。

配信スケジュールを追加する

指定されたスケジュールに基づいて、アップデートしたコンポーネントを選択した管理下の製品に配信するための配信スケジュールを設定できます。

手順

1. [予約アップデート] 画面または [手動アップデート] 画面にアクセスします。
2. [配信計画] セクションで、[管理下の製品に対して異なる配信計画を定義する] を選択します。
3. [+追加] をクリックします。

   [スケジュールの追加] 画面が表示されます。
4. 配信スケジュールを設定します。
5. [管理下の製品/フォルダ] ツリーから、管理下の製品または製品フォルダを選択します。
6. [OK] をクリックして、設定を保存します。

   配信計画を作成したら、次のタスクを実行できます。

- 配信スケジュールの設定を編集するにはスケジュールをクリックします。
- 選択した配信スケジュールを削除するには [削除] をクリックします。

予約アップデートを設定する

Apex Central サーバが、指定したスケジュールに従って、選択したコンポーネントをアップデート元からダウンロードできるようにするために、予約アップデートを設定します。

配信計画に基づいて、アップデートされたコンポーネントを管理下の製品に配信するように Apex Central を設定することもできます。

注意

Control Manager 6.0 Service Pack 3 から Apex Central に直接移行すると、[予約アップデート] 画面の [すべてのパターンファイル/テンプレート (不正プログラムパターンファイル (Deep Discovery) を除く)] コンポーネントでこれまでに設定された [アップデート元]、[ダウンロードスケジュール]、および [配信計画] 設定は保持されます。

警告!

Control Manager 6.0 Service Pack 3 から Apex Central に直接移行すると、[手動アップデート] および [予約アップデート] 画面の [コンポーネント] 設定は初期設定にリセットされます。

手順

1. [運用管理] > [アップデート] > [予約アップデート] に移動します。
2. ドロップダウンリストを使用して、コンポーネントリストをフィルタします。コンポーネントリストは、次の条件に基づいてフィルタできます。
   - 製品: ドロップダウンから管理下の製品を 1 つ以上、またはすべてのトレンドマイクロ製品を選択し、[適用] をクリックします。

- カテゴリ: ドロップダウンからコンポーネントのカテゴリを 1 つ以上選択し、[適用] をクリックします。
- 種類: ドロップダウンからコンポーネントの種類を 1 つ以上選択し、[適用] をクリックします。

3. [コンポーネント] セクションで、コンポーネントのカテゴリを選択するか、またはカテゴリを展開してアップデートするコンポーネントを 選択します。

   詳細については、226 ページの「コンポーネントリスト」を参照してください。

重要

[コンポーネントのインテリジェントダウンロードを有効にする] チェックボックスをオンにすると、Apex Central では選択されたコンポーネントカテゴリに該当するすべてのコンポーネントが自動的に選択されます。アップデートするコンポーネントを個別に選択できません。コンポーネントを個別に選択する場合は、このチェックボックスをオフにしてください。

注意

Apex Central のネットワークトラフィックを最小限に抑えるには、対応する管理下の製品またはサービスがないコンポーネントのダウンロードを無効にします。

---

4. (オプション) [コンポーネントのインテリジェントダウンロードを有効にする] を選択すると、アップデート元から選択したコンポーネントカテゴリに該当する新しいコンポーネントを Apex Central で自動的に検出してダウンロードできるようになります。

注意

コンポーネントのインテリジェントダウンロード機能が無効の場合、Apex Central では予約アップデート時または手動アップデート時にコンポーネントリストで選択されたコンポーネントのみがダウンロードされます。

---

5. [アップデート元] セクションで、次のいずれかのオプションを選択し、必要な設定を行います。

- [トレンドマイクロのアップデートサーバ] – トレンドマイクロのアップデートサーバからコンポーネントのアップデートをダウンロードするには、このオプションを選択します。
- その他のアップデート元 – テキストフィールドにダウンロード元の URL などを入力します。ダウンロード元は「+」アイコンをクリックして 5 つまで設定できます。

  サーバ認証が必要な場合は、[認証情報の指定] をクリックし、ユーザ名とパスワードの情報を入力します。

  詳細については、227 ページの「アップデート元」を参照してください。

注意

Apex Central サーバがアップデート元への接続にプロキシサーバを使用する場合は、[プロキシ設定] 画面でプロキシを設定します。

詳細については、237 ページの「コンポーネント/ライセンスのアップデート、クラウドサービス、および Syslog 転送のためにプロキシを設定する」を参照してください。

---

6. [ダウンロードスケジュール] セクションで、[予約ダウンロードを有効にする] を選択し、コンポーネントのダウンロードスケジュールを指定します。
7. [配信計画] セクションで、配信オプションを選択し、必要な設定を行います。

オプション	説明
選択したすべての管理下の製品に配信する	次のいずれかのスケジュールに基づいて、アップデートしたコンポーネントを選択した管理下の製品に配信するには、このオプションを選択します。 • 猶予期間なし: Apex Central による新しいコンポーネントバージョンのダウンロードが終わると、Apex Central はアップデートしたコンポーネントを管理下の製品にただちに配信します。 • 開始日時: Apex Central は指定された時刻に、アップデートしたコンポーネントを管理下の製品に配信します。 • 保留時間: Apex Central は指定された時間待機してから、アップデートしたコンポーネントを管理下の製品に配信します。
管理下の製品に対して異なる配信計画を定義する	指定された管理下の製品に対して配信スケジュールを設定するには、このオプションを選択します。 次のいずれかを実行します。 • 新しい配信スケジュールを追加するには [+追加] をクリックします。 詳細については、228 ページの「配信スケジュールを追加する」を参照してください。 • 配信スケジュールの設定を編集するにはスケジュールをクリックします。 • 選択した配信スケジュールを削除するには [削除] をクリックします。 注意 配信スケジュールを指定しない場合、Apex Central ではコンポーネントのアップデートがダウンロードされますが、アップデートしたコンポーネントは管理下の製品に配信されません。

オプション	説明
配信しない	Apex Central で、アップデートしたコンポーネントを管理下の製品に自動配信しない場合は、このオプションを選択します。 [製品] 画面で、アップデートしたコンポーネントを管理下の製品に手動で配信できます。 詳細については、216 ページの「管理下の製品のタスクを実行する」を参照してください。

8. [保存] をクリックします。

手動アップデートを設定する

選択したコンポーネントをアップデート元からダウンロードするために、Apex Central サーバで手動アップデートを開始できます。

配信計画に基づいて、アップデートされたコンポーネントを管理下の製品に配信するように Apex Central を設定することもできます。

警告!

Control Manager 6.0 Service Pack 3 から Apex Central に直接移行すると、[手動アップデート] および [予約アップデート] 画面の [コンポーネント] 設定は初期設定にリセットされます。

手順

1. [運用管理] > [アップデート] > [手動アップデート] に移動します。
2. ドロップダウンリストを使用して、コンポーネントリストをフィルタします。コンポーネントリストは、次の条件に基づいてフィルタできます。
   - 製品: ドロップダウンから管理下の製品を 1 つ以上、またはすべてのトレンドマイクロ製品を選択し、[適用] をクリックします。
   - カテゴリ: ドロップダウンからコンポーネントのカテゴリを 1 つ以上選択し、[適用] をクリックします。

- 種類: ドロップダウンからコンポーネントの種類を 1 つ以上選択し、[適用] をクリックします。

3. [コンポーネント] セクションで、コンポーネントのカテゴリを選択するか、またはカテゴリを展開してアップデートするコンポーネントを選択します。

   詳細については、226 ページの「コンポーネントリスト」を参照してください。

   重要

   [コンポーネントのインテリジェントダウンロードを有効にする] チェックボックスをオンにすると、Apex Central では選択されたコンポーネントカテゴリに該当するすべてのコンポーネントが自動的に選択されます。アップデートするコンポーネントを個別に選択できません。コンポーネントを個別に選択する場合は、このチェックボックスをオフにしてください。

   注意

   Apex Central のネットワークトラフィックを最小限に抑えるには、対応する管理下の製品またはサービスがないコンポーネントのダウンロードを無効にします。

4. (オプション) [コンポーネントのインテリジェントダウンロードを有効にする] を選択すると、アップデート元から選択したコンポーネントカテゴリに該当する新しいコンポーネントを Apex Central で自動的に検出してダウンロードできるようになります。

   注意

   コンポーネントのインテリジェントダウンロード機能が無効の場合、Apex Central では予約アップデート時または手動アップデート時にコンポーネントリストで選択されたコンポーネントのみがダウンロードされます。

5. [アップデート元] セクションで、次のいずれかのオプションを選択し、必要な設定を行います。

   - [トレンドマイクロのアップデートサーバ] – トレンドマイクロのアップデートサーバからコンポーネントのアップデートをダウンロードするには、このオプションを選択します。

- その他のアップデート元 – テキストフィールドにダウンロード元の URL などを入力します。ダウンロード元は「+」アイコンをクリックして 5 つまで設定できます。

  サーバ認証が必要な場合は、[認証情報の指定] をクリックし、ユーザ名とパスワードの情報を入力します。

  詳細については、227 ページの「アップデート元」を参照してください。

注意

Apex Central サーバがアップデート元への接続にプロキシサーバを使用する場合は、[プロキシ設定] 画面でプロキシを設定します。

詳細については、237 ページの「コンポーネント/ライセンスのアップデート、クラウドサービス、および Syslog 転送のためにプロキシを設定する」を参照してください。

6. [配信計画] セクションで、配信オプションを選択し、必要な設定を行います。

オプション	説明
選択したすべての管理下の製品に配信する	次のいずれかのスケジュールに基づいて、アップデートしたコンポーネントを選択した管理下の製品に配信するには、このオプションを選択します。 • 猶予期間なし: Apex Central による新しいコンポーネントバージョンのダウンロードが終わると、Apex Central はアップデートしたコンポーネントを管理下の製品にただちに配信します。 • 開始日時: Apex Central は指定された時刻に、アップデートしたコンポーネントを管理下の製品に配信します。 • 保留時間: Apex Central は指定された時間待機してから、アップデートしたコンポーネントを管理下の製品に配信します。

オプション	説明
管理下の製品に対して異なる配信計画を定義する	指定された管理下の製品に対して配信スケジュールを設定するには、このオプションを選択します。 次のいずれかを実行します。 • 新しい配信スケジュールを追加するには [+追加] をクリックします。 詳細については、228 ページの「配信スケジュールを追加する」を参照してください。 • 配信スケジュールの設定を編集するにはスケジュールをクリックします。 • 選択した配信スケジュールを削除するには [削除] をクリックします。 **注意** 配信スケジュールを指定しない場合、Apex Central ではコンポーネントのアップデートがダウンロードされますが、アップデートしたコンポーネントは管理下の製品に配信されません。
配信しない	Apex Central で、アップデートしたコンポーネントを管理下の製品に自動配信しない場合は、このオプションを選択します。 [製品] 画面で、アップデートしたコンポーネントを管理下の製品に手動で配信できます。 詳細については、216 ページの「管理下の製品のタスクを実行する」を参照してください。

7. [ダウンロード] をクリックします。

   [手動アップデート] 画面の上部にダウンロードの進行状況が表示されます。

8. 実行中のダウンロードをキャンセルするには、次の手順を実行します。
   - 進捗バーの [現在のアップデートの停止] ボタンをクリックします。

- [ダウンロード] をクリックして、実行中のダウンロードをキャンセルして新しいダウンロードを開始します。

コンポーネント/ライセンスのアップデート、クラウドサービス、および Syslog 転送のためにプロキシを設定する

Apex Central では、コンポーネント/ライセンスのアップデート、クラウドサービス、および Syslog 転送にプロキシサーバを使用できます。

注意

また、サーバに SOCKS プロトコルを選択した場合は、Syslog 転送にも同じプロキシサーバを使用できます。Syslog 転送は HTTP プロトコルプロキシサーバをサポートしていません。

詳細については、331 ページの「Syslog 転送を設定する」を参照してください。

手順

1. [運用管理] > [設定] > [プロキシ設定] に移動します。

   [プロキシ設定] 画面が表示されます。

2. [コンポーネント/ライセンスのアップデート、クラウドサービス、Syslog 転送、およびハブ Apex Central への接続にプロキシサーバを使用する] を選択します。

3. プロトコルを選択します。

   注意

   Syslog 転送は HTTP プロキシサーバをサポートしていません。Syslog 転送にプロキシサーバを使用するには、SOCKS プロトコルを選択してください。

   - HTTP

- SOCKS 4
- SOCKS 5

4. [サーバの名前または IP アドレス] に、サーバのホスト名または IP アドレスを入力します。
5. [ポート] に、ポート番号を入力します。
6. サーバで認証が必要な場合は、ユーザ名とパスワードを入力します。
7. [保存] をクリックします。

第 12 章

コマンド追跡と製品通信

このセクションでは、Apex Central サーバが発行したコマンドを追跡する方法について説明します。

次のトピックがあります。

コマンド追跡

[コマンド追跡] 画面には、Apex Central サーバから送信された、以前に発行されたすべてのコマンドの一覧が表示されます。この画面を使用して、Apex Central 管理コンソールから管理下の製品に対して発行したコマンドのステータスを監視できます。たとえば、終了するまでに数分間かかることがある ScanNow の開始タスクを発行したら、他のタスクを進めておき、後から [コマンド追跡] 画面を参照して、発行したコマンドのステータスを調べることができます。

コマンドのクエリと表示の詳細については、241 ページの「コマンドのクエリと表示」を参照してください。

次の表は、[コマンド追跡] 画面に表示されるコマンド情報を示しています。

列名	説明
発行日時	Apex Central サーバが管理下の製品に対してコマンドを発行した日付と時刻を示します。
コマンド	Apex Central サーバが発行したコマンドの種類を示します。
ユーザ (アカウント)	コマンドをトリガしたユーザの名前を示します。
成功	コマンドを完了した管理下の製品の数を示します。 [成功] 列の数をクリックすると、コマンドの詳細情報が表示されます。 詳細については、242 ページの「コマンド詳細」を参照してください。
失敗	コマンドを実行できなかった管理下の製品の数を示します。 [失敗] 列の数をクリックすると、コマンドの詳細情報が表示されます。 詳細については、242 ページの「コマンド詳細」を参照してください。

列名	説明
処理中	現在コマンドを実行している管理下の製品の数を示します。 [処理中] 列の数をクリックすると、コマンドの詳細情報が表示されます。 詳細については、242 ページの「コマンド詳細」を参照してください。
すべて	Apex Central がコマンドを発行した管理下の製品の総数を示します。 [すべて] 列の数をクリックすると、コマンドの詳細情報が表示されます。 詳細については、242 ページの「コマンド詳細」を参照してください。

コマンドのクエリと表示

以前に発行されたコマンドを追跡および表示するには、[コマンド追跡] 画面を使用します。

手順

1. [運用管理] > [コマンド追跡] に移動します。

   [コマンド追跡] 画面が表示されます。

2. コマンドのリストをフィルタするには、次の項目を指定します。
   - 開始日時 –管理下の製品がコマンドを送信した時刻を指定します。
   - コマンド –監視するコマンドを選択します。
   - ユーザ –コマンドの送信に使用するアカウント名を指定します。

   ヒント

   すべてのユーザが発行したコマンドをクエリするときは、このフィールドを空白のままにします。

- ステータス —1 つ以上のコマンドステータスを選択し、[適用] をクリックします。

3. [成功]、[失敗]、[処理中]、または [すべて] の列の数をクリックして、コマンドの詳細情報を表示します。

   [コマンド詳細] 画面が表示されます。

   詳細については、242 ページの「コマンド詳細」を参照してください。

コマンド詳細

[コマンド詳細] 画面には、発行済みのコマンドに関する次の情報が表示されます。

列名	説明
前回のレポート日時	管理下の製品から Apex Central サーバに応答が最後に送信された日時を示します。
サーバ/エンティティ	管理下の製品のサーバのホスト名を示します。
ステータス	発行されたコマンドのステータスを示します。
説明	コマンドのステータスに関する追加の詳細を示します。

注意

[コマンド詳細] 画面は、30 秒ごとに更新されます。

通信タイムアウトの設定

[管理対象製品の接続ステータスの間隔] の設定は、エージェントが Apex Central サーバに接続ステータスを送信する頻度を決定します。

- [管理対象製品の接続ステータスの間隔] の設定は、Apex Central 管理コンソールを使用して Apex Central サーバに登録されている管理対象製品にのみ適用されます。

- 接続ステータスの間隔が長いと、消費する帯域幅は減少しますが、Apex Central が通信ステータスをアップデートする前に発生するネットワークイベントが増加します。
- 接続ステータスの実行間隔を短く設定すると、消費する帯域幅は増加しますが、より新しいネットワークステータスが表示されるようになります。

[コマンドのタイムアウト設定] は、Apex Central が管理下のサーバにコマンドの送信を試行する時間を決定します。

手順

1. [運用管理] > [管理下のサーバ] > [通信タイムアウトの設定] に移動します。

   [通信タイムアウトの設定] 画面が表示されます。

2. [管理対象製品の接続ステータスの間隔] セクションで、次の項目を設定します。

   - 管理対象製品のステータスをレポートする間隔: エージェントの通信接続ステータスの間隔を定義します。

     値は 5～480 分の範囲で指定します。

   - 無通信状態が次の時間続いた場合はステータスを異常として設定する: エージェントの通信タイムアウトの間隔を定義します。

     値は 15～1440 分の範囲で指定します。

   重要

   [無通信状態が次の時間続いた場合はステータスを異常として設定する] には、[管理対象製品のステータスをレポートする間隔] の 3 倍以上の値を指定してください。

   ---

3. [コマンドのタイムアウト設定] セクションで、次のいずれかを選択します。

   - 24 時間

- 48 時間
- 72 時間

4. [保存] をクリックします。

パート IV

ポリシー

第 13 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。

   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、255 ページの「ポリシーの対象の指定」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、251 ページの「条件に応じてフィルタ」を参照してください。

   - 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、267 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、256 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、260 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、253 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。
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。

条件	説明
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 13-1. 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。

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。

注意

Active Directory の設定については、124 ページの「Active Directory 統合」を参照してください。

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。

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。

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、256 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、256 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。

   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 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。
  - 248 ページの「新しいポリシーの作成」
  - 260 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、270 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 13-2. 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。
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、266 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。

列	説明
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。 • 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。
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 13-3. 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

ポリシーステータス	説明	対処の提案
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。
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。

ポリシーステータス	説明	対処の提案
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。
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。

ポリシーステータス	説明	対処の提案
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 14 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、278 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、280 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`)。
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。

タスク	説明
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。
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、282 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、283 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、287 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、288 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。

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、282 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、283 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、287 ページの「証明書」を参照してください。

方法	説明
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、288 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。
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 14-1. 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。

ストレージの場所	環境変数	説明
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`

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`
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`

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
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。
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、290 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、295 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、298 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、291 ページの「事前定義済みのパターン」および 291 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/jp/solution/1312344

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、292 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

表 14-2. 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	-	すべて : 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、パターンの文字数は、最小文字数以上、最大文字数以下である必要があります。	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、パターンの文字数は、最小文字数以上、最大文字数以下である必要があります。	すべて - 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 • パターンの最小文字数: 25 • パターンの最大文字数: 80
単一のセパレータ文字	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、セパレータ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。セパレータ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。	すべて - 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.] • セパレータ: @ • 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 (292 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/jp/solution/1312344

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、298 ページの「事前定義済みのキーワードリスト」および 300 ページの「カスタマイズしたキーワードリスト」を参照してください。

事前定義済みのキーワードリスト

情報漏えい対策では、あらかじめトレンドマイクロで定義したキーワードリストが用意されています。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/jp/solution/1312344

キーワードリストの機能

キーワード数の条件

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。

カスタマイズしたキーワードリスト

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、カスタマイズしたキーワードリストを作成します。

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、300 ページの「カスタマイズしたキーワードリストの条件」を参照してください。

カスタマイズしたキーワードリストの条件

表 14-3. キーワードリストに関する条件

条件	ルール
いずれかのキーワードと一致	ファイルには、キーワードリスト内の 1 つ以上のキーワードが含まれている必要があります。
すべてのキーワード	ファイルには、キーワードリスト内のすべてのキーワードが含まれている必要があります。

条件	ルール
<x> 文字以下のすべてのキーワード	ファイルには、キーワードリスト内のすべてのキーワードが含まれている必要があります。さらに、あるキーワードから次のキーワードまでの長さが<x>文字以内である必要があります。 たとえば、WEB、DISK、および USB の 3 つのキーワードがあり、指定した文字数が 20 であるとします。 情報漏えい対策で DISK、WEB、USB の順ですべてのキーワードが検出された場合は、「D」(DISK) から「W」(WEB) までの文字数と「W」から「U」(USB) の文字数が 20 文字以下である必要があります。 次のデータはこの条件を満たします。DISK####WEB############USB 次のデータはこの条件を満たしません。 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。
キーワードの合計スコアがしきい値を超過	ファイルには、キーワードリスト内の 1 つ以上のキーワードが含まれている必要があります。1 つのキーワードしか検出されなかった場合は、そのスコアがしきい値を上回っている必要があります。複数のキーワードが存在する場合は、それらの合計スコアがしきい値を上回っている必要があります。 キーワードごとに 1 ～ 10 のスコアを割り当てます。人事部門での「昇給」など、機密性の高い単語または語句には比較的高いスコアを割り当てる必要があります。それ自体にあまり意味のない単語または語句には低いスコアを割り当てることができます。 しきい値を設定するときに、キーワードに割り当てたスコアを考慮します。たとえば、5 つのキーワードがあり、そのうちの 3 つのキーワードの優先順位が高い場合は、しきい値を優先順位の高い 3 つのキーワードの合計スコア以下にします。これは、ファイルからこの 3 つのキーワードが検出された場合に、機密扱いの対象として十分であることを意味します。

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、305 ページの「カスタマイズした情報漏えい対策テンプレート」および 305 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/jp/solution/1312344

カスタマイズした情報漏えい対策テンプレート

データ識別子の定義が完了したら、独自のテンプレートを作成します。テンプレートは、データ識別子と、条件文を形成する論理演算子 (And、Or、Except) で構成されます。

条件文と論理演算子の働きと例については、305 ページの「条件文と論理演算子」を参照してください。

条件文と論理演算子

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 14-4. 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。 次に例を示します。 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: 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: 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、305 ページの「条件文と論理演算子」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。

列	説明
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
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 14-5. 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。
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。

データ	説明
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 14-6. 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。
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。
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 V

検出

第 15 章

ログ

本章では、Apex Central で生成されたログおよび Apex Central に登録された管理下の製品のログにアクセスする方法について説明します。

次のトピックがあります。

ログクエリ

Apex Central を使用すると、Apex Central データベースを照会して Apex Central で生成されたログおよび登録済みの管理下の製品のログデータを調べることができます。

Apex Central を使用すると、次のことを実行できます。

- 詳細フィルタを使用してログクエリの検索結果を絞り込みます。
- ログ集約を設定して、ログデータを管理下の製品から Apex Central サーバに送信する際のネットワークトラフィックを削減します。
- ログエントリを種類別に手動で削除したり、自動ログ削除を設定したりします。

ログクエリを使用する

[ログクエリ] 画面を使用して、Apex Central で生成されたログおよび登録済みの管理下の製品のログデータをクエリします。また、詳細カスタムフィルタを使用して検索結果を絞り込んだり、検索結果を XML または CSV 形式でエクスポートしたり、ログクエリの検索条件を保存して他の Apex Central 管理者と共有したりできます。

注意

Apex Central では、[製品ディレクトリ] 画面からログクエリを実行することもできます。

詳細については、218 ページの「製品ディレクトリからログをクエリする」を参照してください。

手順

1. [レポート] > [ログ] > [ログクエリ] に移動します。

   [ログクエリ] 画面が表示されます。

2. ログの種類を指定します。

   注意

   ログの種類は、Apex Central レポートで使用される特定のデータビューに対応しています。

   ログの種類とデータビューの詳細については、322 ページの「ログ名とデータビュー」を参照してください。

   a. 最初のドロップダウンコントロールからログの種類を選択します。

   b. [OK] をクリックして、選択したログの種類を適用します。

3. 特定の管理下の製品からのデータに対して検索結果をフィルタするには、次の手順を実行します。

   a. 2 番目のドロップダウンコントロールをクリックします。

   b. 次のいずれかのオプションを使用して、クエリの対象を選択します。

      - ディレクトリ: 製品ディレクトリ構造から管理下の製品を探して選択できます。
      - 種類: 製品の種類を選択し、登録済みのすべての管理下の製品のうち種類が同じ製品のリストから選択できます。
      - タグおよびフィルタ: ユーザ/エンドポイントディレクトリからカスタムタグ、フィルタ、重要なラベルを選択して、特定のエンドポイントにクエリを実行できます。

        注意

        - 最大 10 個のカスタムタグ、フィルタ、重要なラベルを選択してログクエリを実行できます。
        - コンプライアンス、重要、脅威の種類、セキュリティの脅威、または脅威のステータス条件の情報が含まれているカスタムフィルタはログクエリの実行に使用できません。

   c. [OK] をクリックして、選択した対象を適用します。

4. [期間] ドロップダウンコントロールから時間を選択します。
5. カスタム条件を使用して検索結果をフィルタするには、次の手順を実行します。
   a. [詳細フィルタを表示する] をクリックします。
   b. カスタムフィルタの [一致項目] ルールを指定します。
      - すべての条件: データは指定されたすべての条件に一致する必要があります。
      - いずれかの条件: データは指定されたいずれかの条件に一致する必要があります。
   c. [条件の選択] ドロップダウンリストで、フィルタ対象となるデータ列を選択します。

      注意

      [条件の選択] ドロップダウンリストのデータ列は、最初のドロップダウンコントロールで選択するログの種類に基づいて動的に変化します。

      データ列の詳細については、322 ページの「ログ名とデータビュー」、および対応するデータビューの詳細を参照してください。

      2 番目および 3 番目のドロップダウンリストに表示されるフィルタ条件は、選択するデータ列に基づいて動的に変化します。
   d. 2 番目のドロップダウンリストで、演算子を選択します。
   e. 3 番目のドロップダウンリストで、条件を定義します。

      注意

      Apex Central では、ログクエリごとに最大 20 個のカスタムフィルタ条件を指定できます。
6. [検索] をクリックします。

   検索結果は [ログクエリ] 画面の表に表示されます。

注意

- [生成] 列には、管理下の製品が最初に脅威を検出したときのエンドポイントのローカルの日時が表示されます。
- [受信] 列には、Apex Central サーバが管理下の製品サーバからデータを受信したときの Apex Central サーバのローカルの日時が表示されます。

7. (オプション) データ列のリンクをクリックして、詳細細報を確認します。
8. (オプション) 検索結果のデータ列をカスタマイズします。
   - [列のカスタマイズ] をクリックして、表に表示する列を追加または削除します。
   - 列見出しをドラッグして、列の表示順序を並べ替えます。
9. (オプション) ログクエリの結果をエクスポートします。
   a. [CSV 形式で出力] または [XML 形式で出力] をクリックします。

      [ログクエリのページをエクスポートしています] 画面が表示されます。

   b. エクスポートが完了したら、ファイルを開くか保存します。
10. (オプション) ログクエリの検索条件を保存します。

注意

- ログクエリを保存すると、そのクエリの検索条件のみが保存されます。ログクエリの検索結果を保存するには、結果をエクスポートするか、グリッドテーブルを 使用してレポートを作成します。

  レポート作成の詳細については、421 ページのレポートを参照してください。
- 保存したクエリは、同じ Active Directory グループのすべてのユーザに自動的に表示されます。
- 保存したクエリの横にある灰色のユーザアイコン ( ) は、ログクエリが Active Directory グループ外のユーザによって共有されていることを示します。マウスをアイコンに 重ねると、クエリを共有したユーザの名前が表示されます。

a. 保存ボタン () をクリックします。

b. 保存したクエリの名前を指定します。

c. [保存] をクリックします。

ログクエリを保存したら、保存したクエリのボタン () をクリックし、保存したクエリのリストを表示して以下の処理を実行できます。

- 保存したクエリの名前をクリックして、ログクエリを実行します。
- 保存したクエリの名前の横にある共有アイコン () をクリックして、ログクエリをすべての Apex Central ユーザと共有します。
- 保存したクエリの名前の横にある共有停止アイコン () をクリックして、すべての Apex Central ユーザとのログクエリ共有を停止します。
- 削除アイコン () をクリックして、保存したクエリを削除します。

ログ名とデータビュー

Apex Central のログの種類は、カスタムレポートテンプレートの特定のデータビューに対応しています。次のデータビューを使用して、ログクエリ結果のカスタムレポートテンプレートを作成できます。

詳細については、次のトピックを参照してください。

- 422 ページの「カスタムテンプレート」
- 633 ページのデータビュー

表 15-1. セキュリティログ

ログ名	データビュー	説明
システムイベント:		

ログ名	データビュー	説明
ウイルス/不正プログラム	ウイルス/不正プログラム詳細情報	ウイルス/不正プログラムを検出した管理下の製品、ウイルス/不正プログラムの名前、感染エンドポイントなど、ネットワーク上で検出されたウイルス/不正プログラムに関する具体的な情報が表示されます。 詳細については、707 ページの「ウイルス/不正プログラム詳細情報」を参照してください。
スパイウェア/グレーウェア	スパイウェア/グレーウェア詳細情報	スパイウェア/グレーウェアを検出した管理下の製品、スパイウェア/グレーウェアの名前、感染エンドポイントの名前など、ネットワーク上で検出されたスパイウェア/グレーウェアに関する具体的な情報が表示されます。 詳細については、694 ページの「スパイウェア/グレーウェア詳細情報」を参照してください。
不審ファイル	不審ファイルの詳細情報	ネットワークで検出された不審ファイルに関する具体的な情報が表示されます。 詳細については、637 ページの「不審ファイルの詳細情報」を参照してください。
挙動監視	挙動監視の詳細情報	ネットワーク上の挙動監視イベントに関する具体的な情報が表示されます。 詳細については、682 ページの「挙動監視の詳細情報」を参照してください。
変更監視	変更監視情報	インストール済みソフトウェア、実行中のサービス、プロセス、ファイル、ディレクトリ、待機ポート、レジストリキー、レジストリ値など、エンドポイントに加えられる特定の変更を監視するために使用します。 詳細については、688 ページの「変更監視情報」を参照してください。

ログ名	データビュー	説明
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の違反詳細情報	セキュリティエージェントのポリシーや条件への違反など、ネットワーク上のアプリケーションコントロール違反に関する具体的な情報が表示されます。 詳細については、680 ページの「アプリケーションコントロールの違反詳細情報」を参照してください。
デバイスコントロール	デバイスアクセス管理情報	ネットワーク上のデバイスアクセス管理イベントに関する具体的な情報が表示されます。 詳細については、677 ページの「デバイスアクセス管理情報」を参照してください。
エンドポイントセキュリティ遵守	エンドポイントセキュリティ遵守詳細情報	ネットワーク上のエンドポイントセキュリティ遵守に関する具体的な情報が表示されます。 詳細については、683 ページの「エンドポイントセキュリティ遵守詳細情報」を参照してください。
エンドポイントセキュリティ違反	エンドポイントセキュリティ違反詳細情報	ネットワーク上のエンドポイントセキュリティ違反に関する具体的な情報が表示されます。 詳細については、684 ページの「エンドポイントセキュリティ違反詳細情報」を参照してください。
機械学習型検索	機械学習型検索による検出詳細情報	機械学習型検索によって検出された高度な未知の脅威に関する具体的な情報が表示されます。 詳細については、635 ページの「機械学習型検索による検出詳細情報」を参照してください。

ログ名	データビュー	説明
仮想アナライザ	仮想アナライザによる詳細な検出情報	仮想アナライザによって検出された高度な未知の脅威に関する具体的な情報が表示されます。 詳細については、638 ページの「仮想アナライザによる検出情報」を参照してください。
仮想アナライザで検出された不審オブジェクト	仮想アナライザで検出された不審オブジェクトによる影響の詳細情報	仮想アナライザで検出された不審オブジェクトの影響に関する詳細情報が表示されます。 詳細については、640 ページの「仮想アナライザで作成された不審オブジェクトによる影響の詳細情報」を参照してください。
Attack Discovery	Attack Discovery による検出情報	Attack Discovery によって検出された脅威に関する一般情報が表示されます。 詳細については、642 ページの「Attack Discovery による検出情報」を参照してください。
グレー検出数	グレー検出情報	ネットワーク上で検出された、攻撃の痕跡と疑われる項目に関する詳細情報が表示されます。 詳細については、671 ページの「グレーウェア検出情報」を参照してください。
ネットワークイベント:		
スパムメール接続	スパムメール接続情報	ネットワーク上のスパムメールの発生元に関する具体的な情報が表示されます。たとえば、スパムを検知した管理下の製品、管理下の製品により実行された処理の内容、検知されたスパムの総数などです。 詳細については、691 ページの「スパムメール接続情報」を参照してください。

ログ名	データビュー	説明
コンテンツ違反	コンテンツ違反詳細情報	コンテンツ違反が含まれるメールに関する具体的な情報が表示されます。たとえば、コンテンツ違反を検知した管理下の製品、メールの送信者と受信者、コンテンツ違反ポリシーの名称、検知された違反の総数などです。 詳細については、650 ページの「コンテンツ違反詳細情報」を参照してください。
高度な脅威を含むメールメッセージ	高度な脅威を含むメールメッセージ	高度な脅威を含むメールメッセージに関する具体的な情報が表示されます。たとえば、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です。 詳細については、651 ページの「高度な脅威を含むメールメッセージ」を参照してください。
Web レピュテーション	Web レピュテーション詳細情報	Web レピュテーションサービスによって検知されたアプリケーションアクティビティに関するコンプライアンス情報が表示されます。 詳細については、719 ページの「Web レピュテーション詳細情報」を参照してください。
Web 違反	Web 違反詳細情報	ネットワーク上の Web 違反に関する具体的な情報が表示されます。 詳細については、722 ページの「Web 違反詳細情報」を参照してください。
ファイアウォール違反	ファイアウォール違反詳細情報	ネットワーク上のファイアウォール違反に関する具体的な情報が表示されます。たとえば、違反を検知した管理下の製品、転送元および転送先、ファイアウォール違反の総数などです。 詳細については、685 ページの「ファイアウォール違反詳細情報」を参照してください。

ログ名	データビュー	説明
ネットワークコンテンツ検査	ネットワークコンテンツ検査情報	ネットワーク上のネットワークコンテンツ違反に関する具体的な情報が表示されます。 詳細については、689 ページの「ネットワークコンテンツ検査情報」を参照してください。
IPS	IPS の詳細情報	既知の攻撃やゼロデイ攻撃に対する迅速な保護、Web アプリケーションの脆弱性に対する防御、ネットワークにアクセスする不正ソフトウェアの識別などを実施する際に役立つ具体的な情報が表示されます。 詳細については、686 ページの「IPS の詳細情報」を参照してください。
C&C コールバック	C&C コールバック詳細情報	ネットワーク上で検出された C&C コールバックイベントに関する具体的な情報が表示されます。 詳細については、634 ページの「C&C コールバック詳細情報」を参照してください。
脅威の兆候	脅威の兆候の詳細情報	脅威の兆候を検出した管理下の製品、発生元および感染先に関する具体的な情報、ネットワーク上の脅威の兆候の総数など、ネットワーク上の脅威の兆候に関する具体的な情報が表示されます。 詳細については、660 ページの「脅威の兆候の詳細情報」を参照してください。
アプリケーションアクティビティ	アプリケーションアクティビティの詳細	ネットワークセキュリティポリシーに違反するアプリケーションアクティビティに 関する具体的な情報が表示されます。 詳細については、678 ページの「アプリケーションアクティビティの 詳細」を参照してください。

ログ名	データビュー	説明
軽減処理	軽減処理の詳細情報	ネットワーク上の脅威を解決するために Mitigation Server で実行されたタスクに関する具体的な情報が表示されます。 詳細については、658 ページの「軽減処理の詳細情報」を参照してください。
相関	相関の詳細情報	詳細な脅威分析と推奨される修復方法に関する具体的な情報が表示されます。 詳細については、658 ページの「相関の詳細情報」を参照してください。
データ保護イベント:		
情報漏えい対策	情報漏えい対策イベント情報	情報漏えい対策によって検出されたイベントに関する具体的な情報が表示されます。 詳細については、654 ページの「情報漏えい対策イベント情報」を参照してください。
データ検出	データ検出の情報漏えい対策検出情報	データ検出によって検出されたイベントに関する具体的な情報が表示されます。 詳細については、653 ページの「データ検出の情報漏えい対策検出情報」を参照してください。

表 15-2. 製品情報

ログ名	データビュー	説明
管理下の製品:		
製品ステータス	製品のステータス情報	Apex Central サーバに登録された管理下の製品に関する詳細情報が表示されます。たとえば、管理下の製品のバージョンとビルド番号、管理下の製品のサーバオペレーティングシステムなどです。 詳細については、746 ページの「製品のステータス情報」を参照してください。

ログ名	データビュー	説明
製品のイベント	製品のイベント情報	管理下の製品の Apex Central への登録、コンポーネントのアップデート、アクティベーションコードの配信など、管理下の製品のイベントに関する情報が表示されます。 詳細については、745 ページの「製品のイベント情報」を参照してください。
製品監査イベント	製品監査イベントログ	管理下の製品のコンソールアクセスなど、管理下の製品の監査イベントに関する情報が表示されます。 詳細については、743 ページの「製品監査イベントログ」を参照してください。
Apex Central:		
コマンド追跡	コマンド追跡情報	Apex Central が管理下の製品に対して発行したコマンドに関する情報が表示されます。たとえば、Apex Central がコンポーネントのアップデートやアクティベーションコード配信のためのコマンドを発行した日付と時刻や、そのコマンドのステータスなどです。 詳細については、730 ページの「コマンド追跡情報」を参照してください。
Apex Central のイベント	Apex Central のイベント情報	管理下の製品の Apex Central への登録、コンポーネントのアップデート、アクティベーションコードの配信などの Apex Central サーバイベントに関する情報が表示されます。 詳細については、730 ページの「Apex Central のイベント情報」を参照してください。

ログ名	データビュー	説明
管理対象外のエンドポイント	管理対象外のエンドポイント	検出されたエンドポイントのうち、トレンドマイクロ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に関する情報が表示されます。 詳細については、732 ページの「管理対象外のエンドポイント情報」を参照してください。
ユーザのアクセス	ユーザアクセス情報	Apex Central へのユーザアクセス、および Apex Central にログオン中にユーザが実行するアクティビティに関する情報が表示されます。 詳細については、732 ページの「ユーザアクセス情報」を参照してください。
製品ライセンス	製品ライセンス詳細情報	管理下の製品のバージョン、ライセンス使用期限など、管理下の製品またはサービスのアクティベーションコードやライセンスのステータスに関する情報が表示されます。 詳細については、741 ページの「製品ライセンス詳細情報」を参照してください。

ログ集約を設定する

ログ集約を使用すると、選択したデータだけを管理下の製品から Apex Central サーバに送信することにより、ネットワークの帯域幅を節約できます。

警告!

Apex Central は、管理下の製品から Apex Central サーバに送信されないデータをリカバリできません。

手順

1. [レポート] > [ログ] > [ログ集約の設定] に移動します。

   [ログ集約ルールの編集] 画面が表示されます。

2. [ログ集約を有効にする] チェックボックスをオンにします。

3. ログのカテゴリを展開します。

4. 管理下の製品から Apex Central へのデータの送信を停止するには、チェックボックスをオフにします。

5. [保存] をクリックします。

Syslog 転送を設定する

[SysLog 設定] 画面を使用して、サポートされているログを Apex Central から SysLog サーバに転送するよう設定できます。

詳細については、次のトピックを参照してください。

- 334 ページの「Syslog 転送を無効にする」
- 335 ページの「サポート対象のログの種類と形式」

注意

- 以前インストールした Control Manager から Apex Central に移行した場合、Apex Central は、Syslog 転送ツール (<Control Manager のインストールディレクトリ>\LogForwarder.exe) を使用して設定された以前の SysLog 転送設定を自動的にインポートします。
- Apex Central への移行後は、Syslog 転送ツールを実行できなくなります。

手順

1. [運用管理] > [設定] > [Syslog の設定] に移動します。

   [Syslog の設定] 画面が表示されます。

2. [Syslog 転送を有効にする] チェックボックスをオンにします。
3. 転送された Syslog を受信するサーバについて、次の項目を設定します。
   - サーバアドレス: Syslog サーバの IP アドレスまたは FQDN
   - ポート: Syslog サーバのポート番号
   - プロトコル: 転送プロトコルを選択します。

   注意

   Apex Central では、[SSL/TLS] が選択されている場合、有効な自己署名の証明書が初期設定で受け入れられます。

   - サーバ証明書に Subject Alternative Name がある場合は、Subject Alternative Name にサーバの FQDN または IP アドレスを含める必要があります。
   - セキュリティを強化するには、有効なサーバ証明書を使用するか、サーバ証明書を Apex Central にアップロードしてください。

4. (オプション) サーバ証明書をアップロードします。

   重要

   - Apex Central でサポートされているのは、.DER または.PEM エンコードを使用した X.509 形式のサーバ証明書のみです。

     詳細については、https://support.ssl.com/Knowledgebase/Article/View/19/0/der-vs-crt-vs-cer-vs-pem-certificates-and-how-to-convert-them を参照してください。
   - Apex Central では、SSL/TLS 転送で使用するサーバ証明書のアップロードのみがサポートされています。

   a. [サーバ証明書を使用] チェックボックスをオンにします。
   b. [選択] をクリックして、コンピュータからサーバ証明書を選択します。
   c. [開く] をクリックします。

選択したサーバ証明書が Apex Central によってアップロードされます。

5. (オプション) Syslog 転送にプロキシサーバを使用するには、[SOCKS プロキシサーバを使用] チェックボックスをオンにします。

重要

- Apex Central では、SSL/TLS または TCP 転送で SOCKS プロトコルプロキシサーバ経由の Syslog 転送のみがサポートされます。
- Syslog 転送は HTTP プロキシサーバをサポートしていません。Syslog 転送にプロキシサーバを使用するには、[プロキシ設定] をクリックして、[プロキシの設定] 画面で SOCKS プロトコルサーバを選択します。

  詳細については、237 ページの「コンポーネント/ライセンスのアップデート、クラウドサービス、および Syslog 転送のためにプロキシを設定する」を参照してください。

Apex Central は、Syslog 転送に[プロキシの設定] 画面 ([運用管理] > [設定] > [プロキシの設定]) で設定されたプロキシサーバを使用します。

6. ログの形式を選択します。
   - CEF: ログメッセージに標準の Common Event Format (CEF) を使用します。
   - Apex Central 形式: Syslog の facility を「local0」に、severity を「notice」に設定します。

   詳細については、335 ページの「サポート対象のログの種類と形式」を参照してください。
7. Apex Central がログを転送する頻度を設定します。
8. 転送するログの種類を選択します。
   a. [ログの種類] ドロップダウンリストからログのカテゴリを 選択します。

注意

複数のログのカテゴリからログの種類を選択できます。

- セキュリティログ
- 製品情報

b. 転送するログのチェックボックスをオンにします。

[ログの種類] ドロップダウンリストの横に、選択したログの種類の総数が表示されます。

c. (オプション) [ログの種類] ドロップダウンリストから別のログのカテゴリを選択して、転送するログの種類を追加で選択します。

9. (オプション) [接続テスト] をクリックして、サーバ接続をテストします。

注意

接続をテストしても Syslog サーバの設定は保存されません。

Syslog サーバの接続ステータスが画面上部に表示されます。

10. [保存] をクリックします。

- Apex Central が、設定した Syslog サーバへのログの転送を開始します。
- ログ転送ステータスを監視するには、[運用管理] > [コマンド追跡] に移動し、[コマンド] ドロップダウンリストから [Syslog 転送] を選択します。

  詳細については、241 ページの「コマンドのクエリと表示」を参照してください。

Syslog 転送を無効にする

[SysLog 設定] 画面を使用して、Apex Central から Syslog サーバへのログの転送を停止します。

手順

1. [運用管理] > [設定] > [Syslog の設定] に移動します。

   [Syslog の設定] 画面が表示されます。

2. [Syslog 転送を有効にする] チェックボックスをオフにします。

3. [保存] をクリックします。

   Apex Central では、設定した Syslog サーバへのログの転送が停止されます。

サポート対象のログの種類と形式

Apex Central は、次の形式のログを Syslog サーバに転送できます。

- CEF: ログメッセージに標準の Common Event Format (CEF) を使用します。
- Apex Central 形式: Syslog の facility を「local0」に、severity を「notice」に設定します。

次の表は、それぞれのログの種類でサポートされる形式を示しています。

表 15-3. セキュリティログ

ログの種類	CEF	Apex Central 形式
アプリケーションコントロール	○	×
Attack Discovery	○	×
挙動監視	○	○
C&C コールバック	○	×
コンテンツ違反	○	×
情報漏えい対策	○	○
デバイスコントロール	○	○

ログの種類	CEF	APEX CENTRAL 形式
IPS	○	×
ネットワークコンテンツ検査	○	×
機械学習型検索	○	×
スパイウェア/グレーウェア	○	×
不審ファイル	○	×
仮想アナライザ	○	×
ウイルス/不正プログラム	○	×
Web 違反	○	×

表 15-4. 製品情報

ログの種類	CEF	APEX CENTRAL 形式
検索エンジンアップデートステータス	○	○
管理下の製品のログオン/ログオフイベント	○	○
製品監査イベント	○	×
パターンファイルアップデートステータス	○	○

CEF 形式と Apex Central 形式間での Syslog コンテンツのマッピングの詳細については、771 ページの Syslog コンテンツマッピング - CEF を参照してください。

ログの削除

[ログ管理] 画面を使用すると、ログエントリを種類別に手動で削除したり、自動ログ削除を設定したりできます。

警告!

ログデータを手動で削除すると、レポートの生成に影響する可能性があります。

ヒント

Trend Micro では、情報漏えい対策ログをセキュリティ情報とイベントの管理 (SIEM) サーバにバックアップし、少なくとも 2 年間保存することを推奨しています。

手順

1. [検出数] > [ログ] > [ログ管理] に移動します。

   [ログ管理] 画面が表示されます。

2. ログを手動で削除するには、次の手順を実行します。

   a. ログの種類のチェックボックスをオンにします。

   b. 削除するログエントリの種類に対応する行で [すべて削除] をクリックします。

      確認メッセージが表示されます。

   c. [OK] をクリックして、選択した種類のすべてのログを削除します。

3. 自動ログ削除を設定するには、次の手順を実行します。

   a. ログの種類のチェックボックスをオンにします。

   b. [ログエントリの最大数] 列で、保持するログの最大数を指定します。

      注意

      初期設定では、最大 1,000,000 のログエントリが保持されます。

   c. [削除数] 列に、ログの数が [ログエントリの最大数] 列で指定した数に達したときに削除するログ数を指定します。

      注意

      初期設定では、削除数の値は 1,000 のログエントリです。

   d. [ログの最大保存期間] 列に、自動削除を適用する保存日数を指定します。

注意

初期設定では、ログの最大保存期間は 90 日です。

e. [保存] をクリックします。

第 16 章

通知

本章では、Apex Central ネットワーク上で発生するイベントに関する通知を送信する方法について説明します。

次のトピックがあります。

イベント通知

Apex Central では、管理下の製品によって検出されたイベント通知を、個人の受信者や受信者グループに送信できます。サポートされる通知方法には、メールメッセージ、Windows イベントログ通知、SMNP トラップ、Syslog メッセージ、アプリケーション通知などがあります。

詳細については、341 ページの「通知方法の設定」を参照してください。

[イベント通知] 画面を使用して、次のカテゴリのイベントに関する通知を有効または無効にします。

イベントのカテゴリ	説明
高度な脅威アクティビティ	高度な脅威および未知の脅威について、警告を発します。 詳細については、348 ページの「高度な脅威アクティビティのイベント」を参照してください。
コンテンツのポリシー違反	メールの内容および URL セキュリティポリシー違反について、警告を発します。 詳細については、370 ページの「コンテンツのポリシー違反イベント」を参照してください。
情報漏えい対策	情報漏えい対策のイベントおよびテンプレート一致に関する情報を提供します。 詳細については、374 ページの「情報漏えい対策イベント」を参照してください。
既知の脅威アクティビティ	管理下のウイルス対策製品によって検出されたウイルスについて、警告を発します。 詳細については、383 ページの「既知の脅威アクティビティのイベント」を参照してください。
ネットワークアクセス管理	管理下の Network VirusWall 製品からの警告を発します。 詳細については、400 ページの「ネットワークアクセス管理イベント」を参照してください。

イベントのカテゴリ	説明
その他の製品の挙動	製品オプションや、サービスの開始/停止に関する情報を提供します。 詳細については、403 ページの「その他の製品の挙動イベント」を参照してください。
アップデート	コンポーネントのアップデート結果 (成功または失敗) を通知します。 詳細については、411 ページの「アップデート」を参照してください。

通知方法の設定

[通知方法の設定] 画面を使用して、次の通知方法を設定します。

方法	説明
メール通知	管理下の製品によって検出されたイベントについてメール通知を送信するには、[SMTP サーバ設定] を設定します。 詳細については、342 ページの「SMTP サーバを設定する」を参照してください。
SNMP トラップ	管理下の製品によって検出されたイベントについて SNMP トラップ通知を送信するには、[SMTP トラップ設定] を設定します。 詳細については、343 ページの「SNMP トラップを設定する」を参照してください。
Syslog 通知	選択した受信者またはサポート対象の他社製品に Syslog メッセージを送信するには、[Syslog 設定] を設定します。 詳細については、343 ページの「Syslog を設定する」を参照してください。
アプリケーションの起動	通知の送信に使用するアプリケーションを起動するためのユーザ認証を指定します。 詳細については、344 ページの「アプリケーションを設定する」を参照してください。

SMTP サーバを設定する

Apex Central を使用すると、管理下の製品によって検出されたイベントについて、選択した受信者に通知するためにメールメッセージを送信できます。

重要

Apex Central からメールメッセージを送信するには、[SMTP サーバ設定] を設定する必要があります。

手順

1. [検出数] > [通知] > [通知方法]に移動します。

   [通知方法] 画面が表示されます。

2. [SMTP サーバ設定] セクションで、次の項目を指定します。

   a. サーバの FQDN または IP アドレス: 有効な FQDN、IPv4、または IPv6 アドレスを入力します。

   b. ポート: SMTP サーバのポート番号を入力します。

   c. 送信者のメールアドレス: イベント通知を送信するメールアドレスを入力します。

   d. 添付ファイルのサイズ制限 (KB): 添付ファイルの最大サイズをキロバイト単位で指定します。

3. Extended SMTP (ESMTP) を使用するには、次の手順を実行します。

   a. [ESMTP を有効にする] を選択します。

   b. ユーザ名およびパスワードを指定します。

   c. [認証] ドロップダウンリストから認証方法を選択します。

4. [保存] をクリックします。

SNMP トラップを設定する

Apex Central を使用すると、管理下の製品によって検出されたイベントについて、選択した受信者に通知するために SNMP トラップを送信できます。

手順

1. [検出数] > [通知] > [通知方法]に移動します。

   [通知方法] 画面が表示されます。

2. [SNMP トラップ設定] セクションで、次の項目を指定します。

   a. コミュニティ名: SNMP コミュニティ名を入力します。

   b. サーバ IP アドレス: SNMP サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。

3. [保存] をクリックします。

Syslog を設定する

Apex Central を使用すると、管理下の製品によって検出されたイベントについて、選択した受信者に通知するために Syslog メッセージを送信できます。

また、サポート対象の他社製品に直接 Syslog メッセージを転送することもできます。

手順

1. [検出数] > [通知] > [通知方法]に移動します。

   [通知方法] 画面が表示されます。

2. [Syslog 設定] セクションで、次の項目を指定します。

   a. サーバ IP アドレス: Syslog サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。

   b. ポート: Syslog サーバのポート番号を入力します。

c. ファシリティ：ファシリティコードを選択します。

注意

複数の Syslog サーバを追加するには、追加アイコン ( ) を使用します。

3. [保存] をクリックします。

アプリケーションを設定する

Apex Central では、アプリケーションを使用して、管理下の製品によって検出されたイベントについて、選択した受信者に通知できます。

たとえば、net send コマンドを実行するバッチファイルを使用する組織の場合、[通知方法の設定] 画面を使用して、必要な権限があるユーザアカウントの認証情報を入力します。

重要

起動アプリケーションファイルは、Apex Central サーバの次の場所に保存します。

<Apex Centrall インストールディレクトリ>¥Application¥

手順

1. [検出数] > [通知] > [通知方法]に移動します。

   [通知方法] 画面が表示されます。

2. [アプリケーション設定] セクションで、[指定したユーザがアプリケーションを起動する] を選択します。

3. 起動アプリケーションで必要とされる権限があるアカウントのユーザ名とパスワードを入力します。

4. [保存] をクリックします。

連絡先グループ

[連絡先グループ] 画面には、以前に定義したすべての連絡先グループのリストが表示され、レポートやイベント通知の受信者を指定する際に選択できます。Apex Central 連絡先グループを使用すると、同じグループ内のすべての受信者に通知やレポートを送信できます。ユーザアカウントを個別に選択する必要はありません。

次の表は、[連絡先グループ] 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
新しい連絡先グループの追加	新しい連絡先グループを追加するには、[追加] をクリックします。 詳細については、345 ページの「連絡先グループを追加する」を参照してください。
既存の連絡先グループの削除	既存の連絡先グループを選択して、[削除] をクリックします。 警告! 連絡先グループを削除すると、そのグループを使用するすべてのレポートや通知に影響がおよびます。
既存の連絡先グループの編集	受信者を編集するには、既存の連絡先グループの名前をクリックします。 詳細については、346 ページの「連絡先グループを編集する」を参照してください。

連絡先グループを追加する

[グループの追加] 画面を使用して、レポートおよびイベント通知用の新しい連絡先グループを作成します。

手順

1. [レポート] > [通知] > [連絡先グループ] に移動します。

   [連絡先グループ] 画面が表示されます。

2. [追加] をクリックします。

   [グループの追加] 画面が表示されます。

3. 連絡先グループの名前を入力します。

4. 連絡先グループの受信者を指定します。

   - [選択可能なユーザアカウント] リストから、ユーザアカウントを選択して、[>] をクリックします。

     選択したユーザアカウントが [選択したユーザアカウント] リストに表示されます。

     注意

     また、統合された Active Directory 構造からユーザとグループを追加できます。

     詳細については、124 ページの「Active Directory 統合」を参照してください。

   - [追加の受信者] フィールドに、メールアドレスを入力して、<Enter> キーを押します。

     新しく追加されたメールアドレスが [追加の受信者] フィールドの下に表示されます。

     注意

     一度に追加できるメールアドレスは 1 つだけです。

5. [保存] をクリックします。

連絡先グループを編集する

[グループの編集] 画面を使用して、レポートおよびイベント通知用の新しい連絡先グループを作成します。

注意

既存の連絡先グループの名前は編集できません。

手順

1. [レポート] > [通知] > [連絡先グループ] に移動します。

   [連絡先グループ] 画面が表示されます。

2. 編集する連絡先グループの名前をクリックします。

   [グループの編集] 画面が表示されます。

3. 連絡先グループの受信者を指定します。

   - [選択可能なユーザアカウント] リストから、ユーザアカウントを選択して、[>] をクリックします。

     選択したユーザアカウントが [選択したユーザアカウント] リストに表示されます。

     注意

     また、統合された Active Directory 構造からユーザとグループを追加できます。

     詳細については、124 ページの「Active Directory 統合」を参照してください。

   - [追加の受信者] フィールドに、メールアドレスを入力して、<Enter> キーを押します。

     新しく追加されたメールアドレスが [追加の受信者] フィールドの下に表示されます。

     注意

     一度に追加できるメールアドレスは 1 つだけです。

4. [保存] をクリックします。

高度な脅威アクティビティのイベント

[イベント通知] 画面を使用して、ネットワーク上で検出された高度な脅威アクティビティに関する通知を有効にし、設定します。

Attack Discovery による検出

Attack Discovery エンジンによって高度な脅威が検出されたときに管理者に通知するよう次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で [Attack Discovery による検出] をクリックします。

   [Attack Discovery による検出] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出の種類	イベント通知を起動する検出のリスクレベルを選択します。
期間	期間を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、756 ページの「Attack Discovery のトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

挙動監視違反

挙動監視違反が検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[挙動監視違反] をクリックします。

   [挙動監視違反] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。

設定	説明
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

C&C コールバックアラート

エンドポイントと既知の C&C コールバックアドレスの間の通信が検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[C&C コールバックアラート] をクリックします。

   [C&C コールバックアラート] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
C&C リストのソース	1 つ以上の C&C リストのソースを選択します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 757 ページの「C&C コールバックトークン変数」を参照してください。

方法	説明
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 757 ページの「C&C コールバックトークン変数」を参照してください。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

C&C コールバックアウトブレイクアラート

複数のエンドポイントと既知の C&C コールバックアドレスの間の通信が検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[C&C コールバックアウトブレイクアラート] をクリックします。

   [C&C コールバックアウトブレイクアラート] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
C&C リストのソース	1 つ以上の C&C リストのソースを選択します。
コールバック回数	コールバック回数を指定します。
感染ホスト	感染ホストの数を指定します。
期間	期間を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 757 ページの「C&C コールバックトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

相関関係のあるイベントを検出する

相関関係のあるイベントが検出されときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[相関関係のあるイベントの検出] をクリックします。

   [相関関係のあるイベントの検出] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。 **注意** データは複数のホストから集計されるため、トークン変数`%hostIP%`および`%group%`はメール通知では使用できません。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

高度な脅威を含むメールメッセージ

高度な脅威を含むメールメッセージが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[高度な脅威を含むメールメッセージ] をクリックします。

   [高度な脅威を含むメールメッセージ] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
検出数	管理下の製品によって検出された脅威の数を入力します。
期間	期間を指定します。
検出の種類	イベント通知を起動する検出のリスクレベルを選択します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

仮想アナライザによるリスク高の検出

仮想アナライザが極めて不審なオブジェクトを検出したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[仮想アナライザによるリスク高の検出] をクリックします。

   [仮想アナライザによるリスク高の検出] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

リスク高ホストの検出

ネットワークでリスク高ホストが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[リスク高ホストの検出] をクリックします。

   [リスク高ホストの検出] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。

設定	説明
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。
   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。
   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。
6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン 変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

既知の標的型攻撃の挙動

ネットワークで既知の標的型攻撃の挙動が検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[既知の標的型攻撃の挙動] をクリックします。

   [既知の標的型攻撃の挙動] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

文書内の潜在的な攻撃コードの検出

ネットワークで潜在的な攻撃コードを含むドキュメントが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[文書内の潜在的な攻撃コードの検出] をクリックします。

   [文書内の潜在的な攻撃コードの検出] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。

設定	説明
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

機械学習型検索の検出

トレンドマイクロの機械学習型検索により未知のセキュリティ脅威が検出された場合に管理者に通知するには、以下のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[機械学習型検索の検出] をクリックします。

   [機械学習型検索の検出] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

ルートキットまたはハッキングツールの検出

ネットワークでルートキットやハッキングツールが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[ルートキットまたはハッキングツールの検出] をクリックします。

   [ルートキットまたはハッキングツールの検出] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。

設定	説明
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。
   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。
   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。
6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン 変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

SHA-1 拒否リストの検出

ネットワークで SHA-1 値が拒否リスト内のオブジェクトに一致するファイルが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[SHA-1 拒否リストの検出] をクリックします。

   [SHA-1 拒否リストの検出] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。
1 つのエンドポイントに適用するアラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

ウォッチリストに登録された、危険性の高い受信者

ウォッチリストに登録された受信者に不正または不審なメールメッセージや添付ファイルが送信されたことを Deep Discovery Email Inspector が検出したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[ウォッチリストに登録された、危険性の高い受信者] をクリックします。

   [ウォッチリストに登録された、危険性の高い受信者] 画面が表示されます。
4. 次の通知設定を指定します。

条件	説明
メールアドレスのウォッチリスト	監視するメールアドレスを入力します。複数のエントリを入力する場合は、セミコロン (;) で区切って入力してください。
種類	イベント通知を起動する検出のリスクレベルを選択します。
検出数	管理下の製品によって検出された脅威の数を入力します。
期間	検出の期間を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

ワームまたはファイル感染型ウイルスの拡散の検出

ネットワークでワームやファイル感染型ウイルスの特性が検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [高度な脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[ワームまたはファイル感染型ウイルスの拡散の検出] をクリックします。

   [ワームまたはファイル感染型ウイルスの拡散の検出] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出ごとにアラートをトリガする	選択すると、検出ごとにイベント通知が送信されます。
アラートのしきい値を指定する	選択すると、指定された条件に一致する検出に関するイベント通知のみが送信されます。 • 検出数: 検出数を指定します。 • 期間: 期間を時間単位で指定します。
ログを CSV 形式で添付する	選択すると、イベント通知の受信者に、検出に関するログデータを含む*.csv ファイルが送信されます。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 752 ページの「高度な脅威アクティビティのトークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

コンテンツのポリシー違反イベント

[イベント通知] 画面を使用して、ネットワーク上で検出されたコンテンツのポリシー違反に関する通知を有効にし、設定します。

メールのポリシー違反

コンテンツセキュリティポリシーに違反するメールが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [コンテンツ違反ポリシー] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[メールのポリシー違反] をクリックします。

   [メールのポリシー違反] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「コンテンツのポリシー違反のトークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「コンテンツのポリシー違反のトークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。

方法	説明
Syslog 通知	ログメッセージを IP ネットワークで転送する標準です。 Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

Web アクセスポリシー違反

Web アクセスポリシー違反が発生したために URL へのアクセスがブロックされたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [コンテンツ違反ポリシー] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[Web アクセスポリシー違反] をクリックします。

   [Web アクセスポリシー違反] 画面が表示されます。
4. 通知の受信者を選択します。
   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。
   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 764 ページの「Web アクセスポリシー違反トークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 764 ページの「Web アクセスポリシー違反トークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	ログメッセージを IP ネットワークで転送する標準です。 Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

情報漏えい対策イベント

[イベント通知] 画面を使用して、ネットワーク上で検出された情報漏えい対策イベントに関する通知を有効にし、設定します。

イベント詳細のアップデート

イベント詳細がアップデートされたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [情報漏えい対策] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[イベント詳細のアップデート] をクリックします。

   [イベント詳細のアップデート] 画面が表示されます。

4. 通知対象となる通知イベント詳細のアップデートの条件を指定します。

条件	説明
イベント詳細のアップデート	イベント詳細のアップデートの種類を選択します。 • 解決済み • すべての変更

条件	説明
重大度レベルでフィルタ	次のリスクレベルから選択します (複数可)。 • 高 • 中 • 低 • 情報 • 未定義

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「情報漏えい対策トークン変数」を参照してください。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

予約イベント概要

ネットワークで発生した情報漏えい対策イベントの概要を管理者に送信するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [情報漏えい対策] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[予約イベント概要] をクリックします。

   [予約イベント概要] 画面が表示されます。

4. 次の通知設定を指定します。

条件	説明
実行間隔	通知を受信する頻度を日単位または週単位から選択します。

イベントの詳細の添付	イベントログを通知に添付する場合に選択します。
	• 情報漏えい対策コンプライアンス責任者が受信する内容を選択します。
	  • すべての管理されているユーザからのイベント
	  • 直属の部下からのイベントのみ
	  注意
	情報漏えい対策イベントレビューアが受信できるのは、直属の部下からのイベントのみです。
	• ログ詳細の形式を選択します。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「情報漏えい対策トークン変数」を参照してください。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

イベントの大幅な増加

事前に定義された期間に、情報漏えい対策イベントで大幅な増加が発生したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [情報漏えい対策] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[イベントの大幅な増加] をクリックします。

   [イベントの大幅な増加] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
毎時	時間ごとのイベントの数を指定します。
毎日	1 日ごとのイベントの数を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「情報漏えい対策トークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

チャネル別イベントの大幅な増加

事前に定義された期間に、チャネル別の情報漏えい対策イベントで大幅な増加が発生したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [情報漏えい対策] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[チャネル別イベントの大幅な増加] をクリックします。

   [チャネル別イベントの大幅な増加] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
毎時	時間ごとのイベントの数を指定します。
毎日	1 日ごとのイベントの数を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「情報漏えい対策トークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

送信者別イベントの大幅な増加

事前に定義された期間に、送信者別の情報漏えい対策イベントで大幅な増加が発生したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [情報漏えい対策] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[送信者別イベントの大幅な増加] をクリックします。

   [送信者別イベントの大幅な増加] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
毎時	時間ごとのイベントの数を指定します。
毎日	1 日ごとのイベントの数を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「情報漏えい対策トークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

8. [保存] をクリックします。

ユーザ別イベントの大幅な増加

事前に定義された期間に、ユーザ別の情報漏えい対策イベントで大幅な増加が発生したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [情報漏えい対策] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[ユーザ別イベントの大幅な増加] をクリックします。

   [ユーザ別イベントの大幅な増加] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
毎時	時間ごとのイベントの数を指定します。
毎日	1 日ごとのイベントの数を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「情報漏えい対策トークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

テンプレート一致の大幅な増加

事前に定義された期間に、情報漏えい対策テンプレートの一致で大幅な増加が発生したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [情報漏えい対策] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[テンプレート一致の大幅な増加] をクリックします。

   [テンプレート一致の大幅な増加] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
毎時	時間ごとのイベントの数を指定します。
毎日	1 日ごとのイベントの数を指定します。

5. 通知の受信者を選択します。
   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。
   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 759 ページの「情報漏えい対策トークン変数」を参照してください。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

既知の脅威アクティビティのイベント

[イベント通知] 画面を使用して、ネットワーク上で検出された既知の脅威アクティビティに関する通知を有効にし、設定します。

ネットワークウイルスアラート

ネットワークウイルスが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[ネットワークウイルスアラート] をクリックします。

   [ネットワークウイルスアラート] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出数	管理下の製品によって検出された脅威の数を入力します。
影響を受けたユーザ/エンドポイント	影響を受けたユーザ/エンドポイントの数を指定します。
期間	期間を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」、761 ページの「既知の脅威アクティビティのトークン変数」、および 763 ページの「ネットワークアクセス管理トークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」、761 ページの「既知の脅威アクティビティのトークン変数」、および 763 ページの「ネットワークアクセス管理トークン変数」を参照してください。

方法	説明
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

特定スパイウェア用アラート

監視対象のスパイウェア/グレーウェアの脅威リストに含まれているスパイウェア/グレーウェアが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[特定スパイウェア用アラート] をクリックします。

   [特定スパイウェア用アラート] 画面が表示されます。
4. 監視対象のスパイウェア/グレーウェアの名前を指定します。

5. 次の通知設定を指定します。

設定	説明
期間	期間を指定します。

6. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

7. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

8. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

9. [保存] をクリックします。

特定ウイルス用アラート

監視対象のウイルスリストに含まれているウイルスが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[特定ウイルス用アラート] をクリックします。

   [特定ウイルス用アラート] 画面が表示されます。

4. 監視対象のウイルスの名前を指定します。

5. 次の通知設定を指定します。

設定	説明
期間	期間を指定します。

6. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

7. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」、761 ページの「既知の脅威アクティビティのトークン変数」、および 763 ページの「ネットワークアクセス管理トークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」、761 ページの「既知の脅威アクティビティのトークン変数」、および 763 ページの「ネットワークアクセス管理トークン変数」を参照してください。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

8. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
9. [保存] をクリックします。

スパイウェア/グレーウェア検出 - 処理成功

スパイウェア/グレーウェア検出に設定したスパイウェア/グレーウェア検索の処理が成功したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[スパイウェア/グレーウェア検出 - 処理成功] をクリックします。

   [スパイウェア/グレーウェア検出 - 処理成功] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン 変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン 変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。

方法	説明
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

スパイウェア/グレーウェア検出 - さらに処理が必要です

スパイウェア/グレーウェア検出でさらに処理が必要なときに管理者に通知するには、次のイベント通知を設定します。

スパイウェア/グレーウェア検出に設定したスパイウェア/グレーウェア検索の処理が失敗/使用不可のときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[スパイウェア/グレーウェア検出 - さらに処理が必要です] をクリックします。

   [スパイウェア/グレーウェア検出 - さらに処理が必要です] 画面が表示されます。
4. 通知の受信者を選択します。

a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

b. [>] をクリックします。

選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

ウイルス検出 ― 1 次処理成功

ウイルス検出で 1 次処理が成功したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[ウイルス検出 ― 1 次処理成功] をクリックします。

   [ウイルス検出 ― 1 次処理成功] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン 変数」を参照してください。

方法	説明
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

ウイルス検出 ー 1 次処理失敗/2 次処理使用不可

ウイルス検出で 1 次処理が失敗し、2 次処理が使用できないときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[ウイルス検出 — 1 次処理失敗/2 次処理使用不可] をクリックします。

   [ウイルス検出 — 1 次処理失敗/2 次処理使用不可] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。

方法	説明
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

ウイルス検出 — 1 次処理/2 次処理失敗

ウイルス検出で 1 次処理も 2 次処理も失敗したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[ウイルス検出 — 1 次処理/2 次処理失敗] をクリックします。

   [ウイルス検出 — 1 次処理/2 次処理失敗] 画面が表示されます。
4. 通知の受信者を選択します。
   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。
   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

ウイルス検出 ー 2 次処理成功

ウイルス検出で 2 次処理が成功したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[ウイルス検出 ― 2 次処理成功] をクリックします。

   [ウイルス検出 ― 2 次処理成功] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン 変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン 変数」を参照してください。

方法	説明
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

ウイルスアウトブレークアラート

ウイルスアウトブレークが検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [既知の脅威アクティビティ] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[ウイルスアウトブレークアラート] をクリックします。

   [ウイルスアウトブレークアラート] 画面が表示されます。
4. 次の通知設定を指定します。

設定	説明
検出数	管理下の製品によって検出された脅威の数を入力します。
影響を受けたユーザ/エンドポイント	影響を受けたユーザ/エンドポイントの数を指定します。
期間	期間を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 761 ページの「既知の脅威アクティビティのトークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。

方法	説明
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

ネットワークアクセス管理イベント

[イベント通知] 画面を使用して、ネットワーク上で検出された Network VirusWall ポリシー違反または脆弱性に対する攻撃の兆候に関する通知を有効にし、設定します。

Network VirusWall ポリシー違反

Network VirusWall ポリシー違反が検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [ネットワークアクセス管理] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[Network VirusWall ポリシー違反] をクリックします。

   [Network VirusWall ポリシー違反] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

脆弱性に対する攻撃の兆候

Network VirusWall によって脆弱性に対する攻撃の兆候が検出されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [ネットワークアクセス管理] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[脆弱性に対する攻撃の兆候] をクリックします。

   [脆弱性に対する攻撃の兆候] 画面が表示されます。

4. 次の通知設定を指定します。

設定	説明
検出数	Network VirusWall が検出する脆弱性に対する攻撃の兆候の数を指定します。
期間	期間を指定します。
レポート元	脆弱性に対する攻撃の兆候を報告する Network VirusWall デバイスの数を指定します。

5. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

6. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 763 ページの「ネットワークアクセス管理トークン変数」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」および 763 ページの「ネットワークアクセス管理トークン変数」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

7. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
8. [保存] をクリックします。

その他の製品の挙動イベント

[イベント通知] 画面を使用して、ネットワーク上で検出されたその他の製品の挙動に関する通知を有効にし、設定します。

管理下の製品に到達不能

Apex Central と管理下の製品のサーバの間で通信エラーが発生したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [その他の製品の挙動] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[管理下の製品に到達不能] をクリックします。

   [管理下の製品に到達不能] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

サービス開始

サービスが開始されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [その他の製品の挙動] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[サービス開始] をクリックします。

   [サービス開始] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。

方法	説明
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

サービス停止

サービスが停止されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [その他の製品の挙動] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[サービス停止] をクリックします。

[サービス停止] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

リアルタイム検索停止

リアルタイム検索が停止されたときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [その他の製品の挙動] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[リアルタイム検索停止] をクリックします。

   [リアルタイム検索停止] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。

方法	説明
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

リアルタイム検索有効

リアルタイム検索が有効になったときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [その他の製品の挙動] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[リアルタイム検索有効] をクリックします。

[リアルタイム検索有効] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

アップデート

[イベント通知] 画面を使用して、コンポーネントのアップデートステータスに関する通知を有効にし、設定します。

スパムメール判定ルールアップデート成功

スパムメール判定ルールのアップデートが成功したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [アップデート] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[スパムメール判定ルールアップデート成功] をクリックします。

   [スパムメール判定ルールアップデート成功] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

スパムメール判定ルールアップデート失敗

スパムメール判定ルールのアップデートが失敗したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [アップデート] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[スパムメール判定ルールアップデート失敗] をクリックします。

   [スパムメール判定ルールアップデート失敗] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。

方法	説明
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

パターンファイル/テンプレートアップデート成功

パターンファイルまたはクリーンナップテンプレートのアップデートが 成功したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [アップデート] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[パターンファイル/テンプレートアップデート 成功] をクリックします。

   [パターンファイル/テンプレートアップデート 成功] 画面が表示されます。
4. 通知の受信者を選択します。
   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。
   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

パターンファイル/テンプレートアップデート失敗

パターンファイルまたはクリーンナップテンプレートのアップデートが 失敗したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [アップデート] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[パターンファイル/テンプレートアップデート 失敗] をクリックします。

   [パターンファイル/テンプレートアップデート 失敗] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。

方法	説明
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

検索エンジンアップデート成功

検索エンジンのアップデートが成功したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。
2. [アップデート] をクリックします。

   イベントのリストが表示されます。
3. [イベント] 列で、[検索エンジンアップデート成功] をクリックします。

   [検索エンジンアップデート成功] 画面が表示されます。
4. 通知の受信者を選択します。
   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

b. [>] をクリックします。

選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。

7. [保存] をクリックします。

検索エンジンのアップデート失敗

検索エンジンのアップデートに失敗したときに管理者に通知するには、次のイベント通知を設定します。

手順

1. [検出数] > [通知] > [イベント通知] に移動します。

   [イベント通知] 画面が表示されます。

2. [アップデート] をクリックします。

   イベントのリストが表示されます。

3. [イベント] 列で、[検索エンジンのアップデート失敗] をクリックします。

   [検索エンジンのアップデート失敗] 画面が表示されます。

4. 通知の受信者を選択します。

   a. [使用可能なユーザおよびグループ] リストから、連絡先グループまたはユーザアカウントを選択します。

   b. [>] をクリックします。

      選択した連絡先グループまたはユーザアカウントが [選択されたユーザおよびグループ] リストに表示されます。

5. 次の通知方法を有効にします (複数可)。

方法	説明
メール	メール通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [件名] フィールドと [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。
Windows イベントログ通知	通知テンプレートをカスタマイズするには、サポートされるトークン変数を使用するか、または [メッセージ] フィールドでテキストを変更します。 詳細については、752 ページの「通知メッセージのカスタマイズ」を参照してください。

方法	説明
SNMP トラップ通知	SNMP トラップ通知は Management Information Base (MIB) に格納されます。SNMP トラップ通知を表示するには、[通知] > [通知方法の設定] に移動し、[SNMP トラップ設定] で [MIB ファイルのダウンロード] をクリックします。
起動アプリケーション	アプリケーションファイルのフルパスおよびコマンドのパラメータを指定します。
Syslog 通知	Apex Central では、サポート対象の他社製品に直接 Syslog を転送できます。たとえば、Cisco Security Monitoring や Analysis and Response (MARS) などに対応しています。

6. 受信者がイベント通知を受信できるかどうかテストするには、[テスト] をクリックします。
7. [保存] をクリックします。

第 17 章

レポート

このセクションでは、Apex Central に登録されているすべての管理下の製品から収集したデータを使用してレポートを作成する方法について説明します。

次のトピックがあります。

レポートの概要

Apex Central では、すべての登録された管理下の製品からのデータを統合するレポートを生成、ダウンロード、および送信できます。複数の製品コンソールにログオンする必要はありません。

Apex Central を使用して、以下の処理を実行できます。

- 1 回限りのレポートを必要に応じて作成する。
- 予約レポートを追加して、ユーザ指定のスケジュールでレポートを自動的に生成して指定の受信者に送信する。
- データビューからカスタムレポートテンプレートを作成したり、事前定義済みカスタムテンプレートおよびデフォルトテンプレートを 使用したりする。
- カスタムタグ、フィルタ、重要なラベルが割り当てられたエンドポイントのカスタムレポートを生成する。

カスタムテンプレート

[カスタムテンプレート] 画面には、使用可能なすべてのカスタムレポートテンプレートのリストが表示されます。Apex Central は、使用できる事前定義済みカスタムテンプレートを用意しています。事前定義済みテンプレートをコピーして編集したり、特定のレポート要素を選択および設定して新規のテンプレートを作成したりできます。

注意

カスタムテンプレートは、特定の Apex Central ログに対応するデータビューを使用して、レポートデータの対象範囲を定義します。

詳細については、次のトピックを参照してください。

- 322 ページの「ログ名とデータビュー」
- 633 ページのデータビュー

次の表は、[カスタムテンプレート] 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
新しいカスタムテンプレートの追加	新しいカスタムテンプレートを作成するには、[追加] をクリックします。 詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。
カスタムテンプレートの削除	既存のテンプレートを選択して、[削除] をクリックします。
カスタムテンプレートの編集	編集する既存のテンプレートの名前をクリックします。 詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。
カスタムテンプレートのコピー	既存のテンプレートを選択して、[コピー] をクリックします。Apex Central は次の名前を使用して新しいテンプレートをリストに追加します。 <コピー元のテンプレート名>のコピー 詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。
カスタムテンプレートのインポート	適切な形式の XML レポートテンプレートを Apex Central にインポートするには、[インポート] をクリックします。
カスタムテンプレートのエクスポート	既存のテンプレートを選択して、[エクスポート] をクリックします。Apex Central は、テンプレートを XML 形式でエクスポートします。

カスタムテンプレートを追加または編集する

カスタムテンプレートを作成して、会社固有のレポートをさまざまな形式で生成できます。

手順

1. [レポート] > [レポート] > [カスタムテンプレート] に移動します。

   [カスタムテンプレート] 画面が表示されます。

2. テンプレートを追加、編集、またはコピーします。
   - 新しいテンプレートを追加するには、[追加] をクリックします。

     [レポートテンプレートの追加] 画面が表示されます。
   - 既存のテンプレートを編集するには、テンプレートの [名前] をクリックします。

     [レポートテンプレートの編集] 画面が表示されます。
   - 新しいテンプレートの生成に使用する既存のテンプレートのコピーを作成するには、次のようにします。
     a. 使用するテンプレートの [名前] の左側のチェックボックスをオンにします。
     b. [コピー] をクリックします。

        Apex Central は次の名前を使用して新しいテンプレートをリストに追加します。

        <コピー元のテンプレート名>のコピー
     c. 新しく追加されたテンプレートの名前をクリックします。

        [レポートテンプレートの編集] 画面が表示されます。
3. テンプレートに一意の [名前] を指定します。
4. (オプション) 新しいテンプレートの [説明] を入力します。
5. [作業パネル] で、レポート要素を使用可能な「行」にドラッグアンドドロップして、レポートのセクションレイアウトを設計します。

重要

各行には最大 3 つまでのレポート要素を使用できます。

ヒント

[作業パネル] が表示されない場合、[テンプレートの内容] の横の [作業パネルの表示] ボタンをクリックします。

表 17-1. レポート要素

テンプレート要素	説明
静的テキスト	ユーザ指定の内容のコンテナを指定します。  注意 静的テキストには、4,096 文字まで使用できます。 詳細については、427 ページの「[静的テキスト] レポート要素を設定する」を参照してください。
棒グラフ	カスタマイズ可能な棒グラフオブジェクトを挿入します。 詳細については、428 ページの「[棒グラフ] レポート要素を設定する」を参照してください。
折れ線グラフ	カスタマイズ可能な折れ線グラフオブジェクトを挿入します。 詳細については、431 ページの「[折れ線グラフ] レポート要素を設定する」を参照してください。
円グラフ	カスタマイズ可能な円グラフオブジェクトを挿入します。 詳細については、434 ページの「[円グラフ] レポート要素を設定する」を参照してください。
動的テーブル	カスタマイズ可能な動的テーブルオブジェクトまたはピボットテーブルオブジェクトを挿入します。 動的テーブルの情報は、水平か垂直のいずれかの方向で 2 つのデータフィールドを比較します。 詳細については、436 ページの「[動的テーブル] レポート要素を設定する」を参照してください。
グリッドテーブル	カスタマイズ可能なテーブルオブジェクトを挿入します。 グリッドテーブルの情報は、ログクエリにより表示される情報と同じです。 詳細については、439 ページの「[グリッドテーブル] レポート要素を設定する」を参照してください。

6. [改ページを上に挿入]、[行を上に挿入]、[行を下に挿入]、および [この行を削除] ボタンを使用して、レポートの行とページのレイアウトを整えます。

注意

同じ行に追加されるレポート要素は、テンプレートに追加した順に並んで表示されます。このようにして、複数のグラフを同じ行に表示できます。複数のグラフを同じページの別の行に表示するには、新しい行を挿入します。しかし改ページは挿入しないでください。

図 17-1. 棒グラフの上に静的テキストを表示するカスタムレポートテンプレートのセットアップ

7. [保存] をクリックします。

[静的テキスト] レポート要素を設定する

このタスクでは、[静的テキスト] レポート要素がカスタムレポートテンプレートの行にすでに追加済みであることを前提としています。

詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

手順

1. [静的テキスト] レポート要素で、[編集] をクリックします。

   [静的テキストの編集] 画面が表示されます。

2. [名前] フィールドに、テキストボックス要素のタイトルを指定します。

3. [メッセージ] フィールドに、メッセージ本文に表示する説明文を指定します。

   注意

   静的テキストには、4,096 文字まで使用できます。

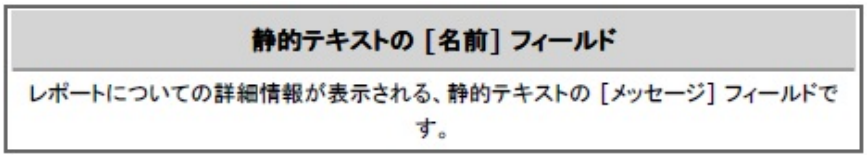


図 17-2. [静的テキスト] レポート出力例

4. [保存] をクリックして、[レポートテンプートの追加] および [レポートテンプレートの編集] 画面に戻ります。

[棒グラフ] レポート要素を設定する

このタスクでは、[棒グラフ] レポート要素がカスタムレポートテンプレートの行にすでに追加済みであることを前提としています。

詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

手順

1. [棒グラフ] レポート要素で、[編集] をクリックします。

   [棒グラフの編集] の [手順 1: データビュー] 画面が表示されます。

2. [データビュー] ディレクトリから、表示するレポートデータのタイプを選択します。

   詳細については、633 ページのデータビューを参照してください。

3. [次へ>] をクリックします。

   [手順 2: クエリ条件の設定] 画面が表示されます。

4. 表示されるデータをフィルタ処理するには、[カスタム条件] を選択します。

5. カスタムフィルタの [一致項目] ルールを指定します。

   - すべての条件: データは指定されたすべての条件に一致する必要があります。
   - いずれかの条件: データは指定されたいずれかの条件に一致する必要があります。

6. フィルタ条件を指定します。各条件は次の 3 つの部分で構成されます。

   - データタイプ: データビューによって返される列に相当します。
   - 演算子: データタイプの値と一致させたり、値を除外したりするために使用します。
   - 値: ドロップダウンコントロールから条件を選択したり、テキストボックスに値を指定したりします。

   注意

   選択したデータビュー、選択したデータタイプ、演算子に応じて表示されるオプションです。

   Apex Central では、最大 20 個のフィルタをサポートします。

7. プラス (+) およびマイナス (−) コントロールを使用して条件の追加および削除を行います。

8. [次へ>] をクリックします。

   [手順 3: 設計の指定] 画面が表示されます。

9. グラフのタイトルとして使用する名前を指定します。

10. [ドラッグ可能フィールド] リストから、次の場所に表示されているデータをドラッグアンドドロップします。

    - データフィールド: グラフに表示するデータの総数を指定します。
    - カテゴリフィールド ― グラフ内でのデータの区切り方法を指定します。
    - シリーズフィールド: 比較として使用される垂直軸と水平軸に表示するデータのタイプを定義します。

11. [データプロパティ] セクションで、以下の項目を設定します。

    - 集計基準: データを表示する方法。
      - インスタンスの総数: 重複する結果がデータに含まれます。
      - 一意のインスタンス数: 重複する結果のタイプのインスタンスが 1 つだけ表示されます。

      たとえば、エンドポイントが「VirusA」の 5 個のインスタンスと「VirusB」の 3 個のインスタンスをデータで検出する場合、グラフ上の検出回数には次の値が表示されます。

      - インスタンスの総数 = 8 (ウイルス検出数。ウイルスの名前は問わない)
      - 一意のインスタンス数 = 2 (一意のウイルスの種類。出現頻度は問わない)

12. [カテゴリプロパティ] セクションで、以下の項目を設定します。

    - グラフの水平軸に表示される [ラベル] の名前を指定します。
    - ソートの順序と方向を選択します。
      - 集計値: データのカウント値に基づいてソートします。
      - カテゴリ名: カテゴリ名に基づいてアルファベット順にソートします。

- レポートに表示されるデータをフィルタ処理するには、[集計結果のフィルタ] チェックボックスをオンにします。
  - 表示する項目の最大数を指定します。
  - 「その他」カテゴリの残りのすべてのデータをグループ化するには、[残りの項目の集計] を有効にします。

13. [シリーズプロパティ] セクションで、データシリーズを説明するために表示される [ラベル名] を指定します。
14. [保存] をクリックします。

    アップデートしたグラフ設定が適用された [レポートテンプレートの追加] および [レポートテンプレートの編集] 画面が表示されます。

[折れ線グラフ] レポート要素を設定する

このタスクでは、[折れ線グラフ] レポート要素がカスタムレポートテンプレートの行にすでに追加済みであることを前提としています。

詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

手順

1. [折れ線グラフ] レポート要素で、[編集] をクリックします。

   [折れ線グラフの編集] の [手順 1: データビュー] 画面が表示されます。
2. [データビュー] ディレクトリから、表示するレポートデータのタイプを選択します。

   詳細については、633 ページのデータビューを参照してください。
3. [次へ>] をクリックします。

   [手順 2: クエリ条件の設定] 画面が表示されます。
4. 表示されるデータをフィルタ処理するには、[カスタム条件] を選択します。

5. カスタムフィルタの [一致項目] ルールを指定します。
   - すべての条件: データは指定されたすべての条件に一致する必要があります。
   - いずれかの条件: データは指定されたいずれかの条件に一致する必要があります。
6. フィルタ条件を指定します。各条件は次の 3 つの部分で構成されます。
   - データタイプ: データビューによって返される列に相当します。
   - 演算子: データタイプの値と一致させたり、値を除外したりするために使用します。
   - 値: ドロップダウンコントロールから条件を選択したり、テキストボックスに値を指定したりします。

   注意

   選択したデータビュー、選択したデータタイプ、演算子に応じて表示されるオプションです。

   Apex Central では、最大 20 個のフィルタをサポートします。
7. プラス (+) およびマイナス (−) コントロールを使用して条件の追加および削除を行います。
8. [次へ>] をクリックします。

   [手順 3: 設計の指定] 画面が表示されます。
9. グラフのタイトルとして使用する名前を指定します。
10. [ドラッグ可能フィールド] リストから、次の場所に表示されているデータをドラッグアンドドロップします。
    - データフィールド: グラフの垂直軸のデータ値を定義します。
    - カテゴリフィールド: グラフの水平軸のデータ値を定義します。
    - シリーズフィールド: 比較として使用される垂直軸と水平軸に表示するデータのタイプを定義します。

11. [データプロパティ] セクションで、以下の項目を設定します。
    - 値ラベル: グラフの垂直に表示されるラベル。
    - 集計基準: データを表示する方法。
        - インスタンスの総数: 重複する結果がデータに含まれます。
        - 一意のインスタンス数: 重複する結果のタイプのインスタンスが 1 つだけ表示されます。

        たとえば、エンドポイントが「VirusA」の 5 個のインスタンスと「VirusB」の 3 個のインスタンスをデータで検出する場合、グラフ上の検出回数には次の値が表示されます。
        - インスタンスの総数 = 8 (ウイルス検出数。ウイルスの名前は問わない)
        - 一意のインスタンス数 = 2 (一意のウイルスの種類。出現頻度は問わない)
12. [カテゴリプロパティ] セクションで、以下の項目を設定します。
    - グラフの水平軸に表示される [ラベル] の名前を指定します。
    - ソートの順序と方向を選択します。
        - 集計値: データのカウント値に基づいてソートします。
        - カテゴリ名: カテゴリ名に基づいてアルファベット順にソートします。
    - レポートに表示されるデータをフィルタ処理するには、[集計結果のフィルタ] チェックボックスをオンにします。
        - 表示する項目の最大数を指定します。
        - 「その他」カテゴリの残りのすべてのデータをグループ化するには、[残りの項目の集計] を有効にします。
13. [シリーズプロパティ] セクションで、データシリーズを説明するために表示される [ラベル名] を指定します。
14. [保存] をクリックします。

アップデートしたグラフ設定が適用された [レポートテンプレートの追加] および [レポートテンプレートの編集] 画面が表示されます。

[円グラフ] レポート要素を設定する

このタスクでは、[円グラフ] レポート要素がカスタムレポートテンプレートの行にすでに追加済みであることを前提としています。

詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

手順

1. [円グラフ] レポート要素で、[編集] をクリックします。

   [円グラフの編集] の [手順 1: データビュー] 画面が表示されます。

2. [データビュー] ディレクトリから、表示するレポートデータのタイプを選択します。

   詳細については、633 ページのデータビューを参照してください。

3. [次へ>] をクリックします。

   [手順 2: クエリ条件の設定] 画面が表示されます。

4. 表示されるデータをフィルタ処理するには、[カスタム条件] を選択します。

5. カスタムフィルタの [一致項目] ルールを指定します。

   - すべての条件: データは指定されたすべての条件に一致する必要があります。
   - いずれかの条件: データは指定されたいずれかの条件に一致する必要があります。

6. フィルタ条件を指定します。各条件は次の 3 つの部分で構成されます。

   - データタイプ: データビューによって返される列に相当します。

- 演算子: データタイプの値と一致させたり、値を除外したりするために使用します。
- 値: ドロップダウンコントロールから条件を選択したり、テキストボックスに値を指定したりします。

注意

選択したデータビュー、選択したデータタイプ、演算子に応じて表示されるオプションです。

Apex Central では、最大 20 個のフィルタをサポートします。

7. プラス (+) およびマイナス (−) コントロールを使用して条件の追加および削除を行います。
8. [次へ>] をクリックします。

   [手順 3: 設計の指定] 画面が表示されます。
9. グラフのタイトルとして使用する名前を指定します。
10. [ドラッグ可能フィールド] リストから、次の場所に表示されているデータをドラッグアンドドロップします。
    - データフィールド: グラフに表示するデータの総数を指定します。
    - カテゴリフィールド – グラフ内でのデータの区切り方法を指定します。
11. [データプロパティ] セクションで、以下の項目を設定します。
    - 集計基準: データを表示する方法。
      - インスタンスの総数: 重複する結果がデータに含まれます。
      - 一意のインスタンス数: 重複する結果のタイプのインスタンスが 1 つだけ表示されます。

      たとえば、エンドポイントが「VirusA」の 5 個のインスタンスと「VirusB」の 3 個のインスタンスをデータで検出する場合、グラフ上の検出回数には次の値が表示されます。

- インスタンスの総数 = 8 (ウイルス検出数。ウイルスの名前は問わない)
- 一意のインスタンス数 = 2 (一意のウイルスの種類。出現頻度は問わない)

12. [カテゴリプロパティ] セクションで、以下の項目を設定します。
    - グラフの水平軸に表示される [ラベル] の名前を指定します。
    - ソートの順序と方向を選択します。
        - 集計値: データのカウント値に基づいてソートします。
        - カテゴリ名: カテゴリ名に基づいてアルファベット順にソートします。
    - レポートに表示されるデータをフィルタ処理するには、[集計結果のフィルタ] チェックボックスをオンにします。
        - 表示する項目の最大数を指定します。
        - 「その他」カテゴリの残りのすべてのデータをグループ化するには、[残りの項目の集計] を有効にします。
13. [保存] をクリックします。

    アップデートしたグラフ設定が適用された [レポートテンプレートの追加] および [レポートテンプレートの編集] 画面が表示されます。

[動的テーブル] レポート要素を設定する

このタスクでは、[動的テーブル] レポート要素がカスタムレポートテンプレートの行にすでに追加済みであることを前提としています。

詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

手順

1. [動的テーブル] レポート要素で、[編集] をクリックします。

[動的テーブルの編集] の [手順 1: データビュー] 画面が表示されます。

2. [データビュー] ディレクトリから、表示するレポートデータのタイプを選択します。

   詳細については、633 ページのデータビューを参照してください。

3. [次へ>] をクリックします。

   [手順 2: クエリ条件の設定] 画面が表示されます。

4. 表示されるデータをフィルタ処理するには、[カスタム条件] を選択します。

5. カスタムフィルタの [一致項目] ルールを指定します。

   - すべての条件: データは指定されたすべての条件に一致する必要があります。
   - いずれかの条件: データは指定されたいずれかの条件に一致する必要があります。

6. フィルタ条件を指定します。各条件は次の 3 つの部分で構成されます。

   - データタイプ: データビューによって返される列に相当します。
   - 演算子: データタイプの値と一致させたり、値を除外したりするために使用します。
   - 値: ドロップダウンコントロールから条件を選択したり、テキストボックスに値を指定したりします。

   注意

   選択したデータビュー、選択したデータタイプ、演算子に応じて表示されるオプションです。

   Apex Central では、最大 20 個のフィルタをサポートします。

7. プラス (+) およびマイナス (−) コントロールを使用して条件の追加および削除を行います。

8. [次へ>] をクリックします。

   [手順 3: 設計の指定] 画面が表示されます。

9. グラフのタイトルとして使用する名前を指定します。
10. [ドラッグ可能フィールド] リストから、次の場所に表示されているデータをドラッグアンドドロップします。
    - 行フィールド: テーブル内のデータの水平方向への区切り方法を定義します。
    - 列フィールド: テーブル内のデータの垂直方向への区切り方法を定義します。
    - データフィールド: 表内で指定された [行フィールド] または [列フィールド] に表示されるデータ値を定義します。

    重要

    [動的テーブル] レポート要素には、1 つの [データフィールド] と、1 つの [行フィールド] または 1 つの [列フィールド] のいずれかが必要です。
11. [データプロパティ] セクションで、以下の項目を設定します。
    - データフィールドのタイトル: データフィールドのラベル
    - 集計基準: データを表示する方法。
        - インスタンスの総数: 重複する結果がデータに含まれます。
        - 一意のインスタンス数: 重複する結果のタイプのインスタンスが 1 つだけ表示されます。

        たとえば、エンドポイントが「VirusA」の 5 個のインスタンスと「VirusB」の 3 個のインスタンスをデータで検出する場合、グラフ上の検出回数には次の値が表示されます。
        - インスタンスの総数 = 8 (ウイルス検出数。ウイルスの名前は問わない)
        - 一意のインスタンス数 = 2 (一意のウイルスの種類。出現頻度は問わない)
12. [行プロパティ] セクションで、以下の項目を設定します。
    - [行ヘッダのタイトル] を指定します。

- ソートの順序と方向を選択します。
  - 集計値: データのカウント値に基づいてソートします。
  - ヘッダのタイトル: カテゴリ名に基づいてアルファベット順にソートします。
- レポートに表示されるデータをフィルタ処理するには、[集計結果のフィルタ] チェックボックスをオンにします。
  - 表示する項目の最大数を指定します。
  - 「その他」カテゴリの残りのすべてのデータをグループ化するには、[残りの項目の集計] を有効にします。

13. [列プロパティ] セクションで、以下の項目を設定します。
    - [列ヘッダのタイトル] を指定します。
    - ソートの順序と方向を選択します。
      - 集計値: データのカウント値に基づいてソートします。
      - ヘッダのタイトル: カテゴリ名に基づいてアルファベット順にソートします。
    - レポートに表示されるデータをフィルタ処理するには、[集計結果のフィルタ] チェックボックスをオンにします。
      - 表示する項目の最大数を指定します。
      - 「その他」カテゴリの残りのすべてのデータをグループ化するには、[残りの項目の集計] を有効にします。
14. [保存] をクリックします。

    アップデートしたグラフ設定が適用された [レポートテンプレートの追加] および [レポートテンプレートの編集] 画面が表示されます。

[グリッドテーブル] レポート要素を設定する

このタスクでは、[グリッドテーブル] レポート要素がカスタムレポートテンプレートの行にすでに追加済みであることを前提としています。

詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

手順

1. [グリッドテーブル] レポート要素で、[編集] をクリックします。

   [グリッドテーブルの編集] の [手順 1: データビュー] 画面が表示されます。

2. [データビュー] ディレクトリから、表示するレポートデータのタイプを選択します。

   詳細については、633 ページのデータビューを参照してください。

3. [次へ>] をクリックします。

   [手順 2: クエリ条件の設定] 画面が表示されます。

4. 表示されるデータをフィルタ処理するには、[カスタム条件] を選択します。

5. カスタムフィルタの [一致項目] ルールを指定します。

   - すべての条件: データは指定されたすべての条件に一致する必要があります。
   - いずれかの条件: データは指定されたいずれかの条件に一致する必要があります。

6. フィルタ条件を指定します。各条件は次の 3 つの部分で構成されます。

   - データタイプ: データビューによって返される列に相当します。
   - 演算子: データタイプの値と一致させたり、値を除外したりするために使用します。
   - 値: ドロップダウンコントロールから条件を選択したり、テキストボックスに値を指定したりします。

注意

選択したデータビュー、選択したデータタイプ、演算子に応じて表示されるオプションです。

Apex Central では、最大 20 個のフィルタをサポートします。

7. プラス (+) およびマイナス (−) コントロールを使用して条件の追加および削除を行います。
8. [次へ>] をクリックします。

   [手順 3: 設計の指定] 画面が表示されます。
9. グラフのタイトルとして使用する名前を指定します。
10. レポートに表示するデータフィールドを選択します。

注意

初期設定では、指定されたデータビューのすべてのフィールドが選択されています。

11. [選択されたフィールド] の [ソート] の順序を選択します。
12. [数量の表示] を選択して、レポートに含める項目の最大数を定義します。
13. [保存] をクリックします。

    アップデートしたグラフ設定が適用された [レポートテンプレートの追加] および [レポートテンプレートの編集] 画面が表示されます。

1 回限りのレポート

[1 回限りのレポート] 画面には、ネットワークに関してこれまでに生成した 1 回限りのレポートすべてのリストが表示されます。この画面を使用して、1 回限りのレポートを新規作成したり、これまでに生成した 1 回限りのレポートを確認したりできます。

次の表は、[1 回限りのレポート] 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
新しい 1 回限りのレポートの追加	[追加] をクリックして、新しい 1 回限りのレポートを作成します。 詳細については、442 ページの「1 回限りのレポートを作成する」を参照してください。
1 回限りのレポートの削除	既存の 1 回限りのレポートを選択し、[削除] をクリックします。
メール受信者への 1 回限りのレポートの転送	既存の 1 回限りのレポートを選択し、[通知] をクリックして、指定した受信者にレポートを添付ファイルとしてメール送信します。
生成した 1 回限りのレポートの確認	表示するレポートの [表示] 列の [表示] リンクをクリックします。
1 回限りのレポートプロファイルの確認	これまでに生成した 1 回限りのレポートの名前をクリックして、レポートプロファイルを確認します。 **注意** これまでに生成した 1 回限りのレポートのプロファイルは編集できません。

1 回限りのレポートを作成する

[1 回限りのレポート] 画面を使用して、レポートをオンデマンドで生成できます。レポートを作成するときには、カスタムテンプレートとデフォルトテンプレートのどちらを使用するか指定してください。

手順

1. [レポート] > [レポート] > [1 回限りのレポート] に移動します。

   [1 回限りのレポート] 画面が表示されます。

2. [追加] をクリックします。

   [1 回限りのレポートの追加] の [手順 1: 内容] 画面が表示されます。

3. [名前] にレポートの名前を入力します。

4. (オプション) [説明] フィールドにレポートの説明を入力します。
5. [レポート内容] セクションで、次のテンプレートタイプのいずれかを選択します。
   - カスタムテンプレート: 1 つ以上のカスタムレポートテンプレートを選択します。

     注意

     複数のカスタムテンプレートを選択すると、単一のレポートが生成され、そこに選択したすべてのテンプレートの形式のデータが表示されます。

     カスタムレポートテンプレートの詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。
   - デフォルトテンプレート: トレンドマイクロが提供する 1 つ以上のデフォルトテンプレートを 選択します。
     a. [レポートのカテゴリ] ドロップダウンからデフォルトテンプレートを選択します。
     b. レポートに表示するデータを選択して、対応するパラメータを指定します。
6. レポートの出力形式を選択します。
   - カスタムテンプレートレポート 出力形式:
     - Adobe PDF 形式 (*.pdf)
     - HTML 形式 (*.html)
     - XML 形式 (*.xml)
     - CSV 形式 (*.csv)
   - デフォルトテンプレートレポート 出力形式:
     - Adobe PDF 形式 (*.pdf)
     - Microsoft Word 形式 (*.docx)

- Microsoft Excel 形式 (*.xlsx)

7. [次へ] をクリックします。

   [1 回限りのレポートの追加] の [手順 2: 対象] 画面が表示されます。

8. 次のいずれかの表示を使用して対象を指定します。

   - 製品ディレクトリ: レポート情報を提供する管理下の製品または管理下の製品を含むフォルダを選択します。
   - タグとフィルタ: レポート情報を提供するユーザまたはエンドポイントを含むカスタムタグ、フィルタ、または重要度ラベルを最大 10 個選択します。

   注意

   - [タグとフィルタ] 表示は、カスタムレポートテンプレートでのみ使用できます。
   - あるユーザアカウントが生成したレポートには、そのユーザアカウントが表示権限を持つエンドポイントのデータのみが含まれます。ユーザアカウントに表示権限のないエンドポイントを含むタグ、フィルタ、または重要度ラベルを選択した場合、権限のないエンドポイントのデータは生成されたレポートから除外されます。
   - [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。

9. [次へ] をクリックします。

   [1 回限りのレポートの追加] の [手順 3: 期間] 画面が表示されます。

10. レポートの期間を指定します。

11. [次へ] をクリックします。

    [1 回限りのレポートの追加] の [手順 4: メッセージの内容と受信者] 画面が表示されます。

12. (オプション) 選択した受信者にレポートを添付ファイルとしてメール送信します。
    a. [件名] フィールドに、レポートが含まれるメールのタイトルを入力します。
    b. [メッセージ] フィールドに、レポートの説明を入力します。
    c. [レポートを添付ファイルとしてメール送信する] チェックボックスをオンにして、指定した受信者にレポートを送信します。
    d. 連絡先グループまたはユーザアカウントを選択します。
    e. >> をクリックします。

       選択した連絡先グループまたはユーザアカウントが受信者リストに表示されます。
13. [完了] をクリックします。

    [1 回限りのレポート] 画面が表示され、新しく追加されたレポート生成タスクが示されます。
14. 生成されたレポートを表示するには、次のようにします。
    a. 表示する生成されたレポートの [表示] 列の [表示] リンクをクリックします。
    b. 生成されたレポートのファイルを開くか、または保存します。

1 回限りのレポートの表示

[1 回限りのレポート] 画面を使用して、これまでに生成した 1 回限りのレポートを表示できます。

手順

1. [レポート] > [レポート] > [1 回限りのレポート] に移動します。

   [1 回限りのレポート] 画面が表示されます。

2. 表示する生成されたレポートの [表示] 列の [表示] リンクをクリックします。
3. 生成されたレポートのファイルを開くか、または保存します。

予約レポート

[予約レポート] 画面には、ユーザ指定のスケジュールで自動的に生成されるすべてのレポートのリストが表示されます。この画面を使用して、これまでに設定した予約レポートに関する基本情報を確認したり、新しい予約レポートを追加したり、予約レポートを有効化/無効化したりできます。

次の表は、[予約レポート] 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
新しい予約レポートプロファイルの追加	[追加] をクリックして、新しい予約レポートプロファイルを作成します。 詳細については、447 ページの「予約レポートの追加」を参照してください。
予約レポートプロファイルの編集	編集する既存の予約レポートプロファイルの名前をクリックします。 詳細については、451 ページの「予約レポートを編集する」を参照してください。
予約レポートプロファイルのコピー	1 つまたは複数の既存予約レポートプロファイルを選択し、[コピー] をクリックして選択したプロファイルを複製します。 コピーした予約レポートプロファイルの名前をクリックします。 詳細については、451 ページの「予約レポートを編集する」を参照してください。
予約レポートプロファイルの削除	既存の予約レポートプロファイルを選択し、[削除] をクリックします。
これまでに生成した予約レポートの確認	確認するレポートの [履歴] 列の [表示] リンクをクリックします。 詳細については、455 ページの「予約レポートの表示」を参照してください。

タスク	説明
予約レポートの有効化または無効化	• 予約レポートを無効にするには、[有効にする] 列の有効化 () アイコンをクリックします。 • 予約レポートを有効にするには、[有効にする] 列の無効化 () アイコンをクリックします。  注意 新しく追加した予約レポートプロファイルは初期設定で有効です。

予約レポートの追加

[予約レポート] 画面を使用して、ユーザ指定のスケジュールでレポートを自動生成します。予約レポートを追加するときには、カスタムテンプレートとデフォルトテンプレートのどちらを使用するか指定してください。

手順

1. [レポート] > [レポート] > [予約レポート] に移動します。

   [予約レポート] 画面が表示されます。

2. [追加] をクリックします。

   [予約レポートの追加] の [手順 1: 内容] 画面が表示されます。

3. [名前] にレポートの名前を入力します。

4. (オプション) [説明] フィールドにレポートの説明を入力します。

5. [レポート内容] セクションで、次のテンプレートタイプのいずれかを選択します。

   • カスタムテンプレート: 1 つ以上のカスタムレポートテンプレートを選択します。

> **注意**
>
> 複数のカスタムテンプレートを選択すると、単一のレポートが生成され、そこに選択したすべてのテンプレートの形式のデータが表示されます。
>
> カスタムレポートテンプレートの詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

- デフォルトテンプレート: トレンドマイクロが提供する 1 つ以上のデフォルトテンプレートを選択します。

  a. [レポートのカテゴリ] ドロップダウンからデフォルトテンプレートを選択します。

  b. レポートに表示するデータを選択して、対応するパラメータを指定します。

6. レポートの出力形式を選択します。
   - カスタムテンプレートレポート出力形式:
     - Adobe PDF 形式 (*.pdf)
     - HTML 形式 (*.html)
     - XML 形式 (*.xml)
     - CSV 形式 (*.csv)
   - デフォルトテンプレートレポート出力形式:
     - Adobe PDF 形式 (*.pdf)
     - Microsoft Word 形式 (*.docx)
     - Microsoft Excel 形式 (*.xlsx)
7. [次へ] をクリックします。

   [予約レポートの追加] の [手順 2: 対象] 画面が表示されます。
8. 次のいずれかの表示を使用して対象を指定します。
   - 製品ディレクトリ: レポート情報を提供する管理下の製品または管理下の製品を含むフォルダを選択します。

- タグとフィルタ: レポート情報を提供するユーザまたはエンドポイントを含むカスタムタグ、フィルタ、または重要度ラベルを最大 10 個選択します。

  注意

  - [タグとフィルタ] 表示は、カスタムレポートテンプレートでのみ使用できます。
  - あるユーザアカウントが生成したレポートには、そのユーザアカウントが表示権限を持つエンドポイントのデータのみが含まれます。ユーザアカウントに表示権限のないエンドポイントを含むタグ、フィルタ、または重要度ラベルを選択した場合、権限のないエンドポイントのデータは生成されたレポートから除外されます。
  - [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。

9. [次へ] をクリックします。

   [予約レポートの追加] の [手順 3: 実行間隔] 画面が表示されます。

10. レポートの生成頻度を指定します。

    - 指定日数ごと: 選択に応じて、1 ～ 6 日ごとに生成されます。
    - 毎週: 毎週、指定された曜日に生成されます。
    - 隔週: 隔週で、指定された曜日に生成されます。
    - 毎月: 毎月の 1 日、5 日、10 日、15 日、20 日、25 日、または最終日、から指定された日に生成されます。

11. データの範囲を指定します。

    - レポートに指定した [予約開始] の時刻までのデータを含める ―レポートには最高 23 時間までのデータを格納できます。これは週次や月次のレポートに若干影響します。一方、[予約開始] に指定する時

刻によっては、「日次」レポートはほぼ 2 日分のデータを格納できます。

- レポートに前日の 23:59:59 までのデータを含める ―レポートのデータ収集は午前 0 時直前に停止します。レポートの期間は正確な期間になります。たとえば、「日次」レポートでは 24 時間になります。ただし、最新のデータは格納されません。

12. 予約を開始する日時を指定します。
    - ただちに開始― レポートの予約実行は、レポートが有効にされた直後に開始されます。
    - 開始日時― レポートの予約実行は、ここで指定された日時に開始されます。

    ヒント

    [yyyy/mm/dd] の横にあるカレンダーアイコンをクリックすると 、動的なカレンダーを使用して日付範囲を指定できます。

13. [次へ] をクリックします。

    [予約レポートの追加] の [手順 4: メッセージの内容と受信者] 画面が表示されます。

14. (オプション) 選択した受信者にレポートを添付ファイルとしてメール送信します。
    a. [件名] フィールドに、レポートが含まれるメールのタイトルを入力します。
    b. [メッセージ] フィールドに、レポートの説明を入力します。
    c. [レポートを添付ファイルとしてメール送信する] チェックボックスをオンにして、指定した受信者にレポートを送信します。
    d. 連絡先グループまたはユーザアカウントを選択します。
    e. >> をクリックします。

       選択した連絡先グループまたはユーザアカウントが受信者リストに表示されます。

15. [完了] をクリックします。

    [予約レポート] 画面が表示され、新しく追加されたレポート生成タスクが示されます。

    注意

    初期設定では、新しく追加された予約レポートは Apex Central によって有効にされます。

16. 生成されたレポートを表示するには、次のようにします。

    a. 表示する予約レポートの [履歴] 列の [表示] リンクをクリックします。

       [予約レポート履歴] 画面が表示されます。

    b. 表示する生成されたレポートの [表示] 列の [表示] リンクをクリックします。

       ヒント

       予約レポートが生成されていない場合、[生成] ボタンをクリックして、予約レポートの設定に基づいてクイックレポートを作成します。

    c. 生成されたレポートのファイルを開くか、または保存します。

予約レポートを編集する

[予約レポート] 画面を使用して、ユーザ指定のスケジュールでレポートを自動生成します。予約レポートを追加するときには、カスタムテンプレートとデフォルトテンプレートのどちらを使用するか指定してください。

手順

1. [レポート] > [レポート] > [予約レポート] に移動します。

   [予約レポート] 画面が表示されます。

2. 予約レポートプロファイルの名前をクリックします。

   [予約レポートの編集] の [手順 1: 内容] 画面が表示されます。

3. [名前] にレポートの名前を入力します。

4. (オプション) [説明] フィールドにレポートの説明を入力します。

5. [レポート内容] セクションで、次のテンプレートタイプのいずれかを選択します。

   - カスタムテンプレート: 1 つ以上のカスタムレポートテンプレートを選択します。

     注意

     複数のカスタムテンプレートを選択すると、単一のレポートが生成され、そこに選択したすべてのテンプレートの形式のデータが表示されます。

     カスタムレポートテンプレートの詳細については、423 ページの「カスタムテンプレートを追加または編集する」を参照してください。

   - デフォルトテンプレート: トレンドマイクロが提供する 1 つ以上のデフォルトテンプレートを選択します。

     a. [レポートのカテゴリ] ドロップダウンからデフォルトテンプレートを選択します。

     b. レポートに表示するデータを選択して、対応するパラメータを指定します。

6. レポートの出力形式を選択します。

   - カスタムテンプレートレポート出力形式:
     - Adobe PDF 形式 (*.pdf)
     - HTML 形式 (*.html)
     - XML 形式 (*.xml)
     - CSV 形式 (*.csv)

- デフォルトテンプレートレポート出力形式:
  - Adobe PDF 形式 (*.pdf)
  - Microsoft Word 形式 (*.docx)
  - Microsoft Excel 形式 (*.xlsx)

7. [次へ] をクリックします。

   [予約レポートの編集] の [手順 2: 対象] 画面が表示されます。

8. 次のいずれかの表示を使用して対象を指定します。
   - 製品ディレクトリ: レポート情報を提供する管理下の製品または管理下の製品を含むフォルダを選択します。
   - タグとフィルタ: レポート情報を提供するユーザまたはエンドポイントを含むカスタムタグ、フィルタ、または重要度ラベルを最大 10 個選択します。

   注意
   - [タグとフィルタ] 表示は、カスタムレポートテンプレートでのみ使用できます。
   - あるユーザアカウントが生成したレポートには、そのユーザアカウントが表示権限を持つエンドポイントのデータのみが含まれます。ユーザアカウントに表示権限のないエンドポイントを含むタグ、フィルタ、または重要度ラベルを選択した場合、権限のないエンドポイントのデータは生成されたレポートから除外されます。
   - [ユーザ/エンドポイントディレクトリ] 画面でタグ、フィルタ、または重要度ラベルを編集すると、ログクエリやレポートで使用されている対応するタグ、フィルタ、重要度ラベルも変更されます。たとえば、[ユーザ/エンドポイントディレクトリ] 画面でカスタムフィルタからあるエンドポイントを削除すると、そのフィルタを使用するログクエリや生成されたレポートから削除されたエンドポイントのデータが除外されます。

9. [次へ] をクリックします。

   [予約レポートの編集] の [手順 3: 実行間隔] 画面が表示されます。

10. レポートの生成頻度を指定します。
    - 指定日数ごと: 選択に応じて、1 ～ 6 日ごとに生成されます。
    - 毎週: 毎週、指定された曜日に生成されます。
    - 隔週: 隔週で、指定された曜日に生成されます。
    - 毎月: 毎月の 1 日、5 日、10 日、15 日、20 日、25 日、または最終日、から指定された日に生成されます。
11. データの範囲を指定します。
    - レポートに指定した [予約開始] の時刻までのデータを含める ―レポートには最高 23 時間までのデータを格納できます。これは週次や月次のレポートに若干影響します。一方、[予約開始] に指定する時刻によっては、「日次」レポートはほぼ 2 日分のデータを格納できます。
    - レポートに前日の 23:59:59 までのデータを含める ―レポートのデータ収集は午前 0 時直前に停止します。レポートの期間は正確な期間になります。たとえば、「日次」レポートでは 24 時間になります。ただし、最新のデータは格納されません。
12. 予約を開始する日時を指定します。
    - ただちに開始― レポートの予約実行は、レポートが有効にされた直後に開始されます。
    - 開始日時― レポートの予約実行は、ここで指定された日時に開始されます。

    ヒント

    [yyyy/mm/dd] の横にあるカレンダーアイコンをクリックすると 、動的なカレンダーを使用して日付範囲を指定できます。
13. [次へ] をクリックします。

    [予約レポートの編集] の [手順 4: メッセージの内容と受信者] 画面が表示されます。
14. (オプション) 選択した受信者にレポートを添付ファイルとしてメール送信します。

a. [件名] フィールドに、レポートが含まれるメールのタイトルを入力します。

b. [メッセージ] フィールドに、レポートの説明を入力します。

c. [レポートを添付ファイルとしてメール送信する] チェックボックスをオンにして、指定した受信者にレポートを送信します。

d. 連絡先グループまたはユーザアカウントを選択します。

e. >> をクリックします。

選択した連絡先グループまたはユーザアカウントが受信者リストに表示されます。

15. [完了] をクリックします。

[予約レポート] 画面が表示され、新しく追加されたレポート生成タスクが示されます。

予約レポートの表示

[予約レポート] 画面を使用して、これまでに生成した予約レポートを表示できます。

手順

1. [レポート] > [レポート] > [予約レポート] に移動します。

[予約レポート] 画面が表示されます。

2. 表示する予約レポートの [履歴] 列の [表示] リンクをクリックします。

[予約レポート履歴] 画面が表示されます。

3. 表示する生成されたレポートの [表示] 列の [表示] リンクをクリックします。

ヒント

予約レポートが生成されていない場合、[生成] ボタンをクリックして、予約レポートの設定に基づいてクイックレポートを作成します。

4. 生成されたレポートのファイルを開くか、または保存します。

レポート管理の設定

レポートの最大数に達したときにレポートを削除するには、[レポート管理] を設定します。

手順

1. [レポート] > [レポート] > [レポート管理] に移動します。

   [レポート管理] 画面が表示されます。

2. 1 回限りのレポートと予約レポートの最大保存数を指定します。

3. [保存] をクリックします。

ユーザのレポートを表示する

[ユーザのレポート] 画面には、現在のユーザが生成したすべてのレポートのリストが表示されます。現在のユーザと同じグループに属するその他のユーザが生成したレポートも確認できます。

手順

1. [レポート] > [レポート] > [ユーザのレポート]に移動します。

   [ユーザのレポート] 画面が表示されます。

2. 表示する生成されたレポートの [表示] 列の [表示] リンクをクリックします。

3. 生成されたレポートのファイルを開くか、または保存します。

第 18 章

情報漏えい対策イベント

情報漏えい対策コンプライアンス責任者やイベントレビューアは、イベント情報のレビューおよび更新に Apex Central を使用します。

次のトピックがあります。

管理者のタスク

イベントレビューを処理できるようにするために、Apex Central 管理者があらかじめ完了しておく必要があるタスクがあります。次の表に、このような必須のタスクと参照先をまとめます。

表 18-1. 管理者のタスク

タスク	参照先
Active Directory に対するマネージャ情報の設定	459 ページの「Active Directory ユーザにマネージャ情報を設定する」
ユーザ情報を取得するための、Active Directory の統合の設定	123 ページの Active Directory とコンプライアンスの設定
情報漏えい対策イベント調査専用のユーザアカウントの作成 情報漏えい対策イベントをレビューするために、次のユーザの役割を割り当てて権限を付与します。 ・ 管理者および情報漏えい対策コンプライアンス責任者 ・ 情報漏えい対策コンプライアンス責任者 ・ 情報漏えい対策イベントレビューア 注意 情報漏えい対策コンプライアンス責任者および情報漏えい対策イベントレビューアの役割は、Active Directory ユーザにのみ割り当てることができます。	・ 459 ページの「情報漏えい対策ユーザの役割について」 ・ 108 ページの「初期設定のユーザの役割」 ・ 97 ページの「ユーザアカウントの追加」
[予約イベント概要] および [イベント詳細のアップデート] 通知の設定	・ 375 ページの「予約イベント概要」 ・ 374 ページの「イベント詳細のアップデート」

タスク	参照先
監査のための、情報漏えい対策ログのエクスポート	318 ページの「ログクエリを使用する」

Active Directory ユーザにマネージャ情報を設定する

情報漏えい対策イベントを調査するマネージャについて、各 Active Directory ユーザにマネージャ情報を設定します。

手順

1. [Active Directory ユーザとコンピュータ] コンソールを開きます。[スタート] > [管理ツール] > [Active Directory ユーザとコンピュータ] をクリックします。

   [Active Directory ユーザとコンピュータ] コンソールが表示されます。

2. ユーザをダブルクリックします。

   [プロパティ] 画面が表示されます。

3. [組織] タブをクリックし、[変更...]をクリックします。

   [ユーザー、連絡先、コンピュータまたはグループの選択] 画面が表示されます。

4. マネージャ情報を指定し、[OK] をクリックします。

5. マネージャとユーザの関係を確認するには、マネージャの [プロパティ] 画面を開き、[組織] タブをクリックして、[直属の部下] のユーザ情報をチェックします。

情報漏えい対策ユーザの役割について

Apex Central は、次の情報漏えい対策 (DLP) ユーザの役割を用意しています。

- Administrator_and_DLP_Compliance_Officer (管理者および情報漏えい対策コンプライアンス責任者)

- DLP_Compliance_Officer (情報漏えい対策コンプライアンス 責任者)
- DLP_Incident_Reviewer (情報漏えい対策イベントレビューア)

注意

Active Directory ユーザアカウントには、「DLP_Compliance_Officer (情報漏えい対策コンプライアンス 責任者)」および「DLP_Incident_Reviewer (情報漏えい対策イベントレビューア)」の役割のみ割り当てることができます。

次の表に、DLP ユーザの役割に関連する機能と特徴をまとめます。

機能	役割	説明
情報漏えい対策ログ	Administrator_and_DLP_Compliance_Officer (管理者および情報漏えい対策コンプライアンス責任者)	• すべての Active Directory ユーザに関する情報漏えい対策ログデータを表示します。 • 情報漏えい対策イベント情報を表示する専用ウィジェットにアクセスできます。
	DLP_Compliance_Officer (情報漏えい対策コンプライアンス責任者)	• アクセスは、直接管理下のユーザに関連する情報漏えい対策ログに限定されています。 • 情報漏えい対策イベント情報を表示する専用ウィジェットにアクセスできます。
	DLP_Incident_Reviewer (情報漏えい対策イベントレビューア)	

機能	役割	説明
イベントの範囲	Administrator_and_DLP_Compliance_Officer (管理者および情報漏えい対策コンプライアンス責任者) DLP_Compliance_Officer (情報漏えい対策コンプライアンス責任者)	• すべての Active Directory ユーザに関する情報漏えい対策イベントデータを表示します。その方法として、次の情報漏えい対策ウィジェットのいずれかで設定アイコン (>) をクリックし、[範囲] として [すべての管理されているユーザ] を選択します。 • 重大度およびステータス別の情報漏えい対策イベント • 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 注意 • 初期設定では、この役割でイベントデータを表示できる各情報漏えい対策ウィジェットの範囲は [直接管理下のユーザ] に限られます。 • 1 つの情報漏えい対策ウィジェットの [範囲] を変更しても、それ以外のウィジェットの範囲には影響しません。 • その他のすべての画面: • 「Administrator_and_DLP_Compliance_Officer (管理者および情報漏えい対策コンプライアンス責任者)」の役割を割り当てられたユーザアカウントは、その製品の範囲に応じて、管理下の製品から報告されたすべての Active Directory ユーザからのデータを表示できます。 • 「DLP_Compliance_Officer (情報漏えい対策コンプライアンス責任者)」の役割では、どのデータも表示できません。
	DLP_Incident_Reviewer (情報漏えい対策イベントレビューア)	直接管理下のユーザに関する情報漏えい対策イベントのデータを表示します。

機能	役割	説明
メニューへのアクセス	Administrator_and_DLP_Compliance_Officer (管理者および情報漏えい対策コンプライアンス責任者)	[情報漏えい対策] タブおよび次のウィジェットにアクセスできます。 ・ 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 詳細については、73 ページの「[情報漏えい対策] タブ」を参照してください。
	DLP_Compliance_Officer (情報漏えい対策コンプライアンス責任者)	
	DLP_Incident_Reviewer (情報漏えい対策イベントレビューア)	
予約イベント概要の通知	Administrator_and_DLP_Compliance_Officer (管理者および情報漏えい対策コンプライアンス責任者)	次の内容を受け取ります。 ・ 毎日または週一度のメールによる通知 ・ 重大度レベル別イベント数の概要リスト ・ Apex Central 管理コンソールへのアクセス
	DLP_Compliance_Officer (情報漏えい対策コンプライアンス責任者)	
	DLP_Incident_Reviewer (情報漏えい対策イベントレビューア)	

機能	役割	説明
イベント詳細のアップデートの通知	Administrator_and_DLP_Compliance_Officer (管理者および情報漏えい対策コンプライアンス責任者)	イベントステータスまたはコメントに対する変更の通知を受け取ります。 注意 「DLP_Incident_Reviewer (情報漏えい対策イベントレビューア)」の役割では、この通知を受け取りません。
	DLP_Compliance_Officer (情報漏えい対策コンプライアンス責任者)	

情報漏えい対策監査ログの作成

管理者はログクエリを使用して情報漏えい対策監査ログを生成し、エクスポートできます。318 ページの「ログクエリを使用する」で説明されているとおりにログクエリを実行し、次の設定を行います。

- ログの種類: [ユーザのアクセス] を選択します。
- 詳細フィルタ: 次のアクティビティ ([アクティビティ]) をカスタム条件に追加します。
  - 情報漏えい対策イベントファイルのダウンロード
  - 情報漏えい対策イベントのアップデート

情報漏えい対策イベントのレビュー処理

Apex Central 管理者が前提条件となるタスクを完了すると、レビューアはイベントのレビュー処理を開始できるようになります。次の表に、このようなタスクと参照先をまとめます。

表 18-2. 情報漏えい対策イベントのレビュー処理

タスク	説明
[予約イベント概要] 通知メッセージの受信	Apex Central は毎日、または 1 週間に一度、概要をメール通知にまとめ、イベントレビューアに送信します。
次のいずれかの方法を使用した、イベントの詳細のレビュー • メッセージに記載されているリンクをクリックし、Apex Central の管理コンソールにログオンする • 添付ファイルがあれば、それを開く	464 ページの「イベント情報リストについて」
イベントステータスを更新し、コメントを記入	466 ページの「イベント詳細のレビュー」

イベント情報リストについて

[イベント情報] 画面には、レビューアが管理可能なイベントのリストが表示されます。イベントのレビューアは、この画面を使用して、次の作業を行うことができます。

- イベントの概要を表示
- イベントに対する処理の実行
- イベント詳細のエクスポート

表 18-3. イベント情報リスト

項目	説明
ID	一意のイベント ID を示します。

項目	説明
受信	Apex Central がイベントデータを受信した日付と時刻を示します。 注意 管理下の製品から情報漏えい対策ログを受信した後、Apex Central がログを処理するには 30 分かかります。その後、イベントレビューアはデータを表示できるようになります。
重大度	イベントの重大度レベルを示します。 注意 情報漏えい対策イベントを受信し、処理した Apex Central は、管理下の製品で変更が発生しても重大度レベルを更新しません。
ポリシー	イベントをトリガした Apex Central ポリシーの名前を示します。 注意 管理下の製品で作成された情報漏えい対策ポリシーをトリガしているイベントについては、N/A と表示されます。
ユーザ	イベントをトリガしたユーザの名前を示します。
マネージャ	ユーザのマネージャ名を示します。
ステータス	イベントの現在のステータスを示します。 • 新規 • 調査中 • エスカレート済み • 解決済み
処理	イベントの管理に利用できる処理を示します。

イベント詳細のレビュー

[イベント情報] 画面の [処理] 列で [編集] アイコンをクリックすると、[イベント詳細] 画面が開き、イベントに関する詳しい情報が表示されます。情報漏えい対策イベントのレビューアは、この画面を使用して、イベントステータスの更新やイベントについてのコメント記入を行います。

表 18-4. イベント詳細

項目	説明
ID	一意のイベント ID を示します。
ステータス	イベントのレビューステータスを更新するには、これを使用します。 利用可能なオプション: • 新規 • 調査中 • エスカレート済み • 解決済み
重大度	イベントの重大度レベルを示します。 注意 情報漏えい対策イベントを受信し、処理した Apex Central は、管理下の製品で変更が発生しても重大度レベルを更新しません。
ポリシー	イベントをトリガした Apex Central ポリシーの名前を示します。 注意 管理下の製品で作成された情報漏えい対策ポリシーをトリガしているイベントについては、N/A と表示されます。
ルール	イベントがトリガされる原因となったルールの名前を示します。

項目	説明
受信	Apex Central がイベントデータを受信した日付と時刻を示します。 注意 管理下の製品から情報漏えい対策ログを受信した後、Apex Central がログを処理するには 30 分かかります。その後、イベントレビューアはデータを表示できるようになります。
生成	管理下の製品でイベントが発生した日付と時刻を示します。
ユーザ	イベントをトリガしたユーザの名前を示します。
マネージャ	ユーザのマネージャ名を示します。
エンドポイント	感染元ホスト名を示します。
IP アドレス	送信元 IP アドレスを示します。
送信者	送信元のメールアドレスを示します。
件名	メールメッセージの件名を示します。
受信者	送信先のメールアドレスを示します。
送信先	デジタル資産またはチャネル (使用可能なソースがない場合) を含むファイルの送信先を示します。
最終更新日時	アセットが最後に変更された日時を示します。
最終更新者	アセットを最後に変更したユーザの名前を示します。
テンプレート	イベントをトリガしたテンプレートの名前を示します。
ファイル	イベントをトリガしたファイルの名前またはこのファイルへのリンクを示します。 注意 このファイルは、管理下の製品に隔離されます。
SHA-1	ファイルのハッシュ情報を示します。
チャネル	転送に使用されるチャネルを示します。

項目	説明
処理	イベントに対して実行された処理を示します。
ユーザの承認理由	ユーザに対する機密データの転送の許可について、ユーザ指定の理由を示します。
一致するコンテンツ	イベントをトリガしたデジタル資産を示します。
コメント	イベントに関するユーザ指定のメモを示します。

パート VI

脅威インテリジェンスとレスポンス

第 19 章

Connected Threat Defense

このセクションでは、標的型攻撃や高度な脅威を、検出して分析し、被害が拡大する前に対処する方法について説明します。

次のトピックがあります。

Connected Threat Defense について

Apex Central では、トレンドマイクロのさまざまな製品やソリューションを統合することで、標的型攻撃や高度な脅威を検出して分析し、被害が拡大する前に対処することができます。

詳細については、「Connected Threat Defense 製品の統合」を参照してください。

機能要件

次の表は、Connected Threat Defense アーキテクチャで使用可能な機能、および各機能と統合する必須の製品とオプションの製品をまとめたものです。各製品の Connected Threat Defense の対応状況については、別途製品 Q&A にて確認してください。

https://success.trendmicro.com/jp/solution/1117782

機能	必須の製品	オプションの製品

脅威の監視	• Apex Central
	• Deep Discovery Inspector 5.0 (またはそれ以降) または次のいずれかの仮想アナライザ製品:
	  • 「Apex One Sandbox as a Service」
	  • 「Deep Discovery Analyzer」
	
	重要
	ログデータを評価するには、少なくとも 1 つのオプションの製品が必要です。
		• Apex One 2019 またはウイルスバスター Corp. 11.0 SP1 (またはそれ以降)
		• Apex One Endpoint Sensor
		• Cloud App Security 5.0 (またはそれ以降)
		• Deep Security Manager 10.0 (またはそれ以降)
		• InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降)
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (またはそれ以降)
		• InterScan for Microsoft Exchange 12.5 (またはそれ以降)

機能	必須の製品	オプションの製品

不審オブジェクトリストの同期
 	
詳細については、478 ページの「不審オブジェクトリスト」および 511 ページの「Connected Threat Defense 製品の統合」を参照してください。
	• Apex Central
	• Deep Discovery Inspector 5.0 (またはそれ以降) または次のいずれかの仮想アナライザ製品:
	  • 「Apex One Sandbox as a Service」
	  • 「Deep Discovery Analyzer」
	
	重要
	不審オブジェクトリストの同期には、少なくとも 1 つのオプションの製品が必要です。
		• Apex One 2019 またはウイルスバスター Corp. 11.0 SP1 (またはそれ以降)
		• Cloud App Security 5.0 (またはそれ以降)
		• Deep Discovery Director
		• Deep Security Manager 10.0 (またはそれ以降)
		• InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降)
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (またはそれ以降)
		• Smart Protection Server 3.3 Patch 2 (またはそれ以降)
		• Trend Micro Endpoint Application Control 2.0 SP1 (またはそれ以降)

機能	必須の製品	オプションの製品

不審オブジェクトのサンプルの送信	• Deep Discovery Inspector 5.0 (またはそれ以降) または次のいずれかの仮想アナライザ製品:
	  • 「Apex One Sandbox as a Service」
	  • 「Deep Discovery Analyzer」
		• Apex One 2019 またはウイルスバスター Corp. 11.0 SP1 (またはそれ以降)
		• Apex One Endpoint Sensor
		• Deep Discovery Email Inspector 3.0 (またはそれ以降)
		• Deep Security Manager 10.0 (またはそれ以降)
		• InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降)
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (またはそれ以降)
		• InterScan for Microsoft Exchange 12.5 (またはそれ以降)

機能	必須の製品	オプションの製品

不審オブジェクト管理	• Apex Central
	• Deep Discovery Inspector 5.0 (またはそれ以降) または次のいずれかの仮想アナライザ製品:
	  • 「Apex One Sandbox as a Service」
	  • 「Deep Discovery Analyzer」
		• Apex One 2019 またはウイルスバスター Corp. 11.0 SP1 (またはそれ以降)
		• Apex One Endpoint Sensor
		• Cloud App Security 5.0 (またはそれ以降)
		• Deep Security Manager 10.0 (またはそれ以降)
		• InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降)
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (またはそれ以降)
		• Trend Micro Endpoint Application Control 2.0 SP1 (またはそれ以降)

機能	必須の製品	オプションの製品
不審オブジェクト検出時の処理 詳細については、482 ページの「不審オブジェクト検出時の処理」を参照してください。	• Apex Central	• Apex One 2019 またはウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降) • Deep Security Manager 10.0 (またはそれ以降) • InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (またはそれ以降) • Smart Protection Server 3.3 Patch 2 (またはそれ以降) • Trend Micro Endpoint Application Control 2.0 SP1 (またはそれ以降)
影響分析	• Apex Central • Apex One Endpoint Sensor **重要** [影響を受けたユーザ] 画面で影響分析を実行する場合も、Deep Discovery Inspector 5.0 (またはそれ以降) が必要です。 詳細については、163 ページの「影響を受けたユーザに対する影響を分析する」を参照してください。	• Deep Discovery Inspector 5.0 (またはそれ以降)

機能	必須の製品	オプションの製品
エンドポイントの隔離 詳細については、508 ページの「エンドポイントを隔離する」を参照してください。	• Apex Central • Apex One 2019 またはウイルスバスター Corp. 11.0 SP1 (またはそれ以降)	• Apex One Endpoint Sensor
IOC の管理	• Apex Central • Apex One Endpoint Sensor	• なし

不審オブジェクトリスト管理

Apex Central では、不審オブジェクトリストを管理下の製品との間で同期したり、ユーザ指定リストや例外リストを作成して不審オブジェクトの拡散を細かく制御したりできます。環境内で不審オブジェクトを検出したときにサポート対象の管理下の製品で実行する具体的な処理を設定することもできます。

Apex Central は、仮想アナライザで検出された不審オブジェクトリストとユーザ指定の不審オブジェクトリスト (除外リストのオブジェクトを除く) を合わせ、そのリストを統合された管理下の製品と同期します。

不審オブジェクトリストを Apex Central と同期できる製品の詳細については、472 ページの「機能要件」の「不審オブジェクトリストの同期」を参照してください。

不審オブジェクトリスト

Apex Central は、多数の管理下の製品の間で、仮想アナライザで検出された不審オブジェクトリストを統合し、すべての不審オブジェクトリストを同期します。それぞれの管理下の製品でリストを実装する方法は、その製品における本機能の実装方法によって異なります。管理下の製品で不審オブジェクトリストを使用および同期する方法の詳細については、その製品の管理者ガイドを参照してください。

注意

管理者は、Apex Central 管理コンソールを使用して不審オブジェクトに対して具体的な検索処理を設定できます。その後、不審オブジェクトリスト設定に基づいて処理を実行するように特定の管理下の製品を設定できます。

詳細については、482 ページの「不審オブジェクト検出時の処理」を参照してください。

リストの種類	説明
仮想アナライザで検出された不審オブジェクト	仮想アナライザを使用する管理下の製品は、分析のために不審なファイルまたは URL を仮想アナライザに送信します。仮想アナライザは、オブジェクトに脅威の可能性があると判断した場合、そのオブジェクトを不審オブジェクトリストに追加します。仮想アナライザは、統合と同期の目的でリストを登録済みの Apex Central サーバに送信します。 Apex Central 管理コンソールで、[脅威インテリジェンス] > [仮想アナライザ不審オブジェクト] > [オブジェクト] タブに移動して、仮想アナライザで検出された不審オブジェクトリストを表示します。 詳細については、487 ページの「不審オブジェクトの検出」を参照してください。
仮想アナライザで検出された不審オブジェクトの除外設定	Apex Central 管理者は、仮想アナライザの不審オブジェクトリストから安全と考えられるオブジェクトを選択し、除外リストに追加できます。 Apex Central 管理コンソールで、[脅威インテリジェンス] > [仮想アナライザ不審オブジェクト] > [除外] タブに移動して、仮想アナライザで検出された不審オブジェクトの除外リストを表示します。 Apex Central は、除外リストを利用する仮想アナライザ (Apex One Sandbox as a Service を除く) にそのリストを送信します。仮想アナライザでは、除外リストに含まれている不審オブジェクトを検出すると、そのオブジェクトは「安全」と認識され、再度分析されません。 詳細については、480 ページの「仮想アナライザで検出された不審オブジェクトリストに除外を追加する」を参照してください。

リストの種類	説明
ユーザ指定の不審オブジェクト	Apex Central の管理者は、[脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] に移動して、現在仮想アナライザで検出された不審オブジェクトリストに含まれていないオブジェクトを不審オブジェクトとして追加できます。 詳細については、493 ページの「脅威の兆候に対する予防的対策」を参照してください。

仮想アナライザで検出された不審オブジェクトリストに除外を追加する

Apex Central では、ファイル SHA-1、ドメイン、IP アドレス、または URL に基づいて、仮想アナライザで検出された不審オブジェクトリストからオブジェクトを除外できます。

重要

ユーザ指定の不審オブジェクトリストは、仮想アナライザの不審オブジェクトリストよりも優先されます。

手順

1. [脅威インテリジェンス] > [仮想アナライザで検出された不審オブジェクト]に移動します。

   [仮想アナライザで検出された不審オブジェクト] 画面が表示されます。

2. [除外] タブをクリックします。
3. [追加] をクリックします。
4. オブジェクトの [種類] を指定します。
   - ファイル: ファイル SHA-1 ハッシュ値を指定します。
   - IP アドレス: IP アドレスを指定します。
   - URL: URL を指定します。

- ドメイン: ドメインを指定します。

  Apex Central では、ワイルドカード文字 (*) を使用して、仮想アナライザで検出された不審オブジェクトリストから特定のサブドメインまたはサブディレクトリを除外できます。

例	説明
https://*.domain.com/	ドメイン「domain.com」のサブドメインを含むすべての URL を、仮想アナライザで検出された不審オブジェクトリストから除外します。 重要 URL にサブディレクトリが含まれている場合は、一致するサブドメインが URL に含まれていてもその URL は除外されません。たとえば、「https://abc.domain.com/abc」は除外されません。
*.abc.domain.com	サブドメイン「abc」のすべてのサブドメインを、仮想アナライザで検出された不審オブジェクトリストから除外します。
https:// *.domain.com/abc/*	ドメイン「domain.com」のサブドメインを含むすべての URL と、サブディレクトリ「abc」のすべてのサブディレクトリを、仮想アナライザで検出された不審オブジェクトリストから除外します。 重要 サブディレクトリ「abc」にサブディレクトリが含まれていない URL も除外されます。たとえば、「https://abc.domain.com/abc」は除外されます。

5. (オプション) 不審オブジェクトの識別に役立つ [メモ] を指定します。
6. [追加] をクリックします。

オブジェクトが仮想アナライザの除外リストに表示されます。管理下の製品が不審オブジェクトリストを利用する場合、その管理下の製品は、次回の同期処理中に新しいオブジェクト情報を受信します。

不審オブジェクト検出時の処理

管理者は Apex Central 管理コンソールを使用して、特定の管理下の製品が仮想アナライザで検出された不審オブジェクトリストまたはユーザ指定の不審オブジェクトリスト内の特定の不審オブジェクトを検出したときに実行する検出時の処理を設定できます。

各製品の Connected Threat Defense の対応状況については、別途製品 Q&A にて確認してください

https://success.trendmicro.com/jp/solution/1117782

表 19-1. 検出時の処理の製品サポート

製品	仮想アナライザリスト	ユーザ指定リスト
Apex One (任意のバージョン)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • ファイル SHA-1: ログ、ブロック • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック

製品	仮想アナライザリスト	ユーザ指定リスト
ウイルスバスター Corp. XG SP1 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック
Deep Security Manager 10.0 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • URL: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • URL: ログ、ブロック
• Deep Discovery Inspector 5.0 (またはそれ以降) • Deep Discovery Email Inspector 3.0 (またはそれ以降)	以下の不審オブジェクトの種類に対して同期処理を実行します。 • ファイル: 検索処理は行われません。 • IP アドレス: 検索処理は行われません。 • URL: 検索処理は行われません。 • ドメイン: 検索処理は行われません。	以下の不審オブジェクトの種類に対して同期処理を実行します。 • ファイル: 検索処理は行われません。 • IP アドレス: 検索処理は行われません。 • URL: 検索処理は行われません。 • ドメイン: 検索処理は行われません。
InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • ファイル SHA-1: ログ、ブロック、または隔離

製品	仮想アナライザリスト	ユーザ指定リスト
InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • ファイル SHA-1: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • ファイル SHA-1: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック
Cloud App Security 5.0 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • URL: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • URL: ログ、ブロック

<table>
<tr><th>製品</th><th>仮想アナライザリスト</th><th>ユーザ指定リスト</th></tr>
<tr><td rowspan="2">Smart Protection Server 3.3 Patch 2 (またはそれ以降)
ウイルスバスター Corp. 11.0 SP1 (以降) と統合された Smart Protection Server
サポートされている Smart Protection Server に Web レピュテーションクエリを送信するトレンドマイクロ製品</td><td>管理下の製品は、Web レピュテーションクエリ時に以下の不審オブジェクトの種類に対して処理を実行します。
URL: ログ、ブロック</td><td>管理下の製品は、Web レピュテーションクエリ時に以下の不審オブジェクトの種類に対して処理を実行します。
URL: ログ、ブロック
重要
Smart Protection Server はユーザ指定の不審オブジェクトリスト内のすべての URL を「高」リスクとして分類します。</td></tr>
<tr><td colspan="2">注意
不審 URL オブジェクトに対して Apex Central で設定した処理を直接実行できるのは特定の管理下の製品のみです。その他の管理下の製品は、その製品に設定された Web レピュテーション設定に基づいて不審 URL オブジェクトに対して処理を実行します。

管理下の製品に表示されるログには、不審オブジェクトの検出に関連する情報が含まれない場合があります。Apex Central は、管理下の製品から送信されたログを解釈して、Apex Central 管理コンソールに不審オブジェクトの検出を表示します。</td></tr>
</table>

配信を設定する

配信を設定すると、Apex Central は仮想アナライザで検出された不審オブジェクトとユーザ指定の不審オブジェクト (除外リストのオブジェクトを除く) を統合し、特定の管理下の製品に送信できます。管理下の製品は、受け取ったオブジェクトのすべてまたは一部を同期して使用します。

Apex Central では、不審 IP アドレスとドメインを TippingPoint に送信することもできます。

注意

[配信設定] では、不審オブジェクトハブおよびノードに関する Apex Central サーバの設定で、不審オブジェクトリストを複数の Apex Central サーバ間で同期するように設定することもできます。

詳細については、593 ページの不審オブジェクトハブおよびノードのアーキテクチャを参照してください。

手順

1. [脅威インテリジェンス] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。

2. 不審オブジェクトを管理下の製品に送信するには、以下の手順を実行します。

   a. [管理下の製品] タブをクリックします。

   b. [不審オブジェクトを管理下の製品に送信する。] チェックボックスをオンにします。

   c. 以下の情報を記録し、管理下の製品で Apex Central から不審オブジェクトを同期する際の設定に使用します。

      - サービス URL: Apex Central のサービス URL
      - API キー: 管理下の製品で Apex Central を識別するコード

   d. [保存] をクリックします。

   e. [今すぐ同期] をクリックします。

3. 不審オブジェクトを TippingPoint に送信するには、以下の手順を実行します。

   a. [TippingPoint] タブをクリックします。

   b. [不審オブジェクト (IP アドレスとドメイン名のみ) を TippingPoint に送信します] チェックボックスをオンにします。

> **注意**
>
> Apex Central は、仮想アナライザで分析された不審な IP アドレスとドメイン名を送信します。TippingPoint は、レピュテーションフィルタを使用して、レピュテーショングループ全体にブロック、許可、または通知の処理を適用します。レピュテーションフィルタの詳細については、TippingPoint のドキュメントを参照してください。

c. 次の項目を指定します。

- サーバ名: TippingPoint 配信用のサーバ URL とポート番号を入力します。
- ユーザ名: TippingPoint コンソールへのアクセス権限があるアカウントのユーザ名を入力します。
- パスワード: アカウントのパスワードを入力します。

d. (オプション) [接続テスト] をクリックして接続を確認します。

e. TippingPoint にドメイン名または IP アドレス情報を送信する重大度レベルを選択します。

- 高のみ: 重大度の高い IP アドレスとドメイン名
- 中/高: 重大度が高および中程度の IP アドレスとドメイン名
- すべて: 重大度が高、中、低の IP アドレスとドメイン名

f. [保存] をクリックします。

g. [今すぐ同期] をクリックします。

不審オブジェクトの検出

環境内の不審オブジェクトの検出は、Apex Central 管理コンソールを使用してさまざまな方法で確認できます。不審オブジェクトの検出を確認する別の方法については、以下を参照してください。

- 488 ページの「危険性の高いエンドポイントや受信者を確認する」
- 488 ページの「仮想アナライザで検出された不審オブジェクトによる影響を分析する」

注意

Apex Central では、環境内の不審オブジェクトにさらされているユーザやエンドポイントを識別することだけができます。Apex Central 管理コンソールでは不審オブジェクトに対して直接の処理を実行できません。

危険性の高いエンドポイントや受信者を確認する

Apex Central は、すべての管理下の製品から受け取った Web レピュテーション、URL フィルタ、ネットワークコンテンツ検査、およびルールベース検出のログを確認し、それらのログを不審オブジェクトリストと照合します。

手順

1. [脅威インテリジェンス] > [仮想アナライザ不審オブジェクト]に移動します。

   [仮想アナライザで検出された不審オブジェクト] 画面が表示されます。

2. [オブジェクト] タブをクリックします。

3. 確認するオブジェクトの左側にある矢印を展開します。

   - [危険性の高いエンドポイント] リストには、引き続き不審オブジェクトの影響を受けているすべてのエンドポイントとユーザが表示されます。
     - 「ファイル」の検出では、[最新の処理結果] 列に管理下の製品によって報告された最新の処理結果が表示されます。
     - その他のすべての検出の種類では、[最新の処理結果] 列に「N/A」と表示されます。
   - [危険性の高い受信者] リストには、引き続き不審オブジェクトの影響を受けているすべての受信者が表示されます。

仮想アナライザで検出された不審オブジェクトによる影響を分析する

[仮想アナライザで検出された不審オブジェクト] 画面では、ネットワークに対する影響分析を実行できます。影響分析では、Endpoint Sensor を使用して

エージェントと通信し、エージェントログの履歴検索を実行して、不審オブジェクトが検出されずに一定期間にわたって環境に影響を与えているかどうか判断します。

[カスタムインテリジェンス] 画面で、ユーザ指定の不審オブジェクトの影響分析を実行することもできます。

詳細については、506 ページの「影響を分析してユーザ指定の不審オブジェクトからの IOC に対応する」を参照してください。

重要

影響分析には、有効な Apex One Endpoint Sensor ライセンスが必要です。有効な Apex One Endpoint Sensor ライセンスがあることを確認し、適切な [Apex One セキュリティエージェント] ポリシーまたは [Apex One (Mac)] ポリシーに対して Endpoint Sensor 機能を有効にしてください。

詳細については、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. [脅威インテリジェンス] > [仮想アナライザ不審オブジェクト] に移動します。

   [仮想アナライザで検出された不審オブジェクト] 画面が表示されます。

2. [オブジェクト] タブをクリックします。

3. リストから 1 つ以上のオブジェクトを選択します。

   注意

   Apex Central は URL オブジェクトの影響分析をサポートしていません。

4. [影響の分析] をクリックします。

   Endpoint Sensor がエージェントと通信し、検出された不審オブジェクトのエージェントログを評価します。

   注意

   影響分析時間はネットワーク環境に応じて異なります。

5. 確認するオブジェクトの左側にある矢印を展開します。
   - [危険性の高いエンドポイント] リストには、引き続き不審オブジェクトの影響を受けているすべてのエンドポイントとユーザが表示されます。
     - 「ファイル」の検出では、[最新の処理結果] 列に管理下の製品によって報告された最新の処理結果が表示されます。
     - その他のすべての検出の種類では、[最新の処理結果] 列に「N/A」と表示されます。
   - [危険性の高い受信者] リストには、引き続き不審オブジェクトの影響を受けているすべての受信者が表示されます。

Endpoint Sensor での履歴調査

履歴調査では、指定した条件に基づいて、履歴イベントと分析チェーンが診断されます。調査結果は、不審アクティビティの 実行フローを示す Root Cause Analysis マップの形式で表示されます。これにより、組織全体を巻き込んだ、標的型攻撃のイベントチェーンを分析できます。

履歴調査では、次の種類のオブジェクトが使用されます。

- DNS レコード
- IP アドレス
- ファイル名
- ファイルパス
- SHA-1 ハッシュ値
- MD5 ハッシュ値
- ユーザアカウント

履歴調査では、エンドポイントの履歴イベントが格納された、標準化されたデータベースに対してクエリを実行します。この方法は、従来のログファイルに比べて使用するディスク容量が少なく、リソースの消費量も少なくなります。

処理プロセスを表示する

[処理プロセス] 画面には、環境内の不審オブジェクトのライフサイクルとその不審オブジェクトがユーザやエンドポイントに与えている現在の影響に関する概要が表示されます。

重要

処理プロセスを表示するには、仮想アナライザを含む製品またはサービスのライセンスが追加で必要です。次のうち少なくとも 1 つの有効なライセンスがあることを確認してください。各製品の Connected Threat Defense の対応状況については、別途製品 Q&A にて確認してください。

https://success.trendmicro.com/jp/solution/1117782

- Apex One Sandbox as a Service
- Deep Discovery Analyzer 6.5 (またはそれ以降)
- Deep Discovery Email Inspector 3.5 (またはそれ以降)
- Deep Discovery Inspector 5.0 (またはそれ以降)

手順

1. [脅威インテリジェンス] > [仮想アナライザ不審オブジェクト]に移動します。
2. 特定の不審オブジェクトについて、表の [処理プロセス] 列にある [表示] リンクをクリックします。

   [処理プロセス] 画面が表示されます。
3. 次のいずれかのタブをクリックして、不審オブジェクトに関する詳細情報を表示します。

タブ	説明
サンプル送信	不審オブジェクトの最初の分析と最新の分析に関連する情報が表示されます。 Apex Central では、次の製品と統合して、仮想アナライザを使用してその他の管理下の製品から送信された不審オブジェクトを分析します。 • Deep Discovery Analyzer 6.5 (またはそれ以降) • Deep Discovery Email Inspector 3.5 (またはそれ以降) • Deep Discovery Inspector 5.0 (またはそれ以降) 注意 Apex One Sandbox as a Service では、[サンプル送信] の情報は提供されません。
分析	送信されたオブジェクトの仮想アナライザによる分析が表示されます。 システムを危険にさらしたり、情報漏えいを引き起こす可能性があるオブジェクトが見つかると、不審オブジェクトのリスクレベルが判定されます。サポートされるオブジェクトには、ファイル (SHA-1 ハッシュ値)、IP アドレス、ドメイン、URL などがあります。 注意 Apex One Sandbox as a Service では、[製品]、[製品のホスト名]、[製品の IP アドレス] の情報は提供されません。
配信	不審オブジェクトリストを同期したすべての製品と、最後の同期時刻が表示されます。 Apex Central は、仮想アナライザで検出された不審オブジェクトリストとユーザ指定の不審オブジェクトリスト (除外リストのオブジェクトを除く) を合わせ、そのリストを統合された管理下の製品と同期します。

タブ	説明
影響の分析と軽減	不審オブジェクトの影響を受けているすべてのエンドポイントとユーザが表示されます。 • 「ファイル」の検出では、[最新の処理結果] 列に管理下の製品によって報告された最新の処理結果が表示されます。 • その他のすべての検出の種類では、[最新の処理結果] 列に「N/A」と表示されます。 [Root Cause Analysis] リンクをクリックすると、オブジェクトがユーザやエンドポイントに与えた影響を調査できます。

脅威の兆候に対する予防的対策

Apex Central では、ネットワーク内でまだ確認されていない不審オブジェクトからネットワークを保護するさまざまな方法を用意しています。ユーザ指定の不審オブジェクトリストを利用するか、OpenIOC ファイルまたは STIX ファイルから痕跡をインポートして、外部ソースによって識別された脅威の兆候に対して処理方法を設定します。

機能	説明
ユーザ指定の不審オブジェクトリスト	ユーザ指定の不審オブジェクトリストを使用すると、登録した仮想アナライザがネットワークで検出していない不審なファイル、ファイル SHA-1、IP アドレス、URL、およびドメインオブジェクトを定義できます。 サポートされている管理下の製品が不審オブジェクトリストを利用する場合、その管理下の製品は、未知の脅威が拡散することを防ぐためにこのリストで見つかったオブジェクトに対して処理を実施できます。 詳細については、次のトピックを参照してください。 • 495 ページの「ユーザ指定の不審オブジェクトリストにオブジェクトを追加する」 • 482 ページの「不審オブジェクト検出時の処理」 • 506 ページの「影響を分析してユーザ指定の不審オブジェクトからの IOC に対応する」
STIX ファイルリスト	STIX ファイルリストを使用すると、STIX (Structured Threat Import Expression) ファイルをインポートし、不審なファイル SHA-1、IP アドレス、URL、およびドメインオブジェクトをユーザ指定の不審オブジェクトリストに抽出できます。 詳細については、次のトピックを参照してください。 • 497 ページの「ユーザ指定の不審オブジェクトリストに STIX オブジェクトを追加する」 • 506 ページの「影響を分析してユーザ指定の不審オブジェクトからの IOC に対応する」
OpenIOC ファイルリスト	OpenIOC ファイルリストを使用すると、OpenIOC ファイルをインポートし、不審なファイル SHA-1、IP アドレス、URL、およびドメインオブジェクトをユーザ指定の不審オブジェクトリストに抽出できます。 詳細については、次のトピックを参照してください。 • 500 ページの「ユーザ指定の不審オブジェクトリストに OpenIOC オブジェクトを追加する」 • 506 ページの「影響を分析してユーザ指定の不審オブジェクトからの IOC に対応する」

ユーザ指定の不審オブジェクトリストにオブジェクトを追加する

不審オブジェクトをユーザ指定の不審オブジェクトリストに追加することにより、ネットワークでまだ確認されていないオブジェクトからネットワークを保護できます。Apex Central には、ファイル、ファイル SHA-1、ドメイン、IP アドレス、または URL に基づいてオブジェクトを追加するオプションがあります。また、不審オブジェクトの検出後にサポート対象のトレンドマイクロ製品で実行する検索処理も指定できます。

詳細については、次のトピックを参照してください。

- 496 ページの「ユーザ指定の不審オブジェクトリストをインポートする」
- 500 ページの「ユーザ指定の不審オブジェクトリストに OpenIOC オブジェクトを追加する」
- 497 ページの「ユーザ指定の不審オブジェクトリストに STIX オブジェクトを追加する」

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス]に移動します。

   [カスタムインテリジェンス] 画面が表示されます。

2. [ユーザ指定の不審オブジェクト] タブをクリックします。

   ユーザ指定の不審オブジェクトリストが表示されます。

3. [追加] をクリックします。

4. オブジェクトの [種類] を指定します。

   - ファイル: [参照] をクリックして不審なオブジェクトファイルをアップロードします。
   - ファイル: ファイル SHA-1 ハッシュ値を指定します。
   - IP アドレス: IP アドレスを指定します。
   - URL: URL を指定します。

- ドメイン: ドメインを指定します。

5. サポート対象の製品でオブジェクトの検出後に実行する [検出時の処理] を指定します。
   - ログ
   - ブロック
   - 隔離

   
   注意
   「隔離」オプションはファイルオブジェクトまたはファイル SHA-1 オブジェクトに対してのみ使用できます。

6. (オプション) 不審オブジェクトの識別に役立つ [メモ] を指定します。
7. (オプション) 有効期限を指定します。
8. [追加] をクリックします。

   ユーザ指定の不審オブジェクトリストにオブジェクトが表示されます。管理下の製品が不審オブジェクトリストを利用する場合、その管理下の製品は、次回の同期処理中に新しいオブジェクト情報を受信します。

ユーザ指定の不審オブジェクトリストをインポートする

適切な形式の CSV ファイルを使用して、複数の不審オブジェクトをユーザ指定の不審オブジェクトリストに追加します。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス]に移動します。

   [カスタムインテリジェンス] 画面が表示されます。

2. [ユーザ指定の不審オブジェクト] タブをクリックします。

   ユーザ指定の不審オブジェクトリストが表示されます。

3. [インポート] をクリックします。
4. 不審オブジェクトのリストを含む CSV ファイルを選択します。

   ヒント

   [サンプル CSV のダウンロード] リンクをクリックして、適切な形式のサンプル CSV ファイルと、ユーザ指定の不審オブジェクトリストの作成に関する詳しい説明を取得します。

5. [インポート] をクリックします。

   ユーザ指定の不審オブジェクトリストに CSV ファイル内のオブジェクトが表示されます。管理下の製品が不審オブジェクトリストを利用する場合、その管理下の製品は、次回の同期処理中に新しいオブジェクト情報を受信します。

ユーザ指定の不審オブジェクトリストに STIX オブジェクトを追加する

信頼する外部ソース (セキュリティフォーラムまたは他の Deep Discovery 仮想アナライザ製品) から正しい形式の Structured Threat Information Expression (STIX) ファイル (`*.xml`) を入手したら、そのファイルを Apex Central にインポートして、不審ファイル SHA-1、IP アドレス、URL、およびドメインオブジェクトをユーザ指定の不審オブジェクトリストに抽出します。ファイルをアップロードするときは、不審オブジェクトの検出後にサポート対象のトレンドマイクロ製品で実行する検索処理も指定できます。

ユーザ指定の不審オブジェクトリストに不審オブジェクトを手動で追加する方法の詳細については、495 ページの「ユーザ指定の不審オブジェクトリストにオブジェクトを追加する」を参照してください。

重要

Apex Central でアップロードがサポートされているのは、次の STIX および Cybox リリースに準拠する、`*.xml` ファイル拡張子の正しい形式の STIX ファイルのみです。

- STIX 1.1
- STIX 1.1.1
- STIX 1.2
- Cybox 2.1

注意

Apex Central は、STIX ファイルがインポートされると自動的にユーザ指定の不審オブジェクトリストに不審オブジェクトを抽出します。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス]に移動します。

   [カスタムインテリジェンス] 画面が表示されます。

2. [STIX] タブをクリックします。

   STIX ファイルリストが表示されます。

3. (オプション) ファイルリストに表示されるファイルをフィルタするには、検索ボックスを使用して [ファイル名]、[概要]、または [ソースの追加元] 列に含まれる文字列全体またはその一部を指定します。

4. [追加] をクリックします。

   [STIX ファイルの追加] 画面が表示されます。

5. アップロードする STIX ファイル (`*.xml`) を選択します。

   a. [ファイルを選択] をクリックします。

   b. アップロードするファイルを 1 つ以上選択します。

注意

- 各ファイルの最大ファイルサイズは 10MB です。
- 同時にアップロードできるファイル数は最大 200 ファイルです。

c. [開く] をクリックします。

6. (オプション) [詳細設定] をクリックして、オブジェクトの検出後にサポート対象の製品で実行する検出時の処理を指定します。

注意

また、ユーザ指定の不審オブジェクトリストの不審オブジェクトに対する検出時の処理を設定することもできます。

詳細については、482 ページの「不審オブジェクト検出時の処理」を参照してください。

7. [追加] をクリックします。

Apex Central は選択した STIX ファイルをアップロードし、ユーザ指定の不審オブジェクトリストに不審オブジェクトを抽出します。

- 特定のファイルのコピーをダウンロードするには、[ファイル名] 列にあるリンクをクリックします。
- ファイル抽出のステータスを追跡するには、[コマンド追跡] 画面を使用します。

  詳細については、240 ページの「コマンド追跡」を参照してください。
- ユーザ指定の不審オブジェクトリストのフィルタ 画面で抽出された不審オブジェクトを表示するには、[抽出されたオブジェクト] 列の数字をクリックします。
- ファイルを削除するには、1 つ以上のファイルのファイル名の横にあるチェックボックスをオンにし、[削除] をクリックします。

注意

- ファイルを削除しても、抽出された不審オブジェクトはユーザ指定の不審オブジェクトリストから削除されません。
- Apex Central でファイルから不審オブジェクトの抽出が完了するまでは、ファイルを削除できません。

ユーザ指定の不審オブジェクトリストに OpenIOC オブジェクトを追加する

適切な形式の OpenIOC ファイル (`*.ioc`) をインポートして、不審ファイル SHA-1、IP アドレス、URL、およびドメインオブジェクトをユーザ指定の不審オブジェクトリストに抽出することにより、ネットワークでまだ確認されていないオブジェクトからネットワークを保護できます。ファイルをアップロードするときは、不審オブジェクトの検出後にサポート対象のトレンドマイクロ製品で実行する検索処理を指定できます。OpenIOC ファイルのアップロード後、アップロードしたファイルを履歴調査またはライブ調査の診断条件として選択することもできます。

ユーザ指定の不審オブジェクトリストに不審オブジェクトを直接手動で追加する方法の詳細については、495 ページの「ユーザ指定の不審オブジェクトリストにオブジェクトを追加する」を参照してください。

重要

Apex Central は OpenIOC 1.0 のみをサポートしています。

注意

初期設定では、OpenIOC ファイルのアップロードが完了した時点で、Apex Central はユーザ指定の不審オブジェクトリストに不審オブジェクトを自動的に抽出します。

または、最初に OpenIOC をアップロードし、ファイルのアップロードが完了した後に手動で不審オブジェクトを抽出することもできます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス]に移動します。

   [カスタムインテリジェンス] 画面が表示されます。

2. [OpenIOC] タブをクリックします。

   OpenIOC ファイルリストが表示されます。

3. (オプション) ファイルリストに表示されるファイルをフィルタするには、検索ボックスを使用して [ファイル名]、[概要]、または [ソースの追加元] 列に含まれる文字列全体またはその一部を指定します。

4. [追加] をクリックします。

   [OpenIOC ファイルの追加] 画面が表示されます。

5. アップロードする OpenIOC ファイル (`*.ioc`) を選択します。

   a. [ファイルを選択] をクリックします。

   b. アップロードするファイルを 1 つ以上選択します。

   注意

   - 各ファイルの最大ファイルサイズは 10MB です。
   - 同時にアップロードできるファイル数は最大 200 ファイルです。
   - ユーザ指定の不審オブジェクトリストでは、不審オブジェクトの種類ごとのオブジェクトの最大数が 10,000 個を超えないようにしてください。

     最大数を超えた場合、その不審オブジェクトの種類に対する抽出するタスクは失敗します。

   c. [開く] をクリックします。

6. (オプション) [詳細設定] で次の設定を行います。

   - 不審オブジェクトを自動的に抽出せずにファイルをアップロードするには、[ファイル SHA1 ハッシュ、IP アドレス、URL、またはドメインを抽出して、不審オブジェクトをユーザ指定の不審オブジェクトリストに追加する] チェックボックスをオフにします。

> **注意**
>
> ファイルのアップロード時の自動抽出を無効にしても、ファイルのアップロードが完了した後にオブジェクトを手動で抽出できます。

- オブジェクトの検出後にサポート対象製品で実行する検出時の処理を指定します。

> **注意**
>
> また、ユーザ指定の不審オブジェクトリストの不審オブジェクトに対する検出時の処理を設定することもできます。
>
> 詳細については、482 ページの「不審オブジェクト検出時の処理」を参照してください。

7. [追加] をクリックします。

> **ヒント**
>
> - ファイルのアップロードステータスを追跡するには、ログの種類に [ユーザのアクセス] を使用してログクエリを実行します。
>
>   詳細については、318 ページの「ログクエリを使用する」を参照してください。
> - 不審オブジェクトの抽出ステータスを追跡するには、[コマンド追跡] 画面を使用します。
>
>   詳細については、240 ページの「コマンド追跡」を参照してください。

Apex Central は、選択した OpenIOC ファイルを OpenIO ファイルリストにアップロードます。

注意

- 初期設定を選択した場合、Apex Central は不審オブジェクトをユーザ指定の不審オブジェクトリストに自動的に抽出します。
- 次のシナリオでは、OpenIOC ファイルリストの [抽出されたオブジェクト] 列に「N/A」と表示されます。
  - 不審オブジェクトを自動的に抽出せずに OpenIOC ファイルをアップロードした場合。
  - Apex Central が OpenIOC ファイルから不審オブジェクトを抽出できなかった場合。

8. アップロードした OpenIOC ファイルから不審オブジェクトを手動で抽出するには、次の手順を実行します。

   a. アップロードしたファイルのファイル名の横にあるチェックボックスをオンにします。

   b. [抽出] をクリックします。

      [抽出されたオブジェクト] 列に、OpenIOC ファイルからユーザ指定の不審オブジェクトリストに抽出された不審オブジェクトの数が表示されます。

      - 特定のファイルのコピーをダウンロードするには、[ファイル名] 列にあるリンクをクリックします。
      - ファイル抽出のステータスを追跡するには、[コマンド追跡] 画面を使用します。

        詳細については、240 ページの「コマンド追跡」を参照してください。
      - ユーザ指定の不審オブジェクトリストのフィルタ 画面で抽出された不審オブジェクトを表示するには、[抽出されたオブジェクト] 列の数字をクリックします。
      - ファイルを削除するには、1 つ以上のファイルのファイル名の横にあるチェックボックスをオンにし、[削除] をクリックします。

注意

- ファイルを削除しても、抽出された不審オブジェクトはユーザ指定の不審オブジェクトリストから削除されません。
- Apex Central でファイルから不審オブジェクトの抽出が完了するまでは、ファイルを削除できません。

9. アップロードした OpenIOC ファイルを診断条件として使用して脅威の今すぐ調べるには、次の手順を実行します。

重要

- 脅威の調査には、有効な Endpoint Sensor ライセンスが必要です。有効な Endpoint Sensor ライセンスがあることを確認するか、サービスプロバイダに問い合わせてアクティベーションコードを入手してください。
- Endpoint Sensor ライセンスをアクティベートしたら、[ポリシー管理] 画面 ([ポリシー] > [ポリシー管理]) で Apex One セキュリティエージェントポリシーまたは Apex One (Mac) ポリシーを作成して、Endpoint Sensor 機能を有効にします。

  詳細については、ポリシー設定画面のオンラインヘルプをご覧ください。

a. アップロードしたファイルのファイル名の横にあるチェックボックスをオンにします。

b. 次のいずれかの脅威の調査を実行します。

調査	説明
履歴調査	履歴調査は、サーバメタデータを使用して詳細な分析対象候補のエンドポイントを特定します。 [影響の分析] ボタンにマウスを重ねて [履歴調査] をクリックします。 注意 履歴調査画面 ([レスポンス] > [履歴調査]) から履歴調査を実行することもできます。 詳細については、529 ページの「履歴調査に対するユーザ定義の条件の使用」を参照してください。 履歴調査に使用されるサーバメタデータに関する具体的な情報については、526 ページの「Endpoint Sensor のメタデータ」を参照してください。
1 回限りの調査	1 回限りの調査はオンデマンドで生成されるライブ調査です。現在ディスクにあるすべてのファイルと現在メモリで実行されているすべてのプロセスを調査します。 [影響の分析] ボタンにマウスを重ねて [ライブ調査] > [手動] に移動します。 注意 1 回限りの調査は、ライブ調査画面 ([レスポンス] > [ライブ調査]) の [1 回限りの調査] タブから実行することもできます。 詳細については、551 ページの「1 回限りの調査を開始する」を参照してください。

調査	説明
予約調査	予約調査は、指定の間隔で自動的に実行されるライブ調査です。 [影響の分析] ボタンにマウスを重ねて [ライブ調査] > [自動 (予約)] を選択します。 **注意** 予約調査は、ライブ調査画面 ([レスポンス] > [ライブ調査]) の [予約調査] タブから実行することもできます。 詳細については、554 ページの「予約調査」を参照してください。

影響を分析してユーザ指定の不審オブジェクトからの IOC に対応する

不審オブジェクトまたは適切な形式の IOC (STIX または OpenIOC) ファイルを Apex Central に追加した後、特定のファイル、ファイル SHA-1、IP アドレス、またはドメインオブジェクトを選択して影響分析を実行してネットワーク内に脅威が存在するかどうかを判断し、他のエンドポイントに脅威が拡散しないよう軽減対策を実行できます。

詳細については、次のトピックを参照してください。

- 496 ページの「ユーザ指定の不審オブジェクトリストをインポートする」
- 500 ページの「ユーザ指定の不審オブジェクトリストに OpenIOC オブジェクトを追加する」
- 497 ページの「ユーザ指定の不審オブジェクトリストに STIX オブジェクトを追加する」

重要

- 影響分析には、有効な Apex One Endpoint Sensor ライセンスが必要です。有効な Apex One Endpoint Sensor ライセンスがあることを確認し、適切な [Apex One セキュリティエージェント] ポリシーまたは [Apex One (Mac)] ポリシーに対して Endpoint Sensor 機能を有効にしてください。

  詳細については、ポリシー設定画面のオンラインヘルプをご覧ください。

- エンドポイントの隔離のために、対象エンドポイントに Apex One セキュリティエージェントをインストールする必要があります。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス]に移動します。

   [カスタムインテリジェンス] 画面が表示されます。

2. [ユーザ指定の不審オブジェクト] タブをクリックします。

   ユーザ指定の不審オブジェクトリストが表示されます。

3. リストから 1 つ以上のオブジェクトを選択します。

   注意

   Apex Central は URL オブジェクトの影響分析をサポートしていません。

4. [影響の分析] をクリックします。

   Endpoint Sensor がエージェントと通信し、検出された不審オブジェクトのエージェントログを評価します。

   注意

   影響分析時間はネットワーク環境に応じて異なります。

5. 確認するオブジェクトの左側にある矢印を展開します。

   - [危険性の高いエンドポイント] リストには、引き続き不審オブジェクトの影響を受けているすべてのエンドポイントとユーザが表示されます。

- 「ファイル」の検出では、[最新の処理結果] 列に管理下の製品によって報告された最新の処理結果が表示されます。
- その他のすべての検出の種類では、[最新の処理結果] 列に「N/A」と表示されます。

- [危険性の高い受信者] リストには、引き続き不審オブジェクトの影響を受けているすべての受信者が表示されます。

エンドポイントを隔離する

危険性の高いエンドポイントを隔離して調査を実行し、セキュリティの問題を解決します。すべての問題を解決したら、すぐに接続を復元します。

重要

- エンドポイントの隔離には、有効な Apex Central ライセンスが必要です。
- バージョン 11 SP1～XG SP1 を実行しているウイルスバスター Corp.クライアントの場合、エンドポイント隔離を実行するにはウイルスバスター Corp. ファイアウォールを有効にする必要があります。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。
2. エンドポイントの表示を選択します。
3. リスト内のエンドポイントの名前をクリックします。
4. 表示される [エンドポイント] 情報画面で [タスク] > [隔離] をクリックします。

   Apex Central では、次の理由により、エンドポイント上で [隔離] オプションが無効になります。

   - エンドポイントのエージェントでサポート対象外のバージョンが実行されている
   - Apex Central へのログオンに使用されているユーザアカウントに必要な権限がない

5. [エンドポイント] 情報画面の上部にメッセージが表示され、その画面で隔離ステータスを監視できます。隔離が終了すると、メッセージが閉じられ、対象エンドポイントにユーザへの通知が表示されます。

   隔離プロセス中に問題が発生した場合、[エンドポイント - <名前>] 画面の上部に問題を通知するメッセージが表示されます。

6. Apex Central ネットワーク上の隔離されたエンドポイントをすべて表示するには、[ユーザ/エンドポイントディレクトリ] ツリーで [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み] ノードを順にクリックします。

7. (オプション) 隔離されたすべてのエンドポイントに許可する送受信トラフィックを設定するには、次の手順を実行します。

   a. [隔離されたエンドポイント上のトラフィック制御] を選択します。

   b. [受信トラフィック] または [送信トラフィック] セクションを展開します。

   c. [プロトコル]、[IP アドレス]、および [送信先ポート] を指定して、許可するトラフィックを指定します。

      コンマを使用して複数の送信先ポートを区切ります。

   d. [送信先ポート] 情報の右側の - コントロールをクリックして、複数の送受信エントリを追加します。

   注意

   許可するトラフィックの設定を変更した後、以前に隔離されたエンドポイントと後で隔離されるエンドポイントはすべて、送受信トラフィックの設定が適用されます。

8. 隔離されたエンドポイントでセキュリティの脅威が解決したら、次の場所からネットワーク接続を復元します。

   - [エンドポイント] 情報画面: [タスク] > [復元]をクリックします。
   - [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み]: 表内のエンドポイントの行を選択して、[タスク] > [ネットワーク接続の復元] をクリックします。

9. 画面の上部にメッセージが表示され、その画面で復元ステータスを監視できます。復元が終了すると、メッセージが閉じられ、対象エンドポイントにユーザへの通知が表示されます。

   復元プロセス中に問題が発生した場合、画面の上部に問題を通知するメッセージが表示されます。

Connected Threat Defense 製品の統合

Connected Threat Defense 戦略では、多くのトレンドマイクロ製品を統合します。次の図は主な製品との関係を示しています。

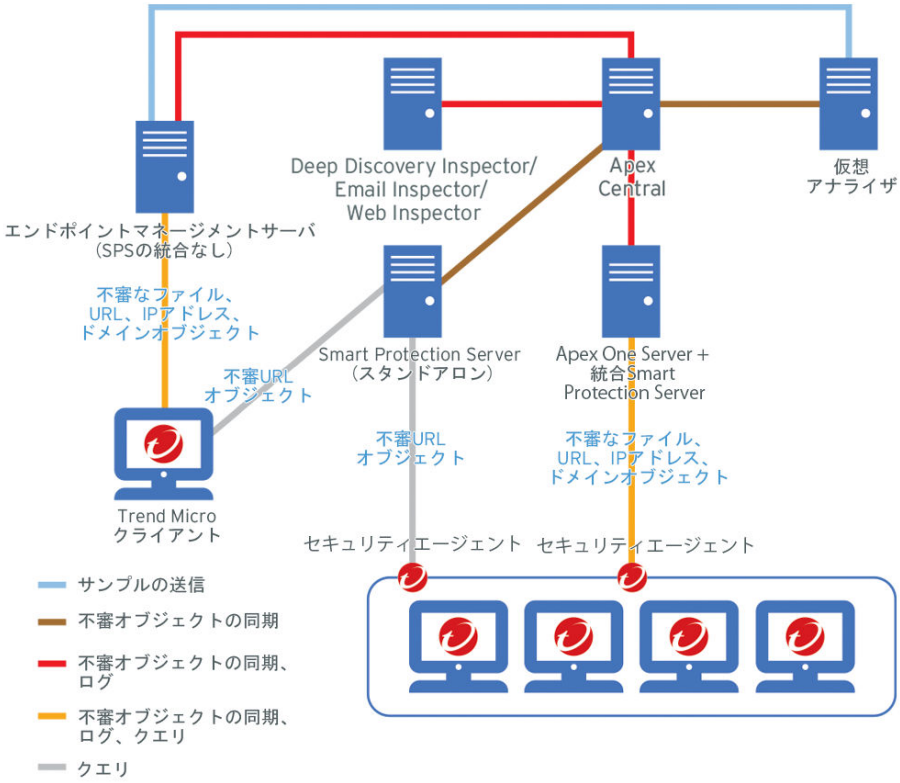


図 19-1. エンドポイント保護のトポロジ例

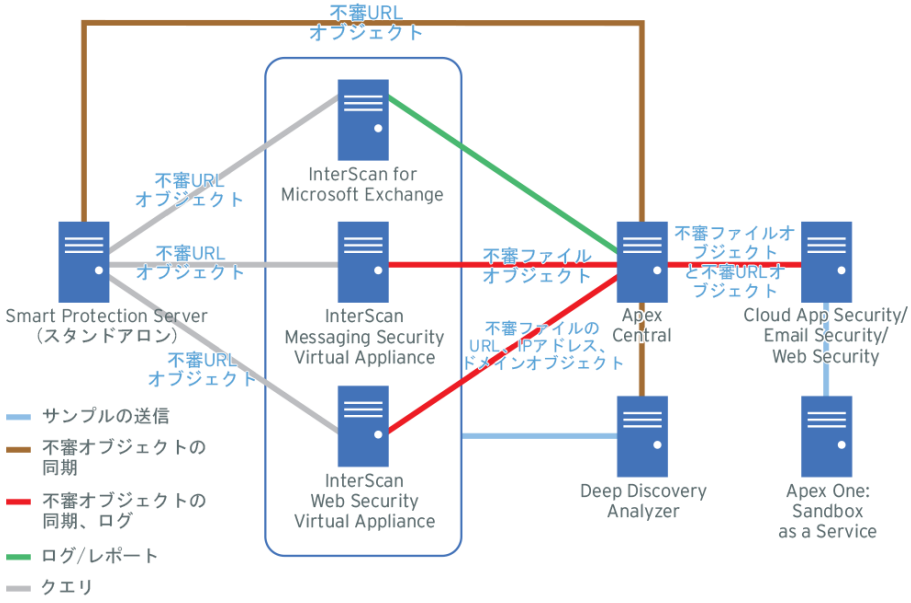


図 19-2. メッセージングとネットワークセキュリティのトポロジを表す例

Apex Central は、ログ分析の実行や検出ファイルと同期した不審オブジェクトリストの比較により、登録された他のトレンドマイクロ製品の監視を強化します。

各主要製品の Apex Central の登録および不審オブジェクトリストの同期については、以下を参照してください。各製品の Connected Threat Defense の対応状況については、別途製品 Q&A にて確認してください。

https://success.trendmicro.com/jp/solution/1117782

Apex Central

要件	説明
製品バージョン	• Apex Central (任意のバージョン) • Control Manager 7.0 (またはそれ以降)
Apex Central の登録	Apex Central 管理コンソールを使用せずに Apex Central に製品を登録した場合、次の Apex Central 登録情報が必要です。 • サーバの FQDN または IP アドレス • ポート: 初期設定では、Apex Central は HTTP ポート 80 または HTTPS ポート 443 を使用します。 Apex Central 管理コンソールを使用して登録した製品の場合、[運用管理] > [管理下のサーバ] > [サーバの登録] に進み、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	不審オブジェクトリストを Apex Central と自動的に同期しない製品の場合、次の API 情報が必要です。 • API キー: API キーを入手するには、Apex Central 管理コンソールを開いて、[脅威インテリジェンス] > [配信設定] に移動します。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • 影響分析 • エンドポイントの隔離 • IOC の管理

Apex One

要件	説明
製品バージョン	• Apex One 2019 • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降)

要件	説明
Apex Central の登録	Apex One Web コンソールの [管理] > [設定] > [Apex Central] 必須の Apex Central 情報: • サーバの FQDN または IP アドレス • ポート: 初期設定では、Apex Central は HTTP ポート 80 または HTTPS ポート 443 を使用します。
不審オブジェクトリストの同期	Apex One Web コンソールの [管理] > [設定] > [不審オブジェクトリスト] 必須の Apex Central 情報: • なし 注意 Apex One は、Apex Central の登録中に、必要な API キー情報を Apex Central サーバから自動的に取得します。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • エンドポイントの隔離

Apex One Endpoint Sensor

要件	説明
アクティベーションコード	追加のライセンスが必要です。サービスプロバイダに問い合わせてアクティベーションコードを入手します。

要件	説明
機能の有効化	Apex Central 管理コンソールから Endpoint Sensor を有効にします。[ポリシー] > [ポリシー管理] に移動し、[製品] リストから [Apex One セキュリティエージェント] を選択してポリシーを作成または変更します。[Endpoint Sensor 設定] を展開して、[Endpoint Sensor を有効にする] チェックボックスをオンにします。 詳細については、ポリシー設定画面のオンラインヘルプをご覧ください。
不審オブジェクトリストの同期	Apex One Endpoint Sensor では、不審オブジェクトリストが Apex Central と同期されません。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 影響分析 • エンドポイントの隔離 • IOC の管理

Apex One Sandbox as a Service

要件	説明
アクティベーションコード	追加のライセンスが必要です。サービスプロバイダに問い合わせてアクティベーションコードを入手します。
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [ライセンス管理] > [Apex Central] に移動して、[Apex One Sandbox as a Service] セクションで [新しいアクティベーションコードを入力してください] をクリックし、アクティベーションコードを入力してアクティベートします。
不審オブジェクトリストの同期	Apex Central への登録後に自動的に実行されます。 初期設定では、不審オブジェクトリストは Apex Central サーバと 10 分ごとに同期されます。

要件	説明
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理

Cloud App Security

要件	説明
製品バージョン	5.0 (またはそれ以降)
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	詳細については、Cloud App Security のオンラインヘルプを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

Deep Discovery Analyzer

要件	説明
製品バージョン	6.5 (またはそれ以降)
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。

要件	説明
不審オブジェクトリストの同期	Apex Central への登録後に自動的に実行されます。 初期設定では、不審オブジェクトリストは Apex Central サーバと 10 分ごとに同期されます。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理

Deep Discovery Director

要件	説明
製品バージョン	5.0 (またはそれ以降)
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	Apex Central への登録後に自動的に実行されます。 初期設定では、不審オブジェクトリストは Apex Central サーバと 10 分ごとに同期されます。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理

Deep Discovery Email Inspector

要件	説明
製品バージョン	3.5 以降

要件	説明
Apex Central の登録	詳細については、Deep Discovery Email Inspector 管理者ガイドを参照してください。
不審オブジェクトリストの同期	詳細については、Deep Discovery Email Inspector 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信

Deep Discovery Inspector

要件	説明
製品バージョン	5.0 (またはそれ以降)
Apex Central の登録	Deep Discovery Inspector の管理コンソールの [管理] > [統合製品/サービス] > [Apex Central] 必要な Apex Central の情報: • サーバの FQDN または IP アドレス • ポート: 初期設定では、Apex Central は HTTP ポート 80 または HTTPS ポート 443 を使用します。 詳細については、Deep Discovery Inspector 管理者ガイドを参照してください。
不審オブジェクトリストの同期	Deep Discovery Inspector の管理コンソールの [管理] > [統合製品/サービス] > [Apex Central] 必要な Apex Central の情報: • API キー: API キーを入手するには、Apex Central 管理コンソールを開いて、[脅威インテリジェンス] > [配信設定] に移動します。 詳細については、Deep Discovery Inspector 管理者ガイドを参照してください。

要件	説明
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理

Deep Discovery Web Inspector

要件	説明
製品バージョン	2.5 以降
Apex Central の登録	詳細については、Deep Discovery Web Inspector 管理者ガイドを参照してください。
不審オブジェクトリストの同期	詳細については、Deep Discovery Web Inspector 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信

Deep Security Manager

重要

Deep Security as a Service では Connected Threat Defense はサポートされていません。Connected Threat Defense の機能は、Deep Security Manager のオンプレミスサーバでのみサポートされています。

要件	説明
製品バージョン	10.0 (またはそれ以降)

要件	説明
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	Apex Central への登録後に自動的に実行されます。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

Trend Micro Email Security

要件	説明
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	詳細については、Trend Micro Email Security 管理コンソールのオンラインヘルプを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

InterScan Messaging Security Virtual Appliance

要件	説明
製品バージョン	9.1 (またはそれ以降)

要件	説明
Apex Central の登録	詳細については、InterScan Messaging Security Virtual Appliance 管理者ガイドを参照してください。
不審オブジェクトリストの同期	Apex Central への登録後に自動的に実行されます。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

InterScan Web Security Virtual Appliance

要件	説明
製品バージョン	6.5 SP2 Patch 4 (またはそれ以降)
Apex Central の登録	詳細については、InterScan Web Security Virtual Appliance 管理者ガイドを参照してください。
不審オブジェクトリストの同期	詳細については、InterScan Web Security Virtual Appliance 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

InterScan for Microsoft Exchange

要件	説明
製品バージョン	12.5 (またはそれ以降)
Apex Central の登録	詳細については、InterScan for Microsoft Exchange 管理者ガイドを参照してください。
不審オブジェクトリストの同期	詳細については、InterScan for Microsoft Exchange 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトのサンプルの送信

Smart Protection Server

要件	説明
製品バージョン	3.3 Patch 2 (またはそれ以降)
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。

要件	説明
不審オブジェクトリストの同期	Smart Protection Server の Web コンソールで、[Smart Protection] > [不審オブジェクト] に移動します。 不審オブジェクトリストのソースに必要な情報: • サービスの URL • ポート番号 リストのソースが Apex Central である場合、初期設定のポートは HTTP ポート 80 または HTTPS ポート 443 です。 • API キー: サーバ管理者から提供されます。 リストのソースが Apex Central である場合、Apex Central 管理コンソールを開き、[運用管理] > [不審オブジェクト] > [配信設定] に移動します。 **注意** Smart Protection Server 3.3 以降の場合は、Apex Central への登録中に、必要な API キー情報が Smart Protection Server に送信されます。 詳細については、Smart Protection Server 管理ガイドを参照してください。
統合された Connected Threat Defense 機能	• 不審オブジェクトリストの同期 • 不審オブジェクト検出時の処理

Endpoint Application Control

要件	説明
製品バージョン	2.0 SP1 Patch 1 (またはそれ以降)
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。

要件	説明
不審オブジェクトリストの同期	Apex Central への登録後に自動的に実行されます。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理

Trend Micro Web Security as a Service

要件	説明
Apex Central の登録	Apex Central の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	詳細については、Trend Micro Web Security as a Service のオンラインヘルプを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

第 20 章

脅威の調査

本章では、脅威の調査を使用して調査を実行し、結果を分析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。

脅威の調査の概要

[脅威の調査] を使用して、ネットワーク内の不審オブジェクトを特定します。

脅威の調査では、Endpoint Sensor および Active Directory からの情報を関連付け、ネットワーク全体のエンドポイントとユーザアカウントに関する攻撃情報を表示できます。

ネットワークが進行中の攻撃または APT (標的型サイバー攻撃) の対象である場合、脅威の調査では次のことが可能です。

- 標的型攻撃によるダメージの範囲を診断する
- 攻撃の侵入と進行に関する情報を提供する
- 効果的なセキュリティインシデント対応の計画を支援する

脅威の調査には次の種類があります。

- 履歴調査では、詳細な分析対象候補のエンドポイントをすばやく特定できます。履歴調査は、サーバのメタデータを使用してすばやく結果を返します。

  詳細については、527 ページの「履歴調査」を参照してください。

- ライブ調査では、現在のシステムの状態を調査します。ライブ調査は指定した期間で実行されるよう設定でき、OpenIOC ルールや YARA ルールを使用した広範な条件がサポートされます。

  詳細については、548 ページの「ライブ調査」を参照してください。

Endpoint Sensor のメタデータ

メタデータとは、エンドポイントから収集され、サーバにアップロードされるデータのことです。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。

詳細については、527 ページの「履歴調査」を参照してください。

収集されるメタデータの種類は、エンドポイントにインストールされた OS によって異なります。

表 20-1. OS によるメタデータ

OS	メタデータ	
Windows	• ホスト (名前/IP アドレス) • ユーザアカウント • ファイル名 • ファイルパス • ハッシュ値 (SHA-1、SHA-256、および MD5)	• レジストリキー • レジストリデータ • レジストリ名 • コマンドライン • URL
macOS	• ホスト (名前/IP アドレス) • ユーザアカウント • ファイル名 • URL	• ファイルパス • ハッシュ値 (SHA-1、SHA-256、および MD5) • コマンドライン

注意

- URL の収集は、コールバックイベントの処理のみに適用され、HTTP プロトコルのみをサポートします。
- メタデータの設定は [ポリシー管理] 画面で行います。
- 履歴調査中に利用可能なデータは、セキュリティエージェントデータのサブセットであり、高リスクのファイルタイプに関する情報のみが含まれています。診断で結果が返されなかった場合、ライブ調査を実行することをお勧めします。

履歴調査

履歴調査では、詳細な分析対象候補のエンドポイントをすばやく特定できます。履歴調査は、サーバのメタデータを使用してすばやく結果を返します。

この画面にアクセスするには、[レスポンス] > [履歴調査] に移動します。

履歴調査画面には 2 つのタブがあります。

タブ	説明
診断	診断を使用して、次のことを実行します。 • 脅威の感染率と、脅威がネットワークに存在している期間を評価します。すべての履歴データが診断の対象になります。 • 単純な条件を使用して脅威の存在を判定します。診断でサポートされる条件は限定的です。 診断では、次の種類の条件がサポートされています。 • ユーザ定義: ユーザ指定の条件を 10 件まで指定またはロードするか、C&C コールバックイベントをロードします。 詳細については、535 ページの「ユーザ定義の条件でサポートされる形式」を参照してください。 • OpenIOC ファイル: OpenIOC ルールを使用して、調査条件を定義します。履歴調査ではすべての条件が破棄され、OpenIOC ファイルで指定された痕跡のいずれかと照合します。 詳細については、543 ページの「履歴調査でサポートされる IOC の痕跡」を参照してください。 サーバのメタデータが診断対象となり、一致が検出されるとすぐに結果ペインが更新されます。サーバのメタデータの診断が完了するまで数分かかる場合があります。 詳細については、529 ページの「履歴調査に対するユーザ定義の条件の使用」を参照してください。

タブ	説明
Root Cause Analysis の結果	診断により一致が検出されると、管理者は Root Cause Analysis を生成して次の処理を実行できます。 • 指定した条件に関連するすべてのオブジェクトのリストを 作成する • 関連するオブジェクトに注意が必要なオブジェクトがないかを特定する • 一致したオブジェクトの実行につながった一連のイベントを確認する Root Cause Analysis の生成が完了するまで時間がかかる場合があります。タスクの進行状況を監視するには、[Root Cause Analysis] タブを使用します。 詳細については、560 ページの「分析チェーン」を参照してください。

履歴調査に対するユーザ定義の条件の使用

注意

現在のシステムの状態を調査するには、[ライブ調査] を使用してください。

詳細については、550 ページの「1 回限りの調査を開始する」を参照してください。

手順

1. [レスポンス] > [履歴調査] に移動します。
2. [ユーザ定義] をクリックします。
3. 次のオプションのいずれかを選択します。
   - [すべての条件に一致]: 指定したすべての条件に一致するオブジェクトを検出します。
   - [いずれかの条件に一致]: 指定したいずれかの条件に一致するオブジェクトを検出します。

4. [新しい条件] をクリックし、条件の種類を選択して、有効な情報を指定します。

   詳細については、535 ページの「ユーザ定義の条件でサポートされる形式」を参照してください。

   条件を管理するには、次の操作を行います。

   - [リセット] をクリックして、指定した条件をすべて解除します。
   - 今後の調査のために条件を保存するには、  をクリックし、条件名を指定します。

   注意

   履歴調査では、最大 10 件のユーザ定義の条件がサポートされています。

5. (オプション) 既存のユーザ定義の条件をロードするには、[条件の選択] をクリックします。

   a. [はい] をクリックします。

      注意

      既存の条件を適用すると、現在指定されている条件がすべて上書きされます。

   b. [保存した条件] タブに移動します。

   c. 条件を選択します。

      条件を管理するには、次の操作を行います。

      - [前回の使用日時] 列を使用して条件を並べ替えます。
      - [削除] アイコンを 使用して、保存した条件を削除します。

   d. [保存した条件の追加] をクリックします。

6. (オプション) C&C コールバックイベントをロードするには、[条件の選択] をクリックします。

   a. [はい] をクリックします。

注意

既存の条件を適用すると、現在指定されている条件がすべて上書きされます。

b. [C&C コールバックイベント] タブに移動します。

c. 条件を選択します。

[期間] をクリックして、指定した時間で C&C コールバックイベントをフィルタします。

d. [C&C コールバックイベントのロード] をクリックします。

注意

[ログクエリ] 画面には、C&C コールバックイベントに関する追加の詳細が表示されるため、選択する前に確認することができます。[ログクエリ] 画面を開くには、[レポート] > [ログ] > [ログクエリ] に移動した後、[ネットワークイベント] > [C&C コールバック] でフィルタします。

7. [診断] をクリックします。

8. 結果ペインで、表示された結果を確認します。

注意

- 履歴調査が実行されるまでしばらく待ちます。この調査では、メタデータに一致するオブジェクトが見つかるとすぐに結果の表に行が追加されます。調査が完了するまでに数分かかる場合があります。
- 履歴調査中に利用可能なデータは、セキュリティエージェントデータのサブセットであり、高リスクのファイルタイプに関する情報のみが含まれています。診断で結果が返されなかった場合、ライブ調査を実行することをお勧めします。

次の詳細を確認できます。

列名	説明
エンドポイント	一致するオブジェクトを含むエンドポイントの名前を示します。 クリックすると、エンドポイントの詳細が表示されます。
ステータス	エンドポイントの現在の接続ステータスを示します。
IP アドレス	一致するオブジェクトを含むエンドポイントの IP アドレスを示します。 IP アドレスはネットワークによって割り当てられます。
オペレーティングシステム	エンドポイントで使用されている OS を示します。
ユーザ	セキュリティエージェントが一致したオブジェクトを最初に記録したときにログインしていたユーザのユーザ名を示します。 ユーザ名をクリックすると、ユーザの詳細が表示されます。
管理サーバ	感染エンドポイントを管理するサーバを示します。
最初に確認された日時	セキュリティエージェントが一致したオブジェクトを最初に記録した日時を示します。

列名	説明
詳細	このアイコンをクリックすると、[一致項目の詳細] 画面が開きます。 [一致項目の詳細] 画面には、以下の詳細が表示されます。 • [条件]: 診断で使用される条件 • [最初に確認された日時]: セキュリティエージェントが一致したオブジェクトを最初に記録した日時 • [CLI/レジストリでの検出数]: コマンドラインまたはレジストリエントリで検出された一致の数 値をクリックすると、詳細が表示されます。 • [評価]: トレンドマイクロインテリジェンスによって割り当てられた評価 評価が「不正」のオブジェクトについては、Threat Connect または VirusTotal で詳細を確認できます。 • [影響を受けたエンドポイント]: 不正という評価である場合、同様の一致したオブジェクトが検出されたエンドポイントの数 この数には、過去 90 日間に影響を受けたエンドポイントだけが含まれます。
アスタリスク (*)	「重要」としてタグ付けされたエンドポイントを示します。

9. さらなる処理が必要なエンドポイントを 1 つ以上選択します。

注意

履歴調査の結果には、macOS エンドポイントが含まれる場合があります。macOS エンドポイントに利用できる処理がないため、これらのエンドポイントのチェックボックスは無効になっています。

処理	説明
Root Cause Analysis の生成	Root Cause Analysis を生成し、一致したオブジェクトの実行につながった一連のイベントを確認します。 詳細については、544 ページの「診断から Root Cause Analysis を開始する」を参照してください。
ライブ調査を開始	現在のシステムの状態に対して同じ条件で新しい調査を実行します。 重要 Windows プラットフォームにインストールされたセキュリティエージェントに対してのみ使用できます。 [ライブ調査] 画面が表示され、既存の条件を使用して 1 回限りの調査が新しく開始されます。 ユーザ定義の条件を使用した診断の場合、[ライブ調査] では、選択したエンドポイントのみが条件として使用されます。 詳細については、550 ページの「1 回限りの調査を開始する」を参照してください。

処理	説明
エンドポイントを隔離	選択したエンドポイントがネットワークから切断されます。 **重要** Windows プラットフォームにインストールされたセキュリティエージェントに対してのみ使用できます。 隔離したエンドポイントでセキュリティの脅威を解決すると、[ディレクトリ] > [ユーザ/エンドポイント] 画面の次の場所に、隔離したエンドポイントのネットワーク接続を復元するオプションが表示されます。 • [エンドポイント] > [すべて]: 表内のエンドポイント名をクリックし、表示された画面で [タスク] > [復元] の順にクリックします。 • [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み]: 表内のエンドポイントの行を選択し、[タスク] > [ネットワーク接続の復元] の順にクリックします。

ユーザ定義の条件でサポートされる形式

重要

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。

種類	項目
ユーザ名 (完全一致のみ)	Active Directory アカウントまたはローカルユーザの名前を指定します。 例: • jane_smith 注意 ローカルユーザアカウントの名前 (<user name>) のみ使用します。ドメイン名は含めないでください。
ファイル名 (完全一致のみ)	拡張子を含む完全なファイル名を指定します。 例: • filename.exe
ファイルディレクトリ (完全一致のみ、オンプレミスのみ)	ファイル名を除くフルパスを指定します。 例: • `c:\windows\system32\wbem\`
ファイルハッシュ値 (完全一致のみ)	ファイルのハッシュ値を指定します。 例: • `SHA-1: a2da9cda33ce378a21f54e9f03f6c0c9efba61fa` 注意 Endpoint Sensor は、初期設定では SHA-1 値だけを記録します。SHA-256 または MD5 ハッシュ値を使用するには、追加のハッシュの種類も含まれるように、エージェントポリシーをアップデートします。

種類	項目
FQDN/IP アドレス/ホスト名 (完全一致のみ)	調査対象エンドポイントが確立したネットワーク接続を識別するためのリモートエンドポイントの FQDN、IP アドレス、またはホスト名を指定します。 注意 IPv6 形式はサポートされていません。 例: • cncserver.com • malicioussite.com • 192.168.0.1
レジストリキー (部分一致検索がサポートされます)	レジストリキー、レジストリ値の名前、またはレジストリ値のデータの全体または一部を指定します。 注意 • リソースがエンドポイントに与える影響を軽減するために、トレンドマイクロは重要なレジストリの場所のアクティビティだけを記録します。 調査が失敗した後にさらに調査を続ける場合には、ライブ調査を実行してください。 • SID 値をレジストリ条件として指定しないでください。調査では、カスタムのレジストリ条件として SID 値がサポートされていません。 • 調査条件としてレジストリデータを使用する場合には、以下の制限があります。 • 条件に含めることができるエントリは、最大で 10 個です。 • 各エントリは 2 文字以上でなければなりません。 • エントリにスペースを含めることはできません。
レジストリ値の名前 (部分一致検索がサポートされます)	
レジストリ値のデータ (部分一致検索がサポートされます)	

種類	項目
CLI コマンド (部分一致検索がサポートされます)	エントリを追加するには、全体または一部のコマンドライン文字列を指定し、<Enter> キーを押します。 **注意** 調査条件としてコマンドラインを使用する場合には、以下の制限があります。 • 条件に含めることができるエントリは、最大で 10 個です。 • 各エントリは 2 文字以上でなければなりません。 • エントリにスペースを含めることはできません。

履歴調査に OpenIOC ファイルを使用する

注意

現在のシステムの状態を調査するには、[ライブ調査] を使用してください。

詳細については、550 ページの「1 回限りの調査を開始する」を参照してください。

手順

1. [レスポンス] > [履歴調査]に移動します。
2. [OpenIOC ファイル] タブをクリックします。

注意

履歴調査で OpenIOC ファイルを使用する場合は、次の制限があります。

- 1 度にロードできる OpenIOC ファイルは 1 つだけです。
- OpenIOC ファイルに指定されている演算子はすべて OR に変更されます。
- サポートされる条件は `IS` のみです。他の条件を使用したエントリは無視され、取り消し線が付けられます。
- サポート対象の痕跡は、収集されたメタデータに適用可能な痕跡のみです。サポート対象外の痕跡を使用したエントリは無視され、取り消し線が付けられます。

  詳細については、543 ページの「履歴調査でサポートされる IOC の痕跡」を参照してください。

3. 新しい OpenIOC ファイルをアップロードして調査するには、次の手順を実行します。
   a. [OpenIOC ファイルのアップロード] をクリックします。
   b. 有効な OpenIOC ファイルを選択します。
   c. [開く] をクリックします。
4. 既存の OpenIOC ファイルを使用して調査するには、次の手順を実行します。
   a. [既存の OpenIOC ファイルを使用] をクリックします。
   b. ファイルを選択します。
   c. [適用] をクリックします。
5. [診断] をクリックします。
6. 結果ペインで、表示された結果を確認します。

注意

- 履歴調査が実行されるまでしばらく待ちます。この調査では、メタデータに一致するオブジェクトが見つかるとすぐに結果の表に行が追加されます。調査が完了するまでに数分かかる場合があります。
- [エンドポイント] ラベルにカーソルを合わせると、診断の進行状況を示すポップアップが表示されます。
- 履歴調査中に利用可能なデータは、セキュリティエージェントデータのサブセットであり、高リスクのファイルタイプに関する情報のみが含まれています。診断で結果が返されなかった場合、ライブ調査を実行することをお勧めします。

次の詳細を確認できます。

列名	説明
エンドポイント	一致するオブジェクトを含むエンドポイントの名前を示します。 クリックすると、エンドポイントの詳細が表示されます。
ステータス	エンドポイントの現在の接続ステータスを示します。
IP アドレス	一致するオブジェクトを含むエンドポイントの IP アドレスを示します。 IP アドレスはネットワークによって割り当てられます。
オペレーティングシステム	エンドポイントで使用されている OS を示します。
ユーザ	セキュリティエージェントが一致したオブジェクトを最初に記録したときにログインしていたユーザのユーザ名を示します。 ユーザ名をクリックすると、ユーザの詳細が表示されます。
管理サーバ	感染エンドポイントを管理するサーバを示します。
最初に確認された日時	セキュリティエージェントが一致したオブジェクトを最初に記録した日時を示します。

列名	説明
詳細	このアイコンをクリックすると、[一致項目の詳細] 画面が開きます。 [一致項目の詳細] 画面には、以下の詳細が表示されます。 • [条件]: 診断で使用される条件 • [最初に確認された日時]: セキュリティエージェントが一致したオブジェクトを最初に記録した日時 • [CLI/レジストリでの検出数]: コマンドラインまたはレジストリエントリで検出された一致の数 値をクリックすると、詳細が表示されます。 • [評価]: トレンドマイクロインテリジェンスによって割り当てられた評価 評価が「不正」のオブジェクトについては、Threat Connect または VirusTotal で詳細を確認できます。 • [影響を受けたエンドポイント]: 不正という評価である場合、同様の一致したオブジェクトが検出されたエンドポイントの数 この数には、過去 90 日間に影響を受けたエンドポイントだけが含まれます。
アスタリスク (*)	「重要」としてタグ付けされたエンドポイントを示します。

7. さらなる処理が必要なエンドポイントを 1 つ以上選択します。

注意

履歴調査の結果には、macOS エンドポイントが含まれる場合があります。macOS エンドポイントに利用できる処理がないため、これらのエンドポイントのチェックボックスは無効になっています。

処理	説明
Root Cause Analysis の生成	Root Cause Analysis を生成し、一致したオブジェクトの実行につながった一連のイベントを確認します。 詳細については、544 ページの「診断から Root Cause Analysis を開始する」を参照してください。
ライブ調査を開始	現在のシステムの状態に対して同じ条件で新しい調査を実行します。 [ライブ調査] 画面が表示され、既存の条件を使用して 1 回限りの調査が新しく開始されます。 OpenIOC ファイルを使用した診断の場合、[ライブ調査] では、現在の OpenIOC ファイルと選択したエンドポイントの両方が条件として使用されます。 詳細については、550 ページの「1 回限りの調査を開始する」を参照してください。
エンドポイントを隔離	選択したエンドポイントがネットワークから切断されます。 **注意** 隔離したエンドポイントでセキュリティの脅威を解決すると、[ディレクトリ] > [ユーザ/エンドポイント] 画面の次の場所に、隔離したエンドポイントのネットワーク接続を復元するオプションが表示されます。 • [エンドポイント] > [すべて]: 表内のエンドポイント名をクリックし、表示された画面で [タスク] > [復元] の順にクリックします。 • [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み]: 表内のエンドポイントの行を選択し、[タスク] > [ネットワーク接続の復元] の順にクリックします。

履歴調査でサポートされる IOC の痕跡

OpenIOC ファイルは、侵入の痕跡 (IOC) を示す情報が 1 つ以上含まれている XML ファイルです。OpenIOC ファイルでは、選択した調査の種類でサポートされるインジケータ (痕跡) 名が使用されていることを確認してください。

次の表は、調査でサポートされる IOC のインジケータを示しています。

表 20-2. 履歴調査でサポートされる IOC の痕跡

カテゴリ	項目	必要な条件
DNSENTRYITEM	HOST	IS
	RECORDDATA/HOST	IS
	RECORDDATA/IPV4ADDRESS	IS
FILEITEM	FILENAME	IS
	SHA1SUM	IS
	SHA2SUM	IS
	MD5SUM	IS
PORTITEM	LOCALIP	IS
	REMOTEIP	IS
PROCESSITEM	ARGUMENTS	CONTAINS
	NAME	IS
	SECTIONLIST/ MEMORYSECTION/SHA1SUM	IS
	SECTIONLIST/ MEMORYSECTION/ SHA256SUM	IS
	SECTIONLIST/ MEMORYSECTION/MD5SUM	IS

カテゴリ	項目	必要な条件
REGISTRYITEM	KEYPATH	CONTAINS
	VALUE	CONTAINS
	VALUENAME	CONTAINS
	USERNAME	IS

注意

選択後、Endpoint Sensor に OpenIOC ファイルのプレビューが表示されます。表示されたプレビューで、OpenIOC ファイルにサポートされる痕跡と条件が含まれているかどうか確認します。サポートされていない組み合わせには取り消し線が付けられ、調査では無視されます。

診断から Root Cause Analysis を開始する

Root Cause Analysis は、一致したオブジェクトの実行につながった一連のイベントを表示する調査ツールです。

診断により一致が検出されると、管理者は Root Cause Analysis を生成して次の処理を実行できます。

- 指定した条件に関連するすべてのオブジェクトのリストを作成する
- 関連するオブジェクトに注意が必要なオブジェクトがないかを特定する
- 一致したオブジェクトの実行につながった一連のイベントを確認する

Root Cause Analysis の生成には時間がかかる場合があります。

手順

1. 履歴調査を実行します。

   結果ペインで、表示された結果を確認します。

   詳細については、529 ページの「履歴調査に対するユーザ定義の条件の使用」を参照してください。

2. 1 つ以上のエンドポイントを特定して選択し、[Root Cause Analysis の生成] をクリックします。
3. 新しい Root Cause Analysis タスクの名前を指定します。
4. 表示された条件を確認します。
   - ユーザ定義の条件を使用した診断では、Root Cause Analysis の生成時に AND 演算子または OR 演算子を使用して複数の条件が組み合わされます。
   - OpenIOC ファイルを使用した診断では、Root Cause Analysis を生成時に現在の OpenIOC ファイルで指定された情報が条件として使用されます。
5. 対象エンドポイントを確認します。

注意

リストからエンドポイントを削除するには、削除アイコンをクリックします。

6. 期間を指定します。

   初期設定では、ログが記録されたすべての期間に対して分析が実行されます。
7. [生成] をクリックします。
8. [Root Cause Analysis の結果] タブに移動し、分析の進行状況を監視します。

   Root Cause Analysis の生成が完了するまで時間がかかる場合があります。

   詳細については、546 ページの「Root Cause Analysis の結果」を参照してください。
9. タスクが完了したら、タスク名をクリックします。

注意

Endpoint Sensor で Root Cause Analysis を生成できない場合、タスク名はリンクとして表示されません。これには、次の原因が考えられます。

- 対象エンドポイントに十分なデータがない。

  データが削除されていないことを確認してください。エージェントのデータベースがデータベースサイズの 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。この問題を回避するには、エージェントのデータベースサイズの 上限を引き上げてください。

- OpenIOC ファイルで指定された条件すべてに一致するオブジェクトを調査で検出できなかった。

  診断では、OpenIOC ファイルのすべての条件が無視され、最初の結果が返されます。ただし、Root Cause Analysis タスクはそれらの条件を調査の条件として再び追加します。その結果、Root Cause Analysis タスクが OpenIOC ファイルの条件とタスクの条件の両方に一致する結果を生成できない場合があります。

10. 結果を確認します。

Root Cause Analysis の結果

Root Cause Analysis タスクの進行状況を監視するには、[レスポンス] > [履歴調査]に移動し、[Root Cause Analysis の結果] タブをクリックします。

診断により一致が検出されると、管理者は Root Cause Analysis を生成して次の処理を実行できます。

- 指定した条件に関連するすべてのオブジェクトのリストを 作成する
- 関連するオブジェクトに注意が必要なオブジェクトがないかを特定する
- 一致したオブジェクトの実行につながった一連のイベントを確認する

Root Cause Analysis の生成が完了するまで時間がかかる場合があります。

詳細については、544 ページの「診断から Root Cause Analysis を開始する」を参照してください。

次の表は、確認可能な調査の詳細を示しています。

列名	説明
ステータス	Root Cause Analysis タスクの進行状況を示します。
名前	Root Cause Analysis タスクの名前を示します。 クリックすると、[分析チェーン] 画面と [オブジェクトの詳細] 画面が開きます。 詳細については、560 ページの「分析チェーン」を参照してください。 **注意** Endpoint Sensor で Root Cause Analysis を生成できない場合、タスク名はリンクとして表示されません。これには、次の原因が考えられます。 • 対象エンドポイントに十分なデータがない。 データが削除されていないことを確認してください。エージェントのデータベースがデータベース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。この問題を回避するには、エージェントのデータベースサイズの上限を引き上げてください。 • OpenIOC ファイルで指定された条件すべてに一致するオブジェクトを調査で検出できなかった。 診断では、OpenIOC ファイルのすべての条件が無視され、最初の結果が返されます。ただし、Root Cause Analysis タスクはそれらの条件を調査の条件として再び追加します。その結果、Root Cause Analysis タスクが OpenIOC ファイルの条件とタスクの条件の両方に一致する結果を生成できない場合があります。
条件	Root Cause Analysis タスクに指定された条件を示します。
一致したオブジェクト	エンドポイントで検出された一致するオブジェクトの数を示します。 値をクリックすると、詳細が表示されます。

列名	説明
アスタリスク (*)	「重要」としてタグ付けされたエンドポイントを示します。
エンドポイント	一致するオブジェクトを含むエンドポイントの名前を示します。 [エンドポイント] の名前をクリックすると、エンドポイントの詳細が表示されます。
IP アドレス	一致するオブジェクトを含むエンドポイントの IP アドレスを示します。 IP アドレスはネットワークによって割り当てられます。
開始	Root Cause Analysis タスクが開始された日時を示します。
経過時間	タスク開始からの経過時間を示します。
作成者	タスクを作成したユーザを示します。

Root Cause Analysis タスクを削除するには、表内のエントリを選択し、[削除] をクリックします。

ライブ調査

ライブ調査では、現在のシステムの状態を調査します。ライブ調査は指定した期間で実行されるよう設定でき、OpenIOC ルールや YARA ルールを使用した広範な条件がサポートされます。

重要

Windows プラットフォームにインストールされたセキュリティエージェントに対してのみ使用できます。

ライブ調査では次の条件がサポートされています。

- OpenIOC ルール: OpenIOC ルールを使用すると、現在ディスク上にあるすべてのファイルが検索されます。

注意

選択後、Endpoint Sensor に OpenIOC ファイルのプレビューが表示されます。表示されたプレビューで、OpenIOC ファイルにサポートされる痕跡と条件が含まれているかどうか確認します。サポートされていない組み合わせには取り消し線が付けられ、調査では無視されます。

詳細については、557 ページの「ライブ調査でサポートされる IOC のインジケータ」を参照してください。

- YARA ルール: YARA ルールを使用すると、現在メモリ内で実行されているすべてのプロセスが検索されます。

注意

Root Cause Analysis の結果は、YARA ルールにのみ使用できます。

ライブ調査は現在実行中のシステムに対して行われるため、この間、ファイルやレジストリエントリには、ロックされているものもあれば、使用中のものもあります。Root Cause Analysis の結果は、OpenIOC ルールまたはレジストリ検索を使用した調査には使用できません。OpenIOC ルールまたはレジストリデータを使用して Root Cause Analysis を生成するには、履歴調査を使用してください。

詳細については、527 ページの「履歴調査」を参照してください。

- レジストリを検索: 対象エンドポイント上で照合するレジストリのキー、名前、およびデータを指定します。

注意

調査は、次のルートキーの下のレジストリ値に対してのみ実行されます。

- HKEY_CURRENT_USER
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS

管理者は、実行するライブ調査の種類を指定できます。

- 1 回限りの調査は 1 回だけ実行されます。この調査は、作成後すぐに実行されます。

詳細については、550 ページの「1 回限りの調査を開始する」を参照してください。

- 予約調査は、指定の間隔で自動的に実行されるように設定できます。

  詳細については、553 ページの「予約調査を開始する」を参照してください。

ライブ調査は、完了までにしばらく時間がかかります。

1 回限りの調査を開始する

手順

1. [レスポンス] > [ライブ調査] に移動します。
2. [1 回限りの調査] タブをクリックします。
3. [新しい調査] をクリックします。
4. この調査に [名前] を指定します。
5. 一致させる必要があるオブジェクトに基づいて [方法] を選択します。
   - OpenIOC を使用してディスクファイルを検索: OpenIOC ファイルで指定されたルールに一致する、ディスク上のオブジェクト

     注意

     選択後、Endpoint Sensor に OpenIOC ファイルのプレビューが表示されます。表示されたプレビューで、OpenIOC ファイルにサポートされる痕跡と条件が含まれているかどうか確認します。サポートされていない組み合わせには取り消し線が付けられ、調査では無視されます。

     詳細については、557 ページの「ライブ調査でサポートされる IOC のインジケータ」を参照してください。
   - YARA を使用してインメモリプロセスを検索: YARA ファイルで指定されたルールに一致する、現在メモリ内に存在するオブジェクト
   - レジストリを検索: ユーザ指定の条件に一致するレジストリのキー、名前、およびデータ

6. [エンドポイントの選択] をクリックし、調査に含めるエンドポイントを指定します。

   注意

   [対象エンドポイント] 画面には、調査対象として選択されたエンドポイントがすべて表示されるとは限りません。

   - 表示されるのは、そのユーザが十分なアクセス権を付与されているエンドポイントのみです。
   - Windows プラットフォームにインストールされたセキュリティエージェントに対してのみ使用できます。

7. [調査を開始] をクリックします。
8. 1 回限りの調査の結果を確認したり、進行状況を確認したりするには、次の手順を実行します。
   a. [レスポンス] > [ライブ調査] に移動します。
   b. [1 回限りの調査] タブをクリックします。

   詳細については、551 ページの「1 回限りの調査を開始する」を参照してください。

1 回限りの調査を開始する

1 回限りの調査とは、1 回だけ実行される調査のことです。

1 回限りの調査の結果を確認したり、進行状況を監視したりするには、[レスポンス] > [ライブ調査] に移動し、[1 回限りの調査] タブをクリックします。

次の詳細を確認できます。

列	説明
ステータス	調査の現在の状態を示します。
進行状況	調査の完了状況を示すパーセンテージを示します。

列	説明
名前	調査を識別するユーザ指定の名前を示します。 クリックすると、調査結果が表示されます。
方法	調査で使用された方法を示します。
条件	• OpenIOC または YARA ルールファイルのファイル名を示します。 • ユーザ指定のレジストリ値を示します。
一致したエンドポイント	指定した条件に一致するオブジェクトを含むエンドポイントの数を示します。
対象エンドポイント	調査対象として選択したエンドポイントの総数を示します。 クリックすると、選択したエンドポイントの詳細が表示されます。 **注意** [対象エンドポイント] 画面には、調査対象として選択されたエンドポイントがすべて表示されるとは限りません。表示されるのは、そのユーザが十分なアクセス権を付与されているエンドポイントのみです。
開始	調査が開始された日時を示します。
経過時間	調査開始からの経過時間を示します。
作成者	調査を作成したユーザを示します。

新しく調査を開始するには、[新しい調査] をクリックします。

1 つ以上の調査を選択すると、次のオプションが有効になります。

- 停止: 調査をキャンセルします。停止された調査は再開できません。
- 削除: 調査を停止し、その調査をリストから削除します。削除された調査は復元できません。

予約調査を開始する

手順

1. [レスポンス] > [ライブ調査] に移動します。
2. [予約調査] タブをクリックします。
3. [新しい調査] をクリックします。
4. この調査に [名前] を指定します。
5. 一致させる必要があるオブジェクトに基づいて [方法] を選択します。
   - OpenIOC を使用してディスクファイルを検索: OpenIOC ファイルで指定されたルールに一致する、ディスク上のオブジェクト

     注意

     選択後、Endpoint Sensor に OpenIOC ファイルのプレビューが表示されます。表示されたプレビューで、OpenIOC ファイルにサポートされる痕跡と条件が含まれているかどうか確認します。サポートされていない組み合わせには取り消し線が付けられ、調査では無視されます。

     詳細については、557 ページの「ライブ調査でサポートされる IOC のインジケータ」を参照してください。
   - YARA を使用してインメモリプロセスを検索: YARA ファイルで指定されたルールに一致する、現在メモリ内に存在するオブジェクト
   - レジストリを検索: ユーザ指定の条件に一致するレジストリのキー、名前、およびデータ
6. [エンドポイントの選択] をクリックし、調査に含めるエンドポイントを指定します。

注意

[対象エンドポイント] 画面には、調査対象として選択されたエンドポイントがすべて表示されるとは限りません。

- 表示されるのは、そのユーザが十分なアクセス権を付与されているエンドポイントのみです。
- Windows プラットフォームにインストールされたセキュリティエージェントに対してのみ使用できます。

7. この調査のスケジュールを指定します。
   - 期間: 調査の開始日と終了日を指定します。調査は、指定した期間内でのみ実行されます。初期設定は 1 か月です。
   - 実行間隔: スケジュール期間内に調査を繰り返す頻度を指定します。初期設定は、[毎日] の [08:00] です。
8. [調査を開始] をクリックします。
9. 予約調査の結果を確認したり、進行状況を監視したりするには、次の手順を実行します。
   a. [レスポンス] > [ライブ調査] に移動します。
   b. [予約調査] タブをクリックします。

      詳細については、554 ページの「予約調査」を参照してください。
   c. 各予約実行の詳細を表示するには、調査名をクリックして、[予約調査の履歴] 画面を開きます。

      詳細については、556 ページの「予約調査の履歴を確認する」を参照してください。

予約調査

予約調査は、一定の間隔で自動的に実行されるように設定されている調査です。

予約調査の結果を確認し、進行状況を監視するには、[レスポンス] > [ライブ調査]に移動し、[予約調査] タブをクリックします。

次の表は、確認可能な詳細を示しています。

列	説明
有効	調査の現在の状態を示します。
名前	調査を識別するユーザ指定の名前を示します。 クリックすると、[予約タスクの履歴] 画面が開きます。
方法	調査で使用された方法を示します。
条件	OpenIOC ファイルのファイル名を示します。 ユーザ指定のレジストリ値を示します。
対象エンドポイント	調査対象として選択したエンドポイントの総数を示します。 クリックすると、選択したエンドポイントの詳細が表示されます。 **注意** [対象エンドポイント] 画面には、調査対象として選択されたエンドポイントがすべて表示されるとは限りません。表示されるのは、そのユーザが十分なアクセス権を付与されているエンドポイントのみです。
頻度	スケジュール期間内に調査を繰り返す頻度を示します。
最新の調査	最新の調査が開始された日時を示します。
前回の経過時間	最新の調査が開始されてからの経過時間を示します。
前回の一致したエンドポイント	最新の調査で指定した条件に一致するオブジェクトを含むエンドポイントの数を示します。
作成者	調査を作成したユーザを示します。

新しく調査を開始するには、[新しい調査] をクリックします。

[削除] をクリックすると、調査は停止され、リストから削除されます。削除された調査は復元できません。

注意

OpenIOC ファイルを削除すると、削除された OpenIOC ファイルを使用する予約調査は自動的に無効になります。

予約調査の履歴を確認する

[予約調査の履歴] 画面を使用すると、過去のスケジュールを確認したり、実行中のスケジュールの進行状況を監視したりできます。

手順

1. [予約調査の履歴] 画面にアクセスします。
   a. [レスポンス] > [ライブ調査]に移動します。
   b. [予約調査] タブで、[名前] 列の値をクリックします。
2. スケジュール概要に表示された詳細を確認します。
   - タスク名: スケジュールに付けられた名前。
   - 期間と頻度: スケジュールで調査が実行されるタイミングと頻度を示します。
   - 方法: スケジュールの実行ごとに使用される条件。クリックすると、全条件が表示されます。
   - 対象エンドポイント: クリックすると、スケジュールに含まれるエンドポイントのリストが表示されます。
3. スケジュールの実行ごとの調査の詳細を確認します。

列名	説明
ステータス	調査の現在の状態を示します。
進行状況	調査の完了状況を示すパーセンテージを示します。

列名	説明
一致したエンドポイント	指定した条件に一致するオブジェクトを含むエンドポイントの数を示します。 クリックすると、[調査結果] 画面が開きます。
開始	調査が開始された日時を示します。
経過時間	調査開始からの経過時間を示します。 完了した調査の場合は、調査の実行にかかった合計時間

4. 1 つ以上の調査を選択すると、次のオプションが有効になります。
   - 停止: 調査をキャンセルします。停止された調査は再開できません。
   - 削除: 調査を停止し、その調査をリストから削除します。削除された調査は復元できません。

ライブ調査でサポートされる IOC のインジケータ

OpenIOC ファイルは、侵入の痕跡 (IOC) を示す情報が 1 つ以上含まれている XML ファイルです。OpenIOC ファイルでは、選択した調査の種類でサポートされるインジケータ (痕跡) 名が使用されていることを確認してください。

次の表は、調査でサポートされる IOC のインジケータを示しています。

重要

IOC ファイルを選択する場合、IOC インジケータに、照合するファイルの場所 (「FileItem/FullPath」または「FileItem/FilePath」) が含まれていることを確認する必要があります。

カテゴリ	項目	必要条件	メモ
FILEITEM	FULLPATH	IS	完全なディレクトリパス、ファイル名、拡張子を参照します
	FILEPATH	IS、CONTAINS、STARTS-WITH、ENDS-WITH	部分一致検索がサポートされます
	FILENAME	IS、CONTAINS、STARTS-WITH、ENDS-WITH	部分一致検索がサポートされます
	MD5SUM	IS	
	SHA1SUM	IS	
	SHA256SUM	IS	
	SIZEINBYTES	IS	
	CREATED	GREATER-THAN、LESS-THAN	必要な形式 (UTC): yyyy-mm-ddThh:mm:ss
	MODIFIED	GREATER-THAN、LESS-THAN	必要な形式 (UTC): yyyy-mm-ddThh:mm:ss
	ACCESSED	GREATER-THAN、LESS-THAN	必要な形式 (UTC): yyyy-mm-ddThh:mm:ss

注意

選択後、Endpoint Sensor に OpenIOC ファイルのプレビューが表示されます。表示されたプレビューで、OpenIOC ファイルにサポートされる痕跡と条件が含まれているかどうか確認します。サポートされていない組み合わせには取り消し線が付けられ、調査では無視されます。

調査結果

調査結果を大まかに確認するには、[調査結果] 画面を使用します。この画面には次の場所からアクセスできます。

- [1 回限りの調査] タブで、調査の [名前] をクリックします。

- [予約調査] タブで、調査の [名前] をクリックし、[一致したエンドポイント] 列の値をクリックします。

この画面には、次の情報が表示されます。

- すでに [一致]、[一致なし]、[処理待ち]、または [キャンセル] と分類されたエンドポイントの総数を示すドーナツグラフ。

  総数の概要はグラフの左側に表示されます。この概要は、調査の進捗に応じてリアルタイムに更新されます。

アイコン	ラベル	説明
●	一致	一致するオブジェクトを含む、調査済みのエンドポイント数を示します。
●	一致なし	一致するオブジェクトがない、調査済みのエンドポイント数を示します。
●	処理待ち	未調査のエンドポイント数を示します。 調査が処理待ちのエンドポイントがなくなると、調査は完了します。
●	キャンセル	調査されていないエンドポイント数を示します。 ユーザによるキャンセル、システムエラー、またはエンドポイントのタイムアウトが原因として考えられます。

- 調査が作成されたときに使用されたパラメータ。

  調査で使用された検索条件を確認するには、[条件] をクリックします。

- 調査対象の各エンドポイントの詳細が記載された結果の表。

  調査ステータスに基づいてエンドポイントがタブに分類されます。この表には次の詳細が表示されます。

列名	説明
アスタリスク (*)	「重要」としてタグ付けされたエンドポイントを示します

列名	説明
エンドポイント	一致するオブジェクトを含むエンドポイントの名前を示します。 [エンドポイント] の名前をクリックすると、エンドポイントの詳細が表示されます。
IP アドレス	一致するオブジェクトを含むエンドポイントの IP アドレスを示します。 IP アドレスはネットワークによって割り当てられます。
OS	エンドポイントで使用されている OS を示します。
ユーザ	Endpoint Sensor エージェントが一致したオブジェクトを最初に記録したときにログインしていたユーザのユーザ名を示します。 ユーザ名をクリックすると、ユーザの詳細が表示されます。
一致項目の詳細	クリックすると、一致項目の詳細が表示されます。
Root Cause Analysis	クリックすると、[Root Cause Analysis] 画面が表示されます。 **注意** Root Cause Analysis の結果は、YARA ルールにのみ使用できます。 ライブ調査は現在実行中のシステムに対して行われるため、この間、ファイルやレジストリエントリには、ロックされているものもあれば、使用中のものもあります。Root Cause Analysis の結果は、OpenIOC ルールまたはレジストリ検索を使用した調査には使用できません。OpenIOC ルールまたはレジストリデータを使用して Root Cause Analysis を生成するには、履歴調査を使用してください。 詳細については、544 ページの「診断から Root Cause Analysis を開始する」を参照してください。
経過時間	調査が開始されてから経過した時間を示します。

分析チェーン

[分析チェーン] タブには、Root Cause Analysis が表示されるほか、調査に役立つ可能性のあるその他の情報も表示されます。

脅威の調査では、Endpoint Sensor および Active Directory からの情報を関連付け、ネットワーク全体のエンドポイントとユーザアカウントに関する攻撃情報を表示できます。

情報	説明
対象エンドポイント	調査されたエンドポイントの詳細情報が表示されます。 エンドポイント名およびユーザ名をクリックして、詳細を表示します。 エンドポイントをネットワークから切断するには、[エンドポイントの隔離] をクリックします。隔離されている間、エージェントが通信できるのはサーバのみです。 **注意** 隔離したエンドポイントでセキュリティの脅威を解決すると、[ディレクトリ] > [ユーザ/エンドポイント] 画面の次の場所に、隔離したエンドポイントのネットワーク接続を復元するオプションが表示されます。 • [エンドポイント] > [すべて]: 表内のエンドポイント名をクリックし、表示された画面で [タスク] > [復元] の順にクリックします。 • [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み]: 表内のエンドポイントの行を選択し、[タスク] > [ネットワーク接続の復元] の順にクリックします。
最初に確認されたオブジェクト	調査対象オブジェクトの作成に関与したとみられる分析チェーン内の最初のオブジェクトです。 多くの場合、これは標的型攻撃の開始地点です。 オブジェクトにカーソルを合わせて をクリックして、分析チェーン内のオブジェクトを特定します。
一致したオブジェクト	調査条件に一致するオブジェクトまたはオブジェクトのリストが表示されます。 Root Cause Analysis でオブジェクトを特定するには、オブジェクトにマウスを重ねて、 をクリックします。

情報	説明
注意が必要なオブジェクト	既存のトレンドマイクロインテリジェンスに基づき、不正オブジェクトの可能性があるチェーン内のオブジェクトを強調表示します。 値は、チェーン内にある一意の注意が必要なオブジェクトの数を表します。 クリックすると、注意が必要なオブジェクトのリストが表示されます。 オブジェクトにカーソルを合わせて をクリックして、分析チェーン内のオブジェクトを特定します。
Root Cause Analysis 領域	イベントに関するオブジェクトの視覚的分析が表示されます。 **注意** 分析チェーン内のノード数が表示できる上限を超える場合は、主要な分析チェーンのみが表示されます。この問題を回避するには、調査条件を絞り込みます。 使用可能なノードをクリックして、選択したオブジェクトの詳細情報を表示します。 分析チェーンを解釈する方法の詳細については、以下を参照してください。 • 563 ページの「オブジェクトの詳細: [プロファイル] タブ」 **注意** 選択したオブジェクトに使用可能なタブが他にない場合は、[プロファイル] タブが既定ビューとなります。 • 564 ページの「オブジェクトの詳細: [関連するオブジェクト] タブ」 • 565 ページの「分析チェーンの移動」 • 566 ページの「Root Cause Analysis のアイコン」

注意

データをエクスポートするには、 をクリックし、次のいずれかを実行します。

- すべての Root Cause Analysis レポートを.png ファイルとしてエクスポートするには、[分析チェーン] を選択します。
- すべてのデータを CSV ファイルとしてエクスポートするには、[オブジェクトの詳細] を選択します。

オブジェクトの詳細: [プロファイル] タブ

[プロファイル] タブには、選択したオブジェクトの種類に適用できる詳細情報が表示されます。

一部のオブジェクトについては、表示される詳細情報が限定的な場合や、実行時に利用可能な詳細情報がない場合があります。

注意

評価が「不正」のオブジェクトについては、Threat Connect または VirusTotal で詳細を確認できます。

[一致したオブジェクト] と [注意が必要なオブジェクト] の場合、このタブには次のオプションも追加で表示されます。

オプション	説明
オブジェクトの強制終了	対象エンドポイントの現在の状態でのみ実行中のオブジェクトのインスタンスをすべて 強制終了します。 **注意** この処理は、種類が「プロセス」の未評価、不正、不審なオブジェクトに対してのみ実行できます。コマンドが成功したかどうかを確認するには、[運用管理] > [コマンド追跡] に移動します。

オプション	説明
不審オブジェクトリストに追加	対象エンドポイントの現在の状態でのみ実行中のオブジェクトのインスタンスをすべて 強制終了し、そのオブジェクトを [ユーザ指定の不審オブジェクト] リストに追加します。 注意 アプリケーションコントロールが有効になっている場合、[ユーザ指定の不審オブジェクト] リストに追加されたオブジェクトのハッシュ値に一致するプロセスは、すべてのエンドポイントで実行を許可されません。また、Endpoint Sensor は種類が「プロセス」のオブジェクトをリストに追加する前に強制終了し、アプリケーションコントロールではそれらの再開が阻止されます。
履歴調査リストに追加	新しい履歴調査の条件としてオブジェクトを追加します。 今すぐ調べるには、[分析チェーン] の上部にある [履歴調査を開始] ボタンをクリックします。 注意 [分析チェーン] 内のあるオブジェクトに対して履歴調査を実行する必要がないと判断した場合は、そのオブジェクトをクリックしてから、[履歴調査リストから削除] ボタンをクリックします。 詳細については、529 ページの「履歴調査に対するユーザ定義の条件の使用」を参照してください。

オブジェクトの詳細: [関連するオブジェクト] タブ

[関連するオブジェクト] タブには、選択したオブジェクトの依存関係がすべて表示されます。

注意

[関連するオブジェクト] タブには、「プロセス」のオブジェクトの追加情報のみが表示されます。

これらは、一致したオブジェクトの実行に必要なオブジェクトです。このタブには次の詳細が表示されます。

プロパティ	説明
処理	オブジェクトによって実行された処理を示します。
ログ	記録された処理の日時を示します。
レーティング	トレンドマイクロの脅威インテリジェンスに基づく、オブジェクトに割り当てられたレーティングを示します。
感染エンドポイント	感染したエンドポイント (ある場合)を示します。
送信先パス	オブジェクトの送信先を示します。

[関連するオブジェクト] タブは、次のオプションを使用して管理できます。

- このタブには、指定した処理に基づいてオブジェクトをフィルタできるドロップダウンがあります。利用可能な処理をすべて表示するには、ドロップダウンをクリックします。
- オブジェクトの詳細を表示するには、[詳細の表示] をクリックします。

分析チェーンの移動

分析チェーンを操作するには、範囲をクリックしてドラッグするか、用意されている操作アイコンを使用します。

アイコン	説明
	Root Cause Analysis には、一致する根本原因チェーンが 1 つ以上含まれる場合があります。 ドロップダウンをクリックすると、選択したエンドポイントのその他の分析チェーンが表示されます。

アイコン	説明
履歴調査を開始	履歴調査リストのオブジェクトを使用して履歴調査を開始する場合にクリックします。 履歴調査リストにオブジェクトがない場合、このオプションは使用できません。 このオプションを有効にするには、[一致したオブジェクト] または [注意が必要なオブジェクト] を履歴調査リストに 1 つ以上追加します。
	クリックすると、フルスクリーンモードになります。 再度クリックすると、フルスクリーンモードを終了します。
	クリックすると、拡大または縮小します。
	カーソルを合わせると、分析チェーンに表示される記号の説明が表示されます。 詳細については、566 ページの「Root Cause Analysis のアイコン」を参照してください。

Root Cause Analysis のアイコン

分析チェーンでは、次のアイコンを使用してオブジェクトの種類が表示されます。

アイコン	名前	説明
	最初に確認されたオブジェクト	一致するオブジェクトを作成した可能性が最も高いオブジェクトを表します
	一致条件	調査条件に一致するオブジェクトを表します
	通常のオブジェクト	脅威をもたらさないことが確認されたオブジェクトを表します これらは通常、一般的なシステムファイルです。
	未評価のオブジェクト	まだ評価されていないオブジェクトを表します
	不審オブジェクト	既知の脅威に類似する挙動を示すオブジェクトを表します
	不正なオブジェクト	既知の脅威に一致するオブジェクトを表します
	システム領域感染型ウイルス	システムのスタートアップ時に起動するオブジェクトです
	ブラウザ	Web ページを表示する機能を備えたオブジェクトです。これは通常、Web ブラウザです
	メールクライアント	メールメッセージを送受信できるオブジェクトです。これは通常、メールクライアントまたはサーバです
	ファイル	ディスク上のファイルであるオブジェクトです
	ネットワーク	ネットワーク接続またはインターネットに関連するオブジェクトです
	プロセス	実行時のプロセスであるオブジェクトです

アイコン	名前	説明
	レジストリ	レジストリキー、エントリ、またはデータであるオブジェクトです
	イベント	オブジェクトにより実行されたアクションを示します
	関連付け	2 つのオブジェクト間の関係を示します

オブジェクトの詳細

[オブジェクトの詳細] タブには、[Root Cause Analysis] タブと同じ情報が表形式で示されます。また、オブジェクトは次のタブに編成されます。

- オブジェクト: 一致したオブジェクトの実行に関与したオブジェクトを親プロセスでグループ化して表示されます。「▶」をクリックするとリストが展開されます。
- 注意が必要なイベント: トトレンドマイクロの既存の脅威インテリジェンスに基づいて、チェーン内の不正な可能性のあるオブジェクトが表示されます。
- ファイルイベント: チェーン内のファイルオブジェクト。
- レジストリイベント: チェーン内のオブジェクトのうち、レジストリのキー、データ、およびエントリ。
- IP アドレス/DNS イベント: オブジェクトのうち、IP アドレスまたは DNS イベント。

次の表で詳しく説明します。

列名	説明
記録されたオブジェクト	記録されたオブジェクトの名前を示します。 オブジェクト名をクリックすると、詳細が表示されます。

列名	説明
PID	記録されたオブジェクトのプロセス ID を示します。
記録	オブジェクトがチェーンに関与した日時を示します。
アクティビティ	オブジェクトによって実行された処理を示します。 オブジェクト名をクリックすると、詳細が表示されます。
オブジェクトのレピュテーション	トレンドマイクロの脅威インテリジェンスに基づく、オブジェクトに割り当てられたレーティングを示します。 評価が「不正」のオブジェクトについては、Threat Connect または VirusTotal で詳細を確認できます。
感染エンドポイント	このオブジェクトが出現するエンドポイントの数を示します。 また、ネットワーク上のエンドポイントの総数に対する感染エンドポイントの割合を示します。 値をクリックすると、エンドポイントの詳細が表示されます。

表の管理には、次のオプションを使用します。

- すべてのタブで、[記録されたオブジェクト] 列のオブジェクトを 1 つ以上選択し、[履歴調査を開始] をクリックして別の調査を開始します。
- [オブジェクト] タブで、フィルタアイコン ( ) をクリックし、指定の条件に従って表をフィルタします。
- [ファイルイベント] タブで、[記録] 列と [オブジェクトのレピュテーション] 列をクリックして表を並べ替えます。

第 21 章

Managed Detection and Response

本章では、Apex Central 管理コンソールを使用して Managed Detection and Response を設定し、調査タスク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。

Managed Detection and Response の概要

[Managed Detection and Response] 画面では、Managed Detection and Response の設定と調査タスクを、Apex Central 管理コンソールから指定した対象に配信できます。

ヒント

- Managed Detection and Response のタスクコマンドのステータスを表示するには、[コマンド追跡] 画面を使用します。

  詳細については、586 ページの「Managed Detection and Response タスクコマンドの追跡」を参照してください。

- Managed Detection and Response サービスをサポートする対象の詳細検索を実行するには、[ユーザ/エンドポイントディレクトリ] 画面を使用します。

  詳細については、589 ページの「サポートされている対象を照会する」を参照してください。

次のタスクを実行するには、[Managed Detection and Response] 画面を使用します。

タスク	説明
Threat Investigation Center サーバへの登録	[設定] タブをクリックして、Apex Central を Threat Investigation Center サーバに登録します。 Apex Central が Trend Micro Threat Investigation Center と統合されると、Managed Detection and Response の機能が有効になります。 詳細については、573 ページの「Threat Investigation Center に Apex Central を登録する」を参照してください。
Threat Investigation Center サーバからの登録解除	[設定] タブをクリックして、Apex Central を Threat Investigation Center サーバから登録解除します。 詳細については、575 ページの「Threat Investigation Center サーバから登録解除する」を参照してください。

タスク	説明
Managed Detection and Response サービスの中止または再開	[設定] タブをクリックして、Managed Detection and Response サービスを中止または再開します。 **重要** Managed Detection and Response サービスを中止すると、新しい調査タスクの受信と Threat Investigation Center サーバへのログの送信が停止されます。Apex Central で実行中のタスクはキャンセルされず、結果も Threat Investigation Center サーバに送信されます。 詳細については、576 ページの「Managed Detection and Response サービスを中止または再開する」を参照してください。
新しい調査タスクの承認または拒否	[保留中のタスク] タブをクリックして、新しい調査タスクを承認または拒否します。 詳細については、577 ページの「調査タスクを承認または拒否する」を参照してください。
配信済みの調査タスクの追跡	[タスクの追跡] タブをクリックして、承認または拒否された調査タスクやコマンドを追跡および確認します。 詳細については、582 ページの「調査タスクを追跡する」を参照してください。
自動分析の表示	[自動分析] タブをクリックして、トレンドマイクロがネットワーク保護の強化のために収集したログデータの情報を表示します。 詳細については、585 ページの「自動分析を表示する」を参照してください。

Threat Investigation Center に Apex Central を登録する

Apex Central が Trend Micro Threat Investigation Center と統合されると、Managed Detection and Response の機能が有効になります。

重要

- Managed Detection and Response の機能を使用するには、サービスプランを購入して有効なサーバアドレスと企業 GUID を取得する必要があります。サービスプランの購入については、トレンドマイクロの営業担当者または販売代理店にお問い合わせください。

手順

1. [レスポンス] > [Managed Detection and Response]に移動します。

   [Managed Detection and Response] 画面が表示されます。

2. [設定] タブをクリックします。

3. 次の情報を指定します。

   - サーバアドレス: トレンドマイクロの営業担当者または販売代理店から受け取った Threat Investigation Center サーバのアドレス
   - 企業 GUID: トレンドマイクロの営業担当者または販売代理店から受け取った Managed Detection and Response サービスの GUID

4. 新しい調査タスクの自動承認を設定します。

   注意

   - 自動承認が有効な場合、Apex Central は、自動承認された新しい調査タスクについて受信者に知らせるメール通知を送信します。
   - 自動承認が無効な場合、Apex Central は、すべての新しい調査タスクについてメール通知を送信し、手動承認を要求します。

   - [調査タスクを自動で承認] チェックボックスをオンにすると、新しい調査タスクの自動承認が有効になります。
   - [調査タスクを自動で承認] チェックボックスをオフにすると、新しい調査タスクの自動承認が無効になります。

5. (オプション) 通知の受信者を設定します。

注意

- 新しいユーザアカウントは、[ユーザアカウント] 画面 ([運用管理] > [アカウント管理] > [ユーザアカウント]) で追加できます。
- 新しい連絡先グループは、[連絡先グループ] 画面 ([レポート] > [通知] > [連絡先グループ]) で追加できます。

- 受信者を追加するには、[使用可能なユーザおよびグループ] リストから連絡先を選択し、> をクリックします。

  選択した連絡先が [選択されたユーザおよびグループ] リストに表示されます。

- 受信者を削除するには、[選択されたユーザおよびグループ] リストから連絡先を選択し、< をクリックします。

  選択した連絡先が [使用可能なユーザおよびグループ] リストに表示されます。

6. [登録] をクリックします。

   - [サーバアドレス] には、登録済みの Threat Investigation Center サーバのアドレスが表示されます。
   - [企業 GUID] が [送信者 ID] に置き換わり、登録済みの Threat Investigation Center サーバから調査タスクを受信する Apex Central サーバの GUID が表示されます。

Threat Investigation Center サーバから登録解除する

重要

登録を解除すると、Managed Detection and Response サービスが自動的に無効になります。

手順

1. [レスポンス] > [Managed Detection and Response]に移動します。

[Managed Detection and Response] 画面が表示されます。

2. [設定] タブをクリックします。
3. [登録解除] をクリックします。

   確認ダイアログが表示されます。
4. [登録解除] をクリックします。

   Managed Detection and Response サービスが自動的に無効になります。

Managed Detection and Response サービスを中止または再開する

重要

Managed Detection and Response サービスを中止すると、新しい調査タスクの受信と Threat Investigation Center サーバへのログの送信が停止されます。Apex Central で実行中のタスクはキャンセルされず、結果も Threat Investigation Center サーバに送信されます。

手順

1. [レスポンス] > [Managed Detection and Response]に移動します。

   [Managed Detection and Response] 画面が表示されます。
2. [設定] タブをクリックします。
3. Managed Detection and Response サービスを中止するには、次の手順を実行します。
   a. [サービスの中止] をクリックします。
   b. 確認ダイアログが表示されたら、次の操作を行います。
      - [サービスの中止] をクリックして Managed Detection and Response サービスを中止します。
      - [キャンセル] をクリックして、Managed Detection and Response サービスを中止せずに [設定] 画面に戻ります。

4. Managed Detection and Response サービスを再開するには、[サービスの再開] をクリックします。

   Apex Central は、新しい調査タスクの受信と Threat Investigation Center サーバへのログの送信を再開します。

調査タスクを承認または拒否する

[Managed Detection and Response] 画面の [保留中のタスク] タブには、Threat Investigation Center から送信された、管理者による手動承認が必要な調査タスクが表示されます。特定のタスクの対象とコマンドを表示し、選択されている対象を変更し、選択されているタスクを承認または拒否することができます。

[Managed Detection and Response] 画面に表示される Threat Investigation Center のタスクコマンドの詳細については、580 ページの「Threat Investigation Center のタスクコマンド」を参照してください。

ヒント

Managed Detection and Response のタスクコマンドのステータスを表示するには、[コマンド追跡] 画面を使用します。

詳細については、586 ページの「Managed Detection and Response タスクコマンドの追跡」を参照してください。

重要

- Apex Central で調査タスクの情報が保持されるのは、Threat Investigation Center から送信後 90 日間のみです。
- 初期設定では、新しい調査タスクは、Apex Central が受信してから 72 時間以内に承認または拒否されない場合、自動的にタイムアウトになります。

  調査タスクのコマンドステータスの詳細については、584 ページの「Threat Investigation Center のコマンドステータス」を参照してください。

手順

1. [レスポンス] > [Managed Detection and Response]に移動します。

   [Managed Detection and Response] 画面が表示されます。

2. [保留中のタスク] タブをクリックします。

   表が表示され、調査タスクと次の情報を記載したリストが示されます。

列	説明
タスクの説明	Threat Investigation Center 管理者が手動で指定したタスク名を示します。
コマンド	選択済みの対象に配信するタスクコマンドを示します。 [Managed Detection and Response] 画面に表示される Threat Investigation Center のタスクコマンドの詳細については、580 ページの「Threat Investigation Center のタスクコマンド」を参照してください。
対象	タスクの対象の数を示します。
有効期限	タスクが期限切れになる Apex Central サーバのローカル時間を示します。 **重要** 初期設定では、新しい調査タスクは、Apex Central が受信してから 72 時間以内に承認または拒否されない場合、自動的にタイムアウトになります。 調査タスクのコマンドステータスの詳細については、584 ページの「Threat Investigation Center のコマンドステータス」を参照してください。

3. 保留中のタスクの対象を表示するには、[タスクの説明] フィールドの横にある右矢印アイコン (▶) をクリックします。

   表が表示され、次の詳細が示されます。

列	説明
エンドポイント	対象エンドポイントの名前を示します。
IP アドレス	対象エンドポイントの IP アドレスを示します。
ユーザ	対象エンドポイントに最後にログオンしたユーザの名前を示します。
Endpoint Sensor サービス	対象エンドポイント上の Endpoint Sensor サービスのステータスを示します。 詳細については、581 ページの「Endpoint Sensor サービスのステータス」を参照してください。 **重要** Apex Central が指定された対象エンドポイントに調査タスクを配信するには、そのエンドポイントで Endpoint Sensor サービスが有効になっている必要があります。

4. 保留中の調査タスクを承認するには、次の手順を実行します。

   a. 承認する各タスクの名前の横にあるチェックボックスをオンにします。

   注意
   タスクのチェックボックスをオンにすると、そのタスクの対象がすべて選択されます。

   b. タスク名の横にある右矢印(▶) をクリックし、タスクに対して選択された対象を変更します。

   重要
   Apex Central が指定された対象エンドポイントに調査タスクを配信するには、そのエンドポイントで Endpoint Sensor サービスが有効になっている必要があります。

   - 含める対象の横にあるチェックボックスをオンにします。

- 除外する対象の横にあるチェックボックスをオフにします。

c. 保留中のタスクごとに前の手順を繰り返します。

d. [承認] をクリックします。

承認済みタスクが [タスク追跡] タブに表示されます。

詳細については、582 ページの「調査タスクを追跡する」を参照してください。

5. 保留中の調査タスクを拒否するには、次の手順を実行します。

a. 拒否する各タスクの名前の横にあるチェックボックスをオンにします。

注意

タスクのチェックボックスをオンにすると、そのタスクの対象がすべて選択されます。

b. タスク名の横にある右矢印(▶)をクリックし、タスクに対して選択された対象を変更します。

- 含める対象の横にあるチェックボックスをオンにします。
- 除外する対象の横にあるチェックボックスをオフにします。

c. 保留中のタスクごとに前の手順を繰り返します。

d. [拒否] をクリックします。

拒否されたタスクが [タスク追跡] タブに表示されます。

詳細については、582 ページの「調査タスクを追跡する」を参照してください。

Threat Investigation Center のタスクコマンド

次の表では、Apex Central の [Managed Detection and Response] 画面に表示される Threat Investigation Center のタスクコマンドについて説明します。

コマンド名	説明
ファイルのサンプルの収集	対象エンドポイントから不審なファイルのサンプルを収集し、そのサンプルを Threat Investigation Center に送信します。
Trend Micro Investigation Kit の実行	対象エンドポイントに Trend Micro Investigation Kit を配信し、実行します。
Advanced Threat Assessment の実行	対象エンドポイントに Trend Micro Anti-Threat Toolkit を配信し、実行します。
Evaluate Impact	対象エンドポイントで影響評価を開始します。
Root Cause Analysis の実行	Threat Investigation Center 管理者が指定した条件を使用して、対象エンドポイントで Root Cause Analysis を開始します。

Endpoint Sensor サービスのステータス

次の表では、[保留中のタスク] タブの [Endpoint Sensor サービス] 列に表示されるエージェントのステータスについて説明します。

ステータス	説明
有効	対象エンドポイントで Endpoint Sensor が有効になっています **重要** Apex Central が指定された対象エンドポイントに調査タスクを配信するには、そのエンドポイントで Endpoint Sensor サービスが有効になっている必要があります。
無効	対象エンドポイントで Endpoint Sensor が無効になっています
サーバのライセンスがサポートされていません	Apex One ライセンスで Endpoint Sensor サービスがサポートされていません
サポートされているセキュリティエージェントバージョンが必要です	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ないか、対象エンドポイントのサーバがサポートされていないバージョンです

調査タスクを追跡する

[Managed Detection and Response] 画面の [タスク追跡] タブを使用して、承認または拒否された調査タスクやコマンドのステータスを追跡および確認できます。

ヒント

Managed Detection and Response のタスクコマンドのステータスを表示するには、[コマンド追跡] 画面を使用します。

詳細については、586 ページの「Managed Detection and Response タスクコマンドの追跡」を参照してください。

重要

Apex Central で調査タスクの情報が保持されるのは、Threat Investigation Center から送信後 90 日間のみです。

手順

1. [レスポンス] > [Managed Detection and Response]に移動します。

   [Managed Detection and Response] 画面が表示されます。

2. [タスク追跡] タブをクリックします。

   表が表示され、調査タスクと次の情報を記載したリストが示されます。

列	説明
タスクの説明	Threat Investigation Center 管理者が手動で指定したタスク名を示します。
コマンド	選択済みの対象に配信するタスクコマンドを示します。 詳細については、580 ページの「Threat Investigation Center のタスクコマンド」を参照してください。
対象	タスクの対象の数を示します。

列	説明
タスクステータス	調査タスクの配信ステータスを示します。 詳細については、583 ページの「Threat Investigation Center のタスクステータス」を参照してください。
最終更新日	最後にステータスが更新された Apex Central サーバのローカル時間を示します。

3. タスクの説明の横にある右矢印アイコン (▶) をクリックして、タスクコマンドの情報を表示します。

   表が表示され、次の詳細が示されます。

列	説明
コマンドステータス	タスクコマンドの配信ステータスを示します。 詳細については、584 ページの「Threat Investigation Center のコマンドステータス」を参照してください。
エンドポイント	対象エンドポイントの名前を示します。
IP アドレス	対象エンドポイントの IP アドレスを示します。
ユーザ	対象エンドポイントに最後にログオンしたユーザの名前を示します。
承認/拒否	タスクが管理者によって承認または拒否された Apex Central サーバのローカル時間を示します。
承認者/拒否者	タスクを承認または拒否した管理者のユーザアカウント名を示します。
最終更新日	最後にステータスが更新された Apex Central サーバのローカル時間を示します。

Threat Investigation Center のタスクステータス

次の表では、[Managed Detection and Response] 画面の [タスク追跡] タブに表示される Threat Investigation Center タスクのステータスについて説明します。

[Managed Detection and Response] 画面に表示される Threat Investigation Center のタスクコマンドの詳細については、580 ページの「Threat Investigation Center のタスクコマンド」を参照してください。

ステータス	説明
実行中	次のシナリオが該当します。 • タスクは承認されたが、Apex One サーバに配信されていない • タスクコマンドは Apex One サーバに配信されたが、指定された対象で完了していない。
完了	タスクは Apex Central 管理者によって承認または拒否され、失敗か成功かにかかわらず指定された対象で完了しました。 詳細については、584 ページの「Threat Investigation Center のコマンドステータス」を参照してください。

Threat Investigation Center のコマンドステータス

次の表では、[タスク追跡] 画面に表示されるコマンドステータスについて説明します。

ステータス	説明
承認待ち	タスクは Apex Central 管理者によって承認または拒否されていません。
拒否	タスクは Apex Central 管理者によって拒否されました。
コマンドを送信しています	タスクが承認されたため、Apex Central は指定した対象にタスクコマンドを送信しています。
実行中	タスクコマンドは Apex One サーバに配信されたが、指定された対象で完了していない。
アップロードしています	管理下の製品がタスクのペイロードをアップロードしています。
成功	タスクコマンドは指定された対象で正常に完了しました。
コマンドを処理できません	タスクコマンドは指定された対象で完了しましたが、失敗しました。

ステータス	説明
コマンドがタイムアウトしました	次のシナリオが該当します。 • タスクが受信から 72 時間以内に Apex Central 管理者によって承認されなかった • 管理下の製品で承認後 9 日以内にタスクコマンドを完了できなかった • タスクコマンドが Apex One サーバでタイムアウトした
エージェントから応答がありません	Apex One サーバが対象のエージェントと通信を確立できません
Endpoint Sensor が無効になっています	対象エンドポイントで Endpoint Sensor が無効になっています
サポートされているセキュリティエージェントバージョンが必要です	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ないか、対象エンドポイントのサーバがサポートされていないバージョンです
サーバのライセンスがサポートされていません	Apex One ライセンスで Endpoint Sensor サービスがサポートされていません

自動分析を表示する

トレンドマイクロは、ネットワーク保護の強化のために、定期的に自動分析を実行してログデータを収集します。トレンドマイクロが収集するログの情報を表示するには、[自動分析] タブを使用します。

重要

Apex Central で調査タスクの情報が保持されるのは、Threat Investigation Center から送信後 90 日間のみです。

手順

1. [レスポンス] > [Managed Detection and Response]に移動します。

   [Managed Detection and Response] 画面が表示されます。

2. [自動分析] タブをクリックします。

   表が表示され、次の詳細が示されます。

列	説明
開始時刻	自動分析タスクが開始されたときのトレンドマイクロサーバのローカル時間を示します。
終了時刻	自動分析タスクが完了したときのトレンドマイクロサーバのローカル時間を示します。
ステータス	自動分析タスクのステータスを示します。
コマンド	自動分析タスクの種類を示します。
対象	自動分析タスクの対象となるエンドポイントの名前または数を示します。

3. 対象を表示するには、[対象] 列内の数字をクリックします。

   [対象] 画面が開き、感染エンドポイントのリストが表示されます。

Managed Detection and Response タスクコマンドの追跡

[コマンド追跡] 画面を使用して、Apex Central サーバから発行された Managed Detection and Response のタスクコマンドの詳細を照会して確認します。

[Managed Detection and Response] 画面に表示される Threat Investigation Center のタスクコマンドの追跡については、582 ページの「調査タスクを追跡する」を参照してください。

手順

1. [運用管理] > [コマンド追跡] の順に移動します。

   [コマンド追跡] 画面が表示されます。

2. コマンドリストをフィルタするには、次のように指定します。

   - 発行済み: Apex Central がタスクコマンドを送信した時刻を指定します。
   - コマンド: コマンドの種類を選択します。

     Apex Central Managed Detection and Response のタスクコマンドには、次のコマンドがあります。

コマンド名	説明
Threat Investigation Center の設定を管理下の製品に配信する	Threat Investigation Center の設定を管理下の製品に配信するためのコマンド
Threat Investigation Center のタスクを管理下の製品に配信する	Threat Investigation Center のタスクを管理下の製品に配信するためのコマンド
Threat Investigation Center の証明書の更新	Apex Central サーバで Threat Investigation Center の証明書を更新するためのコマンド **注意** Threat Investigation Center サーバは、Apex Central サーバ上の Threat Investigation Center 証明書を更新するタスクを、証明書の有効期限の 30 日前に自動的に配信します。
Threat Investigation Center のタスクの取得	Threat Investigation Center サーバからタスクを取得するためのコマンド **注意** タスクコマンドが失敗した場合に、このコマンドは [コマンド追跡] 画面にのみ表示されます。

   - ユーザ: コマンドの送信に使用されたユーザアカウント名を指定します。

ヒント

すべてのユーザが発行したコマンドを照会する場合は、このフィールドを空白のままにします。

- ステータス: コマンドステータスを 1 つ以上選択し、[適用] をクリックします。

3. コマンドの詳細情報を表示するには、[成功]、[失敗]、[実行中]、または [すべて] 列の数字をクリックします。

   [コマンド詳細] 画面が表示されます。

   詳細については、242 ページの「コマンド詳細」を参照してください。

コマンド詳細

[コマンド詳細] 画面には、発行済みのコマンドに関する次の情報が表示されます。

列名	説明
前回のレポート日時	管理下の製品から Apex Central サーバに応答が最後に送信された日時を示します。
サーバ/エンティティ	管理下の製品のサーバのホスト名を示します。
ステータス	発行されたコマンドのステータスを示します。
説明	コマンドのステータスに関する追加の詳細を示します。

注意

[コマンド詳細] 画面は、30 秒ごとに更新されます。

サポートされている対象を照会する

[ユーザ/エンドポイントディレクトリ] 画面を使用すると、Managed Detection and Response サービスをサポートしている対象の詳細検索を実行できます。

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。

   [ユーザ/エンドポイントディレクトリ] 画面が表示されます。

2. 表の上にある [詳細] リンクをクリックします。
3. [検索] ドロップダウンコントロールで、[エンドポイント] を選択します。

   2 番目のドロップダウンコントロールの 検索条件は選択内容に基づいて動的に変化します。

4. 2 番目のドロップダウンコントロールで、[サービス] を選択します。

   3 番目と 4 番目のドロップダウンコントロールが表示されます。

5. 3 番目のドロップダウンコントロールで、[Endpoint Sensor] を選択します。
6. 4 番目のドロップダウンコントロールで、エージェントのステータスを選択します。
   - 有効: Endpoint Sensor サービスが有効になっているエンドポイントを検索します。
   - 無効: Endpoint Sensor サービスが無効になっているエンドポイントを検索します。
7. フィルタの右にあるブール演算子を使用して、複数の検索条件を追加します。
   - OR: 指定した条件で複数の値を検索できます。いずれかの値と一致するレコードがすべて表示されます。
   - AND: 新しい検索条件を選択できます。この条件に指定した値と選択したその他すべての条件の値と一致するレコードのみが表示されます。

8. 次のいずれかをクリックして結果を表示します。
   - 検索: 検索結果がリストに表示されますが、検索条件は保存されません。
   - 新規カスタムフィルタとして保存: 検索結果がリストに表示され、検索条件をカスタムフィルタに保存することを求めるメッセージが表示されます。カスタムフィルタは、ユーザ/エンドポイントディレクトリツリーの [エンドポイント] ノードに表示されます。
9. (オプション) [エンドポイント] タブのドロップダウンコントロールを使用して、表示するデータの期間を指定したり、[表形式] と [表形式] を切り替えたりできます。
10. (オプション) [エクスポート] をクリックして、データを*.csv ファイルまたは*.png 画像でエクスポートします。

> **注意**
> - [表形式] では、データを*.csv ファイルでエクスポートできます。
> - [タイムライン表示] では、データを*.csv ファイルまたは*.png 画像でエクスポートできます。

Managed Detection and Response 用 Threat Investigation Center エージェント

Managed Detection and Response 用 Threat Investigation Center エージェントは、次の情報を Apex Central サーバから Threat Investigation Center サーバに自動的に送信します。

データの種類	説明
Apex Central 検出ログ	Apex Central サーバに登録済みの管理下の製品によって検出されたシステムイベント、ネットワークイベント、データ保護イベントに関連したログを含みます。
Apex Central 情報	Apex Central サーバ情報を含みます。

データの種類	説明
管理下の製品情報	Apex Central サーバに登録済みのトレンドマイクロ製品に関する情報を含みます。
管理下のエンドポイント情報	Apex Central サーバに登録済みのトレンドマイクロ製品によって管理されているエンドポイントに関する情報を含みます。

第 22 章

不審オブジェクトハブおよびノードのアーキテクチャ

本章では、管理者が、不審オブジェクトリストを複数の Apex Central サーバ間で同期するために必要な情報について説明します。

次のトピックがあります。

不審オブジェクトハブおよびノードの Apex Central サーバ

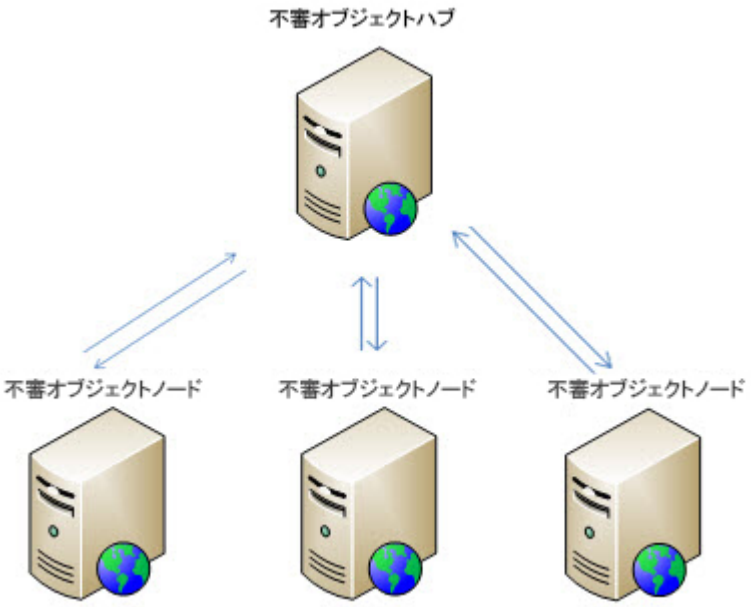
Trend Micro Apex Central™の不審オブジェクトハブおよびノードのアーキテクチャにより、不審オブジェクトリストを複数の Apex Central サーバ間で同期できます。ハブ Apex Central サーバの不審オブジェクトリストは、すべてのノード Apex Central サーバとそれらのサーバに登録されているその他の管理下の製品からの不審オブジェクトリストを統合して、そのリストをノード Apex Central サーバに配信します。

管理者は、不審オブジェクトハブ Apex Central サーバを設定しておく必要があります。また、環境によっては、他の Apex Central サーバを不審オブジェクトノードサーバとして動作するように割り当てる必要もあります。Trend Micro Deep Discovery 製品は、不審オブジェクトハブまたノード Apex Central サーバに登録できます。このアーキテクチャでは、不審オブジェクトに対するすべての処理を不審オブジェクトハブ Apex Central 管理コンソールから設定する必要があります。

重要

すべてのノード Apex Central サーバが適切に同期され続けるように、不審オブジェクトリストに対するすべての操作は、不審オブジェクトハブ Apex Central から実行する必要があります。

不審オブジェクトノード Apex Central から不審オブジェクトに対して実行した検索処理は、接続されたすべてのサーバに同期されるとは限りません。



不審オブジェクトハブとノードを設定する

手順

1. 不審オブジェクトハブ用の Apex Central の管理コンソールにログオンします。
2. [脅威インテリジェンス] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。
3. [管理下の製品] タブをクリックして、次の設定をメモします。
   - サービス URL
   - API キー

4. 不審オブジェクトノードの Apex Central 管理コンソールにログオンします。
5. [脅威インテリジェンス] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。
6. [ハブ Apex Central] タブで、不審オブジェクトハブ用の Apex Central でメモした内容を入力します。
   - サービス URL
   - API キー
7. (オプション) プロキシサーバ経由でハブ Apex Central に接続するには、[プロキシサーバを使用する] チェックボックスをオンにします。

   注意

   プロキシサーバの設定を構成または変更する場合は、[プロキシの設定] をクリックします。
8. [登録] をクリックします。

   確認ダイアログが表示され、サーバが不審オブジェクトハブ Apex Central に正常に登録されたことを示すメッセージが示されます。
9. 不審オブジェクトノードの 各 Apex Central サーバに対してこの処理を繰り返します。
10. 初期設定の同期間隔を設定するには、次の手順を実行します。
    a. [同期頻度] ドロップダウンから期間を選択します。
    b. [保存] をクリックします。

不審オブジェクトノード Apex Central を不審オブジェクトハブ Apex Central から登録解除する

注意

ノードの Apex Central サーバを登録解除した後も、以前に同期されたすべてのオブジェクトがノードの Apex Central サーバの不審オブジェクトリストに残ります。

手順

1. 不審オブジェクトノードの Apex Central 管理コンソールにログオンします。
2. [脅威インテリジェンス] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。
3. [不審オブジェクトハブ Apex Central の設定] セクションで、[登録解除] をクリックします。

   確認ダイアログが表示され、サーバが不審オブジェクトハブ Apex Central から正常に登録解除されたことを示すメッセージが示されます。
4. 複数のノード Apex Central サーバが存在する場合は、各サーバで同様の手順を繰り返してください。

設定に関する補足

不審オブジェクトハブの設定と不審オブジェクトノードの Apex Central サーバの登録が正常に終了したら、次の設定情報に注意してください。

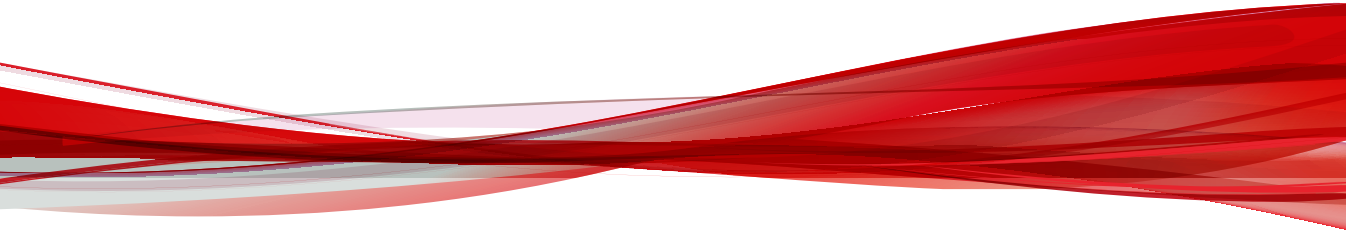
注意

ノードの Apex Central サーバを登録解除した後も、以前に同期されたすべてのオブジェクトがノードの Apex Central サーバの不審オブジェクトリストに残ります。

<table>
<tr><th>設定</th><th>不審オブジェクトハブ APEX CENTRAL</th><th>ノードの APEX CENTRAL</th></tr>
<tr><td>同期間隔</td><td>該当なし</td><td>5 分 (初期設定)</td></tr>
<tr><td rowspan="2">不審オブジェクトリストの同期</td><td>不審オブジェクトハブ Apex Central からノード:
仮想アナライザリスト
ユーザ指定リスト</td><td>ノードの Apex Central からハブ:
仮想アナライザリスト</td></tr>
<tr><td colspan="2">注意
ハブの Apex Central サーバは、ユーザ指定リストまたは除外リストの [メモ] 列のデータをノードの Apex Central サーバにデータを送信しません。
リストを同期する際に、ユーザ指定リストは仮想アナライザリストよりも優先されます。
次回の同期の前にオブジェクトが不審オブジェクトハブ Apex Central のユーザ指定リストと仮想アナライザリストの両方に追加される場合、不審オブジェクトハブ Apex Central サーバは両方のリストをノードの Apex Central サーバに配信します。
ノードの Apex Central の仮想アナライザリストに含まれるオブジェクトが不審オブジェクトハブ Apex Central のユーザ指定リストにも存在する場合、ノードの Apex Central の仮想アナライザリストでの不審オブジェクトのリスクレベルは次回の同期中に [高] に変わります。</td></tr>
<tr><td>不審オブジェクトの設定</td><td>不審オブジェクトハブ Apex Central から不審オブジェクトを設定すると、登録済みのノードの Apex Central サーバ全体で一貫性が確保されます。</td><td>該当なし</td></tr>
</table>

パート VII

Automation Center



第 23 章

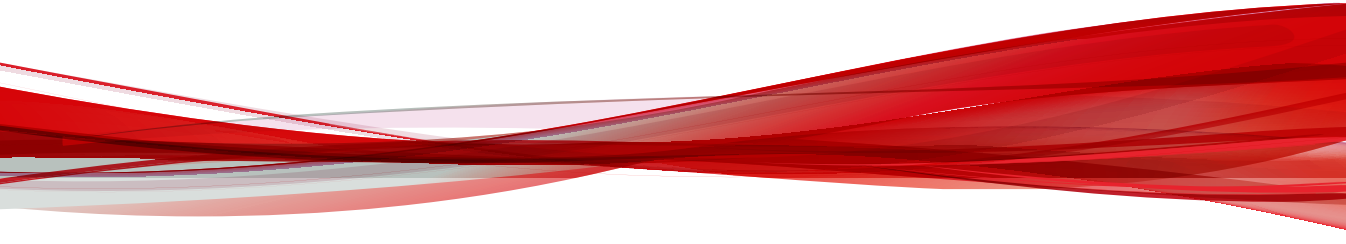
Apex Central Automation Center

Apex Central は、特定の製品の機能にアクセスできるようにする RESTful API を提供しています。この API を使用することで、サードパーティのソリューションを Apex Central と統合したり、不審オブジェクトの情報を収集および共有したり、調査や管理タスクを自動化したりできます。

詳細については、https://automation.trendmicro.com/apex-central/home を参照してください。

パート VIII

ツールとサポート



第 24 章

データベースの管理

ここでは、管理者が Apex Central システムを管理するために必要な情報について説明します。

次のトピックがあります。

Apex Central データベースについて

Apex Central は、ログ、コミュニケータスケジュール、管理下の製品および下位サーバの情報、ユーザアカウント、ネットワーク環境、通知設定などのデータの保存に Microsoft SQL Server データベース (db_ApexCentral.mdf) を使用しています。

Apex Central サーバでは、システム DSN ODBC 接続を使用してデータベース接続が確立されます。Apex Central をインストールすると、システム DSN ODBC 接続と、db_ApexCentral.mdf へのアクセスに使用する ID およびパスワードが生成されます。初期設定の ID は sa です。Apex Central では、パスワードが暗号化されます。

SQL Server のセキュリティを最大限確保するために、db_ApexCentral の管理に使用するすべての SQL アカウントに少なくとも次の権限を設定します。

- サーバの役割の dbcreator
- db_ApexCentral の db_owner の役割

管理下の製品のログは、データベースの拡張を検討する際の要因となります。管理下の製品から Apex Central にさまざまな種類のログが送信されます。

次の表では、ログの種類ごとのログ件数とデータベースサイズを示します。

表 24-1. ログ件数とデータベースサイズ

ログの種類	ログ件数	データベースサイズ (MB)
ウイルス	100,000	150
	500,000	750
	1,000,000	1,500
スパイウェア/グレーウェア	100,000	150
	500,000	750
	1,000,000	1,500

ログの種類	ログ件数	データベースサイズ (MB)
Web セキュリティ	100,000	150
	500,000	750
	1,000,000	1,500
挙動監視	100,000	120
	500,000	600
	1,000,000	1,200
情報漏えい対策	100,000	300
	500,000	1,500
	1,000,000	3,000
ファイルハッシュ検出	100,000	180
	500,000	900
	1,000,000	1,800
Attack Discovery	100,000	1,200
	500,000	6,000
	1,000,000	12,000
IPS	100,000	70
	500,000	350
	1,000,000	700
アプリケーションコントロール	100,000	200
	500,000	1,000
	1,000,000	2,000

ログの保存に必要なデータベース容量は、ログの種類とその数に基づいて計算されます。次に例を示します。

- Apex One の管理下の製品から Apex Central に、毎日 20,000 件のウイルスログと 10,000 件の Web セキュリティログが送信されます。
- Apex Central では、両方の種類のログが 90 日間保存されます。

必要なデータベース容量は、ウイルスログ用に 1.2GB、Web セキュリティログ用に 1GB です。ただし、ログの概要情報やその他の機能を対象としてさらに容量が必要になる場合があります。

Apex Central のデータベースは、スケーラブルなデータベースである SQL Server 上で実行されるため、理論的には、処理可能なデータベースのサイズの上限は、ハードウェアで処理可能なサイズの上限に等しくなります。トレンドマイクロでは、2,000,000 件までのエントリがテストされました。データベースサーバに負荷をかけすぎたり、パフォーマンスの限界まで使用した場合、管理コンソールで接続タイムアウトが起きる可能性があります。

ヒント

トレンドマイクロでは、データベースの増大に十分対応できるバッファ容量を割り当てることと、そのサイズを的確に測定できるようデータベースを監視することをお勧めします。

SQL Server Management Studio による db_ApexCentral のバックアップ

SQL Server を使用している場合、SQL Server Management Studio を使用して Apex Central データベースをバックアップします。

注意

Apex Central データベースは定期的にバックアップすることをお勧めします。管理下の製品を追加またはインストールするなど、Apex Central データベースを変更する際には、必ずバックアップを作成してください。

手順

1. Apex Central サーバがインストールされているコンピュータで、[スタート] > [すべてのプログラム] > [Microsoft SQL Server <version>] > [SQL Server Management Studio] の順にクリックします。

   <version> は、SQL Server Management Studio のバージョンです。

2. メニューバーで、[表示] > [オブジェクト エクスプローラ] の順にクリックします。[オブジェクト エクスプローラ] パネルで、<Host\Instance Name>をダブルクリックして [データベース] をダブルクリックします。

   <Host\Instance Name> は、SQL Server のホスト名と SQL のインスタンス名です。

3. db_ApexCentral を右クリックして、[タスク] > [バックアップ] の順にクリックします。

4. [バックアップ セット] で名前と説明を入力します。

5. [ソース] > [バックアップの種類] で [完全] を選択します。

6. [バックアップ先] で [追加] をクリックして、バックアップファイルの保存先を指定します。

7. 「完了」メッセージが表示されたら、[OK] をクリックします。

SQL Server Management Studio によるバックアップ db_ApexCentral の復元

SQL Server Management Studio を使用して、バックアップした Apex Central データベースを復元します。

手順

1. Apex Central を停止します。

2. [スタート] > [プログラム] > [管理ツール] > [サービス] をクリックして、[サービス] 画面を開きます。

3. 対象の <Apex Central サービス> を右クリックして、[停止] をクリックします。
4. [プログラム] > [SQL Server Management Studio] の順に選択して、SQL Server Management Studio にアクセスします。
5. コンソールで、[SQL Server グループ] > {SQL Server} > [データベース] の順にクリックします。

   {SQL Server} は SQL Server のホスト名です。
6. db_ApexCentral を右クリックし、[すべてのタスク] > [データベースの復元...] の順にクリックします。
7. [データベースとして復元] 画面で、復元するデータベースを選択します。
8. [OK] をクリックして、復元プロセスを開始します。
9. 完了メッセージが表示されたら、[OK] をクリックします。
10. [スタート] > [プログラム] > [管理ツール] > [サービス] をクリックして、[サービス] 画面を開きます。
11. 対象の <Apex Central サービス> を右クリックして、[再起動] をクリックします。
12. Apex Central を開始します。

SQL コマンドによる db_ApexCentral_Log.ldf の縮小

手順

1. SQL Server Management Studio を使用して、Apex Central データベースをバックアップします。
2. 使用可能なデータベースで、`db_ApexCentral` データベースを選択します。

3. 次の SQL スクリプトを実行します。

```
DBCC shrinkfile('db_ApexCentral_log', 10)
```

4. db_ApexCentral_Log.LDF のサイズが 10MB 未満であることを確認します。

   db_ApexCentral_Log.LDF のサイズが縮小されない場合は、次の SQL コマンドを実行して、使用されているデータベース復元モードを確認します。

```
SELECT name as DatabaseName, DATABASEPROPERTYEX(name, 'Recovery') as RecoveryMode FROM master.dbo.sysdatabases where name='db_ApexCentral'
```

   データベース復元モードが FULL の場合は、次の SQL スクリプトを実行します。

```
-- Truncate the log by changing the database recovery model to SIMPLE.
ALTER DATABASE db_ApexCentral
SET RECOVERY SIMPLE;
GO
-- Shrink the truncated log file to 10 MB.
DBCC SHRINKFILE (db_ApexCentral_Log, 10);
GO
-- Reset the database recovery model.
ALTER DATABASE db_ApexCentral
SET RECOVERY FULL;
GO
```

   SQL データベースの縮小および SQL コマンドの詳細については、Microsoft の SQL Server の管理についてのドキュメントを参照してください。

SQL Server Management Studio による db_ApexCentral_log.ldf の縮小

Apex Central データベースのトランザクションログファイルは、…¥data ¥db_ApexCentral_log.LDF です。SQL Server は通常処理の一環として、このトランザクションログを生成します。

db_ApexCentral_log.LDF には、db_ApexCentral.mdf を使用した管理下の製品に対するすべてのトランザクションが記録されます。

SQL Server の初期設定では、トランザクションログのファイルサイズには制限がありません。このままでは、ディスクの空き容量が圧迫されてしまいます。

Microsoft SQL Server 2008 以降での db_ApexCentral_log.ldf ファイルサイズの縮小

手順

1. SQL Server Management Studio を使用して、Apex Central データベースのバックアップを作成します。
2. トランザクションログを削除します。
3. SQL Server で、[プログラム] > [SQL Server Management Studio] の順に選択して、SQL Server Management Studio を起動します。
4. [SQL Server] を選択し、要求されたら、認証情報を指定します。
5. [db_ApexCentral] を右クリックし、[プロパティ] を選択します。

   [プロパティ] ダイアログボックスが表示されます。
6. [オプション] をクリックします。

   [オプション] 画面が表示されます。
7. [復旧モデル] リストから [単純] を選択します。

8. [OK] をクリックします。

第 25 章

Apex Central ツール

本章では、Apex Central のいくつかの設定ツールの使用方法について説明します。

次のトピックがあります。

Apex Central のツールについて

Apex Central では、設定作業に役立ついくつかのツールを用意しています。Apex Central は、ほとんどのツールを次の場所に保存しています。

`<Apex Central インストールディレクトリ>¥WebUI¥download¥tools¥`

エージェント移行ツール (AgentMigrateTool.exe) を使用する

Apex Central に付属のエージェント移行ツールを使用すると、別の Apex Central サーバによって管理されているエージェントを移行できます。

注意

エージェント移行ツールは Windows ベースおよび Linux ベースのエージェントの移行をサポートします。

手順

1. 「管理者」アカウントを使用して移行先のサーバにログオンします。

   重要

   「管理者」アカウントだけがエージェント移行ツールを実行するための十分な権限を持っています。

2. 次の場所から `AgentMigrateTool.exe` を実行します。`<Apex Central インストールディレクトリ>¥`

データベース設定ツールを使用する (DBConfig.exe)

DBConfig.exe ツールにより、ユーザは Apex Central データベース用のユーザアカウント、パスワード、およびデータベース名を変更できます。

このツールには次のオプションがあります。

- DBName: データベース名
- DBAccount: データベースのアカウント
- DBPassword: データベースのパスワード
- Mode: データベース認証モード (SQL Server 認証または Windows 認証)

注意

データベース認証モードの初期設定は、SQL Server 認証モードです。ただし、Windows 認証を設定する際には、Windows 認証モードで行う必要があります。

手順

1. Apex Central サーバでコマンドプロンプトを開きます。
2. 次のコマンドを使用して、DBConfig.exe ファイルが含まれるディレクトリに移動します。

   ```
   cd <Apex Central インストールディレクトリ>\DBConfig
   ```

3. dbconfig と入力し、ENTER キーを押します。

   DBConfig ツールインタフェースが 表示されます。

4. 変更する設定を指定します。

   - 例 1: `DBConfig -DBName="db_<データベース名>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
   - 例 2: `DBConfig -DBName="db_<データベース名>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`

- 例 3:`DBConfig -DBName="db_<データベース名>" -DBPassword="sqlPwd"`

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/jp/solution/1306559

第 26 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの 送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録

付録

付録 A

Apex Central のシステムチェックリスト

このセクションでは、システム関連情報を記入するためのチェックリストを参考として提供します。

次のトピックがあります。

サーバアドレスのチェックリスト

インストール処理の実行中、およびネットワークで使用する Trend Micro Apex Central サーバの設定時には、次のサーバアドレス情報を入力する必要があります。必要なときにいつでも参照できるように、ここに記録しておくことをお勧めします。

表 A-1. サーバアドレスのチェックリスト

必要な情報	Example	設定する値
Apex Central サーバ情報		
IP アドレス	10.1.104.255	
FQDN (完全修飾ドメイン名)	server.example.com	
NetBIOS (ホスト) 名	yourserver	
Web サーバ情報		
IP アドレス	10.1.104.225	
FQDN (完全修飾ドメイン名)	server.example.com	
NetBIOS (ホスト) 名	yourserver	
Apex Central の SQL データベース情報		
IP アドレス	10.1.104.225	
FQDN (完全修飾ドメイン名)	server.example.com	
NetBIOS (ホスト) 名	sqlserver	
コンポーネントダウンロード用のプロキシサーバ		
IP アドレス	10.1.174.225	
FQDN (完全修飾ドメイン名)	proxy.example.com	
NetBIOS (ホスト) 名	proxyserver	
SMTP サーバ情報 (任意: メールメッセージ通知用)		
IP アドレス	10.1.123.225	

必要な情報	EXAMPLE	設定する値
FQDN (完全修飾ドメイン名)	mail.example.com	
NetBIOS (ホスト) 名	mailserver	
SNMP トラップ情報 (任意: SNMP トラップ通知用)		
コミュニティ名	trendmicro	
IP アドレス	10.1.194.225	
Syslog サーバ情報 (任意: Syslog 通知用)		
IP アドレス	10.1.194.225	
サーバポート番号	514	

ポートのチェックリスト

Apex Central では、次のポートをそれぞれの目的に使用します。

ポート	例	設定する値
SMTP	25	
プロキシ	8088	
管理コンソールおよびアップデート/配信コンポーネント	80	

Apex Central 入力規則

Apex Central のインストールまたは管理コンソールの設定には、次の規則が適用されますので注意してください。

- ユーザ名
  - 最大長: 32 文字

- 使用できる文字: A～Z、a～z、0～9、「-」、「_」、「.」、「$」
- フォルダ名
  - 最大文字数: 32 文字
  - 使用できない文字: 「/」、「>」、「&」、「"」、「%」、「^」、「=」

注意

Apex Central サーバのホスト名については、インストール時にアンダースコア (_) を使用できます。

コアプロセスおよび設定ファイル

Apex Central では、システム設定および一時ファイルが XML 形式で保存されます。

次の表は、Apex Central で使用される設定ファイルおよびプロセスを示しています。

表 A-2. Apex Central 設定ファイル

設定ファイル	説明
AuthInfo.ini	プライベートキーファイル名、公開鍵ファイル名、証明書ファイル名、プライベートキーの暗号化されたパスフレーズ、ホスト ID、およびポートに関する情報を含む設定ファイルです。
aucfg.ini	アップデート設定ファイル
TVCS_Cert.pem	SSL 認証で使用される証明書です。
TVCS_Pri.pem	SSL で使用されるプライベートキーです。
TVCS_Pub.pem	SSL で使用される公開鍵です。
ProcessManager.xml	ProcessManager.exe で使用されます。
CmdProcessorEventHandler.xml	CmdProcessor.exe で使用されます。

設定ファイル	説明
DMRegisterinfo.xml	CasProcessor.exe で使用されます。
DataSource.xml	Apex Central のプロセスの接続パラメータを保存します。
SystemConfiguration.xml	Apex Central システム設定ファイル
agent.ini	MCP エージェントのファイルです。

表 A-3. Apex Central コアプロセス

プロセス	説明
ProcessManager.exe	Apex Central のコアプロセスを起動および停止します。
CmdProcessor.exe	他のプロセスによって作成された XML 命令の管理下の製品への送信、製品の登録の処理、アラートの送信、スケジュールされたタスクの実行、大規模感染予防ポリシーの適用などを行います。
LogReceiver.exe	過去のバージョンとの互換性のためにのみに使用します。
LogProcessor.exe	管理下の製品からログを受信し、管理下の製品からエンティティ情報を受信します。
LogRetriever.exe	ログを受信し、Apex Central データベースに保存します。
ReportServer.exe	Apex Central レポートを生成します。
MsgReceiver.exe	Apex Central サーバおよび管理下の製品からメッセージを受信します。
CasProcessor.exe	Apex Central サーバが他の Apex Central サーバを管理できるようにします。
inetinfo.exe	Microsoft Internet Information Service プロセスです。
cm.exe	dmserver.exe および mrf.exe を管理します。
dmserver.exe	Apex Central 管理コンソールのログオンページを提供し、製品ディレクトリ (Apex Central 側) を管理します。

プロセス	説明
sCloudProcessor.NET.exe	ステータスの照会、結果の照会、要求のキャンセルを行うために、Apex Central 管理コンソールまたはその他のプロセスに発行者のジョブ ID を提供するように要求します。ユーザ/エンドポイントディレクトリによって 使用されます。

通信ポートおよびサービスポート

初期設定の Apex Central 通信ポートおよびサービスポートは次のとおりです。

サービス	サービスポート
ProcessManager.exe	20501
CmdProcessor.exe	20101
comdProcessor.NET.exe	21003
LogReceiver.exe	20201
LogProcessor.exe	21001
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
CasProcessor.exe	20801
sCloudProcessor.NET.exe	21002

付録 B

データビュー

ここでは、レポートテンプレートおよびログクエリをカスタマイズするために、Apex Central がサポートしているデータビューについて説明します。

次のトピックがあります。

データビュー: セキュリティログ

ウイルス、スパイウェア/グレーウェア、フィッシングサイトなど、管理下の製品によって検出されたセキュリティ上の脅威に関する情報が表示されます。

高度な脅威情報

管理下の製品によってネットワーク上で検出された APT (標的型サイバー攻撃) に関する概要と詳細データが表示されます。

C&C コールバック詳細情報

ネットワーク上で検出された C&C コールバックイベントに関する具体的な情報が表示されます。

表 B-1. C&C コールバック詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
感染ホスト	コールバックを試行した IP アドレス、ホスト名、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を試行したオブジェクトを示します。
C&C リストのソース	C&C サーバの特定に使用された C&C リストのソースを示します。 • C&C IP リスト • グローバルインテリジェンスリスト • ユーザ指定 IP リスト • 仮想アナライザリスト

データ	説明
ネットワークグループ	管理下の製品 (Deep Discovery Inspector など) の管理者が定義した監視対象ネットワークグループを示します。
C&C リスクレベル	トレンドマイクロがイベントに割り当てるリスクレベルを示します。 • 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
地域/国	C&C サーバが配置されている地域および国を示します。
初回検出日時	コールバックアドレスをトレンドマイクロが最初に検出した日時を示します。
最新検出日時	コールバックアドレスに感染ホストが最後にコンタクトした日時を示します。
不正プログラムファミリ	コールバックアドレスに関連付けられている不正プログラムの名前を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。

機械学習型検索による検出詳細情報

機械学習型検索によって検出された高度な未知の脅威に関する具体的な情報が表示されます。

表 B-2. 機械学習型検索による検出詳細情報

データ	説明
検出時刻	管理下の製品のサーバまたはセキュリティエージェントが脅威を検出した日時を示します。
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
製品のエンティティ名/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • エンドポイントの名前または IP アドレスを示します。
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの IP アドレスを示します。 • エンドポイントの IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。
サーバ	Apex Central における管理下の製品のサーバの表示名を示します。
潜在的な脅威の種類	機械学習型検索が分析を他の既知の脅威と比較した後で、ファイルに含まれている可能性の高い脅威の種類を示します。
セキュリティの脅威	セキュリティの脅威の名前を示します。
ログオンユーザ	イベントの時点でログオンしていたユーザの名前を示します。
種類	検出を開始したオブジェクトの種類(「ファイル」または「プロセス」)を示します。
ファイルパス	ファイルオブジェクトのパスまたはプロセスを実行したプログラムのパスを示します。
ファイル作成日時	ファイルオブジェクトが作成された日付と時刻を示します。
親プロセス	検出されたプロセスを開始したプロセスを示します。
プロセスコマンド	検出されたプロセスを実行したコマンドを示します。
プロセス所有者	検出プロセスをトリガしたユーザ名を示します。

データ	説明
エンドポイントの感染経路	脅威の発生元のチャネルを示します。
感染元	脅威の発生元を示します。
脅威の可能性	ファイル/プロセスが不正プログラムモデルとどの程度一致するかを示します。
処理結果	管理下の製品によって実行された処理の結果を示します。
件名	検出を開始したメールメッセージの件名を示します。
配信時刻	メールメッセージがメールサーバに送信された日時を示します。
送信者	検出を開始したメールメッセージの送信者を示します。
受信者	検出を開始したメールメッセージの受信者を示します。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

不審ファイルの詳細情報

ネットワークで検出された不審ファイルに関する具体的な情報が表示されます。

表 B-3. 不審ファイルの詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
検出	管理下の製品で脅威が検知された日付と時刻を示します。
エンドポイント	エンドポイントの名前を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。

データ	説明
エンドポイントの IP アドレス	エンドポイントの IP アドレスを示します。
エンドポイントのホスト名	エンドポイントのホスト名を示します。
ファイルタイプ	ファイルオブジェクトの種類を示します。
ファイル SHA-1	ファイルオブジェクトの SHA-1 ハッシュ値を示します。
ファイルパス	ファイルオブジェクトのパスまたはプロセスを実行したプログラムのパスを示します。
C&C リストのソース	C&C サーバの特定に使用された C&C リストのソースを示します。 • C&C IP リスト • グローバルインテリジェンスリスト • ユーザ指定 IP リスト • 仮想アナライザリスト
処理	管理下の製品によって実行された処理を示します。
検索の種類	イベントがレポートされた検索の種類 (リアルタイム検索、予約検索、手動検索など) を示します。
作成日時	ファイルオブジェクトが作成された日付と時刻を示します。
変更日時	ファイルオブジェクトが最後に変更された日時を示します。

仮想アナライザによる検出情報

仮想アナライザによって検出された高度な未知の脅威に関する具体的な情報が表示されます。

表 B-4. 仮想アナライザによる検出情報

データ	説明
生成	管理下の製品でデータが生成された日付と時刻を示します。

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
製品	管理下の製品またはサービスの名前を示します。
サーバ名	サーバの名前を示します。
ホスト	ホストの名前を示します。
エントリチャネル	感染経路を示します。
ソース	脅威の発生元を示します。
配信先	脅威の対象の場所を示します。
プロセス名	検出を開始したプロセスの名前を示します。
SHA1	検出を開始したファイルオブジェクトの SHA-1 ハッシュ値を示します。
種類	検出を開始したオブジェクトの種類(「ファイル」または「プロセス」)を示します。
ファイル名	検出を開始したファイルオブジェクトの名前を示します。
ファイルタイプ	検出を開始したファイルオブジェクトの種類を示します。
URL	検出を開始した URL オブジェクトを示します。
送信ルール	仮想アナライザによって送信されたルールを示します。
作成要求日時	仮想アナライザがルールを送信した日時を示します。
完了日時	仮想アナライザが分析を完了した日時を示します。
セキュリティの脅威	セキュリティの脅威の名前を示します。
リスクレベル	仮想アナライザによって割り当てられたリスクレベルを示します。
脅威のカテゴリ	セキュリティの脅威の種類を示します。
最も重大な脅威	重大度レベル別の最も重大な脅威を示します。

データ	説明
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

仮想アナライザで作成された不審オブジェクトによる影響の詳細情報

仮想アナライザで検出された不審オブジェクトの影響に関する詳細情報が表示されます。

データ	説明
種類	不審オブジェクトの種類を示します。
オブジェクト	不審オブジェクトの名前を示します。
検出時の処理	不審オブジェクトを検出した管理下の製品によって実行された検出時の処理を示します。 (例: ログ、ブロック)
リスクレベル	セキュリティの脅威のリスクレベルを示します。
有効期限	不審オブジェクトに設定されている有効期限の日時を示します。
初回サンプル送信日時	管理下の製品が仮想アナライザに不審オブジェクトを最初に送信した日時を示します。
初回サンプル送信製品名	不審オブジェクトを仮想アナライザに最初に送信した管理下の製品の名前を示します。
初回サンプル送信ホスト名	不審オブジェクトを仮想アナライザに最初に送信した管理下のサーバの表示名を示します。
初回サンプル送信 IP アドレス	サンプルを仮想アナライザに送信した最初の製品の IP アドレス (サーバ) を示します。
初回送信時のサンプル名	仮想アナライザに送信された最初のサンプルのファイル名を示します。
初回送信時のサンプルの種類	仮想アナライザに送信された最初のサンプルのファイルの種類を示します。

データ	説明
初回のサンプルソース	仮想アナライザに送信された最初のサンプルの送信元を示します。
初回のサンプルの宛先	仮想アナライザに送信された最初のサンプルの送信先を示します。
最終サンプル送信日時	管理下の製品が仮想アナライザに不審オブジェクトを最後に送信した日時を示します。
最終サンプル送信製品名	サンプルを仮想アナライザに送信した最後の製品を示します。
最終サンプル送信ホスト名	仮想アナライザに不審オブジェクトを最後に送信した管理下の製品の表示名を示します。
最終サンプル送信 IP アドレス	サンプルを仮想アナライザに送信した最後の製品の IP アドレス (サーバ) を示します。
最終送信時のサンプル名	仮想アナライザに送信された最後のサンプルのファイル名を示します。
最終送信時のサンプルの種類	仮想アナライザに送信された最後のサンプルのファイルの種類を示します。
最終送信時のサンプルの SHA-1 値	仮想アナライザに送信された最後のサンプルのファイルの SHA-1 値を示します。
最終送信時のサンプルの検出ルール	仮想アナライザに送信された最後のサンプルの検出名を示します。
最終のサンプルソース	仮想アナライザに送信された最後のサンプルの送信元を示します。
最終のサンプルの宛先	仮想アナライザに送信された最後のサンプルの送信先を示します。
エンドポイントのドメイン名	検出を実行したエンドポイントのドメイン名を示します。
エンドポイントのホスト名	検出を開始したエンドポイントの表示名を示します。
エンドポイントのユーザドメイン名	検出時にエンドポイントにログオンしていたユーザのドメイン名を示します。

データ	説明
エンドポイントのユーザドメインアカウント	検出時にエンドポイントにログオンしていたユーザのドメインアカウントを示します。
エンドポイントのユーザ名	イベントの時点でログオンしていたユーザの名前を示します。
エンドポイントの IP アドレス	エンドポイントの IP アドレスを示します。
不審オブジェクト初回使用日時	エンドポイントで不審オブジェクトが最初に検出された日時を示します。
不審オブジェクト初回使用製品	エンドポイントで不審オブジェクトを最初に検出した管理下の製品の名前を示します。
不審オブジェクト初回使用時の処理	作成された不審オブジェクトをもとに、最初にファイルを検出した製品で実行された処理が表示されます。
不審オブジェクト最終使用日時	エンドポイントで不審オブジェクトが最後に検出された日時を示します。
不審オブジェクト最終使用製品	エンドポイントで不審オブジェクトを最後に検出した管理下の製品の名前を示します。
不審オブジェクト最終使用時の処理	作成された不審オブジェクトをもとに、最後にファイルを検出した製品で実行された処理を示します。
エンドポイントの最後の処理結果	作成された不審オブジェクトをもとに、最後にファイルを検出した製品で実行された処理の結果を示します。

Attack Discovery による検出

Attack Discovery によって提供された情報が表示されます。

Attack Discovery による検出情報

Attack Discovery によって検出された脅威に関する一般情報が表示されます。

表 B-5. Attack Discovery による検出情報

データ	説明
生成	管理下の製品でデータが生成された日付と時刻を示します。
受信	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
エンドポイント	エンドポイントの名前を示します。
製品	管理下の製品またはサービスの名前を示します。
管理サーバのエンティティ名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。
製品バージョン	管理下の製品のバージョンを示します。
Tactics	検知された MITRE ATT&CK™ Tactics を示します。 詳細については、https://attack.mitre.org/tactics/enterprise/を参照してください。
Techniques	検知された MITRE ATT&CK™ Techniques を示します。 詳細については、https://attack.mitre.org/techniques/enterprise/を参照してください。
エンドポイント IP	エンドポイントの IP アドレスを示します。
リスクレベル	Attack Discovery によって割り当てられたリスクレベルを示します。
パターンファイルバージョン	検出の種類に対応する Attack Discovery パターンファイルの番号を示します。
ルール ID	検出ルールのシリアル番号を示します。
ルール名	Attack Discovery で検出する挙動を指定するルールを示します。
関連するオブジェクト	検出数を示します。 数字をクリックすると、詳細が表示されます。 詳細については、644 ページの「Attack Discovery による検出の詳細情報」を参照してください。

データ	説明
生成日時 (ローカル時間)	Attack Discovery が脅威を検出した時刻 (エージェントのローカルタイムゾーンに基づく) を示します。 時刻は UTC のオフセット付きで表示されます。
インスタンス ID	イベントに割り当てられた検出 ID を示します。 同じインスタンス ID を持つエントリは同じイベントに属します。

Attack Discovery による検出の詳細情報

Attack Discovery によって検出された脅威に関する一般情報が表示されます。

表 B-6. Attack Discovery による検出の詳細情報

データ	説明
オブジェクトの値	検出された脅威の標的となったオブジェクトの名前を示します。
オブジェクトの種類	検出された脅威の標的となったオブジェクトの種類を示します。
最初に記録	脅威の検出が Attack Discovery で初めて記録された時刻を示します。
ファイルディレクトリ	検出された脅威の標的となったオブジェクトのディレクトリを示します。
プロセス ID	プロセスの PID を示します。
CLI コマンド	脅威の検出をトリガしたプロセスコマンドを示します。
署名者	証明書署名者を示します。
ユーザドメイン	検出されたユーザアカウントのドメイン名を示します。
ユーザ名	オブジェクトに関連付けられたアカウント名を示します。
偽装ユーザ名	脅威によって偽装されたユーザ名を示します。
認証 ID	ログオンセッションに割り当てられたローカル一意識別子を示します。

データ	説明
整合性レベル	ログオンユーザに割り当てられている保護またはアクセスのレベルを示します。
ファイル SHA-1	オブジェクトファイルの SHA-1 ハッシュ値を示します。
ファイル SHA-256	オブジェクトファイルの SHA-256 ハッシュ値を示します。
ファイルの MD5	オブジェクトファイルの MD5 ハッシュ値を示します。
調査レーティング	ファイルの記録された履歴に基づいてトレンドマイクロの脅威の専門家によって決定されたレーティングを示します。
ファイルセキュリティの所有者	ファイルのプロパティに基づくファイルの現在の所有者を示します。
ファイルセキュリティの所有者のドメイン	ファイルのプロパティに基づくファイルの現在の所有者のドメインを示します。
ファイルセキュリティの以前の所有者	ファイルのプロパティに基づくファイルの以前の所有者を示します。
ファイルセキュリティの以前の所有者のドメイン	ファイルのプロパティに基づくファイルの以前の所有者のドメインを示します。
レジストリキー	脅威がアクセスしたレジストリキーを示します。
レジストリ値の名前	脅威がアクセスしたレジストリ値の名前を示します。
レジストリ値のデータ	脅威がアクセスしたレジストリ値のデータを示します。
AMSI で検出されたアプリケーション名	脅威に関連付けられているアプリケーション名またはスクリプト言語を示します。
AMSI で検出されたアプリケーションのフルパス	脅威に関連付けられているアプリケーションのフルパスを示します。
AMSI で検出されたアプリケーションのバージョン	脅威に関連付けられているアプリケーションのバージョンを示します。

データ	説明
AMSI で検出されたスクリプトファイル	検出されたスクリプトファイルの名前と拡張子を示します。
AMSI で検出されたスクリプトの記述	スクリプトの内容を示します。
AMSI で検出されたスクリプトファイル SHA-1	検出されたスクリプトファイルの SHA-1 ハッシュ値を示します。
AMSI で検出されたスクリプトファイル SHA-256	検出されたスクリプトファイルの SHA-256 ハッシュ値を示します。
送信元 IP アドレス	検出された脅威の送信元 IP アドレスを示します。
送信元ポート番号	検出された脅威の送信元 IP アドレスポート番号を示します。
送信先 IP アドレス	脅威がアクセスした IP アドレスを示します。
送信先 IP アドレスポート番号	脅威がアクセスした IP ポート番号を示します。
送信先 URL	脅威がアクセスした URL を示します。
宛先ドメイン	脅威がアクセスしたドメイン名を示します。
WMI イベント	脅威に関連付けられている WMI イベント情報を示します。
Windows イベントソース	Windows イベントログに従ってイベントをログ記録したソフトウェアの名前を示します。
Windows イベントログの内容	検出をトリガした Windows イベントログの内容を示します。
特権の名前	脅威が変更した認証権限名を示します。
特権の属性	脅威が変更した認証権限属性を示します。
すべて無効にする認証権限	脅威が変更した、すべてを無効にする認証権限のステータスを示します。

コンテンツ違反情報

管理下の製品によってネットワーク上で検出された違反コンテンツに関する概要と詳細データが表示されます。

コンテンツ違反の処理/結果の概要

コンテンツ違反に対して管理下の製品が実行した処理の概要が表示されます。例: コンテンツ違反に対して管理下の製品が実行した処理、処理の実行で影響を受けるメールメッセージの数

表 B-7. コンテンツ違反の処理/結果の概要データビュー

データ	説明
処理	コンテンツポリシーに違反するメールメッセージに対して管理下の製品が実行した処理の種類が表示されます。 例: 通知、添付ファイル削除、削除
ポリシー違反検出数	管理下の製品が指定の処理を実行した違反の数が表示されます。

コンテンツ違反検出の概要 (時間別推移)

一定の期間 (毎日、毎週、毎月) のコンテンツ違反検出の概要が表示されます。例: 概要データが収集された日時、コンテンツ違反の影響を受けるエンドポイント数、ネットワーク上の特定のコンテンツ違反の総数およびコンテンツ違反の総数

表 B-8. コンテンツ違反検出の概要 (時間別推移) データビュー

データ	説明
日時	データの概要が生成された時間が表示されます。
一意のポリシー数	違反ポリシーの数が表示されます。 例:管理下の製品で、1 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー数] は「1」になります。

データ	説明
一意の送信者/ユーザ数	管理下の製品のポリシーに違反するコンテンツを送信したメールアドレスまたはユーザの絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータから送信された、同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[一意の送信者/ユーザ数] は「3」になります。
一意の受信者数	管理下の製品のポリシーに違反するコンテンツを受信したメールメッセージ受信者の絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[一意の受信者数] は「2」になります。
検出数	管理下の製品が検出したポリシー違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

コンテンツ違反ポリシーの概要

特定のポリシーに関連するコンテンツ違反の検出の概要が表示されます。例: 違反ポリシーの名前、コンテンツ違反を検出したフィルタの種類、ネットワーク上のコンテンツ違反の総数

表 B-9. コンテンツ違反ポリシーの概要データビュー

データ	説明
ポリシー	エンドポイントが違反しているポリシーの名前が表示されます。
フィルタの種類	違反をトリガしたフィルタの種類が表示されます。例: コンテンツフィルタ、フィッシングフィルタ、URL レピュテーションフィルタ

データ	説明
一意の送信者/ユーザ数	管理下の製品のポリシーに違反するコンテンツを送信したメールアドレスまたはユーザの絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータから送信された、同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[一意の送信者/ユーザ数] は「3」になります。
一意の受信者数	管理下の製品のポリシーに違反するコンテンツを受信したメールメッセージ受信者の絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[一意の受信者数] は「2」になります。
検出数	管理下の製品が検出したポリシー違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

コンテンツ違反送信者の概要

特定の送信者に関連するコンテンツ違反の検出の概要が表示されます。例: コンテンツの送信者の名前、コンテンツ違反の絶対数、ネットワーク上のコンテンツ違反の総数

表 B-10. コンテンツ違反送信者の概要データビュー

データ	説明
送信者/ユーザ	管理下の製品のポリシーに違反するコンテンツを送信したメールアドレスまたはユーザが表示されます。
検出数	管理下の製品が検出したポリシー違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

データ	説明
一意の受信者数	管理下の製品のポリシーに違反するコンテンツを受信したメールメッセージ受信者の絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[一意の受信者数] は「2」になります。
一意のポリシー数	違反ポリシーの数が表示されます。 例:管理下の製品で、1 台のコンピュータで同一ポリシーの違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー数] は「1」になります。

コンテンツ違反詳細情報

コンテンツ違反が含まれるメールに関する具体的な情報が表示されます。たとえば、コンテンツ違反を検知した管理下の製品、メールの送信者と受信者、コンテンツ違反ポリシーの名称、検知された違反の総数などです。

表 B-11. コンテンツ違反詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
受信者	管理下の製品のポリシーに違反するコンテンツを受信したメール受信者を示します。
送信者/ユーザ	管理下の製品のポリシーに違反するコンテンツを送信したメールアドレスまたはユーザを示します。

データ	説明
件名	ポリシーに違反するメールの件名の内容を示します。
ポリシー	メールが違反しているポリシーの名前を示します。
ポリシー設定	メールが違反しているポリシーの設定を示します。
ファイルの場所	ポリシーに違反しているファイルの場所を示します。
ファイル	ポリシーに違反しているファイルの名前を示します。
URL	指定したポリシーに違反している URL を示します。
リスクレベル	ネットワークに対するリスク (トレンドマイクロによる診断) を示します。 例: 高、中、低
フィルタの種類	違反メールを検出したフィルタの種類を示します。 例: コンテンツフィルタ、サイズフィルタ、添付ファイルフィルタ
サブフィルタの種類	違反メールを検出したサブフィルタの種類を示します。
フィルタ処理	ポリシーに違反するメールに対して検出フィルタが実行した処理を示します。 例: 駆除、隔離、削除
フィルタ処理結果	違反を検出したフィルタによって実行された処理の結果を示します。
処理	管理下の製品によって実行された処理を示します。 例: 配信、削除、通知
検出数	検出の総数を示します。

高度な脅威を含むメールメッセージ

高度な脅威を含むメールメッセージに関する具体的な情報が表示されます。たとえば、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です。

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
受信者	検出を開始したメールメッセージの受信者を示します。
送信者	検出を開始したメールメッセージの送信者を示します。
件名	検出を開始したメールメッセージの件名を示します。
添付ファイル数	メールの添付ファイルの数を示します。
添付ファイル	メールの添付ファイルの名前を示します。
添付ファイルの種類	メールの添付ファイルの種類を示します。
処理	管理下の製品によって実行された処理を示します。 例: 配信、削除、隔離
脅威の種類	セキュリティの脅威の種類を示します。
脅威名	セキュリティの脅威の名前を示します。
リスクレベル	メールのリスクレベルの調査結果を示します。
送信元 IP	メール送信元に最も近いメール転送エージェント (MTA) の IP アドレスを示します。
メッセージ ID	管理者が設定した一意のメッセージ ID を示します。
リンク数	メールに含まれるリンクの数を示します。
リンク	メールに含まれるリンクのリストを示します。

データ検出情報

データ検出に関する情報が表示されます。

データ検出の情報漏えい対策検出情報

データ検出によって検出されたイベントに関する具体的な情報が表示されます。

表 B-12. データ検出の情報漏えい対策検出情報

データ	説明
受信	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
ルール	検出を開始したルールの名前を示します。
エンドポイント	エンドポイントの名前または IP アドレスを示します。
ドメイン	管理下の製品が属するドメインを示します。
ユーザ	イベントの時点でログオンしていたユーザの名前を示します。
ユーザドメイン	ユーザが属するドメインの名前を示します。
ファイルパス	デジタル資産を含む場所のフルパスまたはチャネル (使用可能なソースがない場合) を示します。
ファイル	脅威がアクセスしたファイルオブジェクトの名前を示します。
テンプレート	イベントにより起動された正確なルール名とテンプレートを示します。
処理	管理下の製品によって実行された処理を示します。
詳細	ユーザが機密データの転送を続行している理由などの追加情報を示します。

データ検出エンドポイント情報

表 B-13. データ検出エンドポイント情報

データ	説明
生成	ログデータが管理下の製品で生成された時間が表示されます。

データ	説明
エンドポイント	情報漏えい対策により転送が検出されたコンピュータの IP アドレスまたはホスト名が表示されます。
デバイスクラス	Windows デバイスマネージャに示されているデバイスカテゴリの名前が表示されます。
デバイス表示名	Windows デバイスマネージャに示されているデバイスの表示名が表示されます。
プロバイダ	デバイスを提供しているプロバイダの名称が表示されます。

情報漏えい対策情報

管理下の製品から収集された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を表示します。

情報漏えい対策イベント情報

情報漏えい対策によって検出されたイベントに関する具体的な情報が表示されます。

表 B-14. 情報漏えい対策イベント情報

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
イベント ID	イベントの ID を示します。
重大度	イベントの重大度レベルを示します。
ステータス	イベントの検出ステータスを示します。
マネージャ	部門のマネージャの名前を示します。
部署	部門の名前を示します。

データ	説明
ポリシー	検出を開始したポリシーを示します。
製品のエンティティ名/エンドポイント	エンドポイントの名前を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの IP アドレスを示します。 • エンドポイントの IP アドレスを示します。
製品/エンドポイント MAC	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの MAC アドレスを示します。 • セキュリティエージェントのエンドポイントの MAC アドレスを示します。
管理サーバ	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。
エンドポイント	エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレスまたはホスト名を示します。
イベント発生元 (Active Directory の表示名)	イベント発生元の Active Directory の表示名を示します。
イベント発生元 (Active Directory のアカウント)	イベント発生元の Active Directory のアカウント名を示します。
イベント発生元 (送信者)	発生元のメールアドレスを示します。
Web サイト	イベントを開始した Web サイトの URL を示します。
受信者	送信先のメールアドレスを示します。
件名	メールメッセージの件名を示します。

データ	説明
ファイルの場所	ファイルの場所と名前を示します。
ファイル	イベントが発生したファイルの名前を示します。
ファイル/データのサイズ	イベントを開始したファイルまたはデータのサイズを示します。
ルール	イベントによって開始されたルールの名前を示します。
テンプレート	テンプレート一致が発生したテンプレートの名前を示します。
チャネル	デジタル資産の転送に使用されたエンティティを示します。
配信先	転送の配信先を示します。
処理	管理下の製品によって実行された処理を示します。
イベント	イベント数を示します。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

情報漏えい対策テンプレート一致情報

表 B-15. 情報漏えい対策テンプレート一致情報

データ	説明
ID	ログの一意の ID が表示されます。
受信	管理下の製品がイベント情報を受信した時間が表示されます。
生成	イベントが発生した時間が表示されます。
製品のエンティティ/エンドポイント	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品のエンティティ表示名。Apex Central では、管理下の製品のエンティティ表示名を使用して、管理下の製品を識別します。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレスまたはホスト名。

データ	説明
製品	管理下の製品の名前が表示されます。例: Apex One、InterScan for Microsoft Exchange
製品/エンドポイント IP	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品がインストールされるサーバの IP アドレス。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレス。
製品/エンドポイント MAC	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品がインストールされるサーバの MAC アドレス。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの MAC アドレス。
管理サーバ	エンドポイントが登録されている管理下の製品のエンティティ表示名が表示されます。Apex Central では、管理下の製品のエンティティ表示名を使用して、管理下の製品を識別します。
エンドポイント	エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレスまたはホスト名が表示されます。
イベント発生元 (ユーザ)	ログオンしているユーザ名が表示されます。
受信者	送信先のメールアドレスが表示されます。
件名	メールメッセージの件名が表示されます。
ファイルの場所	ファイルの場所と名前が表示されます。
ファイル	イベントが発生したファイルの名前が表示されます。
ポリシー	イベントにより起動されたポリシーの名前が表示されます。
テンプレート	テンプレート一致が発生したテンプレートの名前が表示されます。
チャネル	デジタル資産の転送に使用されたエンティティが表示されます。

Deep Discovery 情報

管理下の製品によってネットワーク上で検出された不審アクティビティに関する概要と詳細データが表示されます。

相関の詳細情報

詳細な脅威分析と推奨される修復方法に関する具体的な情報が表示されます。

表 B-16. 相関の詳細情報データビュー

データ	説明
生成	管理下の製品でデータが生成された日付と時刻を示します。
IP アドレス	エンドポイントの IP アドレスを示します。
ネットワークグループ	監視対象ネットワークグループを示します。
プロトコル	管理下の製品が脅威を検出したさまざまなプロトコルグループを示します。
脅威の種類	セキュリティの脅威の種類を示します。 例: ウイルス、スパイウェア/グレーウェア、不正行為
重大度	イベントの重大度レベルを示します。
検出	相関ルールに基づく検出の種類を示します。
詳細	検出に関する注釈やコメントを示します。
MAC アドレス	エンドポイントの MAC アドレスを示します。
ホスト名	エンドポイントの名前を示します。
相関ルール ID	相関ルールのルール ID を示します。

軽減処理の詳細情報

ネットワーク上の脅威を解決するために Mitigation Server で実行されたタスクに関する具体的な情報が表示されます。

表 B-17. 軽減処理の詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
Mitigation Server エンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。
エンドポイント IP	エンドポイントの IP アドレスを示します。
エンドポイント	エンドポイントの名前を示します。
データソース	脅威イベント情報を生成した Deep Discovery 製品またはタスクを示します。
データソースホスト	脅威イベント情報を生成した Deep Discovery 製品のホスト名を示します。
脅威イベント	Mitigation Server で記録された脅威関連イベントを示します。 詳細については、http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm を参照してください。
軽減ステータス	ステータスグループ別の脅威イベントを示します。 詳細については、http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm を参照してください。
軽減の詳細	脅威イベントに関する軽減処理の詳細を示します。 詳細については、http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/mitigation_status.htm を参照してください。
検出数	検出の総数を示します。
詳細情報	脅威に関する詳細を示します。

脅威の兆候の詳細情報

脅威の兆候を検出した管理下の製品、発生元および感染先に関する具体的な情報、ネットワーク上の脅威の兆候の総数など、ネットワーク上の脅威の兆候に関する具体的な情報が表示されます。

表 B-18. 脅威の兆候の詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
Mitigation ホスト	Mitigation Server (例: Network VirusWall Enforcer、Threat Mitigator) のホスト名を示します。
トラフィック/接続	転送の方向を示します。
プロトコルグループ	管理下の製品が脅威を検出したさまざまなプロトコルグループを示します。 例: FTP、HTTP、P2P
プロトコル	管理下の製品が脅威の兆候を検出したプロトコルを示します。 例: ARP、 BitTorrent
送信先 IP アドレス	脅威がアクセスした IP アドレスを示します。
送信先ホスト	脅威がアクセスしたエンドポイントの表示名を示します。
送信先ポート	脅威がアクセスした IP ポート番号を示します。
送信先 MAC アドレス	脅威がアクセスした MAC アドレスを示します。
送信先 OS	脅威がアクセスしたエンドポイント上の OS を示します。

データ	説明
送信先ユーザ<x>	対象ホストへのログオンに使用された名前を示します。 <x>はユーザ名を示します。
ログオン (送信先ユーザ<x>)	ログオンのタイムスタンプを示します。 <x>はログオン回数と特定のタイムスタンプを示すを示します。
送信元 IP アドレス	検出された脅威の送信元 IP アドレスを示します。
感染元ホスト名	セキュリティの脅威の発生源であるエンドポイントの名前を示します。
送信元ポート	検出された脅威の送信元 IP アドレスポート番号を示します。
送信元 MAC アドレス	検出された脅威の送信元 MAC アドレスを示します。
送信元 OS	セキュリティの脅威が発生したエンドポイント上の OS を示します。
送信元ユーザ<x>	対象送信元ホストへのログオンに使用された名前を示します。 <x>はユーザ名です。
ログオン (送信元ユーザ<x>)	送信元のログオンのタイムスタンプを示します。 <x>はログオン回数と特定のタイムスタンプを示すを示します。
送信元ドメイン	脅威が発生したエンドポイントのドメインを示します。
セキュリティの脅威の種類を示します。	セキュリティの脅威の種類を示します。 例: ウイルス、スパイウェア/グレーウェア、不正行為
ポリシー/ルール	検出を開始したポリシーまたはルールを示します。
受信者	検出を開始した転送の受信者を示します。
送信者	検出を開始した転送の送信者を示します。
件名	検出を開始したメールメッセージの件名を示します。
添付ファイル名	添付ファイルの名前と拡張子を示します。
添付ファイルの種類	添付されているファイルの種類を示します。

データ	説明
添付ファイルの SHA-1	添付ファイルの SHA-1 ハッシュ値を示します。
URL	脅威の兆候と考えられる URL を示します。
ユーザ (アカウント)	管理下の製品によって脅威が検出されたとき、送信先にログオンしていたユーザの名前を示します。
IM/IRC ユーザ	Deep Discovery Inspector によって違反が検出された際に、メッセンジャーまたは IRC にログオンしていたユーザ名を示します。
ブラウザ/FTP クライアント	脅威の兆候の発生元の Web ブラウザまたは FTP エンドポイントを示します。
ファイル	ファイルオブジェクトの名前、またはプロセスを実行したプログラムを示します。
圧縮ファイル内のファイル	圧縮ファイルに含まれる、影響を受けるファイルオブジェクトの名前を示します。
アーカイブの SHA-1	アーカイブファイルオブジェクトの SHA-1 ハッシュ値を示します。
アーカイブファイルタイプ	アーカイブされたファイルオブジェクトの種類を示します。
共有フォルダ	脅威の兆候の発生元が共有フォルダかどうかを示します。
SHA-1	ファイルオブジェクトの SHA-1 ハッシュ値を示します。
軽減処理	Mitigation Server によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイル削除、ファイルは削除されました
軽減結果	Mitigation Server によって実行された処理の結果を示します。
送信元 IP グループ	脅威の兆候の発生元の IP アドレスのグループを示します。
送信元ネットワークゾーン	脅威の兆候の発生元のネットワークゾーンを示します。
エンドポイントグループ	脅威の兆候が影響を与えるエンドポイントの IP アドレスグループを示します。

データ	説明
エンドポイントネットワークゾーン	脅威の兆候が影響を与えるエンドポイントのネットワークゾーンを示します。
検出数	検出の総数を示します。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されたとします。 この場合、[検出数] は「10」になります。
C&C リストのソース	C&C サーバの特定に使用された C&C リストのソースを示します。 • C&C IP リスト • グローバルインテリジェンスリスト • ユーザ指定 IP リスト • 仮想アナライザリスト
C&C リスクレベル	C&C コールバックのリスクレベルを示します。
注釈	イベントの追加情報を示します。
C&C サーバ	C&C サーバの名前、URL、または IP アドレスを示します。
C&C サーバの種類	C&C サーバの種類を示します。
不正プログラムの種類	不正プログラムの種類を示します。

脅威の兆候の概要 (全体)

ネットワーク上の脅威の兆候に関する具体的な情報が表示されます。例: 違反ポリシー/ルール、発生元および感染先に関する概要情報、ネットワーク上の脅威の兆候の総数

表 B-19. 脅威の兆候の概要 (全体) データビュー

データ	説明
ポリシー/ルール	違反ポリシー/ルールの名前が表示されます。

データ	説明
プロトコル	違反が発生しているプロトコルが表示されます。 例: HTTP、FTP、SMTP
一意のエンドポイント数	脅威の兆候の影響を受けるコンピュータの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同じ種類の脅威の兆候のインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「2」になります。
一意の送信元数	脅威の兆候の発生元の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータからきている同じ種類の脅威の兆候のインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「3」になります。
一意の受信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを受信したメールメッセージ受信者の絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されました。 この場合、[一意の受信者数] は「2」になります。
一意の送信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを送信したメールメッセージ送信者の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータから送信された、同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されました。 この場合、[一意の送信者数] は「3」になります。
検出数	管理下の製品が検出したポリシー/ルール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
軽減処理数	Network VirusWall Enforcer デバイスまたは Trend Micro Threat Mitigator によって処理が実行されたエンドポイントの数が表示されます。

データ	説明
ウイルス駆除されたエンドポイント数	Total Discovery Mitigation Server が駆除を実行するエンドポイントの総数が表示されます。
エンドポイントのクリーンナップ率 (%)	[検出数] の総数との比較で、Total Discovery Mitigation Server が駆除を実行したエンドポイントの割合が表示されます。

脅威の兆候の送信元の概要

特定の発生元からの脅威の兆候検出の概要が表示されます。例: 発生元の名前、感染先およびルール/違反に関する概要情報、ネットワーク上の脅威の兆候の総数

表 B-20. 脅威の兆候の送信元の概要データビュー

データ	説明
送信元 IP	脅威の兆候の発生元の IP アドレスが表示されます。
一意のポリシー/ルール数	発生元のコンピュータが違反しているポリシー/ルールの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー/ルール数] は「1」になります。
一意のエンドポイント数	脅威の兆候の影響を受けるコンピュータの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同じ種類の脅威の兆候のインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「2」になります。
検出数	管理下の製品が検出したポリシー/ルール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

最も脅威の兆候の多いエンドポイントの概要

脅威の兆候が最も頻繁に検出されるエンドポイントの概要が表示されます。例: 感染先の名前、発生元およびルール/違反に関する概要情報、ネットワーク上の脅威の兆候の総数

表 B-21. 最も脅威の兆候の多いエンドポイントの概要データビュー

データ	説明
エンドポイント IP	脅威の兆候の影響を受けるコンピュータの IP アドレスが表示されます。
一意のポリシー/ルール数	発生元のコンピュータが違反しているポリシー/ルールの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー/ルール数] は「1」になります。
一意の送信元数	脅威の兆候の発生元の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータからきている同じ種類の脅威の兆候のインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「3」になります。
検出数	管理下の製品が検出したポリシー/ルール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

最も脅威の兆候の多い受信者の概要

脅威の兆候が最も頻繁に検出される受信者の概要が表示されます。例: 受信者の名前、送信者およびルール/違反に関する概要情報、ネットワーク上の脅威の兆候の総数

表 B-22. 最も脅威の兆候の多い受信者の概要データビュー

データ	説明
受信者	脅威の兆候の影響を受ける受信者のメールアドレスが表示されます。
一意のポリシー/ルール数	発生元のコンピュータが違反しているポリシー/ルールの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー/ルール数] は「1」になります。
一意の送信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを送信したメールメッセージ送信者の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータから送信された、同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されました。 この場合、[一意の送信者数] は「3」になります。
検出数	管理下の製品が検出したポリシー/ルール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

脅威の兆候の送信者の概要

特定の送信者からの脅威の兆候検出の概要が表示されます。例: 送信者の名前、送信者およびルール/違反に関する概要情報、ネットワーク上の脅威の兆候の総数

表 B-23. 脅威の兆候の送信者の概要データビュー

データ	説明
送信者	ポリシー/ルール違反の発生元のメールアドレスが表示されます。

データ	説明
一意のポリシー/ルール数	発生元のコンピュータが違反しているポリシー/ルールの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー/ルール数] は「1」になります。
一意の受信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを受信したメールメッセージ受信者の絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されました。 この場合、[一意の受信者数] は「2」になります。
検出数	管理下の製品が検出したポリシー/ルール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

脅威の兆候のプロトコル検出の概要

特定のプロトコル経由の脅威の兆候検出の概要が表示されます。例: プロトコルの名前、発生元および感染先に関する概要情報、ネットワーク上の脅威の兆候の総数

表 B-24. 脅威の兆候のプロトコル検出の概要データビュー

データ	説明
プロトコル	脅威の兆候が発生しているプロトコルの名前が表示されます。例: HTTP、FTP、SMTP
一意のポリシー/ルール数	発生元のコンピュータが違反しているポリシー/ルールの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されたとします。 この場合、[一意のポリシー/ルール数] は「1」になります。

データ	説明
一意のエンドポイント数	脅威の兆候の影響を受けるコンピュータの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同じ種類の脅威の兆候のインスタンスが 10 件検出されたとします。 この場合、[一意のエンドポイント数] は「2」になります。
一意の送信元数	脅威の兆候の発生元の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータからきている同じ種類の脅威の兆候のインスタンスが 10 件検出されたとします。 この場合、[一意の送信元数] は「3」になります。
一意の受信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを受信したメールメッセージ受信者の絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されたとします。 この場合、[一意の受信者数] は「2」になります。
一意の送信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを送信したメールメッセージ送信者の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータから送信された、同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されたとします。 この場合、[一意の送信者数] は「3」になります。
検出数	管理下の製品が検出したポリシー/ルール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されたとします。 この場合、[検出数] は「10」になります。

脅威の兆候検出の概要 (時間別推移)

一定の期間 (毎日、毎週、毎月) の脅威の兆候検出の概要が表示されます。例: 概要データが収集された日時、発生元および感染先に関する概要情報、ネットワーク上の脅威の兆候の総数

表 B-25. 脅威の兆候検出の概要 (時間別推移) データビュー

データ	説明
日時	データの概要が生成された時間が表示されます。
一意のポリシー/ルール数	発生元のコンピュータが違反しているポリシー/ルールの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されたとします。 この場合、[一意のポリシー/ルール数] は「1」になります。
一意のエンドポイント数	脅威の兆候の影響を受けるコンピュータの絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同じ種類の脅威の兆候のインスタンスが 10 件検出されたとします。 この場合、[一意のエンドポイント数] は「2」になります。
一意の送信元数	脅威の兆候の発生元の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータからきている同じ種類の脅威の兆候のインスタンスが 10 件検出されたとします。 この場合、[一意の送信元数] は「3」になります。
一意の受信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを受信したメールメッセージ受信者の絶対数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されたとします。 この場合、[一意の受信者数] は「2」になります。
一意の送信者数	管理下の製品の脅威の兆候ポリシーに違反するコンテンツを送信したメールメッセージ送信者の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータから送信された、同一ポリシーの脅威の兆候の違反インスタンスが 10 件検出されたとします。 この場合、[一意の送信者数] は「3」になります。

データ	説明
検出数	管理下の製品が検出したポリシー/ルール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されたとします。 この場合、[検出数] は「10」になります。

グレーウェア検出情報

ネットワーク上で検出された、攻撃の痕跡と疑われる項目に関する詳細情報が表示されます。

表 B-26. グレーウェア検出情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
エンドポイント	エンドポイントの名前を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
管理サーバのエンティティ名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。
検出の種類	グレーウェア検出の種類を示します。
ルール	検出を開始したポリシーまたはルールを示します。
詳細	検出に関する追加情報が含まれる JSON オブジェクトを示します。
Tactics	検知された MITRE ATT&CK™ Tactics を示します。 詳細については、https://attack.mitre.org/tactics/enterprise/を参照してください。

データ	説明
Techniques	検知された MITRE ATT&CK™ Techniques を示します。 詳細については、https://attack.mitre.org/techniques/enterprise/を参照してください。

脅威情報 (全体)

ネットワークの脅威の全体像に関する概要と統計データが表示されます。

ネットワーク保護境界情報

ネットワーク全体に影響を与えているセキュリティの脅威のさまざまな概要情報が表示されます。例: 管理下の製品のネットワーク保護の種類 (ゲートウェイ、メール)、セキュリティの脅威の種類、影響を受けるエンドポイント数

表 B-27. ネットワーク保護境界情報データビュー

データ	説明
製品カテゴリ	管理下の製品が属するカテゴリが表示されます。 例: デスクトップ製品、メールサーバ製品、ネットワーク製品
製品	管理下の製品の名前が表示されます。 例: Apex One、InterScan for Microsoft Exchange
セキュリティの脅威のカテゴリ	管理下の製品が検出したセキュリティの脅威のさまざまなカテゴリが表示されます。 例: ウイルス対策、スパイウェア対策、フィッシング対策
一意のエンドポイント数	セキュリティの脅威の影響を受けるコンピュータの絶対数が表示されます。 例: Apex One により、2 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「2」になります。

データ	説明
一意の送信元数	セキュリティの脅威/違反の発生元の絶対数が表示されます。 例: Apex One により、2 台のコンピュータで 3 つの感染元からきている同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「3」になります。
検出数	管理下の製品が検出したセキュリティの脅威/違反の総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

ネットワークセキュリティの脅威分析情報

デスクトップに影響する全体的なセキュリティの脅威の情報が表示されます。例: セキュリティの脅威の名前、セキュリティの脅威検出の総数、影響を受けるエンドポイント数

表 B-28. ネットワークセキュリティの脅威分析情報データビュー

データ	説明
セキュリティの脅威のカテゴリ	管理下の製品が検出したセキュリティの脅威のさまざまなカテゴリが表示されます。 例: ウイルス対策、スパイウェア対策、フィッシング対策
セキュリティの脅威	管理下の製品が検出したセキュリティの脅威の名前が表示されます。
エントリの種類	管理下の製品によって検出されたセキュリティの脅威の検出ポイントが表示されます。 例: ファイル、HTTP、Windows Live メッセンジャー (MSN)

データ	説明
一意のエンドポイント数	セキュリティの脅威の影響を受けるコンピュータの絶対数が表示されます。 例: Apex One により、2 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「2」になります。
一意の送信元数	セキュリティの脅威/違反の発生元の絶対数が表示されます。 例: Apex One により、2 台のコンピュータで 3 つの感染元からきている同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「3」になります。
検出数	管理下の製品が検出したセキュリティの脅威/違反の総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

セキュリティの脅威検出エンドポイント分析情報

感染したエンドポイントに焦点を当てた情報が表示されます。例: エンドポイントの名前、ネットワークにセキュリティの脅威が侵入したさまざまな方法、感染したエンドポイント数

表 B-29. セキュリティの脅威エンドポイント分析情報データビュー

データ	説明
エンドポイント	セキュリティの脅威または違反の影響を受けたコンピュータの名前が表示されます。
セキュリティの脅威のカテゴリ	管理下の製品が検出したセキュリティの脅威のさまざまなカテゴリが表示されます。 例: ウイルス対策、スパイウェア対策、フィッシング対策
セキュリティの脅威名	管理下の製品が検出したセキュリティの脅威の名前が表示されます。

データ	説明
検出数	管理下の製品が検出したセキュリティの脅威/違反の総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
検出	セキュリティの脅威/違反によって影響を受けたコンピュータで最後にセキュリティの脅威/違反が検出された日時が表示されます。

セキュリティの脅威侵入分析情報

検出ポイントに焦点を当てたセキュリティの脅威の情報が表示されます。例: 管理下の製品のネットワーク保護の種類 (ゲートウェイ、メール、デスクトップ)、セキュリティの脅威の名前、最後にセキュリティの脅威が検出された時間

表 B-30. セキュリティの脅威侵入分析情報データビュー

データ	説明
エントリの種類	管理下の製品が検出したセキュリティの脅威の検出ポイントが表示されます。 例: ファイル、FTP、ファイル転送
製品	セキュリティの脅威を検出した管理下の製品の名前が表示されます。 例: Apex One、InterScan for Microsoft Exchange
セキュリティの脅威のカテゴリ	管理下の製品が検出したセキュリティの脅威のカテゴリが具体的に表示されます。 例: ウイルス対策、スパイウェア対策、コンテンツフィルタリング

データ	説明
一意のエンドポイント数	セキュリティの脅威の影響を受けるコンピュータの絶対数が表示されます。 例: Apex One により、2 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「2」になります。
一意の送信元数	セキュリティの脅威/違反の発生元の絶対数が表示されます。 例: Apex One により、2 台のコンピュータで 3 つの感染元からきている同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「3」になります。
検出数	管理下の製品が検出したセキュリティの脅威/違反の総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

セキュリティの脅威送信元分析情報

セキュリティの脅威の発生元に焦点を当てた情報が表示されます。例: セキュリティの脅威の発生元の名前、ネットワークにセキュリティの脅威が侵入したさまざまな方法、感染したエンドポイント数

表 B-31. セキュリティの脅威送信元分析情報データビュー

データ	説明
感染元ホスト	セキュリティの脅威/違反の原因となったコンピュータの名前が表示されます。
セキュリティの脅威のカテゴリ	管理下の製品が検出したセキュリティの脅威のさまざまなカテゴリが表示されます。 例: ウイルス対策、スパイウェア対策、フィッシング対策
セキュリティの脅威	管理下の製品が検出したセキュリティの脅威の名前が表示されます。

データ	説明
検出数	管理下の製品が検出したセキュリティの脅威/違反の総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
検出	セキュリティの脅威/違反によって影響を受けたコンピュータで最後にセキュリティの脅威/違反が検出された日時が表示されます。

ポリシー/ルール違反情報

管理下の製品によってネットワーク上で検出されたポリシー/ルール違反に関する概要と詳細データが表示されます。

デバイスアクセス管理情報

デバイスアクセス管理に関連するネットワーク上のイベントの具体的な情報が表示されます。

表 B-32. デバイスアクセス管理情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した時刻が表示されます。
生成	管理下の製品がデータを生成した時間が表示されます。
製品のエンティティ名/エンドポイント	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品のエンティティ 表示名。Apex Central では、管理下の製品のエンティティ 表示名を使用して、管理下の製品を識別します。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレスまたはホスト名。

データ	説明
製品	管理下の製品の名前が表示されます。 例: Apex One
対象プロセス	違反の対象となったプロセスが表示されます
ファイル名	ファイルの名前が表示されます。
デバイスの種類	アクセスされたデバイスの種類が表示されます。
権限	権限の種類が表示されます。
ユーザ	管理下の製品によってイベントが検出されたときに、エンドポイントにログオンしていたユーザの名前が表示されます。

アプリケーションアクティビティの 詳細

ネットワークセキュリティポリシーに違反するアプリケーションアクティビティに関する具体的な情報が表示されます。

表 B-33. アプリケーションアクティビティの 詳細データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
VLAN ID	脅威の兆候の発生源である送信元の VLAN ID (VID)を示します。
検出元	脅威の兆候を検出したフィルタ、検索エンジン、管理下の製品を示します。
トラフィック/接続	脅威の兆候が発生したネットワークトラフィックの方向、またはネットワーク上の場所を示します。

データ	説明
プロトコルグループ	管理下の製品が脅威の兆候を検出したさまざまなプロトコルグループを示します。 例: FTP、HTTP、P2P
プロトコル	管理下の製品が脅威の兆候を検出したプロトコルを示します。 例: ARP、Bearshare、BitTorrent
説明	トレンドマイクロによるイベントの詳細な説明が表示されます。
エンドポイント	ポリシー/ルールを遵守しているコンピュータのホスト名を示します。
送信元 IP	脅威の兆候の発生源である送信元の IP アドレスを示します。
感染元 MAC	脅威の兆候の発生源である送信元の MAC アドレスを示します。
感染元ポート	脅威の兆候の発生源である送信元のポート番号を示します。
送信元 IP グループ	違反の発生元の IP アドレスのグループを示します。
送信元ネットワークゾーン	違反の発生元のネットワークゾーンを示します。
エンドポイント IP	脅威の兆候が影響を与えるエンドポイントの IP アドレスを示します。
エンドポイントポート	脅威の兆候が影響を与えるエンドポイントのポート番号を示します。
エンドポイント MAC	脅威の兆候が影響を与えるエンドポイントの MAC アドレスを示します。
エンドポイントグループ	脅威の兆候が影響を与えるエンドポイントの IP アドレスグループを示します。
エンドポイントネットワークゾーン	脅威の兆候が影響を与えるエンドポイントのネットワークゾーンを示します。
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

データ	説明
脅威の種類	管理下の製品が検出したセキュリティの脅威の具体的な種類を示します。
検出の重大度	イベントの重大度レベルを示します。
IP アドレス (侵入元/侵入先)	対象エンドポイント (侵入元または侵入先) の IP アドレスを示します。 ネットワーク内で交換される場合は、侵入元の IP アドレスが表示されます。外部トラフィックの場合は、侵入先の IP アドレスが表示されます。
IP アドレス (ピア)	侵入先 IP の逆の IP アドレスを示します。 たとえば、侵入先 IP と侵入元 IP アドレスが同じ場合、ピア IP は、侵入先の IP アドレスになります。
一致する分類イベント	同じ集約ルールに一致するログの件数を示します。
一致する分類イベントの集計	同じルールに一致するログの件数を示します。
ネットワークグループ	グループの名前を示します。
ホストへの影響の重大度	ホストへの影響の重大度を示します。
ログ ID	ログ ID を示します。

アプリケーションコントロールの違反詳細情報

セキュリティエージェントのポリシーや条件への違反など、ネットワーク上のアプリケーションコントロール違反に関する具体的な情報が表示されます。

表 B-34. アプリケーションコントロール違反詳細情報データビュー

データ	説明
生成	管理下の製品でデータが生成された日付と時刻を示します。

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
ユーザ名	イベントの時点でログオンしていたユーザの名前を示します。
エンドポイント	エンドポイントの名前を示します。
処理	管理下の製品によって実行された処理を示します。
ファイル	ファイルオブジェクトの名前、またはプロセスを実行したプログラムを示します。
プロセス	ファイルオブジェクトによって実行されたプロセスを示します。
ポリシー	Apex Central または管理下の製品のコンソールによって適用されるポリシーの名前を示します。
条件	アプリケーションの使用に関するルールの名前を示します。
照合方法	許可条件とブロック条件でアプリケーションを特定するために使用される方法を示します。
バージョン	ソフトウェア安全性評価パターンファイルのバージョンを示します。
ハッシュタイプ	使用されるハッシュアルゴリズムの種類を示します。
ハッシュ値	ファイルオブジェクトのハッシュ値を示します。
証明書署名者	証明書の発行者を示します。
サーバ	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。
接続ステータス	エンドポイントと管理下の製品のサーバ間の接続のステータスを示します。
エンドポイントの IP アドレス	エンドポイントの IP アドレスを示します。
コマンド	発行されたコマンドを示します。
プロセス所有者	コマンドを発行したアカウントのユーザ名を示します。

データ	説明
アプリケーション	ファイルオブジェクトが属するアプリケーションの名前を示します。
一致したファイルパス	ファイルオブジェクトのディレクトリの場所を示します。
検出数	検出の総数を示します。
ファイル更新日時	ファイルオブジェクトが最後に変更された日時を示します。

挙動監視の詳細情報

挙動監視に関連するネットワーク上のイベントに関する具体的な情報が表示されます。

表 B-35. 挙動監視の詳細情報データビュー

データ	説明
エンティティからの受信時間	管理下の製品から Apex Central がデータを受信した時刻が表示されます。
エンティティでの生成時間	管理下の製品がデータを生成した時間が表示されます。
ホスト	アクセスしたコンピュータの IP アドレスまたはホスト名が表示されます。
リスクレベル	ネットワークに対するリスクが表示されます (トレンドマイクロによる診断)。
ログの種類	違反をトリガしたログの種類が表示されます。
ポリシー	違反により起動されたポリシーの名前が表示されます。
件名	具体的なファイルとそのディレクトリが表示されます。
イベントの種類	違反の種類が表示されます。
対象	イベントの種類で特定されたパスまたはディレクトリが表示されます。

データ	説明
処理	管理下の製品によって実行された処理が表示されます。
操作	読み取り/書き込み操作または実行操作が表示されます。
エンドポイント	攻撃されたコンピュータのホスト名が表示されます。
エンドポイント IP	攻撃されたコンピュータの IP アドレスが表示されます。
エンドポイントの感染経路	脅威の発生元のチャネルが表示されます。
クラウドサービスのベンダ	クラウドサービスのベンダの名前が表示されます。

エンドポイントセキュリティ遵守詳細情報

ネットワーク上のエンドポイントセキュリティ遵守に関する具体的な情報が表示されます。

表 B-36. エンドポイントセキュリティ遵守詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
エンドポイント	ポリシー/ルールを遵守しているコンピュータのホスト名を示します。
エンドポイント IP	ポリシー/ルールを遵守しているコンピュータの IP アドレスを示します。
エンドポイント MAC	ポリシー/ルールを遵守しているコンピュータの MAC アドレスを示します。

データ	説明
ポリシー/ルール	遵守しているポリシー/ルールの名前を示します。
サービス	ポリシー/ルールを遵守しているサービス/プログラムの名前を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
説明	トレンドマイクロによるイベントの詳細な説明を示します。
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

エンドポイントセキュリティ違反詳細情報

ネットワーク上のエンドポイントセキュリティ違反に関する具体的な情報が表示されます。

表 B-37. エンドポイントセキュリティ違反詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
エンドポイント	エンドポイントの名前を示します。
エンドポイント IP	エンドポイントの IP アドレスを示します。
エンドポイント MAC	エンドポイントの MAC アドレスを示します。

データ	説明
ポリシー/ルール	検出を開始したポリシー/ルールの名前を示します。
サービス	検出を開始したサービス/プログラムの名前を示します。
ユーザ	イベントの時点でログオンしていたユーザの名前を示します。
強制処理	ポリシー/ルールによって強制的に適用される処理を示します。
修復処理	違反に起因するペイロードを阻止するための処理を示します。
説明	トレンドマイクロによるイベントの詳細な説明を示します。
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じ種類のセキュリティ違反が 10 件検出されました。 この場合、[検出数] は「10」になります。

ファイアウォール違反詳細情報

ネットワーク上のファイアウォール違反に関する具体的な情報が表示されます。たとえば、違反を検知した管理下の製品、転送元および転送先、ファイアウォール違反の総数などです。

表 B-38. ファイアウォール違反詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • エンドポイントの名前または IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange

データ	説明
イベントの種類	検出を開始したイベントの種類を示します。 例: 侵入、ポリシー違反
リスクレベル	ネットワークに対するリスク (トレンドマイクロによる診断) を示します。 例: 高、中、低
トラフィック/接続	転送の方向を示します。
プロトコル	侵入に使用されたプロトコルを示します。 例: HTTP、SMTP、FTP
送信元ポート	検出された脅威の送信元 IP アドレスポート番号を示します。
送信元 IP	検出された脅威の送信元 IP アドレスを示します。
送信先ポート	検出された脅威からアクセスされたポート番号を示します。
送信先 IP	検出された脅威からアクセスされたエンドポイントの IP アドレスを示します。
対象プロセス	違反の対象となったプロセスを示します。
説明	トレンドマイクロによるイベントの詳細な説明を示します。
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルが放置されました
検出数	検出の総数を示します。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

IPS の詳細情報

既知の攻撃やゼロデイ攻撃に対する迅速な保護、Web アプリケーションの脆弱性に対する防御、ネットワークにアクセスする不正ソフトウェアの識別などを実施する際に役立つ具体的な情報が表示されます。

データ	説明
生成	管理下の製品でデータが生成された日付と時刻を示します。
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
サーバ	管理下の製品のサーバの表示名を示します。
製品のエンティティ名/エンドポイント	エンドポイントの名前または IP アドレスを示します。
影響を受けた IP アドレス	脅威の影響を受けたエンドポイントの IP アドレスを示します。
理由/ルール	イベントによってトリガされた IPS ルールを示します。
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。
処理	管理下の製品によって実行された処理を示します。
アプリケーションの種類	イベントによってトリガされた IPS ルールに関連付けられているアプリケーションの種類を示します。
攻撃元	検出された脅威の発生元を示します。
送信元 IP アドレス	検出された脅威の送信元 IP アドレスを示します。
送信元 MAC アドレス	検出された脅威の送信元 MAC アドレスを示します。
送信元ポート	検出された脅威の送信元ポートを示します。
送信先 IP アドレス	脅威がアクセスした IP アドレスを示します。
送信先 MAC アドレス	脅威がアクセスした MAC アドレスを示します。
送信先ポート	脅威がアクセスしたポート番号を示します。
MAC アドレス (侵入元/侵入先)	ネットワークトラフィックの方向に応じて、次のようになります。 • 受信ネットワークトラフィックの送信元 MAC アドレス • 送信ネットワークトラフィックの送信先 MAC アドレス

データ	説明
プロトコル	脅威がネットワークに侵入するために使用したプロトコルを示します。
方向	転送の方向を示します。
優先度	仮想パッチのスタンドアロンバージョンで使用される順位システムに基づく検出の重要性を示します。
重大度	イベントの重大度レベルを示します。

変更監視情報

インストール済みソフトウェア、実行中のサービス、プロセス、ファイル、ディレクトリ、待機ポート、レジストリキー、レジストリ値など、エンドポイントに加えられる特定の変更を監視するために使用します。

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
サーバ	管理下の製品のサーバのホスト名を示します。
変更	整合性ルールによって検出された変更を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
プロセス	イベントが発生したプロセスを示します。
種類	レジストリキーの種類を示します。
キー	レジストリキーを示します。
順位	変更の順位を示します。
重大度	イベントの重大度レベルを示します。

ネットワークコンテンツ検査情報

ネットワーク上のネットワークコンテンツ違反に関する具体的な情報が表示されます。

表 B-39. ネットワークコンテンツ検査情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • エンドポイントの名前または IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
トラフィックの方向	転送の方向を示します。
ローカル IP アドレス	セキュリティエージェントエンドポイントの IP アドレスを示します。
ローカル IP アドレスポート番号	セキュリティエージェントエンドポイントの IP アドレスポート番号を示します。
リモート IP アドレス	外部エンドポイントの IP アドレスを示します。
リモート IP アドレスポート番号	外部エンドポイントの IP アドレスポート番号を示します。
リモートのドメイン	検出に関連付けられたドメイン名を示します。
プロセス	アクセスが施行されたプロセス (path\application_name) を示します。
処理	管理下の製品によって実行された処理を示します。

データ	説明
パターンファイルの種類	検出に関連付けられたパターンファイルの種類を示します。
脅威名	セキュリティの脅威の名前を示します。

スパムメール違反情報

管理下の製品によってネットワーク上で検出されたスパムメールに関する概要と詳細データが表示されます。

スパムメール詳細情報

コンテンツ違反を検出した管理下の製品、違反している特定のポリシーの名前、ネットワーク上のスパムメール違反の総数など、ネットワーク上のスパムメール違反に関する具体的な情報が表示されます

表 B-40. スパムメール詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
受信者	検出を開始したメールメッセージの受信者を示します。
送信者	検出を開始したメールメッセージの送信者を示します。
件名	検出を開始したメールメッセージの件名を示します。
ポリシー	検出を開始したポリシーを示します。

データ	説明
処理	管理下の製品によって実行された処理を示します。
検出数	検出の総数を示します。 例: 管理下の製品で、1 つのエンドポイントで同一のスパムメールの違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

スパムメール違反の概要 (全体)

ネットワーク上のスパムメール違反の概要が表示されます。

データ	説明
受信者ドメイン	スパムメールの影響を受ける受信者のドメインを示します。
一意の受信者数	特定のドメインからスパムメールを受信した受信者の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータで同一ドメインからスパムメールの違反インスタンスが 10 件検出されたとします。 この場合、[一意の受信者数] は「3」になります。
検出数	管理下の製品が検出したスパムメール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一のスパムメールの違反インスタンスが 10 件検出されたとします。 この場合、[検出数] は「10」になります。

スパムメール接続情報

ネットワーク上のスパムメールの発生元に関する具体的な情報が表示されます。たとえば、スパムを検知した管理下の製品、管理下の製品により実行された処理の内容、検知されたスパムの総数などです。

表 B-41. スパムメール接続情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
送信元 IP	検出された脅威の送信元 IP アドレスを示します。
フィルタの種類	イベントを検出したフィルタの種類を示します。
処理	管理下の製品によって実行された処理を示します。 例: 接続の破棄、接続の放置
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じスパムの違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

スパムメール検出の概要 (時間別推移)

一定の期間 (毎日、毎週、毎月) のスパムメール検出の概要が表示されます。例: 概要データが収集された日時、スパムメールの影響を受けるエンドポイント数、ネットワーク上のスパムメール違反の総数

表 B-42. スパムメール検出の概要 (時間別推移) データビュー

データ	説明
集計日時	データの概要が生成された時間が表示されます。

データ	説明
一意の受信者ドメイン数	スパムメールの影響を受ける受信者ドメインの絶対数が表示されます。 例: 管理下の製品で、1 つの受信者ドメインの 2 つのドメインから同一のスパムメールの違反インスタンスが 10 件検出されました。 この場合、[一意の受信者ドメイン数] は「1」になります。
一意の受信者数	特定のドメインからスパムメールを受信した受信者の絶対数が表示されます。 例: 管理下の製品で、3 台のコンピュータで同一ドメインからスパムメールの違反インスタンスが 10 件検出されました。 この場合、[一意の受信者数] は「3」になります。
検出数	管理下の製品が検出したスパムメール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一のスパムメールの違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

スパムメール受信者の概要

特定のエンドポイントでのスパムメール違反の概要が表示されます。例: エンドポイントの名前、そのエンドポイント上のウイルスのインスタンスの総数

表 B-43. スパムメール受信者の概要データビュー

データ	説明
受信者	スパムメールの受信者の名前が表示されます。
検出数	管理下の製品が検出したスパムメール違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一のスパムメールの違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

スパイウェア/グレーウェア情報

管理下の製品によってネットワーク上で検出されたスパイウェア/グレーウェアに関する概要と詳細データが表示されます。

スパイウェア/グレーウェア詳細情報

スパイウェア/グレーウェアを検出した管理下の製品、スパイウェア/グレーウェアの名前、感染エンドポイントの名前など、ネットワーク上で検出されたスパイウェア/グレーウェアに関する具体的な情報が表示されます。

表 B-44. スパイウェア/グレーウェア詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • エンドポイントの名前または IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの IP アドレスを示します。 • エンドポイントの IP アドレスを示します。
製品/エンドポイント MAC	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの MAC アドレスを示します。 • セキュリティエージェントのエンドポイントの MAC アドレスを示します。
管理サーバのエンティティ名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。

データ	説明
スパイウェア/グレーウェア	セキュリティの脅威の名前を示します。
エンドポイント	エンドポイントの名前または IP アドレスを示します。
感染元ホスト	セキュリティの脅威の発生源であるエンドポイントの IP アドレスまたは名前を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
エントリの種類	セキュリティの脅威の侵入ポイントを示します。
詳細情報	特定の検出に関する追加情報を表示するリンクです。
エンドポイントの感染経路	脅威の発生元のチャネルを示します。
Apex One ドメイン階層	セキュリティエージェントが属しているエージェントツリードメインまたはサブドメインを示します。
ドメイン	エンドポイントが配下に置かれている管理下の製品のサーバのドメインを示します。
OS	エンドポイントの OS を示します。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

エンドポイントのスパイウェア/グレーウェア

スパイウェア/グレーウェアが検出されたエンドポイントに関する具体的な情報が表示されます。例: スパイウェア/グレーウェアを検出した管理下の製品、スパイウェア/グレーウェアを検出した検索の種類、検出されたスパイウェア/グレーウェアへのエンドポイント上のファイルパス

表 B-45. エンドポイントのスパイウェア/グレーウェアデータビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • セキュリティエージェントのエンドポイントの名前または IP アドレスを示します。
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの IP アドレスを示します。 • エンドポイントの IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
管理サーバのエンティティ 名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。
スパイウェア/グレーウェア	セキュリティの脅威の名前を示します。
エンドポイント	脅威がアクセスしたエンドポイントの IP アドレスまたは名前を示します。
感染元ホスト	セキュリティの脅威の発生源であるエンドポイントの IP アドレスまたは名前を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。

データ	説明
検索の種類	イベントがレポートされた検索の種類 (リアルタイム検索、予約検索、手動検索など) を示します。
リソース	セキュリティの脅威の影響を受けたリソースを示します。 例: application.exe, H Key Local Machine\SOFTWARE\ACME
リソースの種類	セキュリティの脅威の影響を受けたリソースの種類を示します。 例: レジストリ、メモリリソース
セキュリティの脅威の種類を示します。	セキュリティの脅威の種類を示します。 例: アドウェア、Cookie、ピアツーピアアプリケーション
リスクレベル	セキュリティの脅威のリスクレベルを示します。 例: 高、中、低
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

エンドポイントのスパイウェア/グレーウェアの概要

特定のエンドポイントからのスパイウェア/グレーウェア検出の概要が表示されます。例: エンドポイントの名前、エンドポイント上の特定のスパイウェア/グレーウェアのインスタンス数、ネットワーク上に存在するスパイウェア/グレーウェアのインスタンスの総数

表 B-46. エンドポイントのスパイウェア/グレーウェアの概要データビュー

データ	説明
エンドポイント	スパイウェア/グレーウェアに感染したコンピュータのホスト名または IP アドレスが表示されます。
一意の送信元数	スパイウェア/グレーウェアの感染元の絶対数が表示されます。 例: Apex One により、2 つの感染元からきている同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「2」になります。
一意の検出数	管理下の製品が検出したスパイウェア/グレーウェアの絶対数が表示されます。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意の検出数] は「1」になります。
検出数	管理下の製品が検出したスパイウェア/グレーウェアの総数が表示されます。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

メールのスパイウェア/グレーウェア

スパイウェア/グレーウェアが検出されたメールに関する具体的な情報が表示されます。例: スパイウェア/グレーウェアを検出した管理下の製品、メールメッセージの件名のコンテンツ、スパイウェア/グレーウェアを含んでいるメールメッセージの送信者

表 B-47. メールのスパイウェア/グレーウェアデータビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。

データ	説明
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
スパイウェア/グレーウェア	セキュリティの脅威の名前を示します。
受信者	検出を開始したメールメッセージの受信者を示します。
送信者	検出を開始したメールメッセージの送信者を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
件名	検出を開始したメールメッセージの件名を示します。
ファイル	脅威がアクセスしたファイルオブジェクトの名前を示します。
圧縮ファイル内のファイル	圧縮ファイルに含まれる、影響を受けるファイルオブジェクトの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

ネットワークのスパイウェア/グレーウェア

ネットワークトラフィックで検出されたスパイウェア/グレーウェアのインスタンスに関する具体的な情報が表示されます。例: スパイウェア/グレーウェアを検出した管理下の製品、ネットワークへの侵入にスパイウェア/グレーウェアが使用したプロトコル、スパイウェア/グレーウェアの感染元および感染先に関するおよび具体的な情報

表 B-48. ネットワークのスパイウェア/グレーウェアデータビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • セキュリティエージェントのエンドポイントの名前または IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
スパイウェア/グレーウェア	セキュリティの脅威の名前を示します。
トラフィック/接続	転送の方向を示します。
プロトコル	脅威がネットワークに侵入するために使用したプロトコルを示します。 例: HTTP、SMTP、FTP
エンドポイント IP	脅威がアクセスした IP アドレスを示します。
エンドポイント	脅威がアクセスしたエンドポイントの IP アドレスまたは名前を示します。
エンドポイントポート	脅威がアクセスした IP ポート番号を示します。

データ	説明
エンドポイント MAC	脅威がアクセスした MAC アドレスを示します。
送信元 IP	検出された脅威の送信元 IP アドレスを示します。
感染元ホスト	セキュリティの脅威の発生源であるエンドポイントの IP アドレスまたは名前を示します。
感染元ポート	検出された脅威の送信元 IP アドレスポート番号を示します。
感染元 MAC	検出された脅威の送信元 MAC アドレスを示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
ファイル	脅威がアクセスしたファイルオブジェクトの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

スパイウェア/グレーウェアの概要 (全体)

スパイウェア/グレーウェア検出の概要が具体的に表示されます (管理下の全製品)。例: スパイウェア/グレーウェアの名前、スパイウェア/グレーウェアに感染したエンドポイント数、ネットワーク上に存在するスパイウェア/グレーウェアのインスタンスの総数

表 B-49. スパイウェア/グレーウェアの概要 (全体) データビュー

データ	説明
スパイウェア/グレーウェア	管理下の製品が検出したスパイウェア/グレーウェアの名前が表示されます。
一意のエンドポイント数	スパイウェア/グレーウェアに感染したコンピュータの絶対数が表示されます。 Apex One により、3 台の異なるコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「3」になります。
一意の送信元数	スパイウェア/グレーウェアの感染元の絶対数が表示されます。 例: Apex One により、2 つの感染元からきている同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「2」になります。
検出数	管理下の製品が検出したスパイウェア/グレーウェアの総数が表示されます。

スパイウェア/グレーウェアの処理/結果の概要

スパイウェア/グレーウェアに対して管理下の製品が実行したアクションの概要が表示されます。例: スパイウェア/グレーウェアに対して実行した具体的なアクション、アクションの実行結果、ネットワーク上に存在するスパイウェア/グレーウェアのインスタンスの総数

表 B-50. スパイウェア/グレーウェアの処理/結果の概要データビュー

データ	説明
結果	スパイウェア/グレーウェアに対して管理下の製品が実行したアクションの結果が表示されます。 例: 成功、処理が必要
処理	スパイウェア/グレーウェアに対して管理下の製品が実行したアクションの種類が表示されます。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました

データ	説明
一意のエンドポイント数	スパイウェア/グレーウェアに感染したコンピュータの絶対数が表示されます。 例: Apex One により、3 台の異なるコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「3」になります。
一意の送信元数	スパイウェア/グレーウェアの感染元の絶対数が表示されます。 例: Apex One により、2 つの感染元からきている同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「2」になります。
検出数	管理下の製品が検出したスパイウェア/グレーウェアの総数が表示されます。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

スパイウェア/グレーウェア検出の概要 (時間別推移)

一定の期間 (毎日、毎週、毎月) のスパイウェア/グレーウェア検出の概要が表示されます。例: 概要データが収集された日時、スパイウェア/グレーウェアに感染したエンドポイント数、ネットワーク上に存在するスパイウェア/グレーウェアのインスタンスの総数

表 B-51. スパイウェア/グレーウェア検出の概要 (時間別推移) データビュー

データ	説明
日時	データの概要が生成された時間が表示されます。
一意の検出数	管理下の製品が検出したスパイウェア/グレーウェアの絶対数が表示されます。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意の検出数] は「1」になります。

データ	説明
一意のエンドポイント数	スパイウェア/グレーウェアに感染したコンピュータの絶対数が表示されます。 例: Apex One により、3 台の異なるコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「3」になります。
一意の送信元数	スパイウェア/グレーウェアの感染元の絶対数が表示されます。 例: Apex One により、2 つの感染元からきている同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「2」になります。
検出数	管理下の製品が検出したスパイウェア/グレーウェアの総数が表示されます。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

スパイウェア/グレーウェア送信元の概要

大規模感染の発生源からのスパイウェア/グレーウェア検出の概要が表示されます。例: 感染元ソースの名前、感染元ソースからの特定のスパイウェア/グレーウェアインスタンスの 数、ネットワーク上に存在するスパイウェア/グレーウェアインスタンスの 総数

表 B-52. スパイウェア/グレーウェア送信元の概要データビュー

データ	説明
感染元ホスト	スパイウェア/グレーウェアの感染元ソースの名前が表示されます。
一意のエンドポイント数	スパイウェア/グレーウェアに感染したコンピュータの絶対数が表示されます。 例: Apex One により、3 台の異なるコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「3」になります。

データ	説明
一意の検出数	管理下の製品が検出したスパイウェア/グレーウェアの絶対数が表示されます。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[一意の検出数] は「1」になります。
検出数	管理下の製品が検出したスパイウェア/グレーウェアの総数が表示されます。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

Web からのスパイウェア/グレーウェア

HTTP または FTP トラフィックで検出されたスパイウェア/グレーウェアのインスタンスに関する具体的な情報が表示されます。例: スパイウェア/グレーウェアを検出した管理下の製品、スパイウェア/グレーウェアが発生したトラフィックの方向、スパイウェア/グレーウェアをダウンロードした Web ブラウザまたは FTP クライアント

表 B-53. Web からのスパイウェア/グレーウェアデータビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • セキュリティエージェントのエンドポイントの名前または IP アドレスを示します。

データ	説明
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
スパイウェア/グレーウェア	セキュリティの脅威の名前を示します。
IP	エンドポイントの IP アドレスを示します。
感染元 URL	セキュリティの脅威の発生源である Web/FTP サイトの URL を示します。
トラフィック/接続	転送の方向を示します。
ブラウザ/FTP クライアント	脅威がアクセスした Web ブラウザまたは FTP クライアントを示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じスパイウェア/グレーウェアのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

ウイルス/不正プログラム情報

管理下の製品によってネットワーク上で検出されたウイルスに関する概要と詳細データが表示されます。

ウイルス/不正プログラム詳細情報

ウイルス/不正プログラムを検出した管理下の製品、ウイルス/不正プログラムの名前、感染エンドポイントなど、ネットワーク上で検出されたウイルス/不正プログラムに関する具体的な情報が表示されます。

表 B-54. ウイルス/不正プログラム詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • エンドポイントの名前または IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの IP アドレスを示します。 • エンドポイントの IP アドレスを示します。
製品/エンドポイント MAC	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの MAC アドレスを示します。 • セキュリティエージェントのエンドポイントの MAC アドレスを示します。
管理サーバのエンティティ名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。
ドメイン	エンドポイントが配下に置かれている管理下の製品のサーバのドメインを示します。
ウイルス/不正プログラム	セキュリティの脅威の名前を示します。

データ	説明
エンドポイントの感染経路	脅威の発生元のチャネルを示します。
エンドポイント	エンドポイントの名前または IP アドレスを示します。
感染元ホスト	セキュリティの脅威の発生源であるエンドポイントの IP アドレスまたは名前を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。
処理	管理下の製品によって実行された処理を示します。
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
エントリの種類	セキュリティの脅威の侵入ポイントを示します。
詳細情報	特定の検出に関する追加情報を表示するリンクです。
Apex One ドメイン階層	セキュリティエージェントが属しているエージェントツリードメインまたはサブドメインを示します。
部署	エンドポイントが属している Active Directory 部署を示します。
OS	エンドポイントの OS を示します。
パターンファイル/ルール	検出を開始したパターンまたはルールを示します。
パターンファイル/ルールのバージョン	検出を開始したパターンまたはルールのバージョンを示します。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。
ファイル	ファイルオブジェクトの名前、またはプロセスを実行したプログラムを示します。

データ	説明
ファイルパス	ファイルオブジェクトのパスまたはプロセスを実行したプログラムのパスを示します。

エンドポイントのウイルス/不正プログラム情報

ウイルス/不正プログラムが検出されたエンドポイントに関する具体的な情報が表示されます。例: ウイルス/不正プログラムを検出した管理下の製品、ウイルス/不正プログラムを検出した検索の種類、検出されたウイルス/不正プログラムへのエンドポイント上のファイルパス

表 B-55. エンドポイントのウイルス/不正プログラム情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • セキュリティエージェントのエンドポイントの名前または IP アドレスを示します。
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの IP アドレスを示します。 • セキュリティエージェントエンドポイントの IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
管理サーバのエンティティ名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。

データ	説明
ウイルス/不正プログラム	セキュリティの脅威の名前を示します。 例: NIMDA、BLASTER、I_LOVE_YOU.EXE
エンドポイント	エンドポイントの名前を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
検索の種類	イベントがレポートされた検索の種類 (リアルタイム検索、予約検索、手動検索など) を示します。
ファイル	脅威がアクセスしたファイルオブジェクトの名前を示します。
ファイルパス	脅威がアクセスしたファイルオブジェクトのパスを示します。
圧縮ファイル内のファイル	圧縮ファイルに含まれる、影響を受けるファイルオブジェクトの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

メールのウイルス/不正プログラム情報

ウイルス/不正プログラムが検出されたメールに関する具体的な情報が表示されます。例: ウイルス/不正プログラムを検出した管理下の製品、メールの件名のコンテンツ、ウイルス/不正プログラムを含んでいるメールの送信者

表 B-56. メールのウイルス/不正プログラム情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
ウイルス/不正プログラム	セキュリティの脅威の名前を示します。 例: NIMDA、BLASTER、I_LOVE_YOU.EXE
受信者	検出を開始したメールメッセージの受信者を示します。
送信者	検出を開始したメールメッセージの送信者を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
件名	検出を開始したメールメッセージの件名を示します。
ファイル	脅威がアクセスしたファイルオブジェクトの名前を示します。
圧縮ファイル内のファイル	圧縮ファイルに含まれる、影響を受けるファイルオブジェクトの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

データ	説明
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

ネットワークのウイルス/不正プログラム情報

ネットワークトラフィックで検出されたウイルス/不正プログラムのインスタンスに関する具体的な情報が表示されます。例: ウイルス/不正プログラムを検出した管理下の製品、ネットワークへの侵入にウイルス/不正プログラムが使用したプロトコル、ウイルス/不正プログラムの感染元および感染先に関する具体的な情報

表 B-57. ネットワークのウイルス/不正プログラム情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • エンドポイントの名前または IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
ウイルス/不正プログラム	セキュリティの脅威の名前を示します。 例: `NIMDA`、`BLASTER`、`I_LOVE_YOU.EXE`
エンドポイント	脅威がアクセスしたエンドポイントの IP アドレスまたは名前を示します。
感染元ホスト	セキュリティの脅威の発生源であるエンドポイントの IP アドレスまたは名前を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。

データ	説明
トラフィック/接続	転送の方向を示します。
プロトコル	脅威がネットワークに侵入するために使用したプロトコルを示します。 例: HTTP、SMTP、FTP
エンドポイントコンピュータ	脅威がアクセスしたエンドポイントの IP アドレスまたは名前を示します。
エンドポイントポート	脅威がアクセスした IP ポート番号を示します。
エンドポイント MAC	脅威がアクセスした MAC アドレスを示します。
感染元ソース	セキュリティの脅威の発生源であるエンドポイントの IP アドレスまたは名前を示します。
感染元ポート	検出された脅威の送信元 IP アドレスポート番号を示します。
感染元 MAC	検出された脅威の送信元 MAC アドレスを示します。
ファイル	脅威がアクセスしたファイルオブジェクトの名前を示します。
結果	管理下の製品によって実行された処理の結果を示します。 例: 成功、処理が必要
処理	管理下の製品によって実行された処理を示します。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

ウイルス/不正プログラムの概要 (全体)

ウイルス検出の概要が具体的に表示されます (管理下の全製品)。例: ウイルスの名前、ウイルスに感染したエンドポイント数、ネットワーク上に存在するウイルスのインスタンスの総数

表 B-58. ウイルス/不正プログラムの概要 (全体) データビュー

データ	説明
ウイルス/不正プログラム	管理下の製品が検出したウイルスの名前が表示されます。 例: NIMDA、BLASTER、I_LOVE_YOU.EXE
一意のエンドポイント数	ウイルスに感染したコンピュータの絶対数が表示されます。 例: Apex One により、3 台の異なるコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「3」になります。
一意の送信元数	ウイルスの感染元の絶対数が表示されます。 例: Apex One により、2 つの感染元からきている同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「2」になります。
検出数	管理下の製品が検出したウイルスの総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

ウイルス/不正プログラムの処理/結果の概要

ウイルスに対して管理下の製品が実行したアクションの概要が表示されます。例: ウイルスに対して実行した具体的なアクション、アクションの実行結果、ネットワーク上に存在するウイルスのインスタンスの総数

表 B-59. ウイルス/不正プログラムの処理/結果の概要データビュー

データ	説明
結果	ウイルスに対して管理下の製品が実行したアクションの結果が表示されます。 例: 成功、処理が必要
処理	ウイルスに対して管理下の製品が実行したアクションの種類が表示されます。 例: ファイルはウイルス駆除されました、ファイルは隔離されました、ファイルは削除されました
一意のエンドポイント数	ウイルスに感染したコンピュータの絶対数が表示されます。 例: Apex One により、3 台の異なるコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「3」になります。
一意の送信元数	ウイルスの感染元の絶対数が表示されます。 例: Apex One により、2 つの感染元からきている同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「2」になります。
検出数	管理下の製品が検出したウイルスの総数が表示されます。例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

ウイルス/不正プログラム検出の概要 (時間別推移)

一定の期間のウイルス/不正プログラム検出の概要が表示されます。

データ	説明
日時	データの概要が生成された時間が表示されます。

データ	説明
一意の検出数	検出されたウイルス/不正プログラムの絶対数が表示されます。 例: 管理下の製品で、2 つのエンドポイントから同一のウイルスが検出されたとします。 この場合、[一意の検出数] は「1」になります。
一意のエンドポイント	ウイルス/不正プログラムが検出されたエンドポイントの絶対数が表示されます。 例: 管理下の製品で、4 つのエンドポイントからウイルスが検出されたとします。 この場合、[一意のエンドポイント数] は「4」になります。
一意の送信元	ウイルス/不正プログラムの送信元の絶対数が表示されます。 例: 管理下の製品で、2 つの異なる送信元からのウイルスが 10 件検出されたとします。 この場合、[一意の送信元] は「2」になります。
検出数	管理下の製品が検出したウイルス/不正プログラムの総数が表示されます。 例: 管理下の製品で、1 台のコンピュータからウイルス/不正プログラムが 10 件検出されたとします。 この場合、[検出数] は「10」になります。

ウイルス/不正プログラム検出エンドポイントの概要

特定のエンドポイントからのウイルス/不正プログラム検出の概要が表示されます。例: エンドポイントの名前、エンドポイント上の特定のウイルスのインスタンス数、ネットワーク上に存在するウイルスのインスタンスの総数

表 B-60. ウイルス/不正プログラム検出エンドポイントの概要データビュー

データ	説明
エンドポイント	ウイルスに感染したコンピュータの IP アドレスまたはホスト名が表示されます。

データ	説明
一意の送信元数	ウイルスの感染元の絶対数が表示されます。 例: Apex One により、2 つの感染元からきている同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意の送信元数] は「2」になります。
一意の検出数	管理下の製品が検出したウイルスの絶対数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意の検出数] は「1」になります。
検出数	管理下の製品が検出したウイルスの総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

ウイルス/不正プログラム感染元の概要

大規模感染の発生源からのウイルス検出の概要が表示されます。例: 感染元ソースの名前、感染元ソースからの特定のウイルスインスタンスの数、ネットワーク上に存在するウイルスインスタンスの総数

表 B-61. ウイルス/不正プログラム感染元の概要データビュー

データ	説明
感染元ホスト	ウイルス/不正プログラムの感染元ソースの IP アドレスまたはホスト名が表示されます。
一意のエンドポイント数	ウイルスに感染したコンピュータの絶対数が表示されます。 例: Apex One により、3 台の異なるコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「3」になります。

データ	説明
一意の検出数	管理下の製品が検出したウイルスの絶対数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
検出数	管理下の製品が検出したウイルス/不正プログラムの総数が表示されます。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
部署	エンドポイントが属する部署の名前が表示されます。

Web からのウイルス/不正プログラム情報

HTTP または FTP トラフィックで検出されたウイルス/不正プログラムのインスタンスに関する具体的な情報が表示されます。例: ウイルス/不正プログラムを検出した管理下の製品、トラフィックの方向、ウイルス/不正プログラムをダウンロードした Web ブラウザまたは FTP クライアント

表 B-62. Web からのウイルス/不正プログラム情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • エンドポイントの名前または IP アドレスを示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange

データ	説明
ウイルス/不正プログラム	セキュリティの脅威の名前を示します。 例: NIMDA、BLASTER、I_LOVE_YOU.EXE
エンドポイント	脅威がアクセスしたエンドポイントの IP アドレスまたは名前を示します。
感染元 URL	セキュリティの脅威の発生源である Web/FTP サイトの URL を示します。
ユーザ (アカウント)	イベントの時点でログオンしていたユーザの名前を示します。
トラフィック/接続	転送の方向を示します。
ブラウザ/FTP クライアント	脅威がアクセスした Web ブラウザまたは FTP クライアントを示します。
結果	管理下の製品によって実行された処理の結果を示します。
処理	管理下の製品によって実行された処理を示します。
検出数	検出の総数を示します。 例: Apex One により、1 台のコンピュータで同じウイルスのインスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。
クラウドサービスのベンダ	クラウドサービスのベンダの名前を示します。

Web 違反情報

管理下の製品によってネットワーク上で検出されたインターネット違反に関する概要と詳細データが表示されます。

Web レピュテーション詳細情報

Web レピュテーションサービスによって検知されたアプリケーションアクティビティに関するコンプライアンス情報が表示されます。

表 B-63. Web レピュテーション詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
VLAN ID	脅威の兆候の発生源である送信元の VLAN ID (VID)を示します。
検出元	脅威を検出したフィルタ、検索エンジン、または管理下の製品を示します。
トラフィック/接続	転送の方向を示します。
プロトコルグループ	管理下の製品が脅威の兆候を検出したさまざまなプロトコルグループを示します。 例: FTP、 HTTP、 P2P
プロトコル	管理下の製品が脅威の兆候を検出したプロトコルを示します。 例: ARP、 BitTorrent
説明	トレンドマイクロによるイベントの詳細な説明が表示されます。
エンドポイント	ポリシー/ルールを遵守しているコンピュータのホスト名を示します。
送信元 IP	検出された脅威の送信元 IP アドレスを示します。
感染元 MAC	検出された脅威の送信元 MAC アドレスを示します。
感染元ポート	検出された脅威の送信元 IP アドレスポート番号を示します。
送信元 IP グループ	脅威の兆候の発生元の IP アドレスのグループを示します。
送信元ネットワークゾーン	脅威の兆候の発生元のネットワークゾーンを示します。

データ	説明
エンドポイント IP	脅威の兆候が影響を与えるエンドポイントの IP アドレスを示します。
エンドポイントポート	脅威の兆候が影響を与えるエンドポイントのポート番号を示します。
エンドポイント MAC	脅威の兆候が影響を与えるエンドポイントの MAC アドレスを示します。
エンドポイントグループ	脅威の兆候が影響を与えるエンドポイントの IP アドレスグループを示します。
エンドポイントネットワークゾーン	脅威の兆候が影響を与えるエンドポイントのネットワークゾーンを示します。
ポリシー/ルール	検出を開始したポリシーまたはルールを示します。
URL	検出を開始した URL オブジェクトを示します。
検出数	検出の総数を示します。 例: 管理下の製品で、1 台のコンピュータで同一の種類の違反が 10 件検出されました。 この場合、[検出数] は「10」になります。
C&C リストのソース	C&C サーバの特定に使用された C&C リストのソースを示します。
C&C リスクレベル	C&C サーバのリスクレベルを示します。
脅威の種類	セキュリティの脅威の種類を示します。
検出の重大度	イベントの重大度レベルを示します。
IP アドレス (侵入元/侵入先)	対象エンドポイント (侵入元または侵入先) の IP アドレスを示します。 ネットワーク内で交換される場合は、侵入元の IP アドレスが表示されます。外部トラフィックの場合は、侵入先の IP アドレスが表示されます。
IP アドレス (ピア)	侵入先 IP の逆の IP アドレスを示します。 たとえば、侵入先 IP と侵入元 IP アドレスが同じ場合、ピア IP は、侵入先の IP アドレスになります。

データ	説明
一致する分類イベント	同じ集約ルールに一致するログの件数を示します。
一致する分類イベントの集計	同じルールに一致するログの件数を示します。
ネットワークグループ	グループの名前を示します。
ホストへの影響の重大度	ホストへの影響の重大度を示します。
ログ ID	ログ ID を示します。
攻撃段階	攻撃が発生した段階を示します。
注釈	イベントの追加情報を示します。
C&C サーバ	C&C サーバの名前、URL、または IP アドレスを示します。
C&C サーバの種類	C&C サーバの種類を示します。
送信者	検出を開始した転送の送信者を示します。
受信者	検出を開始した転送の受信者を示します。
件名	Web URL を含んでいるメールメッセージの件名を示します。

Web 違反詳細情報

ネットワーク上の Web 違反に関する具体的な情報が表示されます。

表 B-64. Web 違反詳細情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
管理サーバのエンティティ名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。

データ	説明
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
トラフィック/接続	転送の方向を示します。
プロトコル	違反が発生しているプロトコルを示します。 例: HTTP、FTP、SMTP
URL	検出を開始した URL オブジェクトを示します。
ユーザ/IP	ポリシーに違反しているエンドポイントのユーザまたは IP アドレスを示します。
ユーザグループ	ポリシーに違反しているユーザのユーザグループを示します。
エンドポイント	ポリシーに違反しているエンドポイントの IP アドレスを示します。
エンドポイントホスト	ポリシーに違反しているエンドポイントの IP アドレスまたはホスト名を示します。
製品のホスト名	違反を検出した管理下の製品の IP アドレスまたはホスト名を示します。
フィルタ/ブロックの種類	違反 URL へのアクセスを阻止するフィルタ/ブロックの種類を示します。 例: URL ブロック、URL フィルタ、Web ブロック
ブロックのルール	違反 URL へのアクセスを阻止するブロックのルールを示します。 例: URL ブロック
ポリシー	検出を開始したポリシーを示します。
ファイル	ポリシーに違反しているファイルの名前を示します。
プロセス	ポリシーに違反しているプロセスの名前を示します。
Web レピュテーションレーティング	Web サイトの相対的な安全度の割合 (トレンドマイクロによる定義) を示します。

データ	説明
処理	管理下の製品によって実行された処理を示します。 例: 放置、ブロック
検出数	検出の総数を示します。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

Web 違反の概要 (全体)

特定のポリシーに対する Web 違反の概要が表示されます。例: 違反ポリシーの名前、URL へのアクセスを停止するフィルタ/ブロックの種類、ネットワーク上の Web 違反の総数

表 B-65. Web 違反の概要 (全体) データビュー

データ	説明
ポリシー	URL が違反しているポリシーの名前が表示されます。
フィルタ/ブロックの種類	違反 URL へのアクセスを阻止するフィルタ/ブロックの種類が表示されます。 例: URL ブロック、URL フィルタ、Web ブロック
一意のエンドポイント数	指定のポリシーに違反するエンドポイントの絶対数が表示されます。 例: 管理下の製品で、4 台のコンピュータで同一 URL の違反インスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「4」になります。
一意の URL 数	指定のポリシーに違反する URL の絶対数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[一意の URL 数] は「1」になります。

データ	説明
検出数	管理下の製品が検出した Web 違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一 URL の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

Web 違反検出の概要 (時間別推移)

一定の期間 (毎日、毎週、毎月) の Web 違反検出の概要が表示されます。例: 概要データが収集された日時、違反エンドポイントの数、ネットワーク上の Web 違反の総数

表 B-66. Web 違反検出の概要 (時間別推移) データビュー

データ	説明
日時	データの概要が生成された時間が表示されます。
一意のポリシー数	違反ポリシーの数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されたとします。 この場合、[一意のポリシー数] は「1」になります。
一意のエンドポイント数	指定のポリシーに違反するエンドポイントの絶対数が表示されます。 例: 管理下の製品で、4 台のコンピュータで同一 URL の違反インスタンスが 10 件検出されたとします。 この場合、[一意のエンドポイント数] は「4」になります。
一意の URL 数	指定のポリシーに違反する URL の絶対数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されたとします。 この場合、[一意の URL 数] は「1」になります。

データ	説明
検出数	管理下の製品が検出した Web 違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されたとします。 この場合、[検出数] は「10」になります。

Web 違反検出の概要

一定の期間 (毎日、毎週、毎月) の Web 違反検出の概要が表示されます。例: 概要データが収集された日時、違反エンドポイントの数、ネットワーク上の Web 違反の総数

表 B-67. Web 違反検出の概要データビュー

データ	説明
一意のポリシー数	違反ポリシーの数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー数] は「1」になります。
一意のエンドポイント数	指定のポリシーに違反するエンドポイントの絶対数が表示されます。 例: 管理下の製品で、4 台のコンピュータで同一 URL の違反インスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「4」になります。
一意の URL 数	指定のポリシーに違反する URL の絶対数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[一意の URL 数] は「1」になります。

データ	説明
一意のユーザ/IP 数	指定のポリシーに違反するユーザの絶対数またはエンドポイントの IP アドレス数が表示されます。 例: 管理下の製品で、1 人のユーザから同じ URL の違反インスタンスが 10 個検出されました。 この場合、[一意のユーザ/IP 数] は「1」になります。
一意のユーザグループ数	指定のポリシーに違反するユーザのユーザグループの絶対数が表示されます。 例: 管理下の製品で、1 つのユーザグループから同じ URL の違反インスタンスが 10 個検出されました。 この場合、[一意のユーザグループ数] は「1」になります。
検出数	管理下の製品が検出した Web 違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

Web 違反エンドポイントの概要

特定のエンドポイントからの Web 違反検出の概要が表示されます。例: 違反エンドポイントの IP アドレス、違反ポリシーの数、ネットワーク上の Web 違反の総数

表 B-68. Web 違反エンドポイントの概要データビュー

データ	説明
エンドポイント	Web ポリシーに違反するエンドポイントの IP アドレス/ホスト名が表示されます。
一意のポリシー数	違反ポリシーの数が表示されます。 例: 管理下の製品で、2 台のコンピュータで同一ポリシーのポリシー違反インスタンスが 10 件検出されました。 この場合、[一意のポリシー数] は「1」になります。

データ	説明
一意の URL 数	指定のポリシーに違反する URL の絶対数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[一意の URL 数] は「1」になります。
検出数	管理下の製品が検出した Web 違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

Web 違反フィルタ/ブロックの種類の概要

Web 違反に対して管理下の製品が実行したアクションの概要が表示されます。例: URL へのアクセスを停止するフィルタ/ブロックの種類、ネットワーク上の Web 違反の総数

表 B-69. Web 違反フィルタ/ブロックの種類の概要データビュー

データ	説明
ブロックカテゴリ	違反 URL へのアクセスを阻止するフィルタ/ブロックのさまざまな種類が表示されます。 例: URL ブロック、URL フィルタ、スパイウェア対策
フィルタ/ブロックの種類	違反 URL へのアクセスを阻止するフィルタ/ブロックの具体的な種類が表示されます。 例: URL ブロック、URL フィルタリング、ウイルス
検出数	管理下の製品が検出した Web 違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

Web 違反 URL の概要

特定の URL からの Web 違反検出の概要が表示されます。例: Web 違反が発生した URL 名、その URL へのアクセスを停止するフィルタ/ブロックの種類、ネットワーク上の Web 違反の総数

表 B-70. Web 違反 URL の概要データビュー

データ	説明
URL	Web ポリシーに違反する URL が表示されます。
フィルタ/ブロックの種類	違反 URL へのアクセスを阻止するフィルタ/ブロックの種類が表示されます。 例: URL ブロック、URL フィルタ、Web ブロック
一意のエンドポイント数	指定のポリシーに違反するエンドポイントの絶対数が表示されます。 例: 管理下の製品で、4 台のコンピュータで同一 URL の違反インスタンスが 10 件検出されました。 この場合、[一意のエンドポイント数] は「4」になります。
検出数	管理下の製品が検出した Web 違反の総数が表示されます。 例: 管理下の製品で、1 台のコンピュータで同一の URL の違反インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

データビュー: 製品情報

Apex Central、管理下の製品、コンポーネント、およびライセンスに関する情報が表示されます。

Apex Central 情報

Apex Central へのユーザアクセス、コマンド追跡情報、および Apex Central サーバのイベントに関する情報が表示されます。

Apex Central のイベント情報

管理下の製品の Apex Central への登録、コンポーネントのアップデート、アクティベーションコードの配信などの Apex Central サーバイベントに関する情報が表示されます。

表 B-71. Apex Central のイベント情報データビュー

データ	説明
日時	イベントの発生時間を示します。
イベントの種類	発生したイベントの種類 (例: TMI エージェントへの通知、サーバからユーザへの通知、レポートサービスからユーザへの通知) を示します。
結果	イベントの結果 (例: 成功、失敗) を示します。
説明	アクティビティの 説明 (使用可能な場合) を示します。

コマンド追跡情報

Apex Central が管理下の製品に対して発行したコマンドに関する情報が表示されます。たとえば、Apex Central がコンポーネントのアップデートやアクティベーションコード配信のためのコマンドを発行した日付と時刻や、そのコマンドのステータスなどです。

表 B-72. コマンド追跡情報データビュー

データ	説明
日時	コマンドの発行者がコマンドを発行した時間を示します。
コマンドの種類	発行されたコマンドの種類 (例: 予約アップデート、アクティベーションコード配信) を示します。
コマンドパラメータ	コマンドに関する固有の情報 (例: 固有のパターンファイル名、固有のアクティベーションコード) を示します。
ユーザ (アカウント)	コマンドを発行したユーザを示します。
更新日	選択した Apex Central に対するすべてのコマンドのステータスが最後に確認された時間を示します。

データ	説明
成功	成功したコマンドの数を示します。
失敗	失敗したコマンドの数を示します。
処理中	処理中のコマンドの数を示します。
すべて	コマンドの総数 (成功、失敗、処理中の合計) を示します。

コマンド追跡詳細情報

コマンドに関連する詳細情報が表示されます。例: Apex Central への管理下の製品の登録、コンポーネントのアップデート、アクティベーションコードの配信

表 B-73. コマンド追跡詳細情報データビュー

データ	説明
日時	コマンドが発行された時間が表示されます。
コマンドの種類	発行されたコマンドの種類が表示されます。例: 予約アップデート、アクティベーションコードの配信
コマンドパラメータ	コマンドに関連する固有の情報が表示されます。例: パターンファイル名、アクティベーションコード
製品のエンティティ名	コマンドの発行先である管理下の製品が表示されます。
ユーザ (アカウント)	コマンドを発行したユーザが表示されます。
コマンドステータス	コマンドのステータス (成功、失敗、処理中) が表示されます。
更新日	選択した Apex Central についてすべてのコマンドのステータスが最後に確認された時間が表示されます。
結果の詳細説明	Apex Central がそのイベントに対して提示する説明が表示されます。

管理対象外のエンドポイント情報

検出されたエンドポイントのうち、トレンドマイクロ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に関する情報が表示されます。

表 B-74. 管理対象外のエンドポイント情報データビュー

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。

ユーザアクセス情報

Apex Central へのユーザアクセス、および Apex Central にログオン中にユーザが実行するアクティビティに関する情報が表示されます。

表 B-75. ユーザアクセス情報データビュー

データ	説明
日時	アクティビティが開始された日時を示します。
ユーザ (アカウント)	アクティビティを開始したユーザの名前を示します。
Active Directory グループ	Active Directory グループの名前を示します。
ユーザの役割	Apex Central でユーザアカウントに割り当てられたユーザの役割を示します。
アクティビティ	Apex Central でユーザが実行したアクティビティを示します。例: ログオン、ユーザアカウントの編集、配信計画の追加
結果	アクティビティの結果を示します。
説明	アクティビティの説明 (使用可能な場合) を示します。
役割の説明	ユーザアカウントに割り当てられたユーザの役割の説明を示します。

コンポーネント情報

管理下の製品のコンポーネントのステータス (期限切れであるか、最新であるかなど) やコンポーネント配信に関する詳細および概要情報が表示されます。

エンドポイントパターンファイル/検索エンジンのステータス概要

管理下の製品が使用する各種パターンファイル/検索エンジンに関する概要情報が表示されます。

表 B-76. エンドポイントパターンファイル/検索エンジンのステータス概要

データ	説明
製品のホスト名	管理下の製品がインストールされるサーバのホスト名が表示されます。
ドメイン	ホストのドメイン名が表示されます。
エンドポイント	エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータのホスト名が表示されます。
期限切れのパターンファイル数	期限切れのパターンファイルを使用している管理下の製品の数が表示されます。
最新パターンファイル保有率 (%)	最新の各種パターンファイルを使用している管理下の製品の割合が表示されます。これには、値として「n/a」を返すパターンファイルも含まれます。
期限切れの検索エンジン数	期限切れの検索エンジンを使用している管理下の製品の数が表示されます。
最新検索エンジン保有率 (%)	最新の検索エンジンを使用している管理下の製品の割合が表示されます。これには、値として「n/a」を返す検索エンジンも含まれます。

エンドポイントパターンファイル/ルールアップデートのステータス概要

このデータビューには、パターンファイルまたはルールのアップデートステータスに関する概要情報が表示されます。

表 B-77. エンドポイントパターンファイル/ルールのアップデートのステータス概要データビュー

データ	説明
パターンファイル/ルール	パターンファイルまたはルールの名前が表示されます。
パターンファイル/ルールのステータス	パターンファイルまたはルールが最新バージョンかどうかを示します。
パターンファイル/ルールのバージョン	パターンファイルまたはルールのバージョンが表示されます。
パターンファイル/ルールの前回のアップデート	パターンファイルまたはルールが正常にアップデートされているかどうかを示します。
エンドポイント数	パターンファイルまたはルールの最新バージョンを使用しているエンドポイントの数が表示されます。
エンドポイント総数	パターンファイルまたはルールを使用しているエンドポイントの合計数が表示されます。
比率 (%)	パターンファイルまたはルールの最新バージョンを使用しているエンドポイントの割合が表示されます。

検索エンジンのステータス

管理下の製品が使用する検索エンジンに関する詳細情報が表示されます。例: 検索エンジン名、検索エンジンが最後に配信された時間、検索エンジンを使用している管理下の製品

表 B-78. 検索エンジンのステータスデータビュー

データ	説明
製品のエンティティ/エンドポイント	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品のエンティティ 表示名。Apex Central では、管理下の製品のエンティティ 表示名を使用して、管理下の製品を識別します。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレスまたはホスト名。
製品のホスト名/エンドポイント	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品がインストールされるサーバのホスト名。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレス。
製品/エンドポイント IP	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品がインストールされるサーバの IP アドレス。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレス。
接続ステータス	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品の Apex Central への接続ステータス。例: 標準、異常、オフライン • エンドポイントエージェントの管理下の製品 (Apex One) への接続ステータス。例: 標準、異常、オフライン
製品	管理下の製品の名前が表示されます。例: Apex One、InterScan for Microsoft Exchange
製品バージョン	管理下の製品または管理下の製品エージェントのバージョン番号が表示されます。例: Apex One 2019、Apex Central 2019
製品の役割	ネットワーク環境における、管理下の製品またはエージェント (Apex One セキュリティエージェントなど) がインストールされたコンピュータの役割が表示されます。例: サーバ
検索エンジン	検索エンジンの名前が表示されます。例: ウイルス検索エンジン、ダメージクリーンナップエンジン

データ	説明
検索エンジンバージョン	検索エンジンのバージョンが表示されます。例: ウイルス検索エンジン: 9.770.1001、ダメージクリーンナップエンジン: 8.000.1008
検索エンジンのステータス	検索エンジンの適用状況のステータスが表示されます。例: 最新、期限切れ
検索エンジンの前回のアップデート	検索エンジンを管理下の製品またはエンドポイントに最後に配信した時間が表示されます。

パターンファイル/ルールのステータス

管理下の製品が使用する各種パターンファイルに関する詳細情報が表示されます。例: 各種パターンファイル名、各種パターンファイルが最後に配信された時間、各種パターンファイルを使用している管理下の製品

表 B-79. パターンファイル/ルールのステータスデータビュー

データ	説明
製品のエンティティ/エンドポイント	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品のエンティティ 表示名。Apex Central では、管理下の製品のエンティティ 表示名を使用して、管理下の製品を識別します。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレスまたはホスト名。
OS	このデータ列には、管理下の製品がインストールされるサーバの OS が表示されます。
製品のホスト名/エンドポイント	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品がインストールされるサーバのホスト名。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレス。

データ	説明
製品/エンドポイント IP	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品がインストールされるサーバの IP アドレス。 • エージェント (Apex One セキュリティエージェントなど) がインストールされているコンピュータの IP アドレス。
アップデートエージェント	このデータ列には、管理下の製品のアップデートエージェントが表示されます。
ドメイン	このデータ列には、管理下の製品がインストールされるサーバのドメインが表示されます。
管理サーバのエンティティ 表示名	このデータ列には、管理サーバのエンティティ 表示名が表示されます。
接続ステータス	このデータ列には、次の情報のいずれかが表示されます。 • 管理下の製品の Apex Central への接続ステータス。例: 標準、異常、オフライン • エンドポイントエージェントの管理下の製品 (Apex One) への接続ステータス。例: 標準、異常、オフライン
製品	管理下の製品の名前が表示されます。例: Apex One、 InterScan for Microsoft Exchange
製品バージョン	管理下の製品または管理下の製品エージェントのバージョン番号が表示されます。例: Apex One 2019、Apex Central 2019
製品の役割	ネットワーク環境における、管理下の製品またはエージェント (Apex One セキュリティエージェントなど) がインストールされたコンピュータの役割が表示されます。例: サーバ
パターンファイル/ルール	各種パターンファイルの名前が表示されます。例: ウイルスパターンファイル、スパムメール判定ルール
パターンファイル/ルールのバージョン	各種パターンファイルのバージョンが表示されます。例: ウイルスパターンファイル: 3.203.00、スパムメール判定ルール: 14256
パターンファイル/ルールのステータス	各種パターンファイルの適用状況のステータスが表示されます。例: 最新、期限切れ

データ	説明
パターンファイル/ルールの前回のアップデート	各種パターンファイルを管理下の製品またはエンドポイントに最後に配信した時間が表示されます。
Apex One ドメイン階層	Apex One ドメイン階層のパスが表示されます。

パターンファイル/ルールのステータス概要

管理下の製品が使用する各種パターンファイルに関する概要情報が表示されます。例: 各種パターンファイル名、最新の各種パターンファイルの割合、期限切れの各種パターンファイルの数

表 B-80. パターンファイル/ルールのステータス概要データビュー

データ	説明
パターンファイル/ルール	各種パターンファイルの名前が表示されます。例: ウイルスパターンファイル、スパムメール判定ルール
バージョン	各種パターンファイルのバージョンが表示されます。例: ウイルスパターンファイル: 3.203.00、スパムメール判定ルール: 14256
最新バージョン	最新の各種パターンファイルを使用している管理下の製品の数が表示されます。
古いバージョン	期限切れの各種パターンファイルを使用している管理下の製品の数が表示されます。
最新バージョン率 (%)	最新の各種パターンファイルを使用している管理下の製品の割合が表示されます。これには、値として「n/a」を返すパターンファイルも含まれます。
1 世代前のバージョンの使用率 (%)	1 世代前のバージョンのパターンファイル/ルールを使用している管理下の製品の割合が表示されます。
2 世代前のバージョンの使用率 (%)	2 世代前のバージョンのパターンファイル/ルールを使用している管理下の製品の割合が表示されます。
3 世代前のバージョンの使用率 (%)	3 世代前のバージョンのパターンファイル/ルールを使用している管理下の製品の割合が表示されます。

データ	説明
4 世代前のバージョンの使用率 (%)	4 世代前のバージョンのパターンファイル/ルールを使用している管理下の製品の割合が表示されます。
5 世代前のバージョンの使用率 (%)	5 世代前のバージョンのパターンファイル/ルールを使用している管理下の製品の割合が表示されます。
6 世代以上前のバージョンの使用率 (%)	6 世代以上前のバージョンのパターンファイル/ルールを使用している管理下の製品の割合が表示されます。

製品コンポーネントの配信

管理下の製品が使用するコンポーネントに関する詳細情報が表示されます。例: 各種パターンファイル名、各種パターンファイルのバージョン番号、検索エンジンの配信ステータス

表 B-81. 製品コンポーネントの配信データビュー

データ	説明
製品のエンティティ名	管理下の製品のエンティティ 表示名が表示されます。Apex Central では、管理下の製品のエンティティ 表示名を使用して、管理下の製品を識別します。
製品	管理下の製品の名前が表示されます。例: Apex One、InterScan for Microsoft Exchange
製品バージョン	管理下の製品のバージョン番号が表示されます。例: Apex One 2019、Apex Central 2019
接続ステータス	管理下の製品と Apex Central サーバ、または管理下の製品とそのエンドポイント間の接続ステータスが表示されます。
パターンファイル/ルールのステータス	各種パターンファイルの適用状況のステータスが表示されます。例: 最新、期限切れ
パターンファイル/ルールの配信ステータス	各種パターンファイルの最新のアップデートの配信ステータスが表示されます。例: 成功、失敗、処理中
パターンファイル/ルールの配信	各種パターンファイルを管理下の製品またはエンドポイントに最後に配信した時間が表示されます。

データ	説明
検索エンジンのステータス	検索エンジンの適用状況のステータスが表示されます。例: 最新、期限切れ
検索エンジンの配信ステータス	エンジンの最新のアップデートの配信ステータスが表示されます。例: 成功、失敗、処理中
検索エンジンの配信	検索エンジンを管理下の製品またはエンドポイントに最後に配信した時間が表示されます。

検索エンジンのステータス概要

管理下の製品が使用する検索エンジンに関する概要情報が表示されます。例: 検索エンジン名、検索エンジン配信率、期限切れになっている検索エンジンの数

表 B-82. 検索エンジンのステータス概要データビュー

データ	説明
検索エンジン	検索エンジンの名前が表示されます。例: ウイルス検索エンジン、ダメージクリーンナップエンジン
バージョン	検索エンジンのバージョンが表示されます。例: ウイルス検索エンジン: 9.770.1001、ダメージクリーンナップエンジン: 8.000.1008
最新バージョン	最新の検索エンジンを使用している管理下の製品の数が表示されます。
古いバージョン	期限切れの検索エンジンを使用している管理下の製品の数が表示されます。
最新バージョン率 (%)	最新の検索エンジンを使用している管理下の製品の割合が表示されます。これには、値として「N/A」を返す検索エンジンも含まれます。

ライセンス情報

Apex Central および管理下の製品のライセンスに関するステータス、詳細、および概要情報が表示されます。

製品ライセンス詳細情報

管理下の製品のバージョン、ライセンス使用期限など、管理下の製品またはサービスのアクティベーションコードやライセンスのステータスに 関する情報が表示されます。

表 B-83. 製品のライセンス詳細情報データビュー

データ	説明
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
製品バージョン	管理下の製品またはサービスのバージョンを示します。
管理下のサービス	管理下のサービスの名前を示します。 例: Web レピュテーションサービス
ライセンスステータス	管理下の製品のライセンスのステータスを示します。 例: アクティベート済み、サポート契約終了、更新猶予期間
製品の種類	アクティベーションコードで使用できる、管理下の製品の種類を示します。 例: 体験版、製品版
アクティベーションコードを示します。	管理下の製品またはサービスのアクティベーションコードを示します。
ライセンス有効期限	管理下の製品またはサービスのライセンスの有効期限が切れる日を示します。
ライセンス数	アクティベーションコードで使用できるライセンス数を示します。
説明	アクティベーションコードの説明を示します。

製品ライセンス情報の概要

アクティベーションコードに関する詳細、およびアクティベーションコードを使用する管理下の製品の情報が表示されます。例: アクティベーションコードで許可されるライセンス数、体験版か製品版か、ユーザ定義のアクティベーションコードの説明

表 B-84. 製品のライセンス情報概要データビュー

データ	説明
アクティベーションコード	管理下の製品のアクティベーションコードが表示されます。
ユーザ定義の説明	ユーザが定義したアクティベーションコードの説明が表示されます。
製品/サービス	このアクティベーションコードを使用する管理下の製品またはサービスの数が表示されます。
ライセンスステータス	管理下の製品のライセンスのステータスが表示されます。例: アクティベート済み、サポート契約終了、更新猶予期間
製品の種類	このアクティベーションコードで使用できる、管理下の製品の種類が表示されます。例: 体験版、製品版
ライセンス有効期限	管理下の製品のサポート契約の有効期限が表示されます。
ライセンス数	このアクティベーションコードで使用が許可されるライセンス数が表示されます。

製品ライセンスのステータス

管理下の製品に関する詳細情報、および管理下の製品が使用するアクティベーションコードに関する情報が表示されます。例: 管理下の製品の情報、アクティベーションコードがアクティブであるかどうか、アクティベーションコードによってアクティベートされている管理下の製品の数

表 B-85. 製品のライセンスステータスデータビュー

データ	説明
製品のエンティティ名	管理下の製品のエンティティ 表示名が表示されます。Apex Central では、管理下の製品のエンティティ 表示名を使用して、管理下の製品を識別します。
製品	管理下の製品の名前が表示されます。例: Apex One、InterScan for Microsoft Exchange
製品バージョン	管理下の製品のバージョン番号が表示されます。例: Apex One 2019、Apex Central 2019
サービス	管理下の製品サービスの名前が表示されます。
ライセンスステータス	管理下の製品のライセンスのステータスが表示されます。例: アクティベート済み、サポート契約終了、更新猶予期間
アクティベーションコード	管理下の製品のアクティベーションコードが表示されます。
アクティベーションコード数	管理下の製品が使用するアクティベーションコードの件数が表示されます。
ライセンス有効期限	管理下の製品のサポート契約の有効期限が表示されます。

管理下の製品情報

管理下の製品または管理下の製品のエンドポイントに関するステータス、詳細、および概要情報が表示されます。

製品監査イベントログ

管理下の製品のコンソールアクセスなど、管理下の製品の監査イベントに関する情報が表示されます。

表 B-86. 製品監査イベントログデータビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
ホスト	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの表示名を示します。 • セキュリティエージェントエンドポイントの表示名を示します。
ユーザ	イベントの時点でログオンしていたユーザの名前を示します。
イベントのカテゴリ	イベントの種類を示します。 例: 管理コンソールへのアクセス
イベントのレベル	イベントの重大度レベルを示します。
イベントの説明	イベントの説明を示します。

製品配置の概要

Apex Central に登録されている管理下の製品に関する概要情報が表示されます。例: 管理下の製品名、バージョン番号、管理下の製品の数

表 B-87. 製品の配置概要データビュー

データ	説明
登録先 Apex Central	管理下の製品の登録先の Apex Central サーバが表示されます。
製品カテゴリ	管理下の製品について、脅威からの保護のカテゴリが表示されます。例: サーバベース製品、デスクトップ (コンピュータおよびモバイルデバイス) 製品 注意 デスクトップ製品には、モバイルデバイスのソリューションも含まれます。

データ	説明
製品	管理下の製品の名前が表示されます。例: Apex One、InterScan for Microsoft Exchange
製品バージョン	管理下の製品のバージョン番号が表示されます。例: Apex One 2019、Apex Central 2019
製品の役割	ネットワーク環境での管理下の製品の役割が表示されます。例: サーバ、クライアント
製品	ネットワーク内にある特定の管理下の製品の総数が表示されます。

製品のイベント情報

管理下の製品の Apex Central への登録、コンポーネントのアップデート、アクティベーションコードの配信など、管理下の製品のイベントに関する情報が表示されます。

表 B-88. 製品のイベント情報データビュー

データ	説明
受信日時	管理下の製品から Apex Central がデータを受信した日付と時刻を示します。
生成	管理下の製品でデータが生成された日付と時刻を示します。
製品のエンティティ名	Apex Central における管理下の製品のサーバの表示名を示します。
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、InterScan for Microsoft Exchange
製品バージョン	管理下の製品またはサービスのバージョンを示します。
イベント重大度	イベントの重大度レベルを示します。
イベントの種類	イベントの種類を示します。 例: ウイルスのダウンロードの検出、ファイルのブロック、ロールバック

データ	説明
コマンドステータス	コマンドのステータスを示します。 例: 成功、失敗、処理中
説明	イベントの説明を示します。

製品のステータス情報

Apex Central サーバに登録された管理下の製品に関する詳細情報が表示されます。たとえば、管理下の製品のバージョンとビルド番号、管理下の製品のサーバオペレーティングシステムなどです 。

表 B-89. 製品のステータス情報データビュー

データ	説明
製品のエンティティ/エンドポイント	関連付けられている場所に応じて以下を示します。 • Apex Central における管理下の製品のサーバの表示名を示します。 • セキュリティエージェントのエンドポイントの名前または IP アドレスを示します。
製品のホスト名/エンドポイント	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの表示名を示します。 • セキュリティエージェントエンドポイントの表示名を示します。
製品/エンドポイント IP	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの IP アドレスを示します。 • セキュリティエージェントエンドポイントの IP アドレスを示します。
製品/エンドポイント MAC	関連付けられている場所に応じて以下を示します。 • 管理下の製品のサーバの MAC アドレスを示します。 • セキュリティエージェントのエンドポイントの MAC アドレスを示します。

データ	説明
管理 Apex Central のエンティティ名	管理下の製品サーバから報告を受ける Apex Central サーバの表示名を示します。
管理サーバのエンティティ名	エンドポイントが配下に置かれている、Apex Central の管理下の製品のサーバの表示名を示します。
ドメイン	管理下の製品が属するドメインを示します。
接続ステータス	関連付けられている場所に応じて以下を示します。 • 管理下の製品サーバの Apex Central への接続ステータスを示します。例: 標準、異常、オフライン • セキュリティエージェントエンドポイントの、管理下の製品サーバへの接続ステータスを示します。例: 標準、異常、オフライン
情報漏えい対策オプションステータス	セキュリティエージェントの情報漏えい対策オプションステータスを示します。 例: インストールされています、インストールされていません
パターンファイルのステータス	管理下の製品またはセキュリティエージェントで使用されているパターンファイル/ルールのステータスを示します。 例: 最新、期限切れ
検索エンジンのステータス	管理下の製品またはセキュリティエージェントで使用されている検索エンジンのステータスを示します。 例: 最新、期限切れ
製品	管理下の製品またはサービスの名前を示します。 例: Apex One、 InterScan for Microsoft Exchange
製品バージョン	管理下の製品またはサービスのバージョンを示します。
Endpoint Sensor のバージョン	Endpoint Sensor のバージョンを示します。
アプリケーションコントロールのバージョン	アプリケーションコントロールのバージョンを示します。

データ	説明
仮想パッチのバージョン	仮想パッチのバージョンを示します。
製品のビルド	管理下の製品のビルド番号を示します。
製品の役割	ネットワーク環境での管理下の製品サーバまたはセキュリティエージェントエンドポイントの役割を示します。例: サーバ
OS	管理下の製品サーバまたはセキュリティエージェントエンドポイントにおける OS を示します。
OS バージョン	管理下の製品サーバまたはセキュリティエージェントエンドポイントにおける OS のバージョンを示します。
OS Service Pack	管理下の製品サーバまたはセキュリティエージェントエンドポイントにおける OS の Service Pack 番号を示します。
アップデートエージェント	セキュリティエージェントがアップデートエージェントかどうかを示します。
前回の予約検索	前回の予約検索の日時を示します。
前回の手動検索	前回の手動検索の日時を示します。
前回の ScanNow	前回の ScanNow 処理の日時を示します。
リアルタイム検索	リアルタイム検索が有効かどうかを示します。
ファイアウォール	ファイアウォールが有効かどうかを示します。
パターンファイル/ルールの配信ステータス	パターンファイル/ルールの配信ステータスを示します。
パターンファイル/ルールの配信	パターンファイル/ルールの配信の日時を示します。
検索エンジンの配信ステータス	検索エンジンの配信ステータスを示します。
検索エンジンの配信	検索エンジンの配信の日時を示します。
ログオンユーザ	管理下のエンドポイントに最後にログオンしたユーザの、ダウンレベルのログオン名 (NetBIOS_Domain\User_Name)

データ	説明
前回の起動日時	セキュリティエージェントが前回起動された日時を示します。
オフライン時間	セキュリティエージェントが前回オフラインになった日時を示します。
ユーザ名	イベントの時点でログオンしていたユーザの名前を示します。

付録 C

トークン変数

このセクションでは、イベント通知メッセージをカスタマイズするために Apex Central がサポートしているトークン変数について説明します。

次のトピックがあります。

通知メッセージのカスタマイズ

次の表は、すべてのイベント通知メッセージをカスタマイズする際のトークン変数について示しています。

注意

イベント通知によっては、追加のトークン変数をサポートしていることがあります。特定のイベント通知でサポートされるトークン変数の完全な一覧については、そのイベント通知の通知方法に関する情報を参照してください。

変数	説明
%cmserver%	Apex Central サーバ名を示します。
%computer%	エンドポイントの名前を示します。
%entity%	Apex Central における管理下の製品のサーバの表示名を示します。
%event%	検出されたイベントを示します。
%pname%	管理下の製品の名前を示します。
%pver%	管理下の製品のバージョンを示します。
%time%	イベントが発生した時刻 (hh:mm) を示します。
%vloginuser%	イベントの時点でログオンしていたユーザの名前を示します。
%act%	管理下の製品によって実行された処理を示します。例: ファイルの駆除、削除、隔離

高度な脅威アクティビティのトークン 変数

注意

すべてのイベント通知でサポートされている標準トークン変数のリストについては、752 ページの「通知メッセージのカスタマイズ」を参照してください。

次の表は、高度な脅威アクティビティのイベント通知メッセージをカスタマイズする際のトークン変数について示しています。

変数	説明
%hostIP%	以下のトラフィックの方向に従って Deep Discovery Inspector によって決定される IP アドレスを示します。 • 送信トラフィック (外部ネットワークに向かう内部トラフィック): %hostIP%はネットワークのエンドポイント (侵入元) の IP アドレスです。 • ネットワーク内のトラフィック: %hostIP%はネットワークのエンドポイントの IP アドレスです。 • ネットワーク内のエンドポイントに向かう外部トラフィック: %hostIP%はネットワークのエンドポイントの IP アドレスです。 • ネットワーク外のトラフィック: %hostIP%はネットワークのエンドポイントの IP アドレスです。
%group%	サブネットワークの名前を示します。
%START_TIME%	検出期間の開始日時を示します。 注意 通知の条件に指定した期間によって、開始日時と終了日時が決まります。
%END_TIME%	検出期間の終了日時を示します。 開始時刻と終了時刻で、時間範囲の期間を定義します。特定の期間中にログを受信すると、Apex Central ではログについて計算が行われます。アラート条件に適合する場合、ログがカウントされます。%START_TIME%は期間の開始時間で、%END_TIME% は終了時間です。期間の長さは通知設定の時間のしきい値によって決定します。 注意 通知の条件に指定した期間によって、開始日時と終了日時が決まります。

変数	説明
%detections%	検出数を示します。 例: イベント: 仮想アナライザによるリスク高の検出 IP アドレス: %hostIP% ホスト名: %computer% グループ: %group% 時間範囲: %START_TIME% - %END_TIME% 検出数: %detections%

次の表は、挙動監視違反および機械学習型検索の検出のイベント通知メッセージをカスタマイズする際のトークン変数について示しています。

変数	説明
%hostIP%	以下のトラフィックの方向に従って Deep Discovery Inspector によって決定される IP アドレスを示します。 • 送信トラフィック (外部ネットワークに向かう内部トラフィック): %hostIP%はネットワークのエンドポイント (侵入元) の IP アドレスです。 • ネットワーク内のトラフィック: %hostIP%はネットワークのエンドポイントの IP アドレスです。 • ネットワーク内のエンドポイントに向かう外部トラフィック: %hostIP%はネットワークのエンドポイントの IP アドレスです。 • ネットワーク外のトラフィック: %hostIP%はネットワークのエンドポイントの IP アドレスです。
%START_TIME%	検出期間の開始日時を示します。 注意 通知の条件に指定した期間によって、開始日時と終了日時が決まります。

変数	説明
%END_TIME%	検出期間の終了日時を示します。 開始時刻と終了時刻で、時間範囲の期間を定義します。特定の期間中にログを受信すると、Apex Central ではログについて計算が行われます。アラート条件に適合する場合、ログがカウントされます。%START_TIME%は期間の開始時間で、%END_TIME% は終了時間です。期間の長さは通知設定の時間のしきい値によって決定します。 **注意** 通知の条件に指定した期間によって、開始日時と終了日時が決まります。
%detections%	検出数を示します。 例: イベント: 仮想アナライザによるリスク高の検出 IP アドレス: %hostIP% ホスト名: %computer% グループ: %group% 時間範囲: %START_TIME% - %END_TIME% 検出数: %detections%
%domain%	Apex One ドメイン階層における対象のルートドメインを示します。
%hierarchy%	Apex One ドメイン階層における対象のフルパスを示します。
%BM_policy%	挙動監視ポリシー ID を示します。
%risklevel%	イベントのリスクレベルを示します。
%target%	イベントの対象を示します。

Attack Discovery のトークン変数

次の表は、Attack Discovery のイベント通知メッセージをカスタマイズするためのトークン変数について示しています。

変数	説明
%cmserver%	Apex Central サーバ名を示します。
%computer%	エンドポイントの名前を示します。
%entity%	Apex Central における管理下の製品のサーバの表示名を示します。
%event%	検出されたイベントを示します。
%pname%	管理下の製品の名前を示します。
%pver%	管理下の製品のバージョンを示します。
%time%	イベントが発生した時刻 (hh:mm) を示します。
%vloginuser%	イベントの時点でログオンしていたユーザの名前を示します。
%act%	管理下の製品によって実行された処理を示します。例: ファイルの駆除、削除、隔離
%actresult%	管理下の製品によって実行された処理の結果を示します。例: 成功、処理が必要
%highrisk_detection%	指定された期間のリスク高の検出数を示します。
%highrisk_detection_endpoint%	指定された期間にリスク高が検出されたエンドポイント数を示します。
%mediumrisk_detection%	指定された期間のリスク中の検出数を示します。
%mediumrisk_detection_endpoint%	指定された期間にリスク中が検出されたエンドポイント数を示します。
%start_time%	検出期間の開始日時を示します。
%end_time%	検出期間の終了日時を示します。

C&C コールバックトークン変数

次の表は、C&C コールバックのイベント通知メッセージをカスタマイズする際のトークン変数について示しています。

注意

すべてのイベント通知でサポートされている標準トークン変数のリストについては、752 ページの「通知メッセージのカスタマイズ」を参照してください。

変数	説明
%CnC_LIST_SRC%	コールバックアドレスを含むリストの名前
%CNC_PD_NAME%	ログを送信した管理下の製品のサーバの製品 ID
%CNC_PD_VERSION%	ログを送信した管理下の製品のサーバのバージョン
%CNC_PD_NODE%	ログを送信した管理下の製品のサーバのエンドポイント名
%CNC_PD_IP%	ログを送信した管理下の製品サーバの IP アドレス
%CNC_EVTTIME%	ログが生成された時間
%CNC_AGENTNAME%	コールバックを検出したセキュリティエージェントエンドポイントの名前
%CNC_AGENTIP%	コールバックを検出したセキュリティエージェントエンドポイントの IP アドレス
%CNC_AGENTDOMAIN%	コールバックを検出したセキュリティエージェントエンドポイントの Apex One ドメイン
%CNC_POLICY_RULE%	コールバックを検出したポリシーのルール ID の名前
%CNC_ACTION%	セキュリティログ、個人用ファイアウォール、NCIE ログ、Web セキュリティログの処理結果
%CNC_EMAIL_SENDER%	コールバックと関連付けられたメール送信者

変数	説明
%CNC_EMAIL_SUBJECT%	コールバックと関連付けられたメールの件名
%CNC_RISKLEVEL%	C&C サーバと関連付けられた不正プログラムのグループのリスクレベル
%CNC_DETECT_SOURCE%	検出ルールを定義した C&C リスト
%CNC_CHANNEL%	配信先の形式を示す種類 ID
%CNC_URL%	エンドポイントがアクセスを試行したリモート URL
%CNC_URL_CATEGORY%	エンドポイントがアクセスを試行したサイトの URL カテゴリ
%CNC_IP_PORT%	C&C サーバの IP アドレスとポート
%CNC_EMAIL_REPT%	コールバックと関連付けられたメール受信者
%CNC_FIRST_SEEN%	C&C サーバの最初の既知の検出
%CNC_LAST_SEEN%	C&C サーバの最後の既知の検出
%CNC_LOCATION%	C&C サーバの国番号
%CNC_MALEWARE_FAMILY%	C&C 検出に関連付けられた不正プログラムファミリ
%CNC_ATTACK_GROUP%	C&C グループリスト
%CNC_PROCESS_NAME%	C&C 検出に関連付けられたプロセス名
%CALLBACK_ADDR%	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
%COMPR_HOST%	影響を受けたホストまたはメールアドレス
%CALLBACK_NUM%	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
%COMPR_HOST_NUM%	アウトブレークに関係している感染ホストの数

変数	説明
%CALLBACK_ADDR_NUM%	アウトブレークに関係しているコールバックアドレスの数

コンテンツのポリシー違反のトークン変数

次の表は、コンテンツのポリシー違反のイベント通知メッセージをカスタマイズする際のトークン変数について説明しています。

注意

すべてのイベント通知でサポートされている標準トークン変数のリストについては、752 ページの「通知メッセージのカスタマイズ」を参照してください。

変数	説明
%subject%	メール通知の件名
%sender%	送信者のメールアドレス
%recipient%	受信者のメールアドレス
%filtername%	違反のあったコンテンツフィルタのルールまたはポリシーの名前
%filteract%%	フィルタに割り当てられた処理
%msgact%	メッセージに割り当てられた処理

情報漏えい対策トークン変数

次の表は、情報漏えい対策のイベント通知メッセージをカスタマイズするためのトークン変数について示しています。

注意

すべてのイベント通知でサポートされている標準トークン変数のリストについては、752 ページの「通知メッセージのカスタマイズ」を参照してください。

変数	説明
%DLP_INCIDENT_TOTAL_NUM%	直接管理下のユーザによりトリガされたイベントの総数
%DLP_INCIDENT_HIGH_NUM%	直接管理下のユーザによりトリガされた重大度の高いイベントの総数
%DLP_INCIDENT_MED_NUM%	直接管理下のユーザによりトリガされた中程度の重大度のイベントの総数
%DLP_INCIDENT_LOW_NUM%	直接管理下のユーザによりトリガされた重大度の低いイベントの総数
%DLP_INCIDENT_INFO_NUM%	直接管理下のユーザによりトリガされた情報イベントの総数
%DLP_INCIDENT_UNDEFINED_NUM%	直接管理下のユーザによりトリガされた重大度が未定義のイベントの総数
%DLP_INCIDENT_ALLTOTAL_NUM%	管理下のユーザすべてによりトリガされたイベントの 総数
%DLP_INCIDENT_ALLHIGH_NUM%	管理下のユーザすべてによりトリガされた 重大度の高いイベントの総数
%DLP_INCIDENT_ALLMED_NUM%	管理下のユーザすべてによりトリガされた 重大度が中程度のイベントの総数
%DLP_INCIDENT_ALLLOW_NUM%	管理下のユーザすべてによりトリガされた 重大度の低いイベントの総数
%DLP_INCIDENT_ALLINFO_NUM%	管理下のユーザすべてによりトリガされた 情報イベントの総数
%DLP_INCIDENT_ALLUNDEFINED_NUM%	管理下のユーザすべてによりトリガされた 重大度が未定義のイベントの総数
%DLP_START_TIME%	レポート期間の開始日時
%DLP_END_TIME%	レポート期間の終了日時
%weblink%	通知メッセージにリストされているイベント情報の詳細を表示するためのリンク
%INCIDENTID%	イベントの ID 番号

変数	説明
%SEVERITY%	イベントの重大度レベル
%POLICY%	Apex Central ポリシー名 注意 管理下の製品コンソールで作成された情報漏えい対策ポリシーをトリガしているイベントについては、Apex Central ポリシー名は N/A と表示されます。
%ACCOUNT%	ユーザ名
%OLD_STATUS%	変更前のイベントステータス
%NEW_STATUS%	変更後のイベントステータス
%LATEST_COMMENT%	イベントに関する最新コメント
%DLP_VIOLATION_NUM%	DLP ポリシーに一致する違反の数
%DLP_THRESHOLD%	ポリシー違反の大幅な増加を示すためにトリガする必要がある違反の数
%DLP_TEMPLATE%	インシデントの大幅な増加に一致するテンプレート
%DLP_USER_NAME%	情報漏えい対策ポリシー違反が発生したエンドポイントに関連付けられているユーザ名
%DLP_SENDER%	情報漏えい対策ポリシー違反を発生させたメッセージの送信者
%DLP_CHANNEL%	情報漏えい対策ポリシー違反を発生させたイベントのチャネル
%STATUS_CHANGE_TIME%	イベント詳細のアップデート

既知の脅威アクティビティのトークン 変数

次の表は、既知の脅威アクティビティまたは大規模感染予防サービスのイベント通知メッセージをカスタマイズする際のトークン変数について示しています。

注意

すべてのイベント通知でサポートされている標準トークン変数のリストについては、752 ページの「通知メッセージのカスタマイズ」を参照してください。

変数	説明
%device_ip%	感染エンドポイントの IP アドレス。
%egnver%	• 検索エンジンのバージョン。 • アラートイベントカテゴリで使用されます。アラートイベントカテゴリの通知タイプとして、この変数は管理下の製品サーバに現在インストールされている検索エンジンのバージョンを示します。
%hierarchy%	• Apex One ドメイン階層におけるエンドポイントの場所。 • アラートイベントのカテゴリで使用されます。
%ptnver%	• ウイルスパターンファイルバージョン。 • アラートイベントカテゴリで使用されます。アラートイベントカテゴリの通知タイプとして、この変数は管理下の製品サーバに現在インストールされているウイルスパターンのバージョンを示します。
%scanmethod%	特定のウイルス処理の検索方法。このトークンは次のアラートでのみ使用できます。 • ウイルス検出 — 1 次処理失敗/2 次処理使用不可 • ウイルス検出 — 1 次処理/2 次処理失敗 • ウイルス検出 — 1 次処理成功 • ウイルス検出 — 2 次処理成功
%vcnt%	• ウイルスの検出数。 • ウイルスのアウトブレークアラートで使用されます。

変数	説明
%vdest%	• ウイルス/不正プログラムの送信先。 • 例: メール検出の場合: %vdest% は宛先のユーザ名 ホストベース/エンドポイント検出の場合: %vdest% はエンドポイントの IP アドレスまたはホスト名 • アラートイベントのカテゴリで使用されます。
%vfile%	感染ファイル名。アラートイベントのカテゴリで使用されます。
%vfilepath%	感染ファイルのディレクトリ。アラートイベントのカテゴリで使用されます。
%vname%	ウイルスまたは不正プログラムの名前。アラートイベントのカテゴリで使用されます。
%vsrc%	• ウイルス/不正プログラムの発生源または感染元。 • たとえば、管理下のウイルス対策製品によってメールからウイルス/不正プログラムが検出された場合、メッセージ送信元のユーザ名が%vsrc%の値となります。 • アラートイベントカテゴリおよびネットワークウイルスアラート関連の通知で使用されます。

ネットワークアクセス管理トークン変数

次の表は、ネットワークアクセス管理のイベント通知メッセージをカスタマイズする際のトークン変数について示しています。

注意

すべてのイベント通知でサポートされている標準トークン変数のリストについては、752 ページの「通知メッセージのカスタマイズ」を参照してください。

変数	説明
%action%	ネットワークウイルスに対して実行される Network VirusWall Enforcer の処理 (放置、破棄、または隔離)。
%description%	脆弱性に対する攻撃の兆候イベントで使用されるエラー説明。

Web アクセスポリシー違反トークン変数

次の表は、Web アクセスポリシー違反イベント通知メッセージをカスタマイズする際のトークン変数について示しています。

注意

すべてのイベント通知でサポートされている標準トークン変数のリストについては、752 ページの「通知メッセージのカスタマイズ」を参照してください。

変数	説明
%url%	問題がある可能性がある URL
%vdestip%	対象の URL の IP アドレス
%blockrule%	違反のあったルールの名前
%blocktype%	URL に割り当てられた処理

付録 D

IPv6 のサポート

この付録には、Apex Central での IPv6 のサポート範囲に関する情報が含まれています。

次のトピックがあります。

Apex Central サーバの要件

Apex Central サーバ上で IPv6 スタックをインストールして有効にすると、IPv6 のサポートが自動的に有効になります。

注意

IPv6 の概念、および IPv6 アドレス指定をサポートするネットワークの設定に関連するタスクに詳しいユーザを対象としています。

IPv6 のサポートの制限事項

次の表は、IPv6 のサポートにおける制限事項を示しています。

項目	制限事項
デュアル IP スタック	Apex Central では、デュアル IP スタックのみがサポートされます。IPv4 スタックが削除されると、IPv6 のサポートが正常に機能しない場合があります。
IPv4 ループバックインタフェース	IPv4 ループバックインタフェースが必要です。TCP/IP ソフトウェアが正常に動作していることを確認するには、`127.0.0.1` に ping を実行します。
IPv6 アドレス形式	Apex Central では、%文字を IPv6 サーバアドレスに使用できません。
Apex Central レポート	次の静的レポートでは、IPv6 アドレスがサポートされていません。 • ポリシー違反レポート • サービス違反レポート
Apex Central の機能	次の機能では、IPv6 アドレスがサポートされていません。 • 高度なログクエリの IP アドレス範囲 • 不審オブジェクトのログ用の IPv6 アドレス正規化

IPv6 アドレスの設定

管理コンソールを使用して、IPv6 アドレスを設定できます。設定のガイドラインは次のとおりです。

- Apex Central では、標準の IPv6 アドレス表記を使用できます。

  例:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- また、次のようなリンクローカルの IPv6 アドレスを使用することもできます。

  fe80::210:5aff:feaa:20a2

  警告!

  リンクローカルアドレスを指定する際には注意してください。Apex Central ではリンクローカルアドレスを使用できますが、状況によっては正しく機能しない場合があります。たとえば、アップデート元が別のネットワークセグメントにあり、リンクローカルアドレスで識別されている場合、Apex Central はアップデート元からアップデートできません。

- IPv6 アドレスが URL に含まれる場合は、アドレスを角括弧 [] で囲みます。

IP アドレスが表示される画面

IP アドレスは次の画面に表示されます。

- 製品ディレクトリ
- ログクエリの結果

- サーバの登録
- ダッシュボードウィジェット

付録 E

MIB ファイル

このセクションでは、Apex Central がサポートする Management Information Base (MIB) について説明します。

次のトピックがあります。

Apex Central の MIB ファイルを使用する

Apex Central MIB ファイルを次のリンクからダウンロードし、SNMP をサポートするアプリケーションを使用してファイルを抽出およびインポートします。

https://CM_IP:CM_Port/TVCSDownload/tools/ApexCentral_mib.zip

NVW Enforcer SNMPv2 MIB ファイルの使用

NVW Enforcer SNMPv2 MIB ファイルを次のリンクからダウンロードし、SNMP をサポートするアプリケーションを使用してファイルを抽出してインポートします。

- https://<Control Manager サーバ IP アドレス>:<ポート番号>/TVCSDownload/tools/nvw2_mib2.zip

付録 F

Syslog コンテンツマッピング - CEF

次の表では、Apex Central ログ出力と CEF Syslog の種類の間での Syslog コンテンツのマッピングを示します。

次のトピックがあります。

CEF Attack Discovery による検出ログ

注意

1 つの Attack Discovery による検出ログに関連するオブジェクトが 4 つを超える場合、Apex Central では最初の 4 つのオブジェクトのみが転送されます。

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	イベント ID	700220
ヘッダ (eventName)	ログ名	Attack Discovery Detections
ヘッダ (severity)	重大度	3
deviceExternalId	ID	例: 「38」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT+00:00」
dhost	エンドポイントのホスト名	例: 「ApexOneClient01」
dst	クライアントの IPv4 アドレス	例: 「10.0.8.20」
C6a3	クライアントの IPv6 アドレス	例: 「fd96:7521:9502:6:b5b0:b2b5:4173:3f5d」
duser	ユーザ名	例: 「Admin004」
customerExternalID	インスタンス ID	例: 「8c1e2d8f-a03b-47ea-aef8-5aeab99ea697」
cn1Label	「cn1」フィールドに対応するラベル	「SLF_RiskLevel」

CEF キー	説明	値
cn1	リスクレベル	例: 「0」 • 0: 不明 • 100: リスク低 • 500: リスク中 • 1000: リスク高
cn2Label	「cn2」フィールドに対応するラベル	「SLF_PatternNumber」
cn2	パターンファイル番号	例: 「30.1012.00」
cs1Label	「cs1」フィールドに対応するラベル	「SLF_RuleID」
cs1	ルール ID	例: 「powershell invoke expression」
cat	カテゴリ ID	例: 「point of entry」
cs2Label	「cs2」フィールドに対応するラベル	「SLF_ADEObjectGroup_Info_1」

CEF キー	説明	値

cs2	Attack Discovery のオブジェクト情報	例:
		<pre>process - powershell.exe - {
		"META_FILE_MD5" :
		"9393f60b1739074eb17c5f4ddd
		efe239",
		"META_FILE_NAME" :
		"powershell.exe",
		"META_FILE_SHA1" :
		"887ce4a295c163791b60fc23d2
		85e6d84f28ee4c",
		"META_FILE_SHA2" :
		"de96a6e50044335375dc1ac238
		336066889d9ffc7d73628ef4fe
		1b1b160ab32c",
		"META_PATH" :
		"c:\\windows\\system32\\wi
		ndowspowershell\\v1.0\\",
		"META_PROCESS_CMD" :
		["powershell cmd "],
		"META_PROCESS_PID" : 7132,
		"META_SIGNER" :
		"microsoft windows",
		"META_SIGNER_VALIDATION" :
		true,
		"META_USER_USER_NAME" :
		"Administrator",
		"META_USER_USER_SERVERNAME" :
		"Host",
		"OID" : 1
		}</pre>

cs3Label	「cs3」フィールドに対応するラベル	「SLF_ADEObjectGroup_Info_2」

CEF キー	説明	値

cs3	Attack Discovery のオブジェクト情報	例:
		
		process - powershell.exe - {
		"META_FILE_MD5" :
		"9393f60b1739074eb17c5f4dddefe239",
		"META_FILE_NAME" :
		"powershell.exe",
		"META_FILE_SHA1" :
		"887ce4a295c163791b60fc23d285e6d84f28ee4c",
		"META_FILE_SHA2" :
		"de96a6e50044335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c",
		"META_PATH" :
		"c:\\windows\\system32\\windowspowershell\\v1.0\\",
		"META_PROCESS_CMD" :
		["powershell cmd "],
		"META_PROCESS_PID" : 7132,
		"META_SIGNER" :
		"microsoft windows",
		"META_SIGNER_VALIDATION" :
		true,
		"META_USER_USER_NAME" :
		"Administrator",
		"META_USER_USER_SERVERNAME" :
		"Host",
		"OID" : 1
		}

cs4Label	「cs4」フィールドに対応するラベル	「SLF_ADEObjectGroup_Info_3」

CEF キー	説明	値
cs4	Attack Discovery のオブジェクト情報	例: `process - powershell.exe - { "META_FILE_MD5" : "9393f60b1739074eb17c5f4dddefe239", "META_FILE_NAME" : "powershell.exe", "META_FILE_SHA1" : "887ce4a295c163791b60fc23d285e6d84f28ee4c", "META_FILE_SHA2" : "de96a6e50044335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c", "META_PATH" : "c:\\windows\\system32\\windowspowershell\\v1.0\\", "META_PROCESS_CMD" : ["powershell cmd "], "META_PROCESS_PID" : 7132, "META_SIGNER" : "microsoft windows", "META_SIGNER_VALIDATION" : true, "META_USER_USER_NAME" : "Administrator", "META_USER_USER_SERVERNAME" : "Host", "OID" : 1 }`
cs5Label	「cs5」フィールドに対応するラベル	「SLF_ADEObjectGroup_Info_4」

CEF キー	説明	値

cs5	Attack Discovery のオブジェクト情報	例:
		<pre>process - powershell.exe - {
		"META_FILE_MD5" :
		"9393f60b1739074eb17c5f4dddefe239",
		"META_FILE_NAME" :
		"powershell.exe",
		"META_FILE_SHA1" :
		"887ce4a295c163791b60fc23d285e6d84f28ee4c",
		"META_FILE_SHA2" :
		"de96a6e50044335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c",
		"META_PATH" :
		"c:\\windows\\system32\\windowspowershell\\v1.0\\",
		"META_PROCESS_CMD" :
		["powershell cmd "],
		"META_PROCESS_PID" : 7132,
		"META_SIGNER" :
		"microsoft windows",
		"META_SIGNER_VALIDATION" :
		true,
		"META_USER_USER_NAME" :
		"Administrator",
		"META_USER_USER_SERVERNAME" :
		"Host",
		"OID" : 1
		}</pre>

deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697

CEF キー	説明	値
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|700211|Attack Discovery
Detections|3|deviceExternalId=5 rt=Jan 17 2019 03:38:06 GMT+
00:00 dhost=VCAC-Window-331 dst=10.201.86.150 customerExtern
alID=8c1e2d8f-a03b-47ea-aef8-5aeab99ea697 cn1Label=SLF_RiskL
evel cn1=0 cn2Label=SLF_PatternNumber cn2=30.1012.00 cs1Labe
l=SLF_RuleID cs1=powershell invoke expression cat=point of e
ntry cs2Label=SLF_ADEObjectGroup_Info_1 cs2=process - code9.
exe - {USER: administrator09} deviceNtDomain=APEXTMCM dntdom
=OSCEDomain1 TMCMLogDetectedHost=VCAC-Window-331 TMCMLogDete
ctedIP=10.201.86.150 ApexCentralHost=TW-CHRIS-W2019devicePay
loadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatfo
rm=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF 挙動監視ログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	製品ベンダ	Trend Micro
ヘッダ (pname)	製品名	Apex Central
ヘッダ (pver)	製品バージョン	2019
ヘッダ (eventid)	挙動監視ポリシー ID	BM:1000
ヘッダ (eventName)	ログ名	Behavior Monitoring
ヘッダ (severity)	重大度	3
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」

CEF キー	説明	値
dvchost	ホスト名	例: 「localhost」
cs2Label	「cs2」フィールドに対応するラベル	「Policy」

CEF キー	説明	値
cs2	ポリシーの種類	• 感染実行可能ファイル • スタートアッププログラムの追加 • ホストファイルの変更 • DLL (プログラムライブラリ) インジェクション • Internet Explorer プラグインの追加 • Internet Explorer 設定の変更 • シェル設定の変更 • サービスの追加 • セキュリティポリシー設定の変更 • ファイアウォールポリシー設定の変更 • システムファイルの変更 • システムファイルの複製 • レイヤードサービスプロバイダ • システムプロセスの変更 • 不審な挙動 • 新たに検出されたプログラム • 不正なファイル暗号化 • 脅威の挙動分析 • ユーザ定義ポリシー
sproc	イベントの対象	例: 「C:\\Windows\\SysWOW64\\rundll32.exe」

CEF キー	説明	値
cs3Label	「cs3」フィールドに対応するラベル	「Event_Type」
cs3	イベントの種類	• プロセス • プロセスイメージ • レジストリ • ファイルシステム • ドライバ • SDT • システム API • ユーザモード • 攻撃コード • すべて
cs4Label	「cs4」フィールドに対応するラベル	「Operation」
cs4	イベントの対象によって実行される操作	• プロセス作成 • 開く • 終了 • 削除 • 書き込み • 診断 • ファイル作成 • 閉じる • 実行 • 起動 • 攻撃コード • 未処理のオペレーション

CEF キー	説明	値
cs5Label	「cs5」フィールドに対応するラベル	「Risk_Level」
cs5	リスクレベル	例: 「1」 • 0: 低 • 1: 高
TMCMLogTarget	対象ホスト	例: 「HKCU\\Software\\Microsoft\ \Windows\ \CurrentVersion\\Run\ \COM+」

CEF キー	説明	値
act	変換された処理	• 許可 • 確認 • 拒否 • 終了 • 読み取りのみ許可 • 読み取り/書き込みのみ許可 • 読み取り/実行のみ許可 • フィードバック • 駆除 • 不明 • 診断 • 強制終了。ファイルは復元されました。 • 強制終了。一部のファイルは復元されませんでした。 • 強制終了。ファイルは復元されませんでした。 • 強制終了。再開結果: ファイルは復元されました。 • 強制終了: 再開結果: 一部のファイルは復元されませんでした。 • 強制終了: 再開結果: ファイルは復元されませんでした。
shost	送信元ホスト (エンドポイント)	例: 「shost1」
src	送信元ホスト IP アドレス	例: 10.0.147.105
deviceFacility	製品	例: 「Apex One」

CEF キー	説明	値
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|BM:1000|Behavior Monitor
ing|3|rt=Sep 20 2019 01:02:03 GMT+00:00 dvchost=localhost cs
5Label=Risk_Level cs5=1 cs2Label=Policy cs2=Threat Behavior
Analysis sproc=subject cs3Label=Event_Type cs3=File system
TMCMLogTarget=HKCU\\Software\\Microsoft\\Windows\\CurrentVer
sion\\Run\\COM+ act=Ask cs4Label=Operation cs4=Create Proces
s shost=shost1 src=10.0.76.40 deviceFacility=Apex One reason
=G deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDetecte
```

```
dHost=shost1 TMCMLogDetectedIP=10.0.76.40 ApexCentralHost=TW
-CHRIS-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F
-C697 TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service
Pack 1
```

CEF C&C コールバックログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	CnC: 処理	CnC:Block
ヘッダ (eventName)	名前	CnC Callback
ヘッダ (severity)	重大度	3
deviceExternalId	ID	例: 「12」
cat	ログの種類	例: 「1756」
deviceFacility	製品名	例: 「Apex One」
cs2Label	「cs2」フィールドに対応するラベル	例: 「EI_ProductVersion」
cs2	製品バージョン	例: 「11.0」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
shost	エンドポイントのホスト名	例: 「ApexOneClient01」
src	エンドポイントの IPv4 アドレス	例: 「10.201.86.187」

CEF キー	説明	値
c6a2Label	「c6a2」フィールドに対応するラベル	例: 「SLF_ClientIP」
c6a2	エンドポイントの IPv6 アドレス	例: 「2620:101:4003:7a0:fd4b:52ed:53bd:ae3d」
cs3Label	「cs3」フィールドに対応するラベル	例: 「SLF_DomainName」
cs3	ドメイン名	例: 「DOMAIN1」
cs4Label	「cs4」フィールドに対応するラベル	例: 「SLF_PolicyName」
cs4	ポリシー名	例: 「C&C Server URL in Web Reputation Services database - HTTP (Request)」
act	処理	例: 「2」 • 0: 不明 • 1: 放置 • 2: ブロック • 3: 監視 • 4: 削除 • 5: 隔離 • 6: 警告 • 7: 警告して続行 • 8: オーバーライド
cn1Label	「cn1」フィールドに対応するラベル	例: 「SLF_CCCA_RiskLevel」

CEF キー	説明	値
cn1	C&C リスクレベル	例: 「1」 • 0: SLF_CCCA_RISKLEVEL_UNKNOWN • 1: SLF_CCCA_RISKLEVEL_LOW • 2: SLF_CCCA_RISKLEVEL_MEDIUM • 3: SLF_CCCA_RISKLEVEL_HIGH
cn2Label	「cn2」フィールドに対応するラベル	例: 「SLF_CCCA_DetectionSource」
cn2	C&C リストのソース	例: 「1」 • 0: SLF_CCCA_GLOBAL_LIST • 1: SLF_CCCA_CUSTOM_LIST • 2: SLF_CCCA_CUSTOM_LIST_USER_DEFINED
cn3Label	「cn3」フィールドに対応するラベル	例: 「SLF_CCCA_DetectionFormat」
cn3	コールバックアドレスの形式	例: 「1」 • 0: IP • 1: IP • 2: HTTP • 3: SMTP
request	URL	例: 「http://CC13.jojo.com」
deviceCustomDate1Label	「deviceCustomDate1」フィールドに対応するラベル	例: 「SLF_FirstSeen」

CEF キー	説明	値
deviceCustomDate1	コールバック試行が初めて監視されたときの UTC 時間	例: 「Oct 10 2017 16:58:03 GMT +00:00」
deviceCustomDate2Label	「deviceCustomDate2」フィールドに対応するラベル	例: 「SLF_LastSeen」
deviceCustomDate2	コールバック試行が最後に監視されたときの UTC 時間	例: 「Oct 11 2017 10:58:03 GMT +00:00」
cs5Label	「cs5」フィールドに対応するラベル	例: 「CnCDestination」
cs5	コールバック URL アドレス	例: 「http://CC13.jojo.com」
dst	コールバック IPv4 アドレス	例: 「10.201.86.195」
c6a3Label	「c6a3」フィールドに対応するラベル	例: 「CnCDestination」
c6a3	コールバック IPv6 アドレス	例: 「fe80::38ca:cd15:443c:40bb %11」
deviceProcessName	プロセス名	例: 「C:\\Program Files (x86)\ \Internet Explorer\\iexplore.exe」
dvchost	ホスト名	例: localhost
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697

CEF キー	説明	値
deviceDirection	ネットワークトラフィックの方向	例: 0 この値の意味は、「cat」フィールドの値によって異なります。 「cat」 フィールドの値が 1756、1707、または 1733 の場合: • 0: 不明 • 1: 受信 • 2: 送信 「cat」 フィールドの値が 1739、1741、または 1723 の場合: • 0: 送信 • 1: 受信 • 2: 不明 「cat」フィールドの値が 1705、1735、または 1775 の場合: • -1: 不明 • 0: 送信メール • 1: 受信メール • 2: 内部メール
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|CnC:Block|CnC Callback
|3|deviceExternalId=12 rt=Oct 11 2017 06:34:09 GMT+00:00 cat
=1756 deviceFacility=Apex One cs2Label=EI_ProductVersion cs2
=11.0 shost=ApexOneClient01 src=10.201.86.187 cs3Label=SLF_D
omainName cs3=DOMAIN act=Block cn1Label=SLF_CCCA_RiskLevel c
n1=1 cn2Label=SLF_CCCA_DetectionSource cn2=1 cn3Label=SLF_CC
CA_DestinationFormat cn3=1 dst=10.201.86.195 deviceProcessNa
me=C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe
```

```
deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 dvchost=localhost
TMCMLogDetectedHost=ApexOneClient01 TMCMLogDetectedIP=10.201
.86.187 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C002
90C0360-9CDE11EB-D4B8-F51F-C697 deviceDirection=0 TMCMdevice
Platform=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF コンテンツセキュリティログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンス製品バージョン	2019
ヘッダ (eventid)	MS: フィルタ処理	MS: Clean
ヘッダ (eventName)	ポリシー名	Policy
ヘッダ (severity)	重大度	3
cnt	検出数	例: 10
dhost	すべての受信者のリスト	例: employee_a1@Acompany.com;employee_a2@Acompany.com
duser	受信者の 1 人	例: employee_a1@Acompany.com
act	フィルタ処理	例: 「Clean」 詳細については、796 ページの「フィルタ処理マッピングテーブル」を参照してください。
cs1Label	「cs1」フィールドに対応するラベル	例: 「Policy_Settings」
cs1	ポリシー設定	例: 「Default_policy」

CEF キー	説明	値
cs2Label	「cs2」フィールドに対応するラベル	例: 「Product_Version」
cs2	製品バージョン	例: 「11」
cs3Label	「cs3」フィールドに対応するラベル	例: 「Filter_Type」
cs3	フィルタの種類	例: 「URL reputation filter」 • 0: 不明 • 1: ContentFilter • 2: AttachmentFilter • 3: StandardFilter • 4: SizeFilter • 5: DisclaimerMgr • 6: SpamFilter • 7: OPP • 8: ImportFilter • 9: PhishingFilter • 10: UrlReputationFilter
cs4Label	「cs4」フィールドに対応するラベル	例: 「CLF_ReasonCode」
cs4	理由コード	例: 「access」
cs5Label	「cs5」フィールドに対応するラベル	例: 「CLF_ReasonCodeSource」
cs5	理由コードの送信元	例: 「web」
cs6Label	「cs6」フィールドに対応するラベル	例: 「Action_on_Message」

CEF キー	説明	値
cs6	処理	例: 「3」 • 0: 不明 • 1: 該当なし • 2: 配信 • 3: 削除 • 4: 隔離 • 5: 保留 • 6: 通知 • 7: 置換 • 8: アーカイブ • 100: 削除 (ストリップ) • 101: 放置
cat	ログの種類	例: 「1705」
dvchost	エンドポイントのホスト名	例: 「ApexOneClient01」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
cn1Label	「cn1」フィールドに対応するラベル	例: 「Severity」
cn1	重大度コード	例: 「2」 • 0: 不明 • 1: 情報 • 2: 警告 • 3: エラー • 4: 重大
TMCMLogSeverity	重大度の説明	Second scan engine

CEF キー	説明	値
cn2Label	「cn2」フィールドに対応するラベル	Filter_Action_Result
cn2	フィルタ処理結果	例: 21 詳細については、797 ページの「フィルタ処理結果マッピングテーブル」を参照してください。
deviceExternalId	ID	例: 「5」
fname	ファイル	例: 「RERERW~42w.exe」
msg	件名	例: 「Open this email to win a free phone」
shost	すべての違反送信者/ユーザのリスト	例: "bear" <bear@abc.mail.com>;"yumi" <yumi@abc.mail.com>
suser	違反送信者/ユーザの 1 人	例: "bear" <bear@abc.mail.com>
deviceFacility	製品	例: 「Deep Discovery Email Inspector」
src	メール送信者の IP アドレス	例: 「10.206.155.122」
filepath	不審ファイルの場所	例: 「https://ca91-1.testurl.com:443」
request	不審 URL	例: 「https://ca91-1.testurl.com:443」

CEF キー	説明	値
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|MS:Clean|This is a policy
name|3|deviceExternalId=90045 rt=Sep 17 2018 01:27:42 GMT+00
:00 dhost=user@test.com duser=user@test.com act=Clean cs1Label
=Policy_Settings cs1=This is policy content cs2Label=CLF_Produ
ctVersion cs2=3.2 cs3Label=Filter_Type cs3=URL reputation filt
er cs5Label=CLF_ReasonCodeSource cs5=20 cs6Label=Action_on_Mes
sage cs6=0 cat=1705 dvchost=ApexOneClient01 cn1Label=Severity
cn1=2 TMCMLogSeverity=Second scan engine fname=NE_AEP.1550
msg=plain_qp_no8_av1u_NE_AEP.1550 shost=user2@test.com suser=
user2@test.com cn2Label=Filter_Action_Result cn2=21 deviceFaci
lity=Deep Discovery Email Inspector src=10.206.155.122 reason=
B,G ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C036
0-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windows 7 6.1 (B
uild 7601) Service Pack 1
```

フィルタ処理マッピングテーブル

値	説明
0	不明
1	該当なし
2	駆除
3	削除
4	移動
5	名前の変更
6	放置/ログ
7	削除 (ストリップ)
8	削除
9	隔離
10	挿入/置換
11	アーカイブ
12	スタンプ
13	ブロック
14	承認用メールのリダイレクト
81	暗号化
90	検出
257	リセット

フィルタ処理結果マッピングテーブル

値	説明
0	不明
1	なし
21	ファイルのウイルス駆除
22	ファイルの削除
23	ファイルの隔離
24	ファイル名の変更
25	ファイルの放置
26	ファイルのウイルス駆除不能。放置 (手動処理)
27	ファイルのウイルス駆除不能。削除
28	ファイルのウイルス駆除不能。拡張子変更
29	ファイルのウイルス駆除不能。隔離
30	ファイルの削除
31	ファイルのウイルス駆除不能。削除
32	ファイルの置換
33	ファイルの削除
34	ファイルのアーカイブ
35	ファイルのブロック成功
36	ファイルの隔離成功
37	ファイルのスタンプ成功
38	ファイルのアップロード
39	ファイルのウイルス駆除不能。隔離
40	ファイルのウイルス駆除不能。放置 (手動処理)

値	説明
41	アクセス拒否
42	処理なし
43	システムの再起動成功
44	スパイウェア/グレーウェアは安全でない状態で駆除されました。
45	検索の手動停止成功
46	承認用メールのリダイレクト成功
81	暗号化完了
121	ファイルのウイルス駆除不能
122	ファイルの削除不能
123	ファイルの隔離不能
124	ファイル名の変更不能
125	ファイルの放置不能
126	ファイルのウイルス駆除不能または放置不能
127	ファイルのウイルス駆除不能、または削除不能
128	ファイルのウイルス駆除不能、またはファイル名変更不能
129	ファイルのウイルス駆除不能、または隔離不能
130	ファイルの削除不能
131	ファイルのウイルス駆除または削除不能
132	ファイルの置換不能
133	ファイルの削除不能
134	ファイルのアーカイブ不能
135	ファイルのブロック不能
136	ファイルの隔離不能

値	説明
137	ファイルのスタンプ不能
138	ファイルのアップロード不能
139	ファイルのウイルス駆除不能、または隔離不能
140	ファイルのウイルス駆除不能または放置不能
141	アクセスの拒否不能
142	処理の実行不能
143	処理が必要 - エンドポイントを再起動し、セキュリティの脅威の駆除を完了してください
145	検索の手動停止不能
146	承認用メールのリダイレクト不能
201	処理が必要 – 完全なシステムスキャンを実行してください
202	処理が必要 - Apex One ツールボックスに含まれる「緊急起動ディスク」ツールを使用してこの脅威を取り除いてください。問題が解決しない場合は、テクニカルサポートに問い合わせてください。
203	処理が必要 - Apex One ツールボックスに含まれる「ルートキットバスター」ツールを使用してこの脅威を取り除いてください。問題が解決しない場合は、テクニカルサポートに問い合わせてください。
204	処理が必要 - Apex One ツールボックスに含まれる「調査ログ収集用ウイルス対策ツールキット」ツールを使用してこの脅威を取り除いてください。問題が解決しない場合は、テクニカルサポートに問い合わせてください。

CEF 情報漏えい対策ログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0

CEF キー	説明	値
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	イベント ID	700106
ヘッダ (eventName)	ログ名	Data Loss Prevention
ヘッダ (severity)	重大度	3
cs1Label	「cs1」フィールドに対応するラベル	「Policy GUID」
cs1	ポリシー GUID	例: FAF492CF-164C-4672-9A79-F1AB9CB288A3
cn1Label	「cn1」フィールドに対応するラベル	「Product」
cn1	製品の種類の値	例: 15
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
src	送信元ホスト IP アドレス	例: 10.0.57.160
smac	送信元ホスト MAC アドレス	例: 74-27-00-0C-65-E7
shost	送信元ホスト名	例: shost1
cs4Label	「cs4」フィールドに対応するラベル	「Incident_Source_(AD_Account)」
cs4	違反ユーザ名	例: Trend
suser	メール送信者	例: sender@example.com
request	アクセス先の URL	例: https://example.com/api/content
duser	受信者のコンマ (,) 区切りリスト	例: 「user1@example.com;user2@example.com;」

CEF キー	説明	値
msg	件名	例: 「Sample,20171017」
filepath	ファイルパス	例: 「D:\\Windows Live Mail\\Storage Folders\\Imported Fo e52\\Local Folders\\Sent Items\\Archive Aft de1\\Clients,Adv 22b\\」
fname	トリガファイル名	例: 「2B43363A-000000A4.eml」
fsize	ファイルサイズ (バイト)	例: 「3」
cs5Label	「cs5」フィールドに対応するラベル	「Rule」
cs5	ルール名	例: SAMPLE RULE SET
cs6Label	「cs6」フィールドに対応するラベル	「Template」
cs6	テンプレート名	例: 「Apex One policy」
cn3Label	「cn3」フィールドに対応するラベル	「Channel」
cn3	チャネルの種類	例: 「3」 詳細については、805 ページの「チャネルマッピングテーブル」を参照してください。
cn2Label	「cn2」フィールドに対応するラベル	「Action」
cn2	処理結果	例: 「4」 詳細については、803 ページの「処理結果マッピングテーブル」を参照してください。
cs2Label	「cs2」フィールドに対応するラベル	「Policy」
cs2	ポリシー名	例: 「OfficeScan」

CEF キー	説明	値
cs3Label	「cs3」フィールドに対応するラベル	「Product_Entity/Endpoint」
cs3	エンドポイントのホスト名	例: 「Sample_Host」
dvchost	サーバのホスト名	例: 「localhost」
deviceFacility	製品名	例: 「Apex One」
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
externalId	イベントのログ ID	例: 「101」
cfp1Label	「cfp1Label」フィールドに対応するラベル	「ForensicFileAvailable」
cfp1	フォレンジックファイルのダウンロードが可能かどうかを示す	• 0: ファイルをダウンロードできません • 1: ファイルをダウンロードできます
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|700106|Data Loss Prevent
ion|3|cs3Label=Product_Entity/Endpoint cs3=Sample_Host dvc
host=Sampledvchost cs2Label=Policy cs2=N/A cn1Label=Product
cn1=15 rt=Oct 13 2017 02:54:04 GMT+00:00 src=10.0.9.34 smac=
```

```
34-E6-D7-84-BC-7F shost=shost1 cs4Label=Incident_Source_(AD_
Account) cs4=12467 filePath=D:\\2. DRIVER\\drivers WIN7\\Dri
vers\\DP_CardReader_14032.7z\\O2Micro\\FORCED\\6x86\\ fname=
O2MDFvst.INF cs5Label=Rule cs5=SAMPLE RULE SET cs6Label=Temp
late cs6=Apex One policy cn3Label=Channel cn3=0 cn2Label=Act
ion cn2=4 deviceFacility=Apex One deviceNtDomain=APEXTMCM dn
tdom=OSCEDomain1 externalId=101 cfp1Label=ForensicFileAvaila
ble cfp1=0 dvchost=localhost TMCMLogDetectedHost=ApexOneClie
nt01 TMCMLogDetectedIP=10.201.86.187 ApexCentralHost=TW-CHRI
S-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
 TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack
 1
```

処理結果マッピングテーブル

値	説明
-1	使用不可
0	ブロック
1	削除
2	配信
3	ログ
4	放置 (手動処理)
5	隔離
6	置換
7	アーカイブ
8	アーカイブ (メッセージ本文のみ)
9	隔離 (メッセージ本文のみ)
10	放置 (メッセージ本文のみ)
11	暗号化
12	アラート (エンドポイント)

値	説明
13	アラート (サーバ)
14	データを記録
15	ユーザが承認
16	中継
17	受信者を変更
18	BCC
19	配信を保留
20	スタンプの挿入
21	添付ファイルの削除
22	件名へのタグの挿入
23	X-ヘッダへのタグの挿入
24	復号化
25	再暗号化
26	タグ (メール)
27	暗号化 (ユーザキー)
28	暗号化 (グループキー)
29	移動
30	放置 (暗号化)
31	放置 (ユーザが承認)
32	ブロック (Endpoint Encryption がインストールされていません)
33	ブロック (ユーザが承認)
34	ブロック (Endpoint Encryption ログオフ)
35	ブロック (Endpoint Encryption エラー)

値	説明
36	Web アップロード

チャネルマッピングテーブル

値	説明
65535	使用不可
0	リムーバブルストレージ
1	SMB
2	メール
3	IM
4	FTP
5	HTTP
6	HTTPS
7	PGP
8	データレコーダー
9	プリンタ
10	クリップボード
11	同期
12	P2P
13	Web メール
14	ドキュメント管理
15	クラウドストレージ
121	SMTP メール
122	Exchange クライアントメール

値	説明
123	Lotus Note メール
130	Web メール (Yahoo!メール)
131	Web メール (Hotmail)
132	Web メール (Gmail)
133	Webmail (AOL メール)
140	IM (MSN)
141	IM (AIM)
142	IM (Yahoo メッセンジャー)
143	IM (Skype)
191	P2P (BitTorrent)
192	P2P (EMule)
193	P2P (Winny)
194	P2P (HTCSYN)
195	P2P (iTunes)
196	クラウドストレージ (DropBox)
197	クラウドストレージ (Box)
198	クラウドストレージ (Google Drive)
199	クラウドストレージ (OneDrive)
200	クラウドストレージ (SugarSync)
201	クラウドストレージ (Hightail)
202	インスタントメッセンジャー (QQ)
203	Web メール (その他)
204	クラウドストレージ (Evernote)

値	説明
211	ドキュメント管理 (SharePoint)

CEF デバイスアクセス管理ログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	イベント ID	700107
ヘッダ (eventName)	ログ名	Device Access Control
ヘッダ (severity)	重大度	3
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
cs1Label	「cs1」フィールドに対応するラベル	「Product Entity/Endpoint」
cs1	サーバのホスト名	例: 「Sample_Host」
shost	送信元ホスト名	例: 「shost1」
duser	ユーザ名	例: 「testserver\\administrator」
dvchost	対象ホスト名	例: 「localhost」
cn1Label	「cn1」フィールドに対応するラベル	「Product」

CEF キー	説明	値
cn1	製品 ID	例: 「Apex One」 詳細については、809 ページの「製品 ID マッピングテーブル」を参照してください。
sproc	対象プロセス	例: 「C:\\Windows\\explorer.exe」
fname	ファイル名	例: 「F:\\Autorun.inf」
cn2Label	「cn2」フィールドに対応するラベル	「Device_Type」
cn2	デバイスの種類	例: 「0」 • 0: USB ストレージデバイス • 1: 非ストレージ USB • 2: CD/DVD • 3: フロッピーディスク • 4: ネットワークドライバ
cn3Label	「cn3」フィールドに対応するラベル	「Permission」
cn3	権限	例: 「3」 • 0: 変更 • 1: 読み取りおよび実行 • 2: 読み取り • 3: デバイスの内容のみのリスト表示 • 4: ブロック
deviceFacility	製品名	例: 「Apex One」
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1

CEF キー	説明	値
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|700107|Device Access C
ontrol|3|rt=Aug 16 2017 04:49:15 GMT+00:00 cs1Label=Product_
Entity/Endpoint cs1=Sample_Host shost=shost1 dvchost=localho
st cn1Label=Product cn1=15 sproc=C:\\Windows\\explorer.exe f
name=F:\\Autorun.inf cn2Label=Device_Type cn2=0 cn3Label=Per
mission cn3=3 deviceFacility=Apex One deviceNtDomain=APEXTMC
M dntdom=OSCEDomain1 TMCMLogDetectedHost=shost1 TMCMLogDetec
tedIP=10.0.76.40 ApexCentralHost=TW-CHRIS-W2019 devicePayloa
dId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform
=Windows 7 6.1 (Build 7601) Service Pack 1
```

製品 ID マッピングテーブル

値	説明
0	未知の製品
1	ScanMail for ccMail
2	InterScan for Lotus Domino
3	InterScan for Microsoft Exchange
4	ScanMail for Microsoft Mail

値	説明
5	InterScan for OpenMail
6	Reserved 1
7	Reserved 2
8	Reserved 3
9	Reserved 4
10	InterScan WebProtect
11	Reserved 5
12	Reserved 6
13	Reserved 7
14	PC-cillin Corporate Edition
15	Apex One
16	Apex One for Microsoft SBS
18	ServerProtect for Windows
19	ServerProtect for Windows (SOHO)
20	Apex Central
21	汎用
22	InterScan VirusWall for UNIX
23	InterScan VirusWall for Windows
24	MOCA
25	Golden Gate
26	ActiveUpdate
27	IS_Y2K_SCANNER
28	Y2K VIRUS TECH SUPPORT SRV

値	説明
30	HouseCall
31	PC-cillin ISP サーバ
32	PC-cillin ISP クライアント
33	eManager for ScanMail Exchange
34	InterScan Messaging Security Suite Windows 版
35	InterScan Messaging Security Suite UNIX 版
36	Portalprotect
37	GateLock Corporate Edition
38	ファイアウォール管理 (NetScreen)
39	InterScan Web Security Suite Solaris 版
40	InterScan Web Security Suite Windows NT 版
41	Nokia Message Protector
42	InterScan Web Security Suite Linux 版
43	InterScan Web Security Suite Appliance 版
44	InterScan Messaging Security Appliance
45	InterScan for Small and Medium Business Windows NT 版
46	InterScan Web Security Virtual Appliance
47	InterScan Messaging Security Virtual Appliance
50	InterScan Gateway Security Appliance
51	ServerProtect for Linux
52	ServerProtect for EMC
53	ServerProtect for NetApp
56	下位 Apex Central サーバ

値	説明
60	ダメージクリーンナップサービス
65	Golden Gatefor NT
66	Network VirusWall 1200
67	Network VirusWall MIPS
68	Network VirusWall 2500
69	Network VirusWall 2500 v2
70	脆弱性診断サービス
71	Network Virus Wall Enforcer 1200
72	Network VirusWall Enforcer
73	Network VirusWall Enforcer
75	Trend Micro Threat Mitigator
85	Anti-Spyware Enterprise Edition
87	Trend Micro InterScan for Cisco CSC SSM-20
88	Trend Micro InterScan for Cisco CSC SSM-10
90	IM Security
95	InterScan VirusWall スタンダードエディション
96	InterScan VirusWall スタンダードエディション Linux 版
100	Control Manager エージェント
200	eDoctor Server
300	eDoctor Agent
132	InterScan Messaging Security Suite Solaris 版
120	Threat Discovery Appliance
131	Database Protect for Linux

値	説明
151	Total Discovery Mitigation Server
154	Deep Discovery Inspector
155	InterScan for IBM Domino
156	Deep Discovery Email Inspector
1000	InterScan eManager
1001	InterScan AppletTrap
1002	InterScan VirusWall Java
1003	IS_SEMAIL
1004	InterScan WebProtect for ICAP
10001	NEC StarOffice
20001	Dr. Soloman Anti-virus
20002	Inoculan
20003	Norton Anti-virus
20004	Sophos SWEEP
20005	Intel LANProtect
20006	McAfee Virus Scan
20007	FProt
21000	その他のサードパーティ製品
31001	Apex One (Mac)
31002	Trend Micro Endpoint Encryption
31003	Trend Micro Endpoint Application Control
31004	Trend Micro Deep Security
31006	仮想パッチ

値	説明
31005	Trend Micro Mobile Security
31007	Trend Micro Safe Mobile Workforce
31008	Deep Discovery Analyzer
31009	Trend Micro Endpoint Sensor
31012	Deep Discovery Web Inspector
31101	Trend Micro Email Security
31102	ウイルスバスター ビジネスセキュリティサービス
31103	Trend Micro Web Security as a Service
31104	Cloud App Security
55555	デモ製品

CEF Endpoint Application Control のログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	デバイスイベントクラス ID	• 0: 許可 • 1: ブロック • 2: ロックダウン
ヘッダ (eventName)	イベント名	Endpoint Application Control Violation Information
ヘッダ (severity)	重大度	3

CEF キー	説明	値
deviceExternalId	ID	例: 「39」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
dvchost	コンピュータ名	例: 「localhost」
shost	クライアントホスト名	例: 「shost1」
cs1	製品サーバのパターンファイルバージョン	例: 「1297」
suser	クライアントのユーザ名	例: 「TREND\User」
cs2	クライアントの IPv4 アドレス	例: 「10.0.17.6」
c6a3	クライアントの IPv6 アドレス	例: 「fe80::38ca:cd15:443c:40bb%11」
cn1	クライアントのステータス	• 1: データベースを再構築しています • 2: オンライン • 3: オフライン
filehash	アプリケーションのファイル SHA-1 ハッシュ	例: 「D6712CAE5EC821F910E14945153AE7871AA536CA」
fname	アプリケーションファイル名	例: 「notepad.exe」
cs3	アプリケーションのプロセスコマンドライン	例: 「notepad.exe」
duser	ユーザ名	例: 「Admin004」
cs4	ルール名	例: 「SAMPLE RULE SET」
cs5	ポリシー名	例: 「SAMPLE POLICY」

CEF キー	説明	値
act	ポリシー処理	• 0: 許可 • 1: ブロック • 2: 許可として報告 • 3: ブロックとして報告
deviceFacility	製品名	例: 「Trend Micro Endpoint Application Control」
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|EAC:1|Endpoint Applica
tion Control Violation Information|3|deviceExternalId=39 rt=
Jun 27 2012 03:14:03 GMT+00:00 cs1Label=Version cs1=1.299.00
 suser=TMCM\\QA cs2Label=ApplicationControlEvent_ClientIPAdd
ress_V4 cs2=0.0.0.0 cn1Label=Connection_Status cn1=0 fileHas
h=c0869b72C5606D22D92A6AC986686BB87485A25b fname=P2P_TEST.ex
e cs3Label=Command cs3=C:\\P2P_TEST.exe duser=QA cs4Label=Ru
le cs4=Test cs5Label=Policy cs5=TestPolicy act=Blocked devic
eFacility=Trend Micro Endpoint Application Control deviceNtD
omain=APEXTMCM dntdom=OSCEDomain1 ApexCentralHost=TW-CHRIS-
W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack
1
```

CEF 検索エンジンアップデートステータスのログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	製品ベンダ	Trend Micro
ヘッダ (pname)	製品名	Apex Central
ヘッダ (pver)	製品バージョン	2019
ヘッダ (eventid)	イベント ID	800102
ヘッダ (eventName)	ログ名	Engine Update Status
ヘッダ (severity)	重大度	3
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
shost	製品のエンティティ名/エンドポイント	例: 「shost1」
cs2Label	「cs2」フィールドに対応するラベル	「Product/Endpoint IP」
cs2	製品/エンドポイント IP	例: 「10.0.17.6」
cn1Label	「cn1」フィールドに対応するラベル	「Connection Status」
cn1	接続ステータス	例: 「100」 • 0: 接続不可能 • 1: 稼動中 • 2: 停止中 • 100: 製品稼動中 • 101: 製品停止中、エージェント稼動中 • 102: ローミング

CEF キー	説明	値
cn2Label	「cn2」フィールドに対応するラベル	「Engine」
cn2	検索エンジン	例: 「4096」
cn5Label	「cn5」フィールドに対応するラベル	「Engine Version」
cs5	検索エンジンバージョン	例: 「9.950.1006」
cn3Level	「cn3」フィールドに対応するラベル	「Engine Status」
cn3	検索エンジンのステータス	例: 「1」 • 1: 最新バージョン • 2: 旧バージョン
cs6Label	「cs6」フィールドに対応するラベル	「AUComponent_Type」
cs6	ActiveUpdate コンポーネントの種類	例: 「1」 • 1: 検索エンジン
deviceFacility	管理下の製品の名前	例: 「Apex One」
msg	検索エンジンの種類の表示名	例: ウイルス検索エンジン DLL (Windows 2000/NT、32 ビット)
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|800102|Engine Update S
tatus|3|rt=Apr 20 2017 12:04:34 GMT+00:00 shost=shost1 cs2La
bel=Product/Endpoint_IP cs2=10.0.17.6 cn1Label=Connection_St
```

```
atus cn1=100 cn2Label=Engine cn2=4096 cs5Label=Engine_Versio
n cs5=9.950.1006 cn3Label=Engine_Status cn3=1 cs6Label=AUCom
ponent_Type cs6=1 deviceFacility=Apex One deviceNtDomain=APE
XTMCM dntdom=OSCEDomain1
```

CEF 侵入防御イベントログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	製品ベンダ	Trend Micro
ヘッダ (pname)	製品名	Apex Central
ヘッダ (pver)	製品バージョン	2019
ヘッダ (eventid)	イベント ID	
ヘッダ (eventName)	ログ名	
ヘッダ (severity)	重大度	3
dvchost	管理下のエンドポイントの表示名	例: 「localhost」
rt	ログ生成日時 (UTC)	例: 「Nov 15 2017 08:43:57 GMT +00:00」
src	送信元 IPv4 アドレス	例: 10.1.152.12
c6a2Label	「c6a2」フィールドに対応するラベル	SLF_SourceIPv6
c6a2	送信元 IPv6 アドレス	2001:b011:1004:325b:8db7:6ca9:8fc5:321a
smac	送信元 MAC アドレス	例: 18:31:BF:4F:30:DD
spt	送信元ポート	例: 60886
dst	送信先 IPv4 アドレス	例: 10.1.153.151

CEF キー	説明	値
c6a3Label	「c6a3」フィールドに対応するラベル	SLF_DestinationIPv6
c6a3	送信先 IPv6 アドレス	例: 2001:b011:1004:325b:8db7:6ca9:8fc5:654a
dmac	送信先ホスト MAC アドレス	例: D0:17:C2:95:ED:71
dpt	送信先ポート	例: 139
cn2Label	「cn2」フィールドに対応するラベル	SLF_IsDetectionOnly
cn2	システムが「検出のみ」モードであるかどうかを示す	例: 0 • 0 または NULL = No • 1 = Yes
act	処理	例: LOG SLF_ACTION マップ: • 0 =不明 • 3 =削除 • 6 =ログ • 10 =挿入/置換 • 13 =ブロック • 257 =リセット
deviceDirection	受信方向または送信方向	例: Apex One
cn3Label	「cn3」フィールドに対応するラベル	SLF_Rank
cn3	イベントの重み付けされた優先度	例: 3 重大度 x アセット値から算出
cn4Label	「cn4」フィールドに対応するラベル	SLF_SeverityCode

CEF キー	説明	値
cn4	システム定義のイベント重大度値	例: 1 • 1 =低 • 2 =中 • 3 =高 • 4 =重大
proto	脆弱性を利用されているネットワークプロトコル	例: 10009 • 28 = ICMP • 46 = ICMPv6 • 10003 = TCP • 10004 = UDP • 10005 = IGMP • 10006 = GGP • 10007 = PUP • 10008 = IDP • 10009 = ND • 10010 = RAW
cs2Label	「cs2」フィールドに対応するラベル	SLF_ConnectionType
cs2	ネットワークアプリケーション名	例: DCERPC Services
cn1Label	「cn1」フィールドに対応するラベル	SLF_RuleID
cn1	監視ルールの ID	例: 1005448
cs1Label	「cs1」フィールドに対応するラベル	SLF_RuleContent
cs1	ルール ID および説明の文字列リテラル	例: 1005448 - SMB Null Session Detected - 1

CEF キー	説明	値
cnt	集計数	例: 1
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|Log|1009549 - Detected T
erminal Services (RDP) Server Traffic - 1 (ATT&CK T1015,T104
3,T1076,T1048,T1032,T1071)|3|rt=Apr 20 2020 03:33:20 GMT+00:
00 dvchost=OSCEClient23 deviceFacility=Apex One act=Log,src=
10.1.1.9 dst=80.1.1.9 smac=54-BF-64-84-7F-09 spt=89 dmac=54-
BF-64-84-7F-19 dpt=449 cn2Label=SLF_IsDetectionOnly cn2=0 de
viceDirection=Inbound cn3Label=SLF_Rank cn3=1 cn4Label=SLF_S
everityCode cn4=1 proto=10009 cs2Label=SLF_ConnectionType cs
2=N/A cn1Label=SLF_RuleID cn1=1009549 cs1Label=SLF_RuleConte
nt cs1=1009549 - Detected Terminal Services (RDP) Server Tra
ffic - 1 (ATT&CK T1015,T1043,T1076,T1048,T1032,T1071) cnt=1
deviceNtDomain=APEXTMCM dntdom=OSCEDomain1
```

CEF 管理下の製品のログオン/ログオフイベント

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	イベント ID	700211
ヘッダ (eventName)	ログ名	Managed Product Logon/Logoff Events
ヘッダ (severity)	重大度	3

CEF キー	説明	値
deviceExternalId	ID	例: 「38」
deviceFacility	製品名	例: 「InterScan for Microsoft Exchange」
cs1Label	「cs1」フィールドに対応するラベル	Product_Version
cs1	製品バージョン	例: 「14」
cn1Label	「cn1」フィールドに対応するラベル	Command_Status
cn1	コマンドステータス	例: 「110」
msg	詳細なイベント情報	例: 「Sample Message」
shost	製品サーバ名	例: 「SMEX01」

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|700211|Managed Product L
ogon/Logoff Events|3|deviceExternalId=11 shost=SMEX01 device
Facility=ScanMail for Microsoft Exchange cs1Label=Product_Ve
rsion cs1=14 cn1Label=Command_Status cn1=110 msg=A user with
 the Administrator role(s) has logged on.Detail Information
:UserName:TEST2013\\administrator,IP address:10.204.166.127,
EventType:Log in/out,SourceType:SMEX UI.#015
```

CEF ネットワークコンテンツ検査のログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019

CEF キー	説明	値
ヘッダ (eventid)	NCIE: 処理	NCIE:Pass
ヘッダ (eventName)	名前	Suspicious Connection
ヘッダ (severity)	重大度	3
deviceExternalId	ID	例: 「1」
cat	ログの種類	例: 「1756」
deviceFacility	製品	例: 「Apex One」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
deviceProcessName	プロセス	例: 「C:\\Windows\\system32\ \svchost-1.exe」
src	ローカル IPv4 アドレス	例: 「10.201.86.152」
c6a2Label	「c6a2」フィールドに対応するラベル	例: 「SLF_SourceIP」
c6a2	ローカル IPv6 アドレス	例: 「2620:101:4003:7a0:fd4b:52ed:53bd:ae3d」
spt	ローカル IP アドレスポート番号	例: 「54594」
dst	リモート IPv4 アドレス	例: 「10.69.81.64」
c6a3Label	「c6a3」フィールドに対応するラベル	例: 「SLF_DestinationIP」
c6a3	リモート IPv6 アドレス	例: 「fe80::38ca:cd15:443c:40bb%11」
dpt	リモート IP アドレスポート番号	例: 「80」

CEF キー	説明	値
act	処理	例: 「1」 • 0: 不明 • 1: 放置 • 2: ブロック • 3: 監視 • 4: 削除 • 5: 隔離 • 6: 警告 • 7: 警告して続行 • 8: オーバーライド
deviceDirection	トラフィックの方向	例: 「1」 • 0: なし • 1: 受信 • 2: 送信
cn1Label	「cn1」フィールドに対応するラベル	例: 「SLF_PatternType」
cn1	パターンファイルの種類	例: 「2」 • 0: グローバル C&C パターンファイル • 1: 適合度ルール • 2: ユーザ指定ブロックリスト
cs2Label	「cs2」フィールドに対応するラベル	例: 「NCIE_ThreatName」
cs2	脅威の名前	例: 「Malicious_identified_CnC_querying_on_UDP_detected」

CEF キー	説明	値
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
dvchost	ホスト名	例: localhost
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|NCIE:Pass|Suspicious
Connection|3|deviceExternalId=1 rt=Oct 11 2017 06:34:06 GMT+0
0:00 cat=1756 deviceFacility=Apex One deviceProcessName=C:\\W
indows\\system32\\svchost-1.exe act=Pass src=10.201.86.152 ds
t=10.69.81.64 spt=54594 dpt=80 deviceDirection=None cn1Label=
SLF_PatternType cn1=2 cs2Label=NCIE_ThreatName cs2=Malicious_
```

```
identified_CnC_querying_on_UDP_detected reason=F deviceNtDoma
in=APEXTMCM dntdom=OSCEDomain1 dvchost=shost1 TMCMLogDetected
Host=shost1 TMCMLogDetectedIP=10.1.2.3ApexCentralHost=TW-CHRI
S-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF パターンファイルアップデートステータスのログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	製品ベンダ	Trend Micro
ヘッダ (pname)	製品名	Apex Central
ヘッダ (pver)	製品バージョン	2019
ヘッダ (eventid)	イベント ID	800101
ヘッダ (eventName)	ログ名	Pattern Update Status
ヘッダ (severity)	重大度	3
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
shost	製品のエンティティ名/エンドポイント	例: 「shost1」
cs1Label	「cs1」フィールドに対応するラベル	「OS」
cs1	OS	例: 「Windows 7」
cs2Label	「cs2」フィールドに対応するラベル	「Product/Endpoint IP」
cs2	製品/エンドポイント IP	例: 「10.0.7.20」

CEF キー	説明	値
cs3Label	「cs3」フィールドに対応するラベル	「Update Agent」
cs3	アップデートエージェント	例: 「0」
cs4Label	「cs4」フィールドに対応するラベル	「Domain」
cs4	ドメイン	例: 「Default」
cn1Label	「cn1」フィールドに対応するラベル	「Connection Status」
cn1	接続ステータス	例: 「100」 • 0: 接続不可能 • 1: 稼動中 • 2: 停止中 • 100: 製品稼動中 • 101: 製品停止中、エージェント稼動中 • 102: ローミング
cn2Label	「cn2」フィールドに対応するラベル	「Pattern/Rule」
cn2	パターンファイル/ルール	例: 「2048」
cs5Label	「cs5」フィールドに対応するラベル	「Pattern/Rule Version」
cs5	パターンファイル/ルールのバージョン	例: 「1548」
cn3Label	「cn3」フィールドに対応するラベル	「Pattern/Rule Status」

CEF キー	説明	値
cn3	パターンファイル/ルールのステータス	例: 「1」 • 1: 最新バージョン • 2: 1 つ前のバージョン • 3: 2 つ前のバージョン • 4: 3 つ前のバージョン • 5: 4 つ前のバージョン • 6: 5 つ前のバージョン • 7: 6 つ以上前のバージョン
cs6Label	「cs6」フィールドに対応するラベル	「AUComponent_Type」
cs6	ActiveUpdate コンポーネントの種類	例: 「2」 • 2: パターンファイル
deviceFacility	管理下の製品の名前	例: 「Apex One」
msg	パターンファイルの種類の表示名	例: Virus Pattern
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|800101|Pattern Update
Status|3|rt=Nov 02 2017 12:46:44 GMT+00:00 shost=shost1 cs1L
abel=Operating_System cs1=Windows 7  cs2Label=Product/Endpoi
nt_IP cs2=10.0.7.20 cs3Label=Update_Agent cs3=0 cs4Label=Dom
ain cs4=Default cn1Label=Connection_Status cn1=100 cn2Label=
Pattern/Rule cn2=2048 cs5Label=Pattern/Rule_Version cs5=1548
 cn3Label=Pattern/Rule_Status cn3=1 cs6Label=AUComponent_Typ
```

```
e cs6=2 deviceFacility=Apex One deviceNtDomain=APEXTMCM dntd
om=OSCEDomain1
```

CEF 機械学習型検索ログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	製品ベンダ	Trend Micro
ヘッダ (pname)	製品名	Apex Central
ヘッダ (pver)	製品バージョン	2019
ヘッダ (eventid)	PML: 処理結果	PML:File cleaned
ヘッダ (eventName)	検出名	virusa
ヘッダ (severity)	重大度	3
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
dvchost	製品サーバ	例: 「Sample_Host」
cn1Label	「cn1」フィールドに対応するラベル	「ThreatType」
cn1	潜在的な脅威の種類	例: 「35.143」 詳細については、834 ページの「脅威の種類のマッピングテーブル」を参照してください。
cs2Label	「cs2」フィールドに対応するラベル	「DetectionName」
cs2	セキュリティの脅威	例: 「Troj.Win32.TRX.XXPE002FF017」
shost	感染エンドポイント	例: 「10.0.0.1」
suser	ログオンユーザ	例: 「TREND\\User」

CEF キー	説明	値
cn2Label	「cn2」フィールドに対応するラベル	「DetectionType」
cn2	検出の種類	例: 「0」 • 0: ファイル • 1: プロセス
filePath	ファイルパス	例: "D:\\"
fname	ファイル名	例: ALCORMP.EXE
deviceCustomDate1	ファイル作成日時	例: 「2017-04-26 05:53:27.000」
sproc	システムプロセス	例: 「notepad.exe」
cn4Label	「cn4」フィールドに対応するラベル	「ProcessCommandLine」
cs4	プロセスコマンド	例: 「notepad.exe」
duser	プロセス所有者	例: 「user1」
app	感染経路	例: 「10」 • 0: 不明 • 1: ローカルドライブ • 2: ネットワークドライブ • 3: 自動実行ファイル • 10: Web • 11: メール • 999: ローカルまたはネットワークドライブ
cs3Label	「cs3」フィールドに対応するラベル	「InfectionLocation」
cs3	感染元	例: 「http://10.0.0.1/」

CEF キー	説明	値
dst	製品/エンドポイントの IPv4 アドレス	例: 「10.0.17.6」
c6a3Label	「c6a3」フィールドに対応するラベル	「Product/Endpoint IP」
c6a3	製品/エンドポイントの IPv6 アドレス	例: 「fd66:5168:9882:6:b5b0:b2b5:4173:3f5d」
cn3Label	「cn3」フィールドに対応するラベル	「Confidence」
cn3	脅威の可能性	例: 「82」
act	処理結果	例: 「21」 詳細については、844 ページの「処理マッピングテーブル」を参照してください。
filehash	ファイル SHA-1	例: 「52c17c785b45ee961f68fb17744276076f383085」
dhost	製品のエンティティ名/エンドポイント	例: 「dhost1」
deviceExternalId	ログの番号	例: 「100」
deviceFacility	製品	例: 「Apex One」

CEF キー	説明	値
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|PML:File cleaned|Detecti
on01|3|deviceExternalId=1 rt=Dec 01 2018 16:01:00 GMT+00:00
deviceFacility=15 dvchost=OSCE01 cn1Label=ThreatType cn1=1 c
s2Label=DetectionName cs2=Detection01 shost=10.0.0.1 suser=S
ample_Domain\\Sample_User cn2Label=DetectionType cn2=0 fileP
ath=C:\\test01\\aaa.exe fname=aaa.exe deviceCustomDate1Label
=FileCreationDate deviceCustomDate1=Dec 02 2018 00:01:00 GMT
+00:00 sproc=notepad.exe cs4Label=ProcessCommandLine cs4=not
```

```
epad.exe -test duser=admin01 app=1 cs3Label=InfectionLocatio
n cs3=https://10.1.1.1 dst=80.1.1.1 cn3Label=Confidence cn3=
81 act=21 fileHash=177750B65A21A9043105FD0820B85B58CF148A01
dhost=OSCEClient11 reason=E deviceNtDomain=APEXTMCM dntdom=O
SCEDomain1 TMCMLogDetectedHost=OSCEClient11 TMCMLogDetectedI
P=80.1.1.1 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C
00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windo
ws 7 6.1 (Build 7601) Service Pack 1
```

脅威の種類のマッピングテーブル

値	説明
35140	アドウェア
35141	バックドア
35142	ブラウザ改ざんウイルス
35143	DDoS
35144	ダイヤラー
35145	攻撃コード
35146	ハッキングツール
35147	ジョークプログラム
35148	PUA
35149	ランサムウェア
35150	ルートキット
35151	スパイウェア
35152	トロイの木馬
35153	トロイの木馬型クリッカ
35154	トロイの木馬型ダウンローダ
35155	トロイの木馬型ドロッパ

値	説明
35156	トロイの木馬型プロキシ
35157	トロイの木馬型スパイウェア
35158	ファイル感染型ウイルス
35159	ワーム
35160	システム領域感染型ウイルス

CEF 製品監査イベント

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	製品ベンダ	Trend Micro
ヘッダ (pname)	製品名	Apex Central
ヘッダ (pver)	製品バージョン	2019
ヘッダ (eventid)	イベント ID	1745
ヘッダ (eventName)	ログ名	製品監査イベント
ヘッダ (severity)	重大度	3
cat	ログの種類	1745
deviceFacility	管理下の製品	例: 「Apex One」
dvchost	管理下のエンドポイントの表示名	例: 「localhost」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
cn1Label	「cn1」フィールドに対応するラベル	SLF_CategoryID

CEF キー	説明	値
cn1	カテゴリ ID	例: 「536,870,912」
cn2Label	「cn2」フィールドに対応するラベル	SLF_SeverityLevel
cn2	重大度レベル	例: 「4」 • 1 =エラー • 2 =警告 • 4 =情報 • 16 =監査失敗
suser	イベントを発生させたユーザの名前	例: administrator
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|Delete|1009490 - Block A
dministrative Share - 1 (ATT&CK T1077,T1105)|3|rt=Apr 20 202
0 03:33:15 GMT+00:00 dvchost=OSCEClient22 deviceFacility=Ape
x One act=Delete, src=10.1.1.8 dst=80.1.1.8 smac=54-BF-64-84
-7F-08 spt=88 dmac=54-BF-64-84-7F-18 dpt=448 cn2Label=SLF_Is
DetectionOnly cn2=1 deviceDirection=Outbound cn3Label=SLF_Ra
nk cn3=100 cn4Label=SLF_SeverityCode cn4=4 proto=10008 cs2La
bel=SLF_ConnectionType cs2=Suspicious Client Application Act
ivity cn1Label=SLF_RuleID cn1=1009490 cs1Label=SLF_RuleConte
nt cs1=1009490 - Block Administrative Share - 1 (ATT&CK T107
7,T1105) cnt=1 deviceNtDomain=APEXTMCM dntdom=OSCEDomain1
```

CEF サンドボックス検出ログ

注意

サンドボックス検出ログは、Apex Central 管理コンソールでは「仮想アナライザによる検出」と表記されます。

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	デバイスイベントクラス ID	VAD
ヘッダ (eventName)	イベント名	Virtual Analyzer detection name
ヘッダ (severity)	重大度	3
deviceExternalId	ID	例: 「2」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
deviceFacility	製品	例: 「Apex One」
dvchost	サーバ名	例: 「OSCE01」
dhost	エンドポイント名	例: 「Isolate-ClientA」
dst	エンドポイントの IPv4 アドレス	例: 「10.0.17.6」
c6a3	エンドポイントの IPv6 アドレス	例: 「fe80::38ca:cd15:443c:40bb%11」
app	エントリチャネル	例: 「0」 詳細については、864 ページの「プロトコルマッピングテーブル」を参照してください。

CEF キー	説明	値
sourceServiceName	ソース	例: 「Test1@tmcm.extbeta.com」
destinationServiceName	配信先	例: 「Test2@tmcm.extbeta.com;Test3@tmcm.extbeta.com」
sproc	プロセス名	例: 「VA」
fileHash	ファイル SHA-1 ハッシュ	例: 「D6712CAE5EC821F910E14945153AE7871AA536CA」
fname	ファイル名	例: 「C:\\\\QA_Log.zip」
request	URL	例: 「http://127.1.1.1」
cs1	仮想アナライザによって判別されたセキュリティの脅威の名前	例: 「VAN_RANSOMWARE.umxxhelloransom_abc」
cn1	仮想アナライザによって割り当てられたリスクレベルを示します。	例: 「0」 • 0: リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高 • 9999: 不明
cs2	セキュリティの脅威の種類を示します。	例: 「Anti-security, self-preservation」

CEF キー	説明	値
cs3	クラウドストレージベンダ	例: 「Google Drive」 • Dropbox • Box • Google Drive • Microsoft OneDrive • SugarSync • Hightail • Evernote • Microsoft Exchange Online • Microsoft SharePoint Online • Unknown • N/A
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName

CEF キー	説明	値
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF: 0|Trend Micro|Apex Central|2019|VAD|VAN_RANSOMWARE.um
xxhelloransom_abc|3|deviceExternalId=2 rt=Mar 22 2018 08:23:
23 GMT+00:00 deviceFacility=Apex One dvchost=OSCE01 dhost=
Isolate-ClientA dst=0.0.0.0 app=1 sourceServiceNameTest1@tre
nd.com.tw destinationServiceName=Test2@tmcm.extbeta.com;Test
3@tmcm.extbeta.com sproc=VA fileHash=3395856CE81F2B7382DEE72
602F798B642F14140 fname=C:\\\\QA_Log.zip request=http://127.
1.1.1 cs1Label=Security_Threat cs1=VAN_RANSOMWARE.umxxhellor
ansom_abc cn1Label=Risk_Level cn1=0 cs2Label=Threat_Categori
es cs2=Anti-security, self-preservation cs3Label=Cloud_Servi
ce_Vendor cs3=Google Drive reason=E deviceNtDomain=APEXTMCM
dntdom=OSCEDomain1 TMCMLogDetectedHost=OSCEClient TMCMLogDe
tectedIP=0.0.0.0 ApexCentralHost=TW-CHRIS-W2019 devicePaylo
adId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatfor
m=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF スパイウェア/グレーウェアのログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central

CEF キー	説明	値
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	デバイスイベントクラス ID	Spyware Detected
ヘッダ (eventName)	イベント名	Spyware Detected
ヘッダ (severity)	重大度	3
cnt	検出数	例:「10」
rt	イベントトリガ時刻 (UTC)	例:「Mar 22 2018 08:23:23 GMT +00:00」
cn1Label	「cn1」フィールドに対応するラベル	例:「Pattern Type」
cn1	パターンファイルの種類	例:「1073741840」
cs1Label	「cs1」フィールドに対応するラベル	例:「VirusName」
cs1	スパイウェア/グレーウェア	例:「ADW_OPENCANDY」
cs2Label	「cs2」フィールドに対応するラベル	例:「EngineVersion」
cs2	検索エンジンバージョン	例:「6.2.3027」
cs5Label	「cs5」フィールドに対応するラベル	例:「ActionResult」
cs5	処理	例:「Reboot system successfully」 詳細については、844 ページの「処理マッピングテーブル」を参照してください。
cs6Label	「cs6」フィールドに対応するラベル	例:「PatternVersion」
cs6	パターンファイルバージョン	例:「1297」
cat	ログの種類	例:「1727」
dvchost	エンドポイントのホスト名	例:「ApexOneClient01」

CEF キー	説明	値
deviceExternalId	ID	例: 「3」
fname	リソース	例: 「F:\\Malware\\psas\\rsrc2.bin」
filePath	リソース	例: 「F:\\Malware\\psas\\rsrc2.bin」
dhost	エンドポイントのホスト名	例: 「ApexOneClient01」
dst	エンドポイントの IPv4 アドレス	例: 「50.8.1.1」
c6a3Label	「c6a3」フィールドに対応するラベル	例: 「SLP_DestinationIP」
c6a3	エンドポイントの IPv6 アドレス	例: 「fe80::38ca:cd15:443c:40bb%11」
fileHash	ファイル SHA-1	例: 「D6712CAE5EC821F910E14945153AE7871AA536CA」
deviceFacility	製品名	例: 「Apex One」
duser	ユーザ名	例: 「Admin004」
cn2Label	「cn2」フィールドに対応するラベル	例: 「Scan_Type」
cn2	検索の種類	例: 「ScanNow」 詳細については、846 ページの「スパイウェア検索の種類のマッピングテーブル」を参照してください。
cn3Label	「cn3」フィールドに対応するラベル	例: 「Security_Threat_Type」

CEF キー	説明	値
cn3	セキュリティの脅威の種類	例: 「Adware」 詳細については、847 ページの「スパイウェアのリスクの種類のマッピングテーブル」を参照してください。
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|Spyware Detected|Spywa
re Detected|3|deviceExternalId=3 rt=Oct 06 2017 08:39:46 GMT
+00:00 cnt=1 dhost=ApexOneClient01 cn1Label=PatternType cn1=
1073741840 cs1Label=VirusName cs1=ADW_OPENCANDY cs2Label=Eng
ineVersion cs2=6.2.3027 cs5Label=ActionResult cs5=Reboot sys
tem successfully cs6Label=PatternVersion cs6=1297 cat=1727 d
vchost=ApexOneClient01 fname=F:\\Malware\\psas\\rsrc2.bin fi
lePath=F:\\Malware\\psas\\rsrc2.bin dst=50.8.1.1 deviceFacil
ity=Apex One deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCM
LogDetectedHost=ApexOneClient01 TMCMLogDetectedIP=50.8.1.1
ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-
9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windows 7 6.1 (Bu
ild 7601) Service Pack 1
```

処理マッピングテーブル

値	説明
0	不明
1	該当なし
21	ファイルのウイルス駆除
22	ファイルの削除
23	ファイルの隔離
24	ファイル名の変更
25	ファイルの放置
26	ファイルのウイルス駆除不能。放置 (手動処理)
27	ファイルのウイルス駆除不能。ファイルの削除
28	ファイルのウイルス駆除不能。ファイル名の変更
29	ファイルのウイルス駆除不能。ファイルの隔離
31	ファイルのウイルス駆除不能。ファイルの削除
32	ファイルの置換
34	ファイルのアーカイブ
35	ブロックの成功
36	隔離の成功
37	追加情報がメール本文に正常に追加されました
38	ファイルのアップロード
39	ファイルのウイルス駆除不能。ファイルの隔離
40	ファイルのウイルス駆除不能。放置 (手動処理)
41	アクセス拒否
42	処理なし

値	説明
43	システムの再起動
44	スパイウェア/グレーウェアは安全でない状態で駆除されました。
45	検索の手動停止成功
46	承認用メールのリダイレクト成功
81	暗号化
121	ファイルのウイルス駆除不能
122	ファイルの削除不能
123	ファイルの隔離不能
124	ファイル名の変更不能
125	ファイルの放置不能
126	ファイルのウイルス駆除不能または放置不能
127	ファイルのウイルス駆除不能、または削除不能
128	ファイルのウイルス駆除不能、またはファイル名変更不能
129	ファイルのウイルス駆除不能、または隔離不能
130	添付ファイルの削除不能
131	添付ファイルのウイルス駆除不能、または削除不能
132	次のいずれかになります。 • ファイルの内容の置換不能 • 添付ファイル名がコンテンツルールと一致したため、名前が変更されました
134	ファイルのアーカイブ不能
135	ファイルのブロック不能
136	ファイルの隔離不能
137	メッセージ本文への追加情報の追加不能

値	説明
138	ファイルのアップロード不能
139	ファイルのウイルス駆除不能、または隔離不能
140	ファイルのウイルス駆除不能または放置不能
141	アクセスの拒否不能
142	検出のみの実行不能
143	処理が必要 - エンドポイントを再起動し、セキュリティの脅威の駆除を完了してください
144	未定義
145	検索の手動停止不能
146	承認用メールのリダイレクト不能
201	処理が必要 – 完全なシステムスキャンを実行してください
202	処理が必要 - ウイルスバスター Corp.に含まれる「緊急起動ディスク」ツールを使用してください
203	処理が必要 - ウイルスバスター Corp.ツールボックスに含まれる「ルートキットバスター」ツールを使用してこの脅威を取り除いてください。問題が解決しない場合は、テクニカルサポートに問い合わせてください。
204	処理が必要 - ウイルスバスター Corp.ツールボックスに含まれる「調査ログ収集用ウイルス対策ツールキット」ツールを使用してこの脅威を取り除いてください。問題が解決しない場合は、テクニカルサポートに問い合わせてください。

スパイウェア検索の種類のマッピングテーブル

値	説明
0	不明
1	該当なし

値	説明
11	リアルタイム検索
12	手動検索
13	予約検索
14	リアルタイムメール検索
15	リアルタイムデータベース検索
16	検索開始
17	カード検索
18	ダメージクリーンナップサービス
19	ストレージ検索

スパイウェアのリスクの種類のマッピングテーブル

値	説明
0	不明
1	トラックウェア
2	アドウェア
3	Cookie
4	ダイヤラー
5	低セキュリティ
6	一般
7	キーロガー
8	トロイの木馬
9	疑惑
10	ハイジャック

値	説明
11	パラサイト
12	ブラウザヘルパーオブジェクト (BHO)
13	LSP
15	URL ショートカット
16	ピアツーピアアプリケーション
17	ワーム
19	ダウンローダ
20	ウイルス
21	Eulaware
22	変種
23	中セキュリティ
24	高セキュリティ
25	脆弱性診断サービス

CEF 不審ファイルのログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	FH: 処理	FH:Log
ヘッダ (eventName)	名前	Suspicious Files

CEF キー	説明	値
ヘッダ (severity)	重大度	3
deviceExternalId	ID	例: 「1」
cat	ログの種類	例: 「1766」
deviceFacility	製品	例: 「Apex One」
cn1Label	「cn1」フィールドに対応するラベル	例: 「SLF_ProductVersion」
cn1	製品バージョン	例: 「11」
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
dst	エンドポイントの IPv4 アドレス	例: 「10.201.86.151」
c6a3Label	「c6a3」フィールドに対応するラベル	例: 「Endpoint IPv6 Address」
c6a3	エンドポイントの IPv6 アドレス	例: 「2620:101:4003:7a0:fd4b:52ed:53bd:ae3d」
dhost	エンドポイントのホスト名	例: 「APEX-ONE-CLIENT-1」
cs2Label	「cs2」フィールドに対応するラベル	例: 「SLF_TrueFileType」
cs2	ファイルタイプ	例: 「TEXT」
fileHash	ファイル SHA-1	例: 「D6712CAE5EC821F910E14945153AE7871AA536CA」
cs3Label	「cs3」フィールドに対応するラベル	例: 「SLF_FileSource」

CEF キー	説明	値
cs3	ファイルパス	例: 「C:\\Users\\Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\017545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE」
cn2Label	「cn2」フィールドに対応するラベル	例: 「SLF_SourceType」
cn2	C&C リストのソース	例: 「0」 • 0: サンドボックス • 1: ユーザ定義
act	処理	例: 「1」 • 1: ログ • 2: ブロック • 3: 隔離
cn3Label	「cn3」フィールドに対応するラベル	例: 「SLF_ScanType」
cn3	検索の種類	例: 「1」 • 1: 予約検索 • 2: 手動検索 • 3: ScanNow • 4: リアルタイム検索

CEF キー	説明	値
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|FH:Log|Suspicious File
s|3|deviceExternalId=1 rt=Nov 15 2016 02:47:21 GMT+00:00 cat
=1766 deviceFacility=Apex One cn1Label=SLF_ProductVersion cn
1=11 dst=10.201.86.151 dhost=APEX-ONE-CLIENT-1 cs2Label=SLF_
TrueFileType cs2=SLF_TrueFileType fileHash=D6712CAE5EC821F91
0E14945153AE7871AA536CA cs3Label=SLF_FileSource cs3=C:\\User
s\\Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\0
17545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE cn2Label=
```

```
SLF_SourceType cn2=0 act=Log cn3Label=SLF_ScanType cn3=1 rea
son=E deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDete
ctedHost=APEX-ONE-CLIENT-1 TMCMLogDetectedIP=10.201.86.151
ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-
9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windows 7 6.1 (Bu
ild 7601) Service Pack 1
```

CEF ウイルス/不正プログラムのログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	AV: 処理	AV:File renamed
ヘッダ (eventName)	ウイルス/不正コード名	JS_EXPLOIT.SMDN
ヘッダ (severity)	重大度	3
cnt	検出数	例: 「10」
dhost	エンドポイント	例: 「ApexOneClient01」
duser	ユーザ	例: 「Admin004」
act	処理	例: 「File renamed」 詳細については、844 ページの「処理マッピングテーブル」を参照してください。
rt	ログ生成日時 (UTC)	例: Oct 06 2017 08:39:46 GMT +00:00
cn1Label	「cn1」フィールドに対応するラベル	例: 「VLF_PatternNumber」

CEF キー	説明	値
cn1	パターンファイル/ルールのバージョン	例: 「920500」
cn2Label	「cn2」フィールドに対応するラベル	例: 「VLF_SecondAction」
cn2	2 次処理	例: 「3」 詳細については、857 ページの「2 次処理マッピングテーブル」を参照してください。
cs1Label	「cs1」フィールドに対応するラベル	例: 「VLF_FunctionCode」
cs1	検索の種類	例: 「12」 • 0: 不明 • 1: 該当なし • 11: リアルタイム検索 • 12: 手動検索 • 13: 予約検索 • 16: ScanNow • 17: カード検索 • 18: ダメージクリーンナップサービス • 19: ストレージ検索
cs2Label	「cs2」フィールドに対応するラベル	例: 「VLF_EngineVersion」
cs2	検索エンジンバージョン	例: 「9.500.1005」
cs3Label	「cs3」フィールドに対応するラベル	例: 「CLF_ProductVersion」
cs3	製品バージョン	例: 「11」

CEF キー	説明	値
cs4Label	「cs4」フィールドに対応するラベル	例: 「CLF_ReasonCode」
cs4	理由コード	例: 「virus log」
cs5Label	「cs5」フィールドに対応するラベル	例: 「VLF_FirstActionResult」
cs5	1 次処理結果	例: 「Unable to clean file」 詳細については、844 ページの「処理マッピングテーブル」を参照してください。
cs6Label	「cs6」フィールドに対応するラベル	例: 「Second Action Result」
cs6	2 次処理結果	例: 「Unable to clean file.Passed」 詳細については、844 ページの「処理マッピングテーブル」を参照してください。
cat	ログの種類	例: 「1703」
dvchost	製品サーバ名	例: 「ApexOneServer01」
cn3Label	「cn3」フィールドに対応するラベル	例: 「CLF_SeverityCode」
cn3	重大度コード	例: 「2」 • 0: 不明 • 1: 情報 • 2: 警告 • 3: エラー • 4: 重大
deviceExternalId	ID	例: 「3」
fname	ファイル	例:「FakeMalwareRebootDel.exe」

CEF キー	説明	値
filePath	ファイルパス	例: 「C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\Rar$DR01.046\\」
msg	圧縮ファイル内のファイル	例: 「BMAC Schedule of Events.xls」
shost	配信元ホスト、UNC、メールアドレス 注意 このキーはシステムのログに含まれない場合があります。	例: 「xxx@test.com」
dst	エンドポイントの IPv4 アドレス	例: 「50.8.1.1」
c6a3Label	「c6a3」フィールドに対応するラベル	例: 「SLP_DestinationIP」
c6a3	エンドポイントの IPv6 アドレス	例: 「fe80::38ca:cd15:443c:40bb%11」
fileHash	ファイル SHA-1	例: 「D6712CAE5EC821F910E14945153AE7871AA536CA」
deviceFacility	製品	例: 「Apex One」

CEF キー	説明	値
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|AV:File renamed|JS_EXP
LOIT.SMDN|3|deviceExternalId=104 rt=Feb 18 2016 14:34:00 G
MT+00:00 cnt=1 dhost=ApexOneClient01 duser=Admin004 act=Fi
le renamed cn1Label=VLF_PatternNumber cn1=920500 cn2Label=
VLF_SecondAction cn2=3 cs1Label=VLF_FunctionCode cs1=Manua
l Scan cs2Label=VLF_EngineVersion cs2=9.500.1005 cs3Label=
CLF_ProductVersion cs3=10.6 cs4Label=CLF_ReasonCode cs4=vi
rus log cs5Label=VLF_FirstActionResult cs5=File renamed cs
6Label=VLF_SecondActionResult cs6=N/A cat=1703 dvchost=Ape
xOneServer01 cn3Label=CLF_ServerityCode cn3=2 fname=0348C6
93056617D34FC5B5BAB4643885FEE5FEDF;0xD5D56AC2 filePath=C:\
\Users\\Administrator\\Desktop\\trend_test_virus\\Trojans\
\ msg=BMAC Schedule of Events.xls shost=xxx@test.com dst=1
0.201.129.24 devic eFacility=Apex One reason=B deviceNtDom
ain=APEXTMCM dntdom=O SCEDomain1 ApexCentralHost=TW-CHRIS-
W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
```

2 次処理マッピングテーブル

値	説明
0	不明
1	該当なし
2	駆除
3	削除
4	移動
5	拡張子変更
6	放置/ログ
7	削除 (ストリップ)
8	削除
9	隔離
10	挿入/置換
11	アーカイブ
12	スタンプ
13	ブロック
14	承認用メールのリダイレクト
81	暗号化
90	検出
257	リセット

CEF Web セキュリティログ

CEF キー	説明	値
ヘッダ (logVer)	CEF 形式バージョン	CEF:0
ヘッダ (vendor)	アプライアンスベンダ	Trend Micro
ヘッダ (pname)	アプライアンス製品	Apex Central
ヘッダ (pver)	アプライアンスバージョン	2019
ヘッダ (eventid)	WB: フィルタ/ブロックの種類	WB:1
ヘッダ (eventName)	「ブロックのルール」または「フィルタ/ブロックの種類」	5
ヘッダ (severity)	重大度	3
app	プロトコル	例: 「3」 詳細については、864 ページの「プロトコルマッピングテーブル」を参照してください。
cnt	検出数	例: 「10」
dpt	サーバポート番号	例: 「80」
act	処理	例: 「0」 • 0: 不明 • 1: 放置 • 2: ブロック • 3: 監視 • 4: 削除 • 5: 隔離 • 6: 警告 • 7: 警告して続行 • 8: オーバーライド

CEF キー	説明	値
rt	イベントトリガ時刻 (UTC)	例: 「Mar 22 2018 08:23:23 GMT +00:00」
src	エンドポイントの IPv4 アドレス	例: 「10.1.128.34」
c6a2Label	「c6a2」フィールドに対応するラベル	例: 「SLF_SourceIP」
c6a2	エンドポイントの IPv6 アドレス	例: 「2620:101:4003:7a0:fd4b:52ed:53bd:ae3d」
cs1Label	「cs1」フィールドに対応するラベル	例: 「SLF_PolicyName」
cs1	ポリシー	例: 「External User Policy」
cs4Label	「cs4」フィールドに対応するラベル	例: 「CLF_ReasonCode」
cs4	理由コード	例: 「access」
cs5Label	「cs5」フィールドに対応するラベル	例: 「CLF_ReasonCodeSource」
cs5	理由コードの送信元	例: 「web」
deviceDirection	トラフィック/接続	例: 「2」 • 0: なし • 1: 受信 • 2: 送信
cat	フィルタ/ブロックの種類	例: 「7」 詳細については、862 ページの「フィルタ/ブロックの種類のマッピングテーブル」を参照してください。
dvchost	エンドポイントのホスト名	例: 「ApexOneClient08」

CEF キー	説明	値
cn1Label	「cn1」フィールドに対応するラベル	例: 「CLF_SeverityCode」
cn1	重大度コード	例: 「0」 • 0: 不明 • 1: 情報 • 2: 警告 • 3: エラー • 4: 重大
deviceExternalId	ID	例: 「38」
fname	ファイル	例: 「test.txt」
request	URL	例: 「http://www.violetsoft.net/counter/insert.php?dbserver\=db1&c_pcode\=25&c_pid\=funpop1&c_kind\=4&c_mac\=FE-ED-BE-EF-0C-E1」
deviceFacility	製品	例: 「Apex One」
duser	ユーザ名	例: 「Admin004」
shost	クライアントホスト名	例: 「ABC-HOST-WKS12」
cs2Label	「cs2」フィールドに対応するラベル	例: 「Blocking_Rule」
cs2	ブロックのルール	例: 「content filter」
deviceProcessName	プロセス名	例: 「C:\\Windows\ \system32\ \svchost-1.exe」
cn3Label	「cn3」フィールドに対応するラベル	例: 「ReputationScore」
cn3	レピュテーションスコア	例: 「49」
dst	サーバ IP アドレス	例: 「10.69.81.64」

CEF キー	説明	値
cn2Label	「cn2」フィールドに対応するラベル	例: 「SLF_SeverityLevel」
cn2	重大度レベル	例: 「100」 • 100: 高 • 300: 中/高 • 500: 中 • 700: 中/低 • 900: 低
reason	重大な脅威の種類	例: 「E」 • A: 既知の APT (標的型サイバー攻撃) • B: ソーシャルエンジニアリング攻撃 • C: 脆弱性に対する攻撃 • D: 侵入拡大 • E: 未知の脅威 • F: C&C コールバック • G: ランサムウェア
deviceNtDomain	Active Directory ドメイン	例: APEXTMCM
dntdom	Apex One ドメイン階層	例: OSCEDomain1
TMCMLogDetectedHost	ログイベントが発生したエンドポイント名	例: MachineHostName
TMCMLogDetectedIP	ログイベントが発生した IP アドレス	例: 10.1.2.3
ApexCentralHost	Apex Central ホスト名	例: TW-CHRIS-W2019
devicePayloadId	一意のメッセージ GUID	例: 1C00290C0360-9CDE11EB-D4B8-F51F-C697

CEF キー	説明	値
TMCMdevicePlatform	エンドポイントの OS	例: Windows 7 6.1 (Build 7601) Service Pack 1

ログの例:

```
CEF:0|Trend Micro|Apex Central|2019|WB:7|7|3|deviceExterna
lId=38 rt=Nov 15 2017 08:43:57 GMT+00:00 app=17 cntLabel=Agg
regatedCount cnt=1 dpt=80 act=1 src=10.1.128.46 cs1Label=SLF
_PolicyName cs1=External User Policy deviceDirection=2 cat=7
 dvchost=ApexOneClient08 fname=test.txt request=http://www.v
ioletsoft.net/counter/insert.php?dbserver\=db1&c_pcode\=25&c
_pid\=funpop1&c_kind\=4&c_mac\=FE-ED-BE-EF-0C-E1 deviceFacil
ity=Apex One shost=ABC-HOST-WKS12 reason=G deviceNtDomain=AP
EXTMCM dntdom=OSCEDomain1 TMCMLogDetectedHost=ABC-HOST-WKS12
TMCMLogDetectedIP=10.1.128.46 ApexCentralHost=TW-CHRIS-W2019
devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdev
icePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

フィルタ/ブロックの種類のマッピングテーブル

値	説明
0	不明
1	ファイル名
2	Web メールサイト
3	Web サーバ
4	URL パターン
5	Java/VB スクリプト
6	実ファイルタイプ
7	ユーザ定義
8	サーバ定義

値	説明
9	Web ポリシー
11	フィッシング
12	フィッシング/スパイウェア/グレーウェア
13	フィッシング/ウイルス/不正プログラム流布
14	フィッシング/偽の署名
15	フィッシング/不正サイト
16	フィッシング/不正アプレット
17	フィッシングレピュテーション
20	IP 変換ポリシー
21	Java 検索ポリシー
22	不正モバイルコードポリシー
31	ファーミング
32	URL ブロック
33	URL フィルタ
34	クライアント IP ブロック
35	宛先ポートブロック
36	Web レピュテーション
41	未サポートのファイルタイプ
42	ファイル数の上限を超えています
43	ファイルサイズの上限を超えています
44	圧縮レイヤ数の上限を超えています
45	解凍時間の上限を超えています
46	圧縮率の上限を超えています

値	説明
47	パスワード保護されたファイル
48	制限されたスパイウェアのタイプ
60	文字列のパターン
70	HTTP 検査
-1	ウイルス/不正プログラム
-2	スパイウェア/グレーウェア
-3	ネットワークウイルス
-4	IntelliTrap
-5	ウイルス/不正プログラムの兆候
-6	スパイウェアの兆候
-7	不正行為
-8	不審な挙動

プロトコルマッピングテーブル

値	説明
0	不明
1	SMTP
2	POP3
3	IRC
4	DNS 応答
5	HTTP
6	FTP
7	TFTP

値	説明
8	SMB
9	Windows Live Messenger (MSN)
10	AIM
11	Yahoo!メッセンジャー
12	Gmail
13	Yahoo!メール
14	Windows Live Hotmail
15	RDP
16	DHCP
17	Telnet
18	LDAP
19	ファイル転送
20	SSH
21	Dameware
22	VNC
23	Cisco Telnet
24	Kerberos
25	DCE RPC
26	SQL
27	pcAnywhere
28	ICMP
29	SNMP
30	ウイルスパターンファイル TCP

値	説明
31	ウイルスパターンファイル UDP
32	HTTPS
33	SMB2
34	MMS
35	IMAP4
36	RADIUS
37	RADMIN
38	FTP 応答
48	RTSP/RTP-UDP
49	RTSP/RTP-TCP
50	RTSP/RDT-UDP
51	RTSP/RDT-TCP
52	WMSP
53	SHOUTCast
54	RTMP
68	DNS 要求
256	BitTorrent
257	Kazaa
258	LimeWire
259	BearShare
260	Bluester
261	eDonkey eMule
262	Edonkey2000

値	説明
263	FileZilla
264	Guncleus
265	Gnutella
266	Winny
267	Napster
268	Morpheus
269	Napster
270	Shareaza
271	WinMX
272	MLDonkey
273	Direct Connect
274	Soulseek
275	OpenAP
276	KURO
277	iMesh
278	Skype
279	Google Talk
317	Cabos
318	Zultrax
319	Foxy
320	eDonkey
321	Ares
322	Miranda

値	説明
323	Kceasy
324	MoodAmp
325	Deepnet Explorer
326	FreeWire
327	Gimme
328	GnucDNA GWebCache
329	Jubster
330	MyNapster
331	Nova GWebCache
332	Swapper GWebCache
333	Xnap
334	Xolox
335	Ppstream
640	AIM Express
641	Chikka SMS Messenger
642	eBuddy
643	ICQ2Go
644	ILoveIM Web Messenger
645	IMUnitive
646	Mabber
647	Meebo
648	Yahoo!Web Messenger
848	SIP2

値	説明
1024	GPass
10001	IP アドレス
10002	ARP
10003	TCP
10004	UDP
10005	IGMP
60	ORACLE
44	MySQL
520	MSSQL
337	Postgres
41	ICMPv6
10006	GGP
10007	PUP
10008	IDP
10009	ND
10010	RAW

索引

さ

た

は

ら

わ