Trend Micro Control Manager™ 7.0

管理者ガイド

※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。

http://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx

著作権について

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

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、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、および Trend Micro Policy-based Security Orchestration は、トレンドマイクロ株式会社の登録商標です。

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

Copyright © 2017. Trend Micro Incorporated. All rights reserved.

P/N: CMEM77942/170818_JP_R2 (2018/12)

目次

第 3 章：ダッシュボード

第 4 章：アカウント管理

第 5 章：ライセンス管理

第 6 章：Active Directory とコンプライアンスの設定

第 7 章：ユーザ/エンドポイントディレクトリ

第 12 章：コンポーネントアップデート

第 13 章：コマンド追跡

パート IV：セキュリティ監視

第 14 章：ログ

第 15 章：通知

第 20 章：Control Manager ツール

第 21 章：不審オブジェクトハブおよびノードの Control Manager アーキテクチャ

第 22 章：不審オブジェクトリストエクスポート/インポートツールユーザガイド

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™ Control Manager™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

Control Manager 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	Control Manager 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。
システム要件	Control Manager 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
管理者ガイド	Control Manager と管理下の製品の設定および管理方法に加えて、Control Manager 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、Control Manager コンソールからもアクセスできます。
Connected Threat Defense 入門	Control Manager と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ための方法を説明した PDF ドキュメント
ウィジェットおよびポリシー管理ガイド	Control Manager 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を説明した PDF ドキュメント
情報漏えい対策リスト	情報漏えい対策用の事前定義済みデータ識別子およびテンプレートを記載した PDF ドキュメント

ドキュメント	説明
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?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。

- Control Manager の管理者: Control Manager 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: Control Manager 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

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

用語

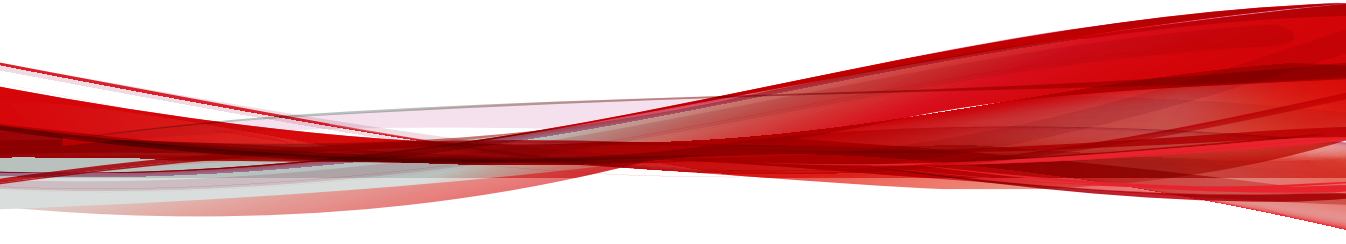
次の表は、Control Manager 付属のドキュメントで使用されている用語を示しています。

用語	説明
管理者 (または Control Manager 管理者)	Control Manager サーバを管理しているユーザ
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
Control Manager コンソールまたは管理コンソール	Control Manager 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、ウイルスバスター Corp.管理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	Control Manager 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

用語	説明
サーバ	Control Manager サーバがインストールされているエンドポイント
セキュリティリスク	ウイルス、不正プログラム、スパイウェア、グレーウェア、および Web からの脅威の総称
製品サービス	Microsoft 管理コンソール (MMC) を使用してホストされる Control Manager サービス
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

Control Manager の概要

本章では、Trend Micro™ Control Manager™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。

Control Manager について

Trend Micro™ Control Manager™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。Control Manager 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。

Control Manager 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。Control Manager 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。さらに柔軟性を高めるため、Control Manager では、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。

Control Manager 7.0 の新機能

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

機能	説明
Active Directory 統合の拡張機能	このバージョンの Control Manager 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。 詳細については、132 ページの「Active Directory 統合」を参照してください。
ダッシュボードの拡張機能	ダッシュボードの設計が見直され、ネットワーク保護ステータスの可視性が高まりました。
新しい Dwell Time ウィジェット	このウィジェットには、影響を受けたユーザのエンドポイント上に脅威が存在していた期間に基づく重大な脅威の概要が表示されます。

機能	説明
新しい管理下の全製品のレポート	管理下の全製品の新しいレポートテンプレートを使用すると、ネットワーク上のすべての脅威検出に関する包括的な情報を入手したり、影響を受けたユーザ/エンドポイントまたはチャネルおよび製品別の脅威の検出に関する実用的な概要を確認したりできます。
新しい通知メニュー	新しい [通知] メニューを使用すると、以前の [イベントセンター] 画面に簡単にアクセスできます。この画面は、[イベント通知] に名前が変更されました。このメニューには、[通知方法の設定] 画面 (以前の [一般的なイベント設定]) および [連絡先グループ] 画面 (以前の [ユーザグループ]) も含まれています。 詳細については、311 ページの「通知方法の設定」を参照してください。
新しい読み取り専用のユーザの役割	新しい読み取り専用のユーザの役割を割り当てると、ユーザアカウントで Control Manager 管理コンソールの情報を簡単に確認できるようになります。設定を変更するためのアクセス権を付与する必要はありません。
新しいレポート形式	次の形式の静的レポートを生成できるようになりました。 • Microsoft Word 形式 (*.docx) • Microsoft Excel 形式 (*.xlsx) 注意 • このバージョンの Control Manager では、ActiveX 形式および Crystal Report 形式のサポートが廃止されました。 • Control Manager の前のバージョンから移行した場合、以前に Control Manager 7.0 で生成された Crystal Report を引き続きダウンロードできます。
オペレーションセンター	[オペレーションセンター] 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。 詳細については、53 ページの「オペレーションセンター」を参照してください。

機能	説明
プラットフォームとブラウザのサポート	このバージョンの Control Manager では、以下がサポートされています。 • Microsoft™ Windows™ Server 2016 • Microsoft™ Internet Explorer™ 11 • Microsoft™ Edge™ • Google™ Chrome™ • Microsoft™ SQL Server™ 2016 注意 このバージョンの Control Manager では、以下のサポートが廃止されました。 • Microsoft™ Windows™ Server 2003 • Microsoft™ Internet Explorer™ 8、9、または 10 • Microsoft™ SQL Server™ 2005
ポリシー管理の拡張機能	ポリシーを、複数の同期済み Active Directory フォレストの組織単位から選択した対象に割り当てられるようになりました。 ネットワーク管理に空白期間が生じないようにするため、指定された対象にユーザアカウントがアクセスできない場合でも、そのユーザアカウントをポリシーの所有者に指定できます。 デバイスコントロールに関するポリシーをユーザごとに配信出来るようになりました。
セキュリティクライアントのインストール	ウイルスバスター Corp.または Trend Micro Security (for Mac) のセキュリティクライアントのインストールパッケージを、Control Manager コンソールから直接作成してダウンロードします。
簡素化されたログクエリ	以前の [新規アドホッククエリ] および [保存されたアドホッククエリ] 画面は、新たに [ログクエリ] 画面に統合されました。拡張された [ログクエリ] 画面では新しいデザインが採用され、これまでよりも簡単に、1 つの画面から、ログの照会、高度な検索の実行、ログクエリの保存および共有、検索結果のエクスポートができるようになりました。

機能	説明
不審オブジェクト管理の拡張機能	以前は未知とされた脅威に対する保護を強化するために、[ユーザ指定の不審オブジェクト] 画面を使用して不審オブジェクトファイルをアップロードすることにより、登録済みの管理下の製品で脅威を検出できるようになりました。ファイル SHA-1 ハッシュ値を手動で入力する必要はありません。 不審ファイル、URL、および IP アドレスに加えて、[オブジェクト] 列で不審ドメインを展開して詳細情報を確認できるようになりました。 [オブジェクト] 列で不審オブジェクトを展開すると、「重要な」ユーザまたはエンドポイントが星印で示され、[危険性の高い受信者] リストまたは [危険性の高いエンドポイント] リストの上部に表示されます。[最新の処理結果] 列には、管理下の製品で行われた最新の修復処理が表示されます。また、[最新の処理結果] の列名をクリックして検出リストを並べ替え、追加の軽減処理が必要な脅威を上部に表示することもできます。 ケース処理プロセスを簡素化するために、以前は分かれていた [影響診断] タブと [軽減] タブが 1 つの [影響診断と軽減] タブに統合されました。
Transport Layer Security 1.2 のサポート	このバージョンの Control Manager は、ネットワーク通信の保護を強化するために、Transport Layer Security (TLS) 1.2 プロトコルをサポートしています。
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 Control Manager 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。 詳細については、112 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。
アップデートメニューの強化とコンポーネントのインテリジェントダウンロード	設計が見直された [アップデート] メニューでは、[予約アップデート] 画面または [手動アップデート] 画面を使用して、コンポーネントのアップデートをこれまでよりも簡単に管理および配信できます。 また、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の新しいコンポーネントを Control Manager 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。

機能	説明
ユーザ/エンドポイントディレクトリの拡張機能	従来の [表形式] に加えて、ユーザまたはエンドポイントの情報を [タイムライン表示] で表示できるようになったため、脅威がいつ検出されたかを時系列順に視覚化し、指定した期間のパターンをこれまでよりも簡単に特定できます。 また、ユーザ/エンドポイントディレクトリから*.csv ファイルまたは*.png 画像でデータをエクスポートできます。 **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。 詳細については、148 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。

主な機能と利点

Control Manager には、次の機能と利点があります。

機能	利点
オペレーションセンター	[オペレーションセンター] 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。
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 Control Manager の情報を幅広く確認できます。
ユーザ/エンドポイントディレクトリ	Control Manager 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。

機能	利点
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 Control Manager 管理コンソールから手動検索を実行したりできます。
グローバルポリシー管理	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 Control Manager 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	Control Manager 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	Control Manager 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	特定の管理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、Control Manager 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。

機能	利点
コマンド追跡	コマンド追跡を使用すると、Control Manager 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。
セキュリティクライアントのインストール	ウイルスバスター Corp.または Trend Micro Security (for Mac) のセキュリティクライアントのインストールパッケージを、Control Manager コンソールから直接作成してダウンロードします。

Control Manager アーキテクチャ

Trend Micro Control Manager 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。Control Manager 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、Control Manager 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
Control Manager 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。Control Manager 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 Control Manager 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_ControlManager.mdf`) を使用します。 • Control Manager の管理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 Control Manager は、個々の受信者または受信者グループに Control Manager 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 Control Manager レポートは、Control Manager システム上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、Control Manager 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 Control Manager と通信します。MCP エージェントは、Control Manager 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	Control Manager 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 Control Manager を管理できるようになります。 Control Manager 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、Control Manager 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、Control Manager 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、Control Manager 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。

Trend Micro Smart Protection Network への参加

スマートフィードバックにより脅威に関する情報を継続的に収集して分析することで、保護の強化ができます。 スマートフィードバックに参加すると、ご使用のデバイスから情報が収集され、新しい脅威の特定に役立ちます。 ご使用のデバイスから収集する情報を、次に示します。

- ファイルのチェックサム
- アクセスされた Web アドレス
- サイズやパスなどのファイル情報
- 実行可能ファイルの名前

ヒント

スマートフィードバックに参加しない場合も、ご使用のデバイスは保護されます。 参加は任意であり、いつでも参加の取り消しができます。 トレンドマイクロ製品のすべてのお客さまに対する全体的な保護の強化に役立つので、スマートフィードバックへの参加をお勧めします。

Smart Protection Network の詳細については、https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html を参照してください。

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、Control Manager 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

Control Manager の管理コンソールは、Control Manager 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、Control Manager 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。

Control Manager では、次の Web ブラウザがサポートされます。

- Microsoft Internet Explorer™ 11
- Microsoft Edge™
- Google Chrome™

Web 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™、または Google Chrome™ 重要 Internet Explorer または Edge を使用して Control Manager Web 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

Control Manager 管理コンソールへの HTTPS アクセスの設定

Control Manager のインストールの際には、管理コンソールへ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。

Control Manager 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、Control Manager 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。

手順

1. 証明書発行機関 (Trend Micro SSL など) から「SSL サーバ証明書」を取得します。
2. Control Manager サーバにログオンします。
3. [スタート] > [プログラム] > [管理ツール] > [インターネット サービス マネージャ] の順にクリックして、Internet Information Server (IIS) の Microsoft Management Console (MMC) を開きます。

4. IIS サーバの隣にある [+] 記号をクリックして、仮想サイトリストを展開します。
5. [既定の Web サイト] を右クリックして、[プロパティ] を選択します。
6. [既定の Web サイトのプロパティ] 画面で次の手順を実行します。
   a. [ディレクトリセキュリティ] タブをクリックします。
   b. [サーバ証明書] をクリックし、新しいサーバ証明書ウィザードを使用してサーバ証明書要求を作成します。
   c. [次へ] をクリックします。
   d. サーバ証明書の割り当て方法を選択する画面で、[キー マネージャのバックアップ ファイルから証明書をインポート] を選択し、[次へ] をクリックします。
   e. キーの絶対パスとファイル名を入力し (たとえば、`cm_cert.key`)、[次へ] をクリックします。
   f. キーのパスワードを指定し、[次へ] をクリックします。
   g. [インポートされた証明書の概要] 画面で、[次へ] をクリックしてサーバ証明書を実装するか、または [戻る] をクリックして設定を変更します。
7. [OK] をクリックして既定の Web サイトのサーバ証明書を適用し、[既定の Web サイト] リストに戻ります。
8. [既定の Web サイト] リストから「Control Manager」仮想ディレクトリを右クリックして、[プロパティ] を選択します。
9. [ディレクトリ セキュリティ] タブをクリックして、[セキュリティ保護された通信] で [編集] をクリックします。

   [セキュリティ保護された通信] 画面が表示されます。
10. [セキュリティ保護されたチャネル (SSL) を要求する] と [128 ビット暗号化を要求する] を選択します。
11. [OK] をクリックして、[セキュリティ保護された通信] 画面を閉じます。
12. [OK] をクリックして変更を適用し、[既定の Web サイト] リストに戻ります。

次回 HTTP を使用して管理コンソールにアクセスすると、次のメッセージが表示されます。

ページは、セキュリティチャネルを通して表示される必要があります。

管理コンソールにアクセスする

Control Manager 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 Control Manager 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 Control Manager 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 Control Manager 管理コンソールにログオンすることはできます。

手順

1. Control Manager 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、Control Manager サーバで、[スタート] > [プログラム] > [Trend Micro Control Manager] > [Trend Micro Control Manager] 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、Control Manager 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。

   - Control Manager 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 Control Manager 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。

   Control Manager 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に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、次のいずれかを実行してください。

- 管理コンソールの右上で、<アカウント名> > [ログオフ] をクリックします。
- `<Ctrl>` + `<W>` キーを押します。

Web コンソールの設定

Control Manager の Web コンソールの設定では、Web 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] > [Web コンソールの設定] に移動します。

   [Web 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
Web 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 Control Manager サーバの画面のデータが更新されるようになります。 • Web コンソールの更新間隔: Web 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。
Web コンソールのタイムアウト	[Web 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。 • Web 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、Web 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。

セクション	設定
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。

3. [保存] をクリックします。

Smart Protection Network の設定

トレンドマイクロスマートフィードバックを有効にすると、脅威情報が Trend Micro Smart Protection Network に送信されます。これにより、トレンドマイクロでは新しい脅威を迅速に識別して対応できるようになるため、ネットワークの保護が強化されます。

また、一部のウィジェットでは、機能させるために Smart Protection Network の設定を有効にする必要があります。これは、それらのウィジェットでは Trend Micro Smart Protection Network から直接データを受信するためです。

注意

E-mail レピュテーション、ファイルレピュテーション、および Web レピュテーションは、すべて Smart Protection Network に含まれます。

手順

1. [運用管理] > [設定] > [Smart Protection Network の設定] に移動します。

   [Smart Protection Network の設定] 画面が表示されます。

2. [トレンドマイクロスマートフィードバックと Smart Protection Network を有効にする (推奨)] を選択します。

3. [時間間隔] ドロップダウンリストで、Control Manager から完全に匿名の脅威情報を Smart Protection Network に送信する頻度を選択します。
4. (オプション) [業種] ドロップダウンリストから、ユーザの企業が属する業界を選択します。
5. [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、Control Manager 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、Control Manager 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 Control Manager 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。

- Control Manager 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」参照してください。

- Trend Micro Smart Protection Network

  詳細については、44 ページの「Smart Protection Network の設定」参照してください。

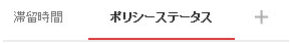
タブはウィジェット用のコンテナを用意します。[ダッシュボード] では、最大 30 のタブがサポートされます。

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。

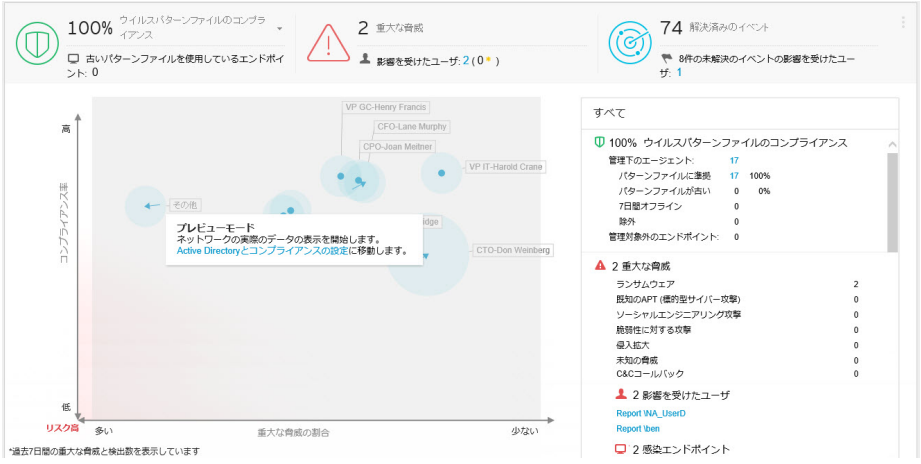
手順

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。

オペレーションセンター



[オペレーションセンター] は特別なタブ/ウィジェットで、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を統合してネットワーク保護ステータスの概要を表示します。また、[オペレーションセンター] 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、131 ページの Active Directory とコンプライアンスの設定参照してください。

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。
- 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

[オペレーションセンター] タブのこのセクションには、ネットワークの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、セキュリティ運用チャート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、58 ページの「オペレーションセンターのグラフ」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、ウイルスバスター Corp.クライアントとウイルスバスター ビジネスセキュリティサービスクライアントの割合 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、137 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、148 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。
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ウイルスバスター Corp.クライアントの割合 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、139 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、148 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

[オペレーションセンター] タブのこのセクションには、ネットワーク上の重大な脅威の検出の総数、影響を受けたユーザの総数、影響を受けた重要なユーザの数 (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、181 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。

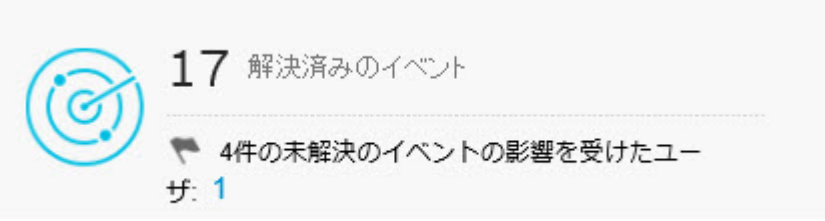
詳細については、148 ページの「ユーザ/エンドポイントディレクトリ」を参照してください。

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
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

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
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

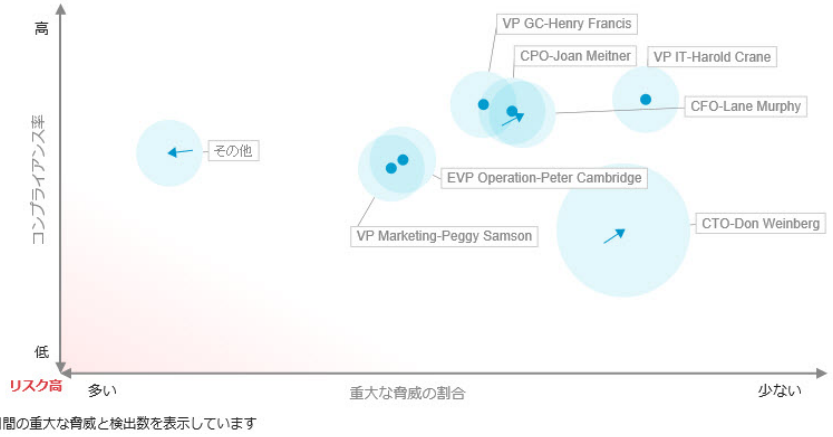


[オペレーションセンター] タブのこのセクションには、ネットワーク上の解決済みのイベントと未解決のイベントの総数が表示されます。

[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、147 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。

オペレーションセンターのグラフ



[オペレーションセンター] 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、131 ページの Active Directory とコンプライアンスの設定参照してください。

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、141 ページの「エンドポイントおよびユーザのグループ設定」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、54 ページの「コンプライアンスインジケータ」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、60 ページの「[オペレーションセンター] の [詳細] ペイン」参照してください。

[オペレーションセンター] の [詳細] ペイン

[オペレーションセンター] 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、54 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、58 ページの「オペレーションセンターのグラフ」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、ウイルスバスター Corp.クライアントとウイルスバスター ビジネスセキュリティサービスクライア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。
	
	• 管理下のクライアント: ウイルスバスター Corp.およびウイルスバスター ビジネスセキュリティサービスクライア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クライアントの数
	  • 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クライアントの数
	  • 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クライアントの数
	  • 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: ウイルスバスター Corp.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クライア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。
	
	• 137 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」
	• 147 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ウイルスバスター Corp.クライア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。
	
	• 管理下のクライアント: 情報漏えい対策が有効なウイルスバスター Corp.クライア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クライアントの数
	
	  • 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クライアントの数
	
	  • 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クライアントの数
	
	  • 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: 情報漏えい対策が有効なウイルスバスター Corp.クライア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。
	
	• 139 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」
	
	• 147 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重大な脅威の総数が表示されます。 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、166 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、154 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、162 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。
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。

データ	説明
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、147 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
- Control Manager 上位の脅威
- 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

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重大な脅威の種類の総数と、脅威の各種類によって影響を受けた重要なユーザとその他のユーザの数が表示されます。

- 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、181 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。

[範囲] ドロップダウンを使用して、データを表示する期間を選択します。

この表には、重大度の順に重大な脅威の種類が示されます。

- [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、表示するユーザをクリックします。

  詳細については、154 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。

[脅威の種類] 列には、次の脅威の種類が表示されます。

注意

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。

脅威の種類	説明
ランサムウェア	身代金が支払われない限り、ユーザによるシステムへのアクセスを阻止または制限する不正プログラム
既知の APT (標的型サイバー攻撃)	標的とした対象を執拗に追跡して侵入し、不正行為をする攻撃。単独のイベントではなく、キャンペーン (一定期間にわたって失敗と成功を繰り返しながら対象ネットワークの奥深くに侵入する試み) で行われることが多い。
ソーシャルエンジニアリング攻撃	PDF ファイルなどのドキュメントに存在するセキュリティの脆弱性を悪用する不正プログラムまたはハッカーによる攻撃
脆弱性に対する攻撃	通常、プログラムおよびオペレーティングシステムに存在するセキュリティの弱点を悪用する不正プログラムまたはハッカーによる攻撃
侵入拡大	ディレクトリ、メール、管理サーバ、およびその他の資産の検索してネットワークの内部構造をマップし、そのシステムにアクセスするための認証情報を入手して、攻撃者がシステム間を移動する攻撃
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
重大な脅威によって影響を受けたユーザの合計	この列に表示されるこのカウントは、少なくとも 1 つの重大な脅威が検出されている 「[重要なユーザ]」 と 「[その他のユーザ]」 の総数を示します。各ユーザは複数の重大な脅威の影響を受けている可能性があります。

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。

[重要なユーザ] タブまたは [その他のユーザ] 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、181 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「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。

[重要なユーザ] タブまたは [その他のユーザ] 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、181 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。

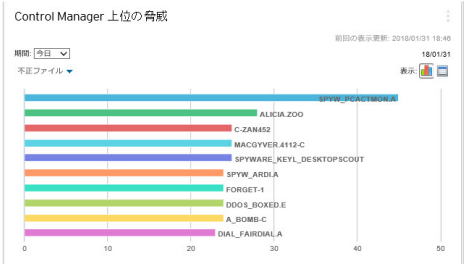
- 表示するユーザの [脅威] 列の数字をクリックします。

  詳細については、162 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

Control Manager 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、Control Manager 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。

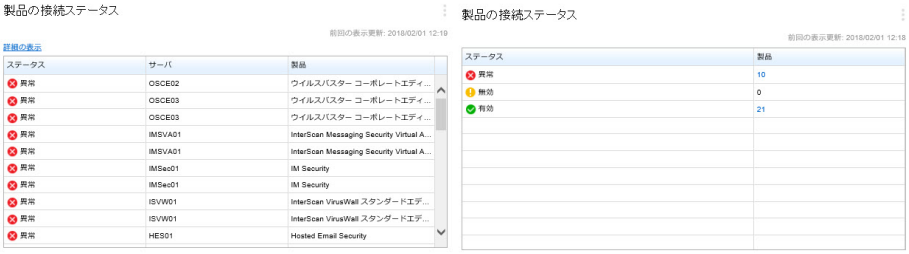
- ウィジェットの製品範囲を変更するには、[範囲] フィールドの二重矢印ボタン ( ) をクリックし、データの収集元となる製品を選択します。
- ウィジェットに表示されるコンポーネントを編集するには、[パターンファイル] フィールドまたは [検索エンジン] フィールドからコンポーネントを選択または選択解除します。
- 管理下の製品、エンドポイント、またはその両方のコンプライアンス情報を表示するには、[ソース] を指定します。
- 管理下の製品によって報告されたすべてのコンポーネントのデータを表示するか、Control Manager によって管理されるコンポーネントのデータのみを表示するかを指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

データ	説明
エンドポイント/すべて	• エンドポイント: 期限切れのコンポーネントがあるエンドポイントの数 [エンドポイント/すべて] 列の最初の数字をクリックすると、期限切れ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。 • すべて: コンポーネントを使用するエンドポイントの総数 [エンドポイント/すべて] 列の 2 番目の数字をクリックすると、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。  注意 この列は、[ソース] に対して [エンドポイント] が選択されている場合に表示されます。
古いバージョンの割合	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 [管理下の製品] または [エンドポイント] 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、Control Manager 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、296 ページの「ログクエリ」を参照してください。

管理下の製品との通信および接続ステータスアイコンの詳細については、次のトピックを参照してください。

- 194 ページの「管理下の製品との通信」
- 213 ページの「接続ステータスアイコン」

ステータス	説明
アクティブ	製品サービスが実行中であり、Control Manager 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。

ステータス	説明
非アクティブ	製品サービスが実行されていないか、Control Manager 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 Control Manager サーバと通信していないことを示します。 詳細については、196 ページの「管理対象製品の接続ステータスの間隔を設定する」を参照してください。

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
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
ネットワークトラフィック	ウイルスバスター Corp.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
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ウイルスバスター Corp.クライアントでローカルフォルダ内のウイルスバスター Corp.によって検出されたランサムウェア
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
挙動	ウイルスバスター Corp.の挙動監視によって検出されたランサムウェア

[情報漏えい対策イベントの調査] タブ

[情報漏えい対策イベントの調査] タブには、イベントステータス、重大度レベル、管理下のユーザに基づいて、情報漏えい対策イベントに関する情報を表示す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。

- 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

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。

[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。

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。
範囲	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。

[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。

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

[保存] をクリックして変更を適用し、ウィジェットのデータを更新します。

ユーザ別の情報漏えい対策イベントウィジェット

このウィジェットを使用して、重大度レベルと管理下のユーザに基づく情報漏えい対策イベント数を確認できます。データは重大度レベル別にフィルタ

処理できます。また、特定のユーザによって開始された新規のイベントおよび重大度の高いイベントの総数も表示できます。初期設定では、ユーザのアカウント権限で許可されている、すべての管理下の製品のデータがウィジェットに表示されます。ウィジェットには最大 50 ユーザが表示されます。

[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。

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。
範囲	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。

[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に定義されています。

- 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

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。

[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。

[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。

データ	説明
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
イベント	発生した情報漏えい対策イベントの数
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

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。

[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。

[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
イベント	情報漏えい対策イベントの数

データ	説明
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

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。

[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。

[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。

[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。

[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
イベント	発生した情報漏えい対策イベントの数

[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。Control Manager 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	Control Manager に登録されている管理下の製品
バージョン	管理下の製品のバージョン
言語	管理下の製品の言語のバージョン
ビルド	管理下の製品のビルド番号

データ	説明
最新バージョン	最新であるとみなされる製品の数 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 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

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、Control Manager 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、Control Manager によって管理されるコンポーネントのデータのみを表示するかを指定するには、[表示] を選択します。

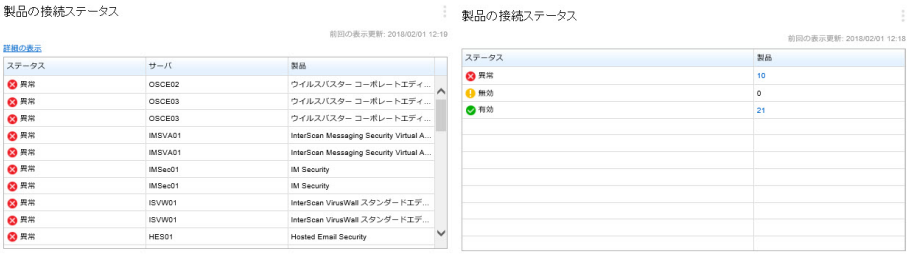
データ	説明
パターンファイル	パターンファイル、テンプレート、またはスパムメール判定ルールの名前が表示されます。
検索エンジン	検索エンジンの名前が表示されます。

データ	説明
最新バージョン	次の情報が表示されます。 • Control Manager 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。

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

データ	説明
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、Control Manager 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、296 ページの「ログクエリ」を参照してください。

管理下の製品との通信および接続ステータスアイコンの詳細については、次のトピックを参照してください。

- 194 ページの「管理下の製品との通信」
- 213 ページの「接続ステータスアイコン」

ステータス	説明
アクティブ	製品サービスが実行中であり、Control Manager 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。
非アクティブ	製品サービスが実行されていないか、Control Manager 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 Control Manager サーバと通信していないことを示します。 詳細については、196 ページの「管理対象製品の接続ステータスの間隔を設定する」を参照してください。

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。

- Trend Micro Endpoint Sensor
- Endpoint Encryption
- Trend Micro Mobile Security
- Trend Micro Security (for Mac)
- ウイルスバスター Corp.
- Vulnerability Protection
- 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。Control Manager 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
オンライン	上位サーバに接続されているエージェント
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
合計	エンドポイントの総数

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] タブ

[脅威の検出] 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に定義されています。

- Control Manager 上位の脅威
- Control Manager 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

Control Manager 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。

Control Manager 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
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
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
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)
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)

- 脅威の種類

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別の、ファイルサーバ上のセキュリティの脅威
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別の、ネットワーク上のセキュリティの脅威
不明	認識できないセキュリティの脅威
メール	[データの範囲] で指定されている管理下の製品別の、メールサーバ上のセキュリティの脅威
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別の、デスクトップ上のセキュリティの脅威
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別の、ゲートウェイ上のセキュリティの脅威

データ	説明
Control Manager サーバ	[データの範囲] で指定されている管理下の製品別の、Control Manager サーバ上のセキュリティの脅威

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。Control Manager 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
検出数	検出されたセキュリティの脅威の数
割合 (%)	検出されたセキュリティの脅威の総数の割合

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。

- 24 時間
- 1 週間
- 2 週間
- 1 か月

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。Control Manager 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	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 **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 **注意** 脅威の種類がその他の場合、この列は表示されません。
検出数	検出されたセキュリティの脅威の数
割合 (%)	検出されたセキュリティの脅威の総数の割合

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。

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のタイトルを変更するには、[タイトル] フィールドを使用します。
- 脅威の種類を指定するには、[脅威の種類] ドロップダウンを使用します。

[保存] をクリックして変更を適用し、終了します。

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。Control Manager 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] のリストを表示します。
更新	最終更新日
検出数	Network VirusWall Enforcer デバイスで検出されたサービス違反の数

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。

- ポリシー違反の検出ウィジェットのタイトルを変更するには、[タイトル] フィールドを使用します。
- 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。

> **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
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

データ	説明
地域/国	C&C サーバが設置されている地域および国
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
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
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
検出元	イベントをログに記録した管理下の製品の名前

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。

- [タイトル] フィールドを使用して、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。
- 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。
- [C&C リストのソース] ドロップダウンを使用して、C&C ソースを指定します。ドロップダウンに [グローバルインテリジェンス]、[仮想アナライザ]、および [ユーザ指定] の C&C リストのソースが表示されます。
- [表示する項目] ドロップダウンを使用して、ウィジェットに表示する項目の数を選択します。ドロップダウンには最大でトップ 50 項目が表示されます。

[保存] をクリックして変更を適用し、終了します。

第 4 章

アカウント管理

このセクションでは、Control Manager 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、Control Manager 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、115 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、105 ページの「ユーザアカウントの追加」参照してください。 **注意** Control Manager 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、132 ページの「Active Directory 統合」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 Control Manager 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 Control Manager 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、112 ページの「2 要素認証を有効または無効にする」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、Control Manager 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、112 ページの「2 要素認証を有効または無効にする」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、111 ページの「ユーザアカウントの編集」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、43 ページの「Web コンソールの設定」参照してください。
ユーザアカウントの有効化	Control Manager 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、111 ページの「ユーザアカウントの編集」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 Control Manager 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、111 ページの「ユーザアカウントの編集」参照してください。 • Control Manager 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

root アカウントは、Control Manager のインストール時に作成されます。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

Control Manager のアカウントは、Control Manager 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。Control Manager 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

Control Manager 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

- root、管理者、または管理者 (情報漏えい対策コンプライアンス責任者) のアカウントのみが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、132 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 Control Manager にログオンできます。

  詳細については、41 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

Control Manager 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 Control Manager 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 Control Manager 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 Control Manager 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、114 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** • Control Manager 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、Control Manager 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、311 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

- Control Manager 7.0 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 Control Manager 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、132 ページの「Active Directory 統合」を参照してください。

- Control Manager 6.0 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 Control Manager 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、115 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、109 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、109 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」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、217 ページの「管理下の製品のタスクを実行する」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、Control Manager 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、218 ページの「管理下の製品を設定する」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、221 ページの「ディレクトリ管理」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 Control Manager 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

- root アカウントは、Control Manager 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 DLP_Compliance_Officer 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、Control Manager 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 Control Manager 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. [完了] 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 Control Manager 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。[ユーザアカウント] 画面を使用して、すべての Control Manager ユーザアカウントに対して要素認証を有効または無効にします。

重要

Control Manager 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、114 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、311 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。
- Control Manager コンソールから Trend Micro Customer Licensing Portal (CLP) アカウントの 2 要素認証を有効にすることはできません。

  詳細については、Trend Micro Customer Licensing Portal に関するドキュメントを参照してください。

- 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 Control Manager 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。

      - Control Manager 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。

      Control Manager 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、111 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] > [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. 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 Control Manager 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。

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** • Control Manager 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、112 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。 • Control Manager 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、311 ページの「SMTP サーバを設定する」参照してください。
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 Control Manager 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 Control Manager 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 Control Manager バージョン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

- root、管理者、および管理者 (情報漏えい対策コンプライアンス責任者) のアカウントのみが、ユーザの役割を追加または編集できます。
- 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、109 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、120 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 Control Manager が提供する初期設定のユーザの役割は削除できません。

タスク	説明
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、121 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 Control Manager 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、117 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

Control Manager 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 Control Manager 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

root、管理者、および管理者 (情報漏えい対策コンプライアンス責任者) のアカウントのみが、新規のユーザアカウントを作成して、ユーザの役割を割り当てることができます。

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。

- 120 ページの「ユーザの役割の追加」
- 121 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。
Administrators	• 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。
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。 • 143 ページの「レポートライン」 • 105 ページの「ユーザアカウントの追加」

役割	説明
Operators	• 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。 • すべてのログクエリの実行、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、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_Users	• 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、および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。
ReadOnly	• 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_Users	• 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

旧バージョンの Operator と Power User の役割には、ポリシー管理のメニュー項目に対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、226 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

Control Manager 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、111 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、Control Manager 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、Control Manager 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。

Control Manager のアクティベーションおよびライセンス情報

Control Manager 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。

Control Manager 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または販売代理店からアクティベーションコードを入手した後に Control Manager のアクティベーションを実行できます。

注意

Control Manager 7.0 では、従来のスタンダード版と アドバンス版のライセンスの区別はなくなり、同じ機能を利用できるようになります。

重要

Control Manager のアクティベーション後、変更を有効にするには、Control Manager 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] > [Control Manager] 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. Control Manager 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。

Control Manager ライセンス情報を確認および更新する

注意

Control Manager 7.0 では、従来のスタンダード版と アドバンス版のライセンスの区別はなくなり、同じ機能を利用できるようになります。

手順

1. [運用管理] > [ライセンス管理] > [Control Manager] 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. Control Manager 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. Control Manager 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. Trend Micro Customer Licensing Portal で現在のライセンスに関する情報を確認するには、次の手順を実行します。

   a. [ライセンス情報をオンラインで確認] をクリックします。

   b. トレンドマイクロのアカウントとパスワードを使用して Customer Licensing Portal にログオンします。

   c. [ユーザの製品/サービス] メニュータブをクリックします。

d. [製品/サービス] カテゴリを展開して、登録済みのトレンドマイクロ製品のライセンス情報を確認します。

管理下の製品のアクティベーションと登録

Control Manager 7.0、管理下の製品 (ウイルスバスター Corp.、InterScan for Microsoft Exchange)、およびその他のサービスを利用するには、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 Control Manager 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。

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。
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。

列名	説明
ステータス	アクティベーションコードのステータスを表示します。 • アクティベート済み • サポート契約終了
種類	アクティベーションコードの種類を表示します。 • 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。
シート数	このアクティベーションコードで使用できるシート数が表示されます。
ライセンス情報をオンラインで確認	このリンクをクリックすると、初期設定の Web ブラウザで Trend Micro Customer Licensing Portal が開きます。 このポータルでは、トレンドマイクロビジネスアカウントを管理できます。これには、社内で使用している製品のアクティベーションコードと、トレンドマイクロの SaaS ソリューション契約が含まれます。

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。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、Control Manager 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 Control Manager 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. [完了] をクリックします。

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

管理下の製品のライセンスの更新

Control Manager 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. [保存] をクリックします。

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、Control Manager に現在登録されている製品はサポートされていません。

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、Control Manager 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

Control Manager 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、105 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、148 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、[セキュリティ運用] 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、135 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

Control Manager 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

Control Manager 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。

注意

- 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. [同期間隔] ドロップダウンリストから、Control Manager が Active Directory サーバとデータを同期する間隔を選択します。

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) [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。

7. [保存] をクリックします。

Active Directory サーバの接続を設定して保存したら、次のタスクを実行できます。

- [今すぐ同期] をクリックして、データを Active Directory サーバと手動で同期します。

  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。

- [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 Control Manager データベースから手動で削除します。

  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、Control Manager 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、132 ページの「Active Directory 接続を設定する」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。 • Control Manager 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。 Control Manager 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。
Control Manager データベースにアクセスできない	Control Manager 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、478 ページの「Control Manager データベースについて」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、545 ページのテクニカルサポート参照してください。

コンプライアンスインジケータ

Control Manager には次のコンプライアンスインジケータが含まれており、インジケータの設定および Active Directory サーバから同期したユーザと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を実行します。コンプライアンスインジケータの情報は、[オペレーションセンター] ダッシュボードタブで確認できます。

- 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 (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いる管理下のウイルスバスター Corp.、ウイルスバスター ビジネスセキュリティサービスクライアントの割合
- 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、許容される数の機密データ検出イベントが含まれる、管理下のウイルスバスター Corp. クライアントおよび Cloud App Security エージェントの割合

次に、Control Manager でコンプライアンスの計算を実行し、コンプライアンス情報を [オペレーションセンター] ダッシュボードタブに表示するための手順の概要を示します。

手順

1. Active Directory サーバに接続して、ユーザとエンドポイントの情報を同期します。

   詳細については、132 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。

   - 137 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」
   - 139 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 のサイトとレポートラインに基づいてエンドポイントと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、141 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 の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、[オペレーションセンター] タブを設定します。

詳細については、次のトピックを参照してください。

- 53 ページの「オペレーションセンター」
- 50 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 (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、管理下のウイルスバスター Corp.、ウイルスバスター ビジネスセキュリティサービスクライアントの割合を表示するために、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 [オペレーションセンター] タブで設定できます。

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. [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
対応す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、さまざまアラートレベルのしきい値 (準拠する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 Control Manager 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、175 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、175 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

[オペレーションセンター] 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、管理下のウイルスバスター Corp. クライアントおよび Cloud App Security 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。
しきい値	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、さまざまアラートレベルのしきい値 (準拠する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 Control Manager 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、175 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、175 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

Control Manager では、次の情報に基づいて [セキュリティ運用] 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、Control Manager 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、[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	管理下のセキュリティ状況ウィジェットに表示する名前 **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

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. 管理下のセキュリティ状況ウィジェットでグループを識別する [表示名] を指定します。
5. 管理下のセキュリティ状況ウィジェットでグループを識別する [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、Control Manager によって元のサイトがリストから削除されます。

ヒント

Control Manager 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. 管理下のセキュリティ状況ウィジェットでグループを識別する [表示名] を指定します。
6. 管理下のセキュリティ状況ウィジェットでグループを識別する [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	[管理下のセキュリティ状況] ダッシュボードに表示する名前 注意 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 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. 管理下のセキュリティ状況ウィジェットでグループを識別する [表示名] を指定します。

6. 管理下のセキュリティ状況ウィジェットでグループを識別する [ノードの色] を選択します。

7. [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。

8. [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、Control Manager 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

Control Manager 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. 管理下のセキュリティ状況ウィジェットでグループを識別する [表示名] を指定します。
6. 管理下のセキュリティ状況ウィジェットでグループを識別する [ノードの色] を選択します。
7. [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、Control Manager 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、Control Manager 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、149 ページの「ユーザの詳細情報」参照してください。

- エンドポイント: Control Manager 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、158 ページの「エンドポイントの詳細」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

Control Manager 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。

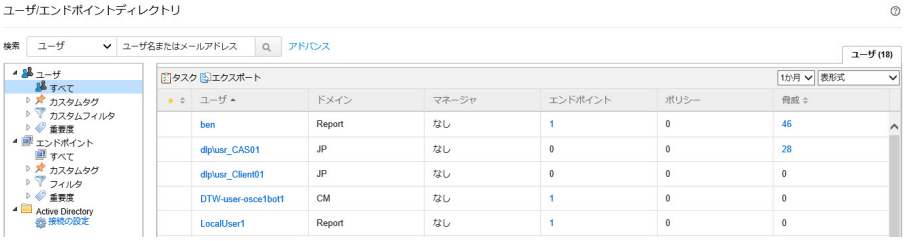
フォレストの信頼の詳細については、Active Directory 管理者にお問い合わせください。

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、171 ページの「詳細検索の使用」および175 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、Control Manager 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、181 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

ユーザ (アカウント)	Control Manager 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: Control Manager 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、Control Manager 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、Control Manager 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、157 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。NA 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。

ドメイン	• Active Directory と同期できる場合、Control Manager 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、Control Manager 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。

列	説明
マネージャ	Active Directory と同期できる場合、Control Manager 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、157 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。 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、158 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。 [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、156 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。 [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、154 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。 • ウイルスバスター Corp.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)	Control Manager 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。 [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、154 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、154 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、Control Manager 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ことができます。

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 Control Manager 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

Control Manager 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

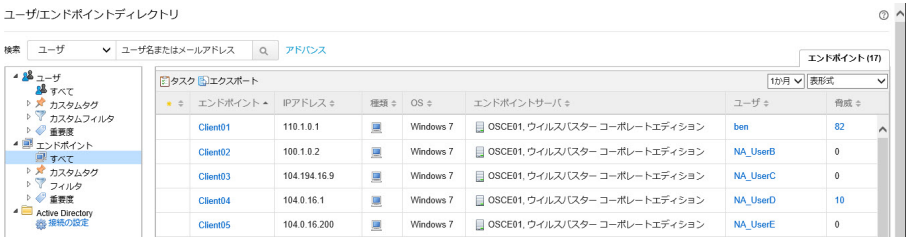
Control Manager では、Active Directory のグローバルカタログ (GC) からデータが同期されます。

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、Control Manager 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、181 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 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、164 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
種類	マシンまたはデバイスの種類: 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	マシンまたはデバイスで稼働している OS: サポートされている Windows デスクトップ/サーバシステム、Mac OS、iOS、Android、Symbian、および Windows Mobile
ドメイン	Active Directory 統合が有効な場合はドメイン名が表示されます。

列	説明
ユーザ	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。 詳細については、157 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。 [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、162 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 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、164 ページの「ポリシーステータス」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。 [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、162 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。

列	説明
<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、162 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 - <名前> の情報

[エンドポイント] 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。関連情報を表示するには、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、162 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、164 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、164 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、165 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] 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、176 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、446 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。

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。

この画面は、Control Manager コンソールの [影響を受けたユーザ] 画面の [ダッシュボード] > [概要] タブの脅威にさらされているエンドポイントウィジェットからアクセスできます。

- 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、168 ページの「影響を受けたユーザに対する影響を診断する」および446 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ことができます。

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 Control Manager 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。

Control Manager 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、177 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446 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。

- IP アドレス
- 種類
- OS
- ユーザ

注意

Control Manager 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。

Active Directory の詳細

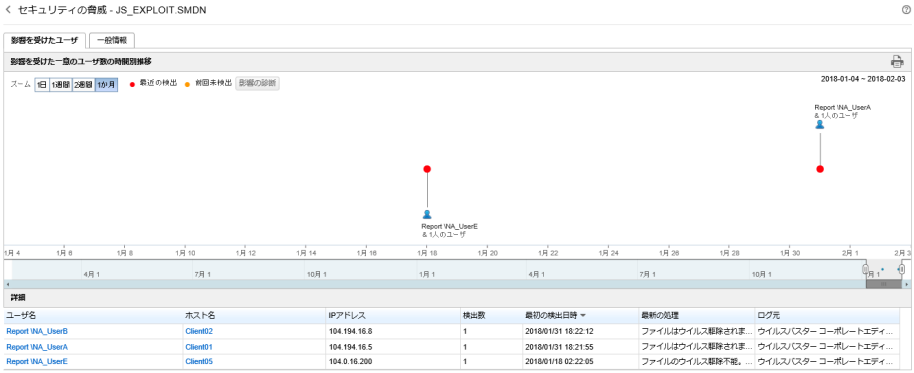
Active Directory ノードには、統合された Active Directory 構造が表示されます。Active Directory ノードの組織単位を表示すると、リストには次の 2 つのタブがあります。

- ユーザ: 詳細については、149 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、158 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

[脅威情報] 画面の [影響を受けたユーザ] タブを使用して、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。

この画面には、表の脅威名をクリックして、[ユーザ] または [エンドポイント] 画面の [セキュリティの脅威] タブからアクセスできます。



- 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。
  - [影響の診断] をクリックして、詳細なログ分析を実行し、エンドポイントに存在していた脅威が前回未検出だったかどうかを判断します。

重要

[脅威情報] 画面から影響診断を実行するには、Endpoint Sensor 1.5 (またはそれ以降) と Deep Discovery Inspector 3.8 (またはそれ以降) を Control Manager に登録する必要があります。

詳細については、168 ページの「影響を受けたユーザに対する影響を診断する」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: ログデータの影響診断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診断する

Control Manager の [影響を受けたユーザ] 画面で環境内のセキュリティの脅威の全体または一部の過去の影響診断を実行できます。

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、IP アドレス、およびドメインの影響を診断します。

Endpoint Sensor は、エージェントと通信し、クライア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診断します。

CONTROL MANAGER バージョン	管理下の製品
影響診断を実行するには、次のバージョンの Control Manager が必要です。 • Control Manager 7.0 以降	Control Manager は、影響診断の実行に少なくとも次の製品の 1 つを必要とします。 • Endpoint Sensor 1.5 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降) **重要** 影響診断を実行するには、Deep Discovery Inspector で Retro Scan を有効にする必要があります。

手順

1. Control Manager 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。

   ヒント

   [ファイルパス / メールの件名 / ルール名] 列を使用して、不審オブジェクトの検出数を特定できます。「仮想アナライザ」または「ユーザ指定」リスト別に不審オブジェクトが検出されます。

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

   Deep Discovery Inspector および Endpoint Sensor (使用可能な場合) は、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を検索します。

詳細については、170 ページの「Deep Discovery Inspector の Retro Scan」および437 ページの「Endpoint Sensor 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

Control Manager 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、173 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」で上司が「Mary」または「Bill」であり、財務部門で名前に「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、178 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
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
Active Directory 内の場所	検索を開始する部署
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
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
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 ([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「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 詳細については、181 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 詳細については、141 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 詳細については、141 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
IP アドレス	IPv4 アドレス範囲 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。そのエントリを含む IP アドレスを持つ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: 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	Os の種類: Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10、Windows 2000、Windows 2003、Windows 2008、Windows 2012、Windows 2016、Mac OS、iOS、Android、Symbian、Windows Mobile など
Active Directory 内の場所	検索を開始する部署
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 ([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、162 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。

カテゴリ	説明
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 詳細については、135 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 詳細については、181 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 詳細については、141 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 詳細については、141 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

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。

- 296 ページの「ログクエリ」
- 672 ページの「ユーザアクセス情報」

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へのアクセス権を持つすべてのユーザは、カスタムタグを作成および表示できます。ただし、カスタムタグを削除または変更できるのは作成したユーザに限られます。

重要

Control Manager のインストール中に作成された管理者アカウントは、すべてのカスタムタグに対するフルコントロールを持ち、どのユーザが作成したタグであっても削除または変更できます。

カスタムタグの作成

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

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。

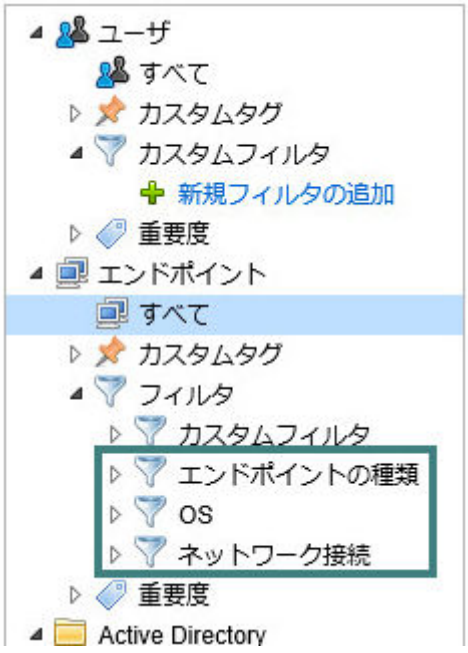
詳細については、180 ページの「カスタムフィルタの作成」および181 ページの「ユーザまたはエンドポイントの重要度」を参照してください。

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、179 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。

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、149 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: 手動で隔離されるエンドポイント

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

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 「w12p.tmcm.co」内で名前に「Ja」が付くすべてのユーザをフィルタします。

詳細については、173 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。Control Manager 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、175 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

- 初期設定では、重要度は「ドメイン管理者」(ユーザ) と「ドメインコントローラ」(エンドポイント) に割り当てられます。
- 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。
- 重要度の割り当てと解除は、[ユーザ/エンドポイントディレクトリ] にアクセスできるすべてのユーザが実行できます。

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。
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、149 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 Control Manager 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

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

- Control Manager 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 (Control Manager 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、Control Manager 管理コンソールを使用して Control Manager 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。

管理下の製品の管理コンソールを使用して Control Manager に登録される製品の詳細については、449 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 Control Manager 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」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 Control Manager 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、190 ページの「管理下のサーバを編集する」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 Control Manager 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、191 ページの「管理下のサーバを削除する」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、192 ページの「管理下の製品のプロキシ設定」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、193 ページの「クラウドサービスを設定する」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、222 ページの「ディレクトリ管理を使用する」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、187 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 Control Manager 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 Control Manager への登録方法が表示されます。 • 自動 —管理下の製品は Control Manager 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、449 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、193 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	Control Manager 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。
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、190 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、191 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 Control Manager 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 Control Manager に登録します。

  詳細については、449 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、222 ページの「ディレクトリ管理を使用する」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、およびポート番号 (ある場合) を入力します。
   - 表示名: Control Manager 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

Control Manager 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. 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、192 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. [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、Control Manager 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、192 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。

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、Control Manager 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. [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. 管理下のサーバを削除するには、[処理] 列の [削除] アイコンをクリックします。

4. [OK] をクリックします。

   削除されたサーバが登録解除されます。

> **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。

管理下の製品のプロキシ設定

Control Manager 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、190 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. [プロキシ設定] をクリックします。

   [プロキシ設定] 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 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、Control Manager 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://tm.login.trendmicro.com/simplesaml/saml2/idp/SSOService.php) 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、[Control Manager 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

Control Manager 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、Control Manager サーバに登録されていない管理下の製品と Control Manager 管理コンソールを介して通信します。

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、Control Manager 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 Control Manager 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

Control Manager では、Control Manager サーバに登録された管理下の製品に対して Control Manager 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

Control Manager 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。

   注意

   - 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 Control Manager 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 Control Manager 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。

   注意

   - 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 Control Manager 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 Control Manager 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 Control Manager 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、Control Manager 管理コンソールを使用して Control Manager 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、Control Manager 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。

Control Manager サービスを停止し再起動する

次の Control Manager サービスのいずれかを再起動する場合は、Windows の [サービス] 画面を使用します。

- Trend Micro Management Infrastructure
- Trend Micro Control Manager

注意

- これらは、Windows OS のバックグラウンドで動作するサービスです。アクティベーションコードを必要とするトレンドマイクロのサービスではありません。
- ここでは Windows Server 2008 R2 で Control Manager を使用していることを前提に説明しています。

手順

1. [スタート] > [すべてのプログラム] > [管理ツール] > [サービス] に移動します。

   [サービス] 画面が表示されます。

2. Control Manager サービスを停止するには、次の手順を実行します。

   a. <Control Manager サービス>を右クリックします。

      ポップアップメニューが表示されます。

   b. [停止] をクリックします。

3. Control Manager サービスを再起動するには、次の手順を実行します。

   a. <Control Manager サービス>を右クリックします。

      ポップアップメニューが表示されます。

   b. [開始] をクリックします。

第 9 章

セキュリティクライア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。

セキュリティクライアントのインストールパッケージをダウンロードする

[セキュリティクライアントのダウンロード] 画面では、Control Manager コンソールからウイルスバスター Corp.または Trend Micro Security (for Mac) のセキュリティクライアントのインストールパッケージを作成できます。この画面を使用して、セキュリティクライアント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したり、対象エンドポイントでセキュリティクライア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 を表示したりできます。

表 9-1. インストール前の設定

セキュリティクライアント	設定
ウイルスバスター Corp.	ウイルスバスター Corp.クライアントのインストール前に、次のことを実行します。 • 初期設定のウイルスバスター Corp.クライア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、ウイルスバスター Corp.クライアントのプロキシサーバ設定を構成します。
Trend Micro Security (for Mac)	Trend Micro Security (for Mac) エージェントをインストールする前に、次のことを実行します。 • 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、ウイルスバスター Corp.クライアントのプロキシサーバ設定を構成します。

エンドポイントにセキュリティクライア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。

- 202 ページの「ウイルスバスター Corp.クライアントのインストール」
- 202 ページの「Trend Micro Security (for Mac) エージェントのインストール」

手順

1. [運用管理] > [セキュリティクライア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: ウイルスバスター Corp.クライアント用の 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: ウイルスバスター Corp.クライアント用の 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 OS: Trend Micro Security (for Mac) 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、セキュリティクライア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。
   - クライアントのダウンロード: セキュリティクライアントのインストールパッケージのコピーを管理下の製品のサーバから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クライア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

ウイルスバスター Corp.サーバの場合、ウイルスバスター Corp.クライアントパッケージでは、クライアントパッケージング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。

ウイルスバスター Corp.クライアントのインストール

ウイルスバスター Corp.クライアントのインストール方法については、ウイルスバスター Corp.のドキュメントを参照してください。

ウイルスバスター Corp.クライア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。

www.go-tm.jp/corp/req

Trend Micro Security (for Mac) エージェントのインストール

このセクションでは、Trend Micro Security (for Mac) 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。

詳細は、Trend Micro Security (for Mac) のドキュメントを参照してください。

エージェントのインストール要件

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

注意

この製品バージョンでは、Mac OS X Snow Leopard™ 10.6.8 (またはそれ以前) がサポートされなくなります。Mac OS X Snow Leopard にインストールされているエージェントがある場合、エージェントを更新しないでください。また、このエージェントを管理できる Trend Micro Security (for Mac) 2.0 SP1 サーバがあることを確認してください。

エージェントのインストール方法とセットアップファイル

Trend Micro Security (for Mac) エージェントは、次のいずれかの方法でインストールできます。

- エンドポイントでインストールパッケージ (`tmsminstall.zip`) を起動して 1 台のエンドポイントにインストールする方法
- Apple Remote Desktop からインストールパッケージ (`tmsminstall.mpkg.zip`) を起動して複数のエンドポイントにインストールする方法
- Trend Micro Security (for Mac) エージェントが含まれる OS イメージを配信して複数のエンドポイントにインストールする方法。インストール後、Trend Micro Security (for Mac) エージェントは Trend Micro Security (for Mac) サーバに自動的に登録されます。

必要なエージェントインストールパッケージを Trend Micro Security (for Mac) サーバから取得し、エンドポイントにコピーします。

パッケージを取得する方法はいくつかあります。

- Trend Micro Security (for Mac) 管理コンソールで、[エージェント] > [エージェントセットアップファイル] の順に選択し、[エージェントインストールファイル] の下のリンクをクリックします。

注意

この画面には、エージェントのアンインストールパッケージへのリンクも表示されています。これらのパッケージを使用してエンドポイントからエージェントプログラムを削除します。削除するエージェントプログラムのバージョンに応じてパッケージを選択します。

Trend Micro Security (for Mac) エージェントのアンインストール方法については、206 ページの「エージェントのアンインストール」を参照してください。

- <サーバのインストールフォルダ>`TMSM_HTML¥ActiveUpdate¥ClientInstall¥`に移動します。
- Control Manager Web コンソールから

エージェントのインストール後のタスク

手順

1. 以下を確認します。
   - Trend Micro Security (for Mac) エージェントのアイコン ( ) がエンドポイントのメニューバーに表示されていること。
   - Trend Micro Security (for Mac) エージェントファイルは <エージェントのインストールフォルダ> にあります。
   - Web コンソールのエージェントツリーにエージェントが表示されていること。エージェントツリーにアクセスするには、メインメニューの [エージェント管理] をクリックします。
2. クライアントコンソールで [アップデート] をクリックして、Trend Micro Security (for Mac) コンポーネントをアップデートします。エージェントは Trend Micro Security (for Mac) サーバからコンポーネントをダウンロードします。

エージェントからサーバに接続できない場合、エージェントはトレンドマイクロのアップデートサーバから直接ダウンロードを実行します。アップデートサーバに接続するには、インターネット接続が必要です。

3. エンドポイントで手動検索を開始します。

次に進む前に

インストール後にエージェントで問題が発生した場合は、エージェントをアンインストールしてから再インストールしてみてください。

エージェントのアンインストール

エージェントプログラムのアンインストールは、そのプログラムで問題が発生した場合にのみ実行します。エンドポイントがセキュリティリスクから保護されるように、すぐにエージェントプログラムを再インストールしてください。

手順

1. Trend Micro Security (for Mac) サーバからエージェントアンインストールパッケージ (`tmsmuninstall.zip`) を取得します。Trend Micro Security (for Mac) Web コンソールで、[エージェント] > [エージェントセットアップ

ファイル] に進み、[エージェントアンインストールファイル] の下にあるリンクをクリックします。

2. エンドポイントにパッケージをコピーして起動します。
3. [名前] と [パスワード] を入力して、アンインストールプロセスを開始します。

注意

対象のエンドポイントに対する管理者権限があるアカウントの名前とパスワードを指定します。

4. アンインストールが正常に実行されたら、[閉じる] をクリックしてアンインストールプロセスを完了します。

次に進む前に

サーバからエージェントの登録を解除します。

1. Web コンソールで、[エージェント管理] をクリックして、アンインストールされたエージェントを選択します。
2. [エージェントツリー管理] > [グループ/エージェントの削除] をクリックします。

第 10 章

製品ディレクトリ

このセクションでは、Control Manager 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] 画面には、Control Manager サーバに登録されているすべての Management Communication Protocol (MCP) 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、296 ページの「ログクエリを使用する」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>: Control Manager 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: Control Manager 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。
- 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

Control Manager 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] のアイコンの詳細については、次のトピックを参照してください。

- 212 ページの「管理下の製品を表すアイコン」
- 213 ページの「接続ステータスアイコン」

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、214 ページの「管理下の製品のステータス概要を確認する」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、217 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、218 ページの「管理下の製品を設定する」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、217 ページの「管理下の製品のタスクを実行する」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、219 ページの「製品ディレクトリからログをクエリする」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、221 ページの「ディレクトリ管理」参照してください。

管理下の製品を表すアイコン

製品ディレクトリは、次のアイコンを使用して、Control Manager サーバに登録された管理下の製品を表します。

アイコン	説明
	Hosted Email Security
	HouseCall
	侵入防御ファイアウォールドメイン
	InterScan eManager
	InterScan VirusWall スタンダードエディション NT
	InterScan VirusWall スタンダードエディション UNIX
	InterScan WebProtect
	InterScan Web Security as a Service
	Network VirusWall
	ウイルスバスター コーポレートエディション
	ウイルスバスター コーポレートエディションドメイン

アイコン	説明
	Partner Security Integration
	InterScan for Microsoft Exchange
	InterScan for Microsoft Exchange クラスタ
	ServerProtect for NetWare インフォメーションサーバ
	ServerProtect for Windows インフォメーションサーバ
	ServerProtect for Windows ドメイン
	ServerProtect for NetWare (一般サーバ)
	ServerProtect for Windows (一般サーバ)
	ServerProtect for Windows ドメイン
	階層化された Control Manager サーバ
	Endpoint Encryption
	Endpoint Encryption ドメイン
	ウイルスバスター ビジネスセキュリティサービス
	ウイルスバスター ビジネスセキュリティサービスドメイン

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、Control Manager 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。

詳細については、194 ページの「管理下の製品との通信」を参照してください。

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
	通信タイムアウト **注意** まだ通信を確立しようとしています。	不明
	停止中 **注意** 再試行が 3 回失敗した後は、通信を確立できません。	停止中

管理下の製品のステータス概要を確認する

Control Manager 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 Control Manager 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

Control Manager 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、Control Manager 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。
   - Control Manager 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。共通タスクには次のものが含まれます。

- コンポーネントの配信
- 検索コマンドの送信
- クライアントの同期

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 Control Manager 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、281 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、Control Manager 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

Control Manager を使用すると、管理下の製品の管理コンソールにログオンするか、または Control Manager 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: ドメインのログオン情報を使用して管理下の製品の管理コンソールにログオンします。
- <管理下の製品>の設定: 管理下の製品の管理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、管理下の製品の管理コンソールにログオンします。
  - [はい] をクリックして、管理下の製品の管理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

Control Manager 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、[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、296 ページの「ログクエリ」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

Control Manager 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。

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。

注意点	影響
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。

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、Control Manager 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、102 ページの「ユーザアカウント」を参照してください。

ディレクトリ管理を使用する

[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。

Control Manager 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、Control Manager 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。

重要

製品ディレクトリ構造を変更すると、Control Manager 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、102 ページの「ユーザアカウント」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。

     警告!

     管理下の製品が含まれるカスタムフォルダを削除すると、Control Manager は管理下の製品を Control Manager サーバから自動的に登録解除します。

   - 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

Control Manager では、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。

注意

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もあります。

- Control Manager 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する] を選択した場合
- 破損した Control Manager 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

手順

1. 管理下の製品のサーバで Control Manager サービスを再起動します。

   注意

   詳細については、198 ページの「Control Manager サービスを停止し再起動する」参照してください。

2. エージェントがエージェント自身を再登録するのを待ちます。

   注意

   初期設定では、古い Control Manager エージェントはサーバへの接続を 8 時間おきに確認します。レコードが削除されていることを検出すると、エージェントは自動的に自身を再登録します。

3. 手動で MCP エージェントを Control Manager サーバに再登録します。

第 11 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。

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

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、『Control Manager ウィジェットおよびポリシー管理ガイド』を参照してください。

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。

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

   注意

   管理下の製品またはエンドポイントを対象に含めるには、管理下の製品またはエンドポイントの製品のバージョンが Control Manager のポリシー管理をサポートしていることを確認します。サポートされる製品のバージョンに関する情報は、[ポリシーテンプレートの設定] 画面 ([ポリシー] > [ポリシーリソース] > [ポリシーテンプレートの設定]) で確認できます。

   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、233 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、229 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、244 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、Control Manager 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、Control Manager 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化されていることを確認します。

- ウイルスバスター Corp.クライア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。
  - ウイルスバスター Corp.クライアントの継承、カスタマイズ、拡張可能な設定の一覧については、234 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、238 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。Control Manager 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。

   Control Manager 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。Control Manager 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 Control Manager がポリシー設定を適用するたびに上書きされます。

   - Control Manager では、24 時間ごとに対象にポリシー設定が適用されます。ポリシーの適用は 24 時間ごとに行われるため、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。
- Control Manager のポリシーで割り当てられたウイルスバスター Corp. クライアントが別のウイルスバスター Corp. ドメインに移動された場合、クライアント設定は、そのウイルスバスター Corp. ドメインで定義された設定に一時的に変更されます。Control Manager で再度ポリシーを適用すると、クライア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。
  - ウイルスバスター Corp.
  - Mobile Security
  - Trend Micro Security (for Mac)
- 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、Control Manager 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。

Control Manager 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。

Control Manager 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、231 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 Control Manager 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** • 最大 X 個の IP アドレスの範囲を指定できます。 • 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 Control Manager に登録された場合、その管理下の製品またはエンドポイントを IP アドレスで検索できるようになるまで約 1 時間かかります。

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

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 Control Manager 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。Control Manager 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

Control Manager 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。Control Manager 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

  Control Manager では、エンドポイントが必ず適切なポリシーに割り当てられるように、日次エンドポイント割り当てスケジュールが使用されます。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。

前述の処理が実行される場合、Control Manager 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 11-1. 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 Control Manager 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 Control Manager 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、132 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

Control Manager 管理者は、ウイルスバスター Corp.クライア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。ウイルスバスター Corp.管理者は、ウイルスバスター Corp.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、Control Manager からウイルスバスター Corp.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、Control Manager 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 [予約検索の設定]→[対象] タブ→[スケジュール] 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]/[予約検索の設定]→[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	●		●
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]/[予約検索の設定]→[検索除外] タブ	●		● 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 [子ポリシーの制限] 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

ウイルスバスター Corp.クライアントの子ポリシーの設定はコピーできません。ウイルスバスター Corp.クライア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、Control Manager 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。
- Control Manager 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、ウイルスバスター Corp.クライアントの親ポリシーが必要になります。ウイルスバスター Corp.クライアントの親ポリシーは、[親ポリシー] 列の値が「なし」になっています。

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 [ウイルスバスター Corp.クライアント] 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、234 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、Control Manager 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。
   - Control Manager 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、Control Manager から対象にポリシーが配信されます。

ウイルスバスター Corp.クライア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、234 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。Control Manager 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。Control Manager 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。

Control Manager 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 Control Manager 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。

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、247 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 Control Manager 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。

ウイルスバスター Corp.クライアントのポリシーで、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 Control Manager 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、Control Manager 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 Control Manager 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。Control Manager 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 11-2. 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。 • Control Manager 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、Control Manager 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。 • Control Manager 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。
親ポリシー	この列は、ウイルスバスター Corp.クライア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、ウイルスバスター Corp.クライアントを選択した場合にのみ表示されます。 子ポリシーの場合、親ポリシーから変更された設定の数が表示されます。すべての設定が親ポリシーと同じ場合は、「0」と表示されます。 ポリシーが子ポリシーでない場合は、「なし」と表示されます。

列	説明
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か、オフラインクライアント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。
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。

列	説明
所有者	現在ポリシーを割り当てられているユーザが表示されます。 **注意** 初期設定の所有者は、ポリシーを作成したユーザです。 • ポリシーの所有者を、指定された適用先へのアクセス権がないユーザアカウントに変更する場合、新しい所有者はポリシーの設定を変更できますが、ポリシーデータは表示できません。 • ポリシーを Active Directory グループに割り当てることで、複数の所有者を割り当てることもできます。 詳細については、243 ページの「ポリシーの所有者を変更する」参照してください。
最終編集者	ポリシーを最後に編集したユーザが表示されます。

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。Control Manager 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、ウイルスバスター Corp.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。

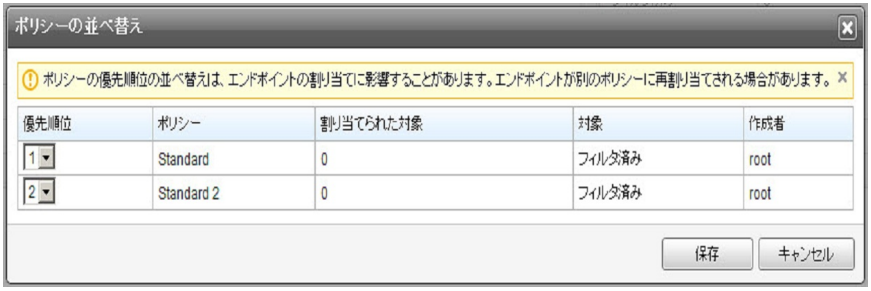
   [ポリシー管理] 画面が表示されます。

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. [並べ替え] 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、Control Manager 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。

ポリシーテンプレートのアップデート

[ポリシーテンプレートの設定] 画面には、管理者が有効にできるまたはアップグレードできる次のコンポーネントのリストが表示されます。

- ポリシー管理フレームワーク: 全体的なポリシー構造
- 製品サポート: 管理下の製品およびエンドポイント用の設定テンプレート

注意

ポリシー管理をサポートする製品バージョンを確認するには、[テンプレートのバージョン] 列の情報アイコンの上にマウスのカーソルを移動します。

手順

1. 最新の Control Manager ウィジェットプールおよびポリシーテンプレート (Control Manager 6.0 以降向け) コンポーネントをダウンロードします。

   Control Manager コンポーネントのダウンロード方法の詳細については、274 ページの「コンポーネントアップデート」を参照してください。

   [ダッシュボード] 画面および [ポリシー管理] 画面の上部に青色の通知が表示されます。

2. いずれかの画面の通知ボックス内の [アップデート] をクリックします。
3. アップデートが完了したら、[OK] をクリックします。

   画面の表示が更新され、ログオン画面が表示されます。

4. 管理コンソールにログオンします。
5. [ポリシー] > [ポリシーリソース] > [ポリシーテンプレートの設定] に移動します。

   [ポリシーテンプレートの設定] 画面が表示されます。

6. [ポリシーフレームワーク] 行の [アップデート <バージョン番号>] をクリックします。
7. 新しいポリシーテンプレートを追加するには、[処理] 列の [有効にする] をクリックします。

   これによって管理者は、[ポリシー管理] 画面で [製品] リストから新しい設定テンプレートを選択できるようになります。

8. 既存のテンプレートをアップデートするには、[処理] 列の [アップデート <バージョン番号>] をクリックします。

   注意

   アップデートの詳細を表示するには、[処理] 列の [詳細] をクリックします。

   アップデートが完了すると、管理者は、既存のポリシーを編集することによって、アップデートされた機能を確認できます。[設定] の下で、新規機能タイトルの横に赤色のメッセージが表示されます。

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。

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、251 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、256 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、258 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、251 ページの「事前定義済みのパターン」および252 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、こちらを参照してください。

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、253 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 11-3. 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]
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

条件	ルール	例
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 (253 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、Control Manager 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、こちらを参照してください。

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、259 ページの「事前定義済みのキーワードリス

ト」および260 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

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

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

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、260 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 11-4. 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。

条件	ルール
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。
<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。
   - いずれかのキーワードと一致
   - 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、265 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265 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、次の情報漏えい対策に関する Web サイトをご確認ください。http://tmqa.jp/dlp_list

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、265 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 11-5. 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、265 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。

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 Control Manager 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 11-6. 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	Control Manager 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	Control Manager 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	Control Manager がポリシーを正常に配信しました。	なし
エンドポイントからサーバに接続できません	• エンドポイントは、ポリシー設定を受信しませんでした。 • サーバがビジー状態です。	• エンドポイントの接続ステータスを確認します。 • エンドポイントを社内のネットワークに接続します。 • ポリシーステータスがアップデートされるのを待機します。

ポリシーステータス	説明	対処の提案
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 Control Manager 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。
アクティベートされていない製品サービス	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アクティベートされていません。	管理下の製品で関連サービ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	Control Manager 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。

ポリシーステータス	説明	対処の提案
<Control Manager サーバ名>による管理	現在、別の Control Manager 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	Control Manager は、対象の管理下の製品へのアクセスにシングルサインオン機能を使用できません。	• 製品ディレクトリでシングルサインオン機能を確認します。 • MCP エージェントの接続ステータスを確認します。 • [管理下のサーバ] リストで、サーバ接続の種類を [自動] から [手動] に変更します。
Web サービスの設定エラーが発生しました	Web サービスエラーが発生しました。	IIS 設定を確認します。
製品通信エラーが発生しました	製品コンソールにアクセスできません。	• 管理下の製品の管理コンソールに接続できるかどうか確認します。 • 管理下の製品の設定を確認します。
製品に接続できません	Control Manager 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。

ポリシーステータス	説明	対処の提案
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 12 章

コンポーネントアップデート

このセクションでは、Control Manager 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

Control Manager 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ホストします。

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。Control Manager 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

Control Manager 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	Control Manager 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	Control Manager 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。

ダウンロード元

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 Control Manager サーバを設定します。Control Manager 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、Control Manager は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、Control Manager 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。

Control Manager サーバがアップデート元から新規のコンポーネントバージョンをダウンロードした後、指定された時間、または遅延期間が生じた後のいずれかに、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 Control Manager を設定できます。

コンポーネントのアップデートを細かく分けて管理する場合、さまざまな配信スケジュールに基づいて、アップデートされたコンポーネントを選択した管理下の製品に配信するように Control Manager 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。
- Control Manager 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、Control Manager 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。
- 管理下の製品が Control Manager サーバと通信して、コンポーネントをダウンロードするタイミングを設定できます。

  詳細については、195 ページの「エージェント通信スケジュールの設定」を参照してください。

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

Control Manager 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、予約コンポーネントの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 Control Manager を設定することもできます。

注意

Control Manager 7.0 に移行すると、[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 7.0 に移行すると、[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. [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、274 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、Control Manager 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

   Control Manager 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 Control Manager 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。

このオプションを選択すると、Control Manager では選択したカテゴリ内のすべての既存コンポーネントについてもアップデートがダウンロードされます。

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、Control Manager 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既存コンポーネントのアップデー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 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、275 ページの「ダウンロード元」を参照してください。

注意

Control Manager 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、285 ページの「コンポーネントおよびライセンスのアップデート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: Control Manager 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、Control Manager 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。 • 開始時刻: Control Manager 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: Control Manager 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、276 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、Control Manager 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	Control Manager 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、217 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、Control Manager 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 Control Manager を設定することもできます。

警告!

Control Manager 7.0 に移行すると、[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. [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、274 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、Control Manager 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

   Control Manager 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 Control Manager 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。

   このオプションを選択すると、Control Manager では選択したカテゴリ内のすべての既存コンポーネントについてもアップデートがダウンロードされます。

   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、Control Manager 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既存コンポーネントのアップデー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 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、275 ページの「ダウンロード元」を参照してください。

注意

Control Manager 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、285 ページの「コンポーネントおよびライセンスのアップデート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: Control Manager 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、Control Manager 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。 • 開始時刻: Control Manager 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: Control Manager 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、276 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、Control Manager 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	Control Manager 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、217 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。

コンポーネントおよびライセンスのアップデートのためにプロキシを設定する

Control Manager を使用すると、コンポーネントのダウンロードとライセンスのアップデートにプロキシサーバを使用できます。

手順

1. [運用管理] > [設定] > [プロキシ設定] に移動します。

   [接続の設定] 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およびクラウドサービス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。

   - 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 13 章

コマンド追跡

このセクションでは、Control Manager 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、Control Manager 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、Control Manager 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、289 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
発行済み	Control Manager 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
コマンド	Control Manager サーバが発行したコマンドの種類
ユーザ (アカウント)	コマンドをトリガしたユーザの名前
成功	コマンドを完了した管理下の製品の数 [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、290 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 [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、290 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 [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、290 ページの「コマンド詳細」を参照してください。
すべて	Control Manager がコマンドを発行した管理下の製品の総数 [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、290 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。
   - 発行済み —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、290 ページの「コマンド詳細」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 Control Manager サーバに応答が最後に送信された日時
サーバ/エンティティ	管理下の製品のサーバのホスト名
ステータス	発行されたコマンドのステータス
説明	コマンドのステータスに関する追加の詳細

注意

[コマンド詳細] 画面は、30 秒ごとに更新されます。

コマンドのタイムアウト設定

[通信タイムアウトの設定] 画面を使用して、コマンドタイムアウトを設定します。コマンドがタイムアウトになると、Control Manager は発行済みのコマンドの実行を停止します。

手順

1. [運用管理] > [設定] > [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. [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

3. [保存] をクリックします。

パート IV

セキュリティ監視

第 14 章

ログ

本章では、Control Manager で生成されたログおよび Control Manager 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

Control Manager を使用すると、Control Manager データベースを照会して Control Manager 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。

Control Manager 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 Control Manager 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、Control Manager 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 Control Manager 管理者と共有したりできます。

注意

Control Manager 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、219 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. [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、Control Manager 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、300 ページの「ログクエリデータビュー」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、管理下の製品を探して選択します。

      - 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。

   c. 特定の管理下の製品または製品の種類を選択します。

   d. [OK] をクリックして、選択した管理下の製品または製品の種類を適用します。

4. [時間] 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、300 ページの「ログクエリデータビュー」、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

Control Manager 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。

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。

エクスポート中であることを示すメッセージが表示されます。

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、387 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 Control Manager 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 Control Manager 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。

ログクエリデータビュー

Control Manager のログの種類は、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。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。

表 14-1. セキュリティログ

ログの種類	データビュー	説明
システムイベント:		
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、566 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、580 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、639 ページの「不審ファイルの詳細情報」を参照してください。

ログの種類	データビュー	説明
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、609 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、コンピュータの特定の領域での変更を監視するために使用します。 詳細については、613 ページの「変更監視情報」を参照してください。
Endpoint Application Control 違反	エンドポイントアプリケーションコントロール違反詳細情報	違反しているポリシーやルールの名前など、ネットワーク上のエンドポイントアプリケーション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、610 ページの「エンドポイントアプリケーションコントロール違反詳細情報」を参照してください。
デバイスコントロール違反	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、610 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、605 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。

ログの種類	データビュー	説明
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、603 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。
機械学習型検索の詳細情報	機械学習型検索の詳細情報	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、640 ページの「機械学習型検索の詳細情報」を参照してください。
仮想アナライザによる検出	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、642 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。
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。 詳細については、599 ページの「スパムメール接続情報」を参照してください。
コンテンツ違反	コンテンツ違反詳細情報	ネットワーク上の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、594 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	不審または不正な動作パターンを含むメー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、595 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。

ログの種類	データビュー	説明
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出されたポリシー違反やルール違反に関するセキュリティの脅威情報が表示されます。 詳細については、620 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、619 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。 詳細については、601 ページの「ファイアウォール違反詳細情報」参照してください。
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、602 ページの「ネットワークコンテンツ検査情報」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、611 ページの「IPS の詳細情報」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、637 ページの「C&C コールバック詳細情報」参照してください。

ログの種類	データビュー	説明
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、631 ページの「脅威の兆候の詳細情報」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、606 ページの「アプリケーションアクティビティの詳細」参照してください。
軽減	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、635 ページの「軽減処理の詳細情報」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、636 ページの「相関の詳細情報」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、650 ページの「情報漏えい対策イベント情報」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、654 ページの「データ検出の情報漏えい対策検出情報」参照してください。

表 14-2. 製品情報

ログの種類	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	Control Manager サーバに登録されている管理下の製品に関する具体的な情報が表示されます。 詳細については、659 ページの「製品のステータス情報」参照してください。
製品のイベント	製品のイベント情報	管理下の製品の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、662 ページの「製品のイベント情報」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	管理下の製品に関する監査情報が表示されます。 詳細については、663 ページの「製品監査イベントログ」参照してください。
Control Manager:		
コマンド追跡	コマンド追跡情報	管理下の製品に対して発行されたコマンドに関する具体的な情報が表示されます。 詳細については、673 ページの「コマンド追跡情報」参照してください。
Control Manager のイベント	Control Manager のイベント情報	Control Manager サーバの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、672 ページの「Control Manager のイベント情報」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	Control Manager へのユーザアクセス、および Control Manager にログオン中にユーザが実行するアクティビティが表示されます。 詳細については、672 ページの「ユーザアクセス情報」参照してください。

ログの種類	データビュー	説明
製品ライセンス	製品ライセンス詳細情報	アクティベーションコードに関する情報、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。 詳細については、657 ページの「製品ライセンス詳細情報」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 Control Manager 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!

Control Manager は、管理下の製品から Control Manager 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. [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 Control Manager 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。

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。

ヒント

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) 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ます。

手順

1. [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. 対応する行で [すべて削除] をクリックします。

      警告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 15 章

通知

本章では、Control Manager 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

Control Manager 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 のシステムログ通知、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、311 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
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、336 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、339 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、349 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、365 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。
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、369 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。

イベントのカテゴリ	説明
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、376 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、311 ページの「SMTP サーバを設定する」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、312 ページの「SNMP トラップを設定する」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、313 ページの「Syslog を設定する」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、314 ページの「アプリケーションを設定する」参照してください。

SMTP サーバを設定する

Control Manager 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

Control Manager 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. [通知] > [通知方法の設定] に移動します。

   [通知方法の設定] 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. [ESMPT 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

Control Manager 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. [通知] > [通知方法の設定] に移動します。

   [通知方法の設定] 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

Control Manager 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. [通知] > [通知方法の設定] に移動します。

   [通知方法の設定] 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

Control Manager 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。

手順

1. [通知] > [通知方法の設定] に移動します。

   [通知方法の設定] 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。Control Manager 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、315 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、316 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. [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、132 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. [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、132 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。

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. [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。

条件	説明
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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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、677 ページの「通知メッセージのカスタマイズ」および679 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。
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、677 ページの「通知メッセージのカスタマイズ」および679 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
Syslog 通知	Control Manager 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. [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。

設定	説明
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、677 ページの「通知メッセージのカスタマイズ」および679 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. [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、678 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。

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. [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、677 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. [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。

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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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。
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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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。

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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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。
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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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、677 ページの「通知メッセージのカスタマイズ」および678 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. [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、677 ページの「通知メッセージのカスタマイズ」および680 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、677 ページの「通知メッセージのカスタマイズ」および680 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。
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。 Control Manager 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。

セキュリティレベル違反

セキュリティ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. [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、[セキュリティレベル違反] をクリックします。

   [セキュリティレベル違反] 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、677 ページの「通知メッセージのカスタマイズ」および680 ページの「セキュリティレベル違反トークン変数」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、677 ページの「通知メッセージのカスタマイズ」および680 ページの「セキュリティレベル違反トークン変数」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	ログメッセージを IP ネットワークで転送する標準です。 Control Manager 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. [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
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、677 ページの「通知メッセージのカスタマイズ」および681 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. [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、677 ページの「通知メッセージのカスタマイズ」および681 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. [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。

設定	説明
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、677 ページの「通知メッセージのカスタマイズ」および681 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. [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、677 ページの「通知メッセージのカスタマイズ」および681 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. [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、677 ページの「通知メッセージのカスタマイズ」および681 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. [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、677 ページの「通知メッセージのカスタマイズ」および681 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. [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、677 ページの「通知メッセージのカスタマイズ」および681 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. [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、677 ページの「通知メッセージのカスタマイズ」、683 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684 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、677 ページの「通知メッセージのカスタマイズ」、683 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684 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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」、683 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684 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、677 ページの「通知メッセージのカスタマイズ」、683 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684 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
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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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. [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 ー 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 ー 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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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/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. [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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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 － 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. [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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」および683 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、677 ページの「通知メッセージのカスタマイズ」および683 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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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. [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、677 ページの「通知メッセージのカスタマイズ」および684 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、677 ページの「通知メッセージのカスタマイズ」および684 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	Control Manager 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

Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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。

リアルタイム検索開始

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. [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、[リアルタイム検索開始] をクリックします。

   [リアルタイム検索開始] 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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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. [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、677 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、677 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	Control Manager 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. [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、677 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、677 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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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. [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、677 ページの「通知メッセージのカスタマイズ」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、677 ページの「通知メッセージのカスタマイズ」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	Control Manager 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 16 章

レポート

このセクションでは、Control Manager 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

Control Manager 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。

Control Manager 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。Control Manager 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、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。

レポートデータビューの詳細については、561 ページのデータビューを参照してください。

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、389 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、389 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。Control Manager 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、389 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 Control Manager 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。Control Manager 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] > [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。

     Control Manager 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 16-1. 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、393 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、394 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、397 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、400 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、402 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、405 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 16-1. 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、389 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。

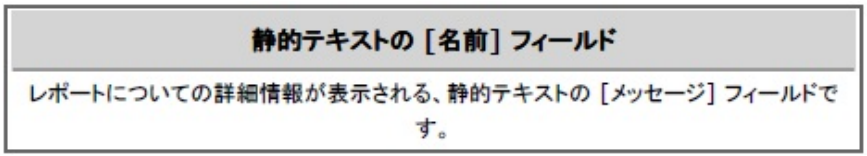


図 16-2. 静的テキストレポート出力例

4. [保存] をクリックして、[レポートテンプレートの追加] 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 (横)] 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、389 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 (横)] 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、561 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。

   Control Manager 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、389 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、561 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。

   Control Manager 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、389 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、561 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。

Control Manager 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、389 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、561 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。

   Control Manager 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、389 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、561 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。

Control Manager 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、408 ページの「1 回限りのレポートを作成する」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] > [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、389 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。

   注意

   - このバージョンの Control Manager では、ActiveX 形式および Crystal Report 形式のサポートが廃止されました。
   - Control Manager の前のバージョンから移行した場合、以前に Control Manager 7.0 で生成された Crystal Report を引き続きダウンロードできます。

   - 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. レポート情報を提供する管理下の製品またはその管理下の製品を含むフォルダを選択します。

9. たとえば、Network VirusWall Enforcer デバイスからのデータをレポートに含める場合は、次のいずれかを選択してレポート生成元クライアントを指定します。

   - すべてのクライアント - すべての Network VirusWall Enforcer デバイスがレポートの生成元になります。
   - IP アドレスの範囲 - 特定の IP アドレスの範囲がレポートの生成元になります。
   - セグメント - 特定のネットワークセグメントがレポートの生成元になります。

10. [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。

11. レポートの期間を指定します。

12. [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。

13. (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。

14. [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。

15. 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] > [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、413 ページの「予約レポートの追加」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、417 ページの「予約レポートを編集する」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、417 ページの「予約レポートを編集する」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、421 ページの「予約レポートの表示」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] > [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、389 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。

注意

このバージョンの Control Manager では、ActiveX 形式および Crystal Report 形式のサポートが廃止されました。

- 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. レポート情報を提供する管理下の製品またはその管理下の製品を含むフォルダを選択します。

9. たとえば、Network VirusWall Enforcer デバイスからのデータをレポートに含める場合は、次のいずれかを選択してレポート生成元クライアントを指定します。

   - すべてのクライアント - すべての Network VirusWall Enforcer デバイスがレポートの生成元になります。
   - IP アドレスの範囲 - 特定の IP アドレスの範囲がレポートの生成元になります。
   - セグメント - 特定のネットワークセグメントがレポートの生成元になります。

10. [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。

11. 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、または最後の日、から指定された日に生成されます。

12. 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。

13. 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。

14. [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。

15. (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。

16. [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 Control Manager によって有効にされます。

17. 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] > [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、389 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。

   注意

   このバージョンの Control Manager では、ActiveX 形式および Crystal Report 形式のサポートが廃止されました。

   - 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. レポート情報を提供する管理下の製品またはその管理下の製品を含むフォルダを選択します。

9. たとえば、Network VirusWall Enforcer デバイスからのデータをレポートに含める場合は、次のいずれかを選択してレポート生成元クライアントを指定します。
   - すべてのクライアント - すべての Network VirusWall Enforcer デバイスがレポートの生成元になります。
   - IP アドレスの範囲 - 特定の IP アドレスの範囲がレポートの生成元になります。
   - セグメント - 特定のネットワークセグメントがレポートの生成元になります。

10. [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。

11. 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、または最後の日、から指定された日に生成されます。

12. 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。

13. 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。

14. [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。

15. (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。

16. [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] > [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] > [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 17 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

Control Manager 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。

機能	必須の製品	オプションの製品
脅威の監視	• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降) **注意** 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。	• ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 10.0 (またはそれ以降) • Endpoint Sensor 1.5 (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 2 (またはそれ以降) • InterScan for Microsoft Exchange 12.5 (またはそれ以降) • Cloud App Security 5.0 (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、427 ページの「不審オブジェクトリスト」および449 ページの「Connected Threat Defense 製品の統合」を参照してください。	• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降) 注意 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。	• Smart Protection Server 3.0 Patch 1 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 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 2 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降)
不審オブジェクトのサンプルの送信	• Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降)	• Deep Security 10.0 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Endpoint Sensor 1.5 (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 2 (またはそれ以降) • InterScan for Microsoft Exchange 12.5 (またはそれ以降) • Deep Discovery Email Inspector 3.0 (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	• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降)	• ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 10.0 (またはそれ以降) • Endpoint Sensor 1.5 (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 2 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降)
不審オブジェクト検出時の処理 詳細については、430 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。	• Control Manager 7.0 (またはそれ以降)	• Smart Protection Server 3.0 Patch 1 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 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 2 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降)
影響診断	• Control Manager 7.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降)	• なし

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、446 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。	• Control Manager 7.0 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降)	• Endpoint Sensor 1.5 (またはそれ以降)
IOC の管理	• Control Manager 7.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降)	• なし

不審オブジェクトリスト管理

Control Manager では、不審オブジェクトリストを管理下の製品の間で同期したり、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。

Control Manager 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 Control Manager と同期できる製品の詳細については、424 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

Control Manager 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合わせ、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、Control Manager 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、430 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 Control Manager サーバに送信します。 Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] > [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のリストを表示します。
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	Control Manager 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。 Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] > [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設定を確認します。 Control Manager は、除外リストを利用する仮想アナライザ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、429 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	Control Manager の管理者は、[運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] で、仮想アナライザの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、441 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

Control Manager 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. [運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] 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 SHA-1: ファイルの 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。

  Control Manager 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。

EXAMPLE	説明
https://*.domain.com/	ドメイン「domain.com」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。
*.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」のすべてのサブドメインと、サブディレクトリ「abc」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。

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 Control Manager 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。

表 17-1. 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
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 10.2 (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 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。

製品	仮想アナライザリスト	ユーザ指定リスト
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
InterScan Web Security Virtual Appliance 6.5 Patch 2 (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 3.0 Patch 1 (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 Control Manager 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。Control Manager は、管理下の製品から送信されたログを解釈して、Control Manager 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、Control Manager 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。

Control Manager 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。

手順

1. [運用管理] > [不審オブジェクト] > [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します] 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 Control Manager を仮想アナライザとして設定する際に使用します。

      - サービス URL: Control Manager のサービス URL
      - API キー: 管理下の製品で Control Manager 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. [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

      Control Manager は、Deep Discovery Inspector および Deep Discovery Analyzer によって分析された不審 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。

   b. 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。

c. (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。

d. 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

4. [保存] をクリックします。

5. [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、Control Manager 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。

- 435 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」
- 437 ページの「Endpoint Sensor を使用して影響を分析する」

注意

Control Manager 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。Control Manager 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

Control Manager 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。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • 少なくとも 1 つのオプション製品	• Control Manager によって管理されるトレンドマイクロ製品 • Endpoint Sensor 1.5 (またはそれ以降) 重要 • Endpoint Sensor 1.5 は、ファイルおよび IP アドレスの不審オブジェクトの種類に関する情報のみを提供します。 • Endpoint Sensor 1.6 (またはそれ以降) は、ファイル、IP アドレスおよびドメインの不審オブジェクトの種類に関する情報のみを提供します。

手順

1. Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。
2. 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 を使用して影響を分析する

Endpoint Sensor は、エージェントと通信し、クライア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。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降) **重要** • Endpoint Sensor 1.5 は、ファイルおよび IP アドレスの不審オブジェクトの種類に関する情報のみを提供します。 • Endpoint Sensor 1.6 (またはそれ以降) は、ファイル、IP アドレスおよびドメインの不審オブジェクトの種類に関する情報のみを提供します。	• なし

手順

1. Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。
2. 診断するオブジェクトの横のチェックボックスをオンにします。
3. [影響の診断] をクリックします。

   Endpoint Sensor はエージェントと通信し、検出された不審オブジェクトのクライアントログを評価します。

Endpoint Sensor の Retro Scan

Retro Scan は、指定された検索条件に基づいて、過去のイベントとそのアクティビティチェーンを調査します。調査結果は、疑わしいアクティビティの

実行フローを示すマインド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。

Retro Scan の調査では、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

Retro Scan は、エンドポイントのイベント履歴が格納された、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、リソースを消費しません。

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ついて概要が表示されます。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (または以降) または Deep Discovery Analyzer 5.1 (または以降) • [影響診断] および [軽減] のデータを表示するには、少なくとも 1 つのオプションの製品が必要です。	• Control Manager によって管理されるトレンドマイクロ製品 • Endpoint Sensor 1.5 (またはそれ以降) 重要 • Endpoint Sensor 1.5 は、ファイルおよび IP アドレスの不審オブジェクトの種類に関する情報のみを提供します。 • Endpoint Sensor 1.6 (またはそれ以降) は、ファイル、IP アドレスおよびドメインの不審オブジェクトの種類に関する情報のみを提供します。

手順

1. Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] 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。 Control Manager 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 5.1 (またはそれ以降) • Deep Discovery Endpoint Inspector 3.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降)
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。
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。 Control Manager 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。
影響の診断と軽減	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。 [不審アクティビティ] 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

Control Manager 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、または侵入の痕跡 (IOC) 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、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。 442 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」 430 ページの「不審オブジェクト検出時の処理」
侵入の痕跡	IOC ファイルをインポートしてネットワークのエンドポイントで詳細な履歴分析を実施し、脅威の兆候が環境に影響を及ぼしているかどうかを判断します。 IOC での影響診断には、エンドポイントの動作の推移に関する詳細なログ情報が必要です。Endpoint Sensor 1.5 (またはそれ以降) がインストールされているエンドポイントのみが、この種類の詳細分析に必要なログ情報を収集します。 ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) のクライアントと統合することで、感染したエンドポイントを隔離し、エンドポイントで識別された脅威が拡散することを防ぎます。 444 ページの「影響を診断して 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。Control Manager には、ファイル、ファイル SHA-1、ドメイン、IP アドレス、および 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 (ドメインオブジェクトを除く) の検出後にサポート対象のトレンドマイクロの製品で実行する検索処理を指定することもできます。

手順

1. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [追加] をクリックします。

3. 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 SHA-1: ファイルの 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。

4. 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

この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。

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。

   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. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。
2. [インポート] をクリックします。
3. 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。

4. [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。

影響を診断して IOC に対応する

適切な形式の IOC ファイルを信頼された外部ソース (セキュリティフォーラムや他の Deep Discovery 仮想アナライザ製品) から取得した後、そのファイルを Control Manager にインポートしてネットワーク内に脅威が存在するかどうかを判別し、脅威が他のエンドポイントに拡散するのを防ぐために軽減処理を実行します。

重要

- 外部 IOC データの影響を診断するには、Endpoint Sensor 1.5 (またはそれ以降) が Control Manager に登録され、対象エンドポイントにインストールされている必要があります。
- エンドポイントを隔離するには、ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) のクライアントをインストールし、対象エンドポイントでウイルスバスター Corp.のファイアウォールを有効にする必要があります。

手順

1. [運用管理] > [侵入の痕跡] に移動します。

   [侵入の痕跡 (IOC)] 画面が表示されます。

2. [追加] をクリックします。
3. 調査のソースとして使用する IOC ファイルを選択します。
4. [アップロード] をクリックします。

   ファイルに含まれるサポート対象の痕跡を示した画面が表示されます。

5. 調査を開始するには、リストから IOC ファイルを選択して、[影響の診断] をクリックします。

   [調査を開始する] 画面が表示されます。

6. [対象エンドポイント] ドロップダウンから、[すべて] または [指定] を選択して、調査するエンドポイント名または IP アドレスを入力します。

   複数のエンドポイント名または IP アドレスを追加するには、新しい行を使用します。

7. [調査を開始する] をクリックします。

   注意

   調査が完了するまでには多少の時間がかかります。[進行状況] 列で調査の進行状況を確認してください。

8. 診断が完了したら、[危険] 列の数字をクリックして詳細を確認するか、または感染したエンドポイントで処理を実行します。

   注意

   [保留/問題あり] 列には、まだ診断が終了していないエンドポイントの数が表示されます。たとえば、エンドポイントがネットワークに再接続するまで、そのエンドポイントでは診断を開始できません。

   [侵入の痕跡]→[危険性の高いエンドポイント] 画面が表示されます。

9. 不審なオブジェクトがネットワーク全体に拡散しないようにするには、[処理] 列で [隔離] をクリックして、感染したエンドポイントでネットワークトラフィックを停止します。

   重要

   エンドポイントを隔離するには、ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) のクライアントをインストールし、対象エンドポイントでウイルスバスター Corp.のファイアウォールを有効にする必要があります。

10. [許可するトラフィックの変更] ボタンをクリックして、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必要に応じて設定します。

    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。

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。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) **重要** エンドポイントを隔離するには、ウイルスバスター Corp.クライアントをインストールし、対象エンドポイントでウイルスバスター Corp.のファイアウォールを有効にする必要があります。	• Endpoint Sensor 1.5 (またはそれ以降)

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 - <名前>] 画面で [タスク] > [隔離] をクリックします。

   Control Manager 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。

   - エンドポイントのクライアントでサポート対象外のバージョンが実行されています。
   - Control Manager 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ありません。

5. [エンドポイント - <名前>] 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. Control Manager 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] ノードをクリックします。
7. [許可するトラフィックの変更] ボタンをクリックして、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必要に応じて設定します。

   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 - <名前>: [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]: 表の中のエンドポイントの行を選択して、[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。

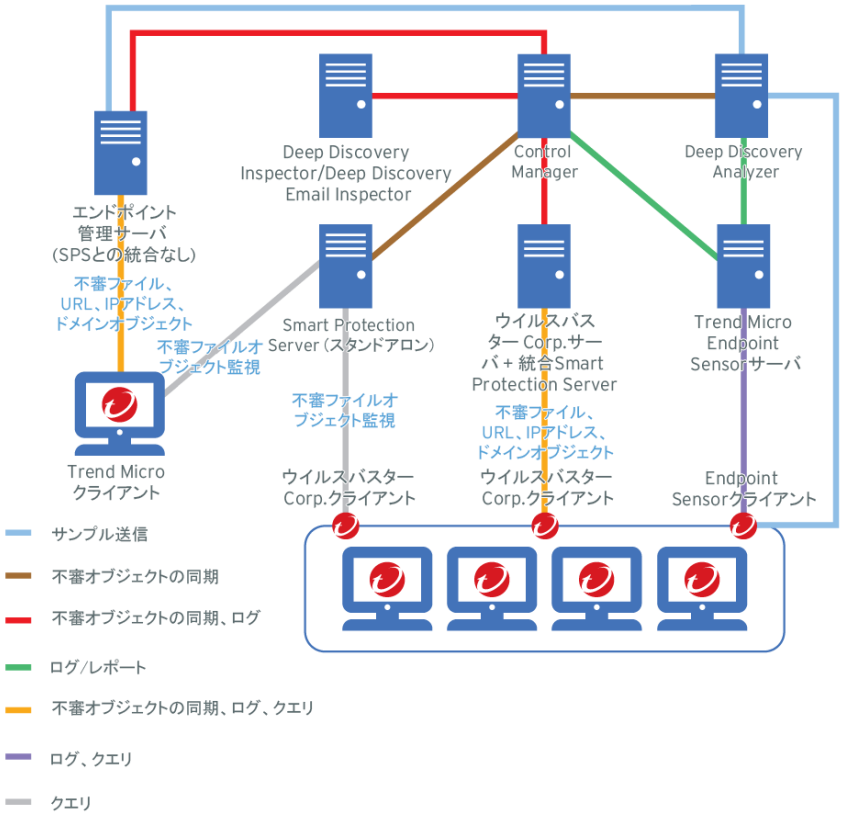


図 17-1. エンドポイントの保護

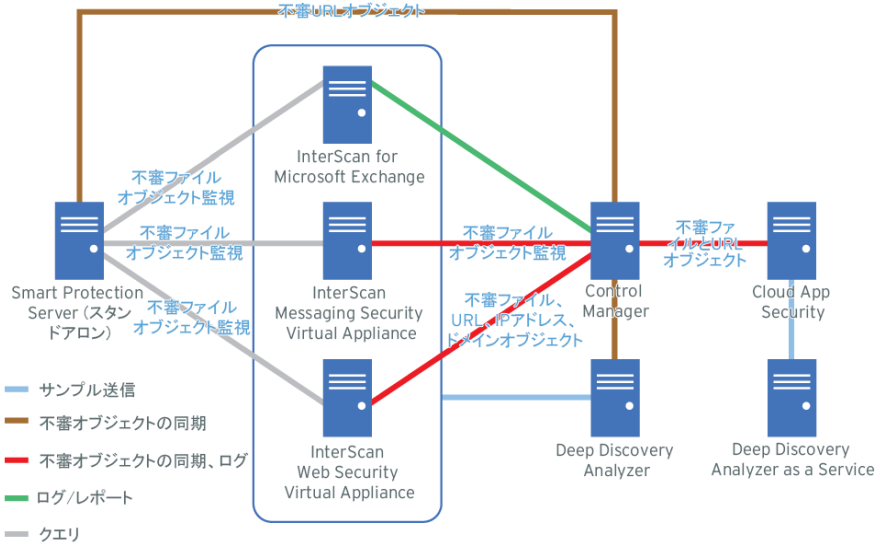


図 17-2. メッセージングとネットワークセキュリティ

Control Manager 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を比較することにより、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 Control Manager 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。

- 451 ページの「Control Manager」
- 452 ページの「Deep Discovery Analyzer」
- 453 ページの「Trend Micro Endpoint Sensor」
- 453 ページの「Deep Discovery Inspector」
- 454 ページの「Deep Security」
- 455 ページの「ウイルスバスター Corp.」

- 456 ページの「Smart Protection Server」
- 457 ページの「InterScan Messaging Security Virtual Appliance」
- 458 ページの「InterScan Web Security Virtual Appliance」
- 459 ページの「InterScan for Microsoft Exchange」
- 459 ページの「Trend Micro Endpoint Application Control 」
- 459 ページの「Deep Discovery Email Inspector」
- 460 ページの「Cloud App Security」

Control Manager

要件	説明
製品バージョン	7.0 (またはそれ以降)
Control Manager 登録情報	Control Manager コンソールを使用して Control Manager に登録されていない製品の場合、次の Control Manager 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、Control Manager は HTTP ポート 80 または HTTPS ポート 443 を使用します。 Control Manager 管理コンソールを使用して登録されている製品の場合、[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 Control Manager 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、Control Manager 管理コンソールを開いて、[運用管理] > [不審オブジェクト] > [配信設定] に移動します。

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 • 不審オブジェクト管理 • 影響診断 • エンドポイントの隔離 • IOC の管理

Deep Discovery Analyzer

要件	説明
製品バージョン	5.1 (またはそれ以降)
Control Manager の登録	Control Manager 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	Control Manager への登録後に自動的に実行します。 初期設定では、不審オブジェクトリストは Control Manager サーバと 10 分ごとに同期します。
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 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理

Trend Micro Endpoint Sensor

注意

- 以前の名前は Deep Discovery Endpoint Sensor です (バージョン 1.5 以前)。
- Endpoint Sensor では不審オブジェクトリストの同期はサポートされません。

要件	説明
製品バージョン	1.5 (またはそれ以降)
Control Manager の登録	Control Manager 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。
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 • 影響診断 • エンドポイントの隔離 • IOC の管理

Deep Discovery Inspector

要件	説明
製品バージョン	3.8 (またはそれ以降)

要件	説明
Control Manager の登録	Deep Discovery Inspector の管理コンソールの [運用管理] > [統合製品/サービス] > [Control Manager] 必須の Control Manager 情報: • サーバの FQDN または IP アドレス • ポート: 初期設定では、Control Manager 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 [運用管理] > [統合製品/サービス] > [Control Manager] 必須の Control Manager 情報: • API キー: API キーを入手するには、Control Manager 管理コンソールを開いて、[運用管理] > [不審オブジェクト] > [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。
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 Security

要件	説明
製品バージョン	10.0 以降
Control Manager の登録	Control Manager 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	Control Manager への登録後に自動的に実行します。
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

ウイルスバスター Corp.

要件	説明
製品バージョン	11.0 SP1 (またはそれ以降)
Control Manager の登録	ウイルスバスター Corp.管理コンソールの [運用管理] > [設定] > [Control Manager] 必須の Control Manager 情報: • サーバの FQDN または IP アドレス • ポート: 初期設定では、Control Manager 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	ウイルスバスター Corp.管理コンソールの [運用管理] > [設定] > [不審オブジェクトリスト] 必須の Control Manager 情報: • なし 注意 ウイルスバスター Corp.は、Control Manager の登録中に、必要な API キー情報を Control Manager サーバから自動的に取得します。

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 • 不審オブジェクト管理 • エンドポイントの隔離

Smart Protection Server

要件	説明
製品バージョン	3.0 Patch 1 (またはそれ以降)
Control Manager の登録	Control Manager 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 の管理コンソールから: • Smart Protection Server 3.0 Patch 1 の場合は、[Smart Protection] > [C&C コンタクトアラート] に移動します。 • Smart Protection Server 3.0 Patch 2 以降の場合は、[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 Control Manager 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 Control Manager である場合、Control Manager 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、Control Manager 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

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
Control Manager 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	Control Manager への登録後に自動的に実行します。
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 2 (またはそれ以降)
Control Manager 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)
Control Manager 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

Trend Micro 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)
Control Manager の登録	Control Manager 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	Control Manager への登録後に自動的に実行します。
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

Deep Discovery Email Inspector

要件	説明
製品バージョン	3.0 (またはそれ以降)

要件	説明
Control Manager 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

Cloud App Security

要件	説明
製品バージョン	5.0 (またはそれ以降)
Control Manager の登録	Control Manager 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 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 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

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 Control Manager 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、Control Manager 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	463 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	131 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。	• 465 ページの「情報漏えい対策ユーザの役割について」 • 117 ページの「初期設定のユーザの役割」 • 105 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	• 341 ページの「予約イベント概要」 • 339 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	296 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。

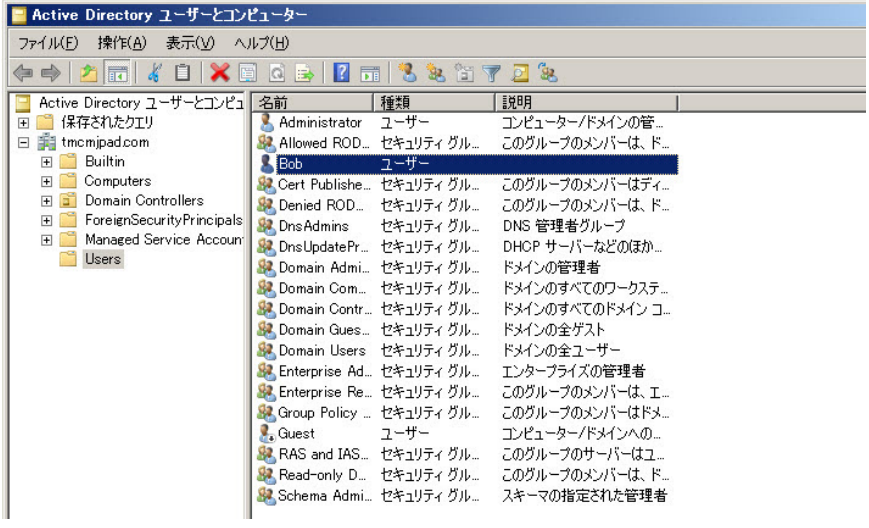


図 18-1. [Active Directory ユーザとコンピュータ] コンソール

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。

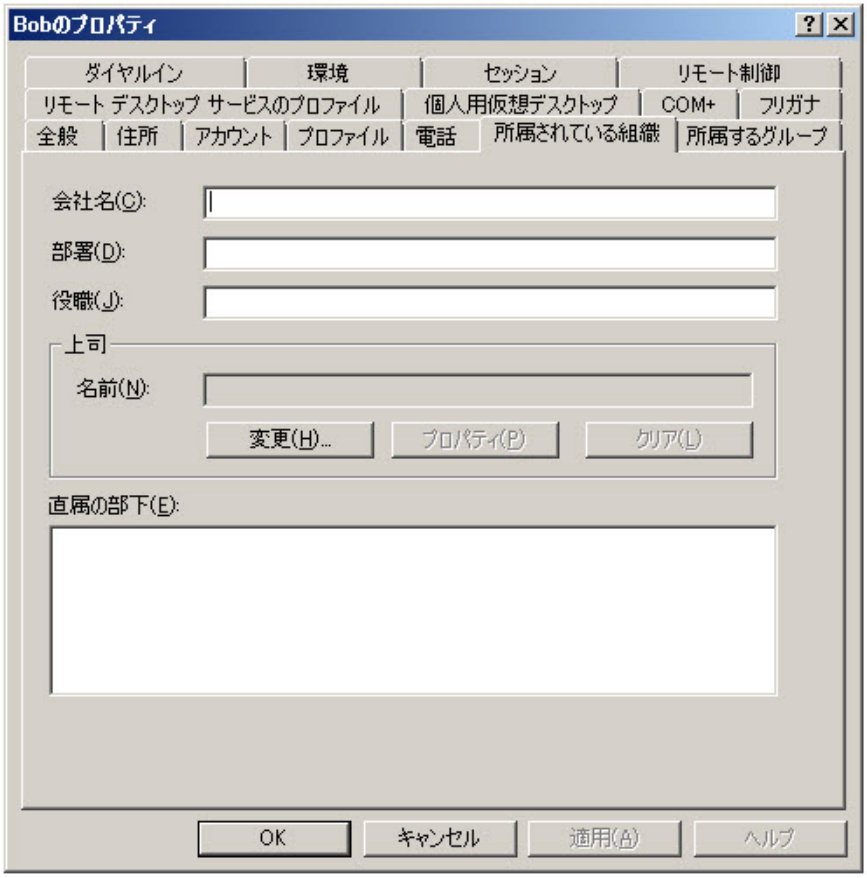


図 18-2. [プロパティ] 画面

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。

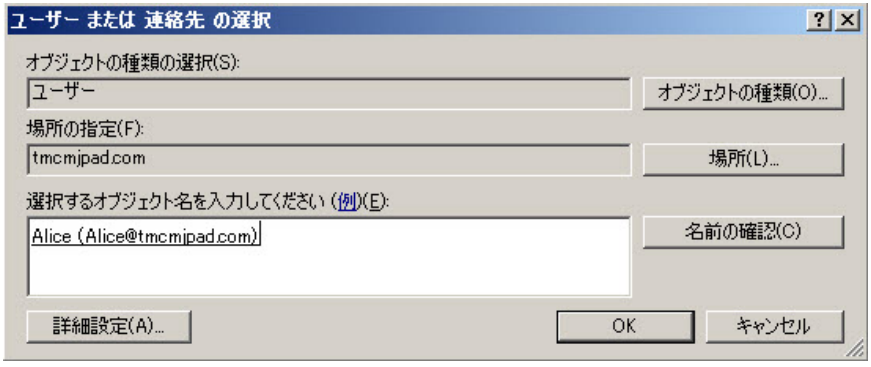


図 18-3. [ユーザー、連絡先、コンピュータまたはグループの選択] 画面

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

Control Manager 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。

- 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

Active Directory ユーザアカウントには、「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	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。
	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。
	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	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	• 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イベントの調査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イベントの調査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イベントの調査ウィジェットの [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: • 「」「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。 • 「」「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。
	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	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	[情報漏えい対策イベントの調査] 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、78 ページの「[情報漏えい対策イベントの調査] タブ」を参照してください。
予約イベント概要の通知	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	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 • Control Manager 管理コンソールへのリンク
イベント詳細のアップデートの通知	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	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 「」「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。

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。296 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。

- データの範囲:Control Manager の選択
- データビュー:[ユーザアクセス情報] を選択します
- クエリ条件:次の処理をカスタム条件に追加します。
  - 情報漏えい対策ログの削除
  - アクセスログの削除
  - 情報漏えい対策イベントファイルのダウンロード
  - アクセスログ管理の有効化
  - 情報漏えい対策ログ管理の有効化
  - アクセスログ管理の無効化
  - 情報漏えい対策ログ管理の無効化
  - 情報漏えい対策イベントのアップデート
  - 情報漏えい対策ログの管理設定の変更
  - アクセスログの管理設定のアップデート

情報漏えい対策イベントのレビュー処理

Control Manager 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	Control Manager 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。

タスク	説明
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、Control Manager 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	470 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	471 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
受信	Control Manager がイベントデータを受信した日付と時刻 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、Control Manager 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。

項目	説明
重大度	イベントの重大度レベル **注意** 情報漏えい対策イベントを受信し、処理した Control Manager 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 Control Manager ポリシーの名前 **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
マネージャ	ユーザのマネージャ名
ステータス	イベントの現在のステータス • 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

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
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 注意 情報漏えい対策イベントを受信し、処理した Control Manager 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 Control Manager ポリシーの名前 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
受信	Control Manager がイベントデータを受信した日付と時刻 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、Control Manager 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

項目	説明
ユーザ	イベントをトリガしたユーザの名前
マネージャ	ユーザのマネージャ名
送信者	送信元のメールアドレス
受信者	送信先のメールアドレス
エンドポイント	送信元ホスト名
IP	送信元 IP アドレス
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
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
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 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
件名	メールメッセージの件名
チャネル	転送に使用されるチャネル
処理	イベントに対して実行された処理
ユーザの承認理由	クライアントユーザが管理者に機密データの転送許可を求めた際に提示した理由
コメント	イベントに関するユーザ指定のメモ

パート V

ツールとサポート

第 19 章

データベースの管理

ここでは、管理者が Control Manager 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。

Control Manager データベースについて

Control Manager 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_ControlManager.mdf`) を使用しています。

Control Manager 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。Control Manager をインストールすると、システム DSN ODBC 接続と、`db_ControlManager.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。Control Manager 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_ControlManager 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_ControlManager の役割の db_owner

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 Control Manager にさまざまな種類のログが送信されます。トレンドマイクロでは、次の一般的な種類のログについてデータベースサイズを測定します。

- ウイルスログ
- スパイウェアログ
- Web セキュリティログ
- コンテンツセキュリティログ

データベースサイズについては、次の表を参照してください。

表 19-1. 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	156
	500,000	667
	1,000,000	1,191
スパイウェア	100,000	156
	500,000	770
	1,000,000	1,570
コンテンツセキュリティ	100,000	121
	500,000	543
	1,000,000	1,263
Web セキュリティ	100,000	99
	500,000	562
	1,000,000	1,106

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。

- ウイルスバスター Corp.の管理下の製品から Control Manager 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。
- Control Manager 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。

Control Manager 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_ControlManager 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 Control Manager データベースをバックアップします。

注意

Control Manager 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、Control Manager 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. Control Manager 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_ControlManager 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_ControlManager の復元

SQL Server Management Studio を使用して、バックアップした Control Manager データベースを復元します。

手順

1. Control Manager 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 <Control Manager 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_ControlManager 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 <Control Manager サービス> を右クリックして、[再起動] をクリックします。
12. Control Manager を開始します。

SQL コマンドによる db_ControlManager_Log.LDF の縮小

手順

1. SQL Server Management Studio を使用して、Control Manager データベースのバックアップを作成します。
2. 使用可能なデータベースで、db_ControlManager 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_ControlManager_log', 10)
```

4. db_ControlManager_Log.LDF のサイズが 10MB 未満であることを確認します。

   db_ControlManager_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_ControlManager'
```

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_ControlManager
SET RECOVERY SIMPLE;
GO
-- Shrink the truncated log file to 10 MB.
DBCC SHRINKFILE (db_ControlManager_Log, 10);
GO
-- Reset the database recovery model.
ALTER DATABASE db_ControlManager
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 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_ControlManager_log.ldf の縮小

Control Manager データベースのトランザクションログファイルは、…¥data ¥db_ControlManager_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_ControlManager_log.ldf には、db_ControlManager.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_ControlManager_log.ldf ファイルサイズの縮小

手順

1. SQL Server Management Studio を使用して、Control Manager 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、Windows 認証情報を指定します。
5. [db_ControlManager] 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。
9. `db_ControlManager_log.ldf` ファイルのサイズを確認してください。10MB に縮小されているはずです。

第 20 章

Control Manager ツール

本章では、Control Manager 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。

Control Manager のツールについて

Control Manager 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。Control Manager は、ほとんどのツールを次の場所に保存しています。

`<Control Manager 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

Control Manager7.0 に付属のエージェント移行ツールを使用すると、Control Manager6.0 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。`<Control Manager 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 Control Manager 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

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. Control Manager 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を見つけます。

   ```
   cd <Control Manager 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。

http://esupport.trendmicro.com/solution/ja-jp/1306559.aspx

第 21 章

不審オブジェクトハブおよびノードの Control Manager 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 Control Manager 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 Control Manager アーキテクチャ

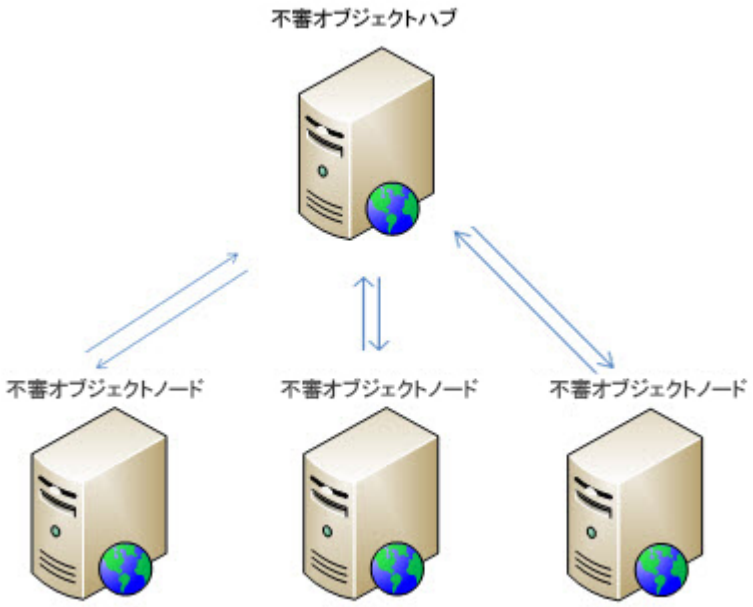
Trend Micro Control Manager™の不審オブジェクトハブおよびノードのアーキテクチャにより、不審オブジェクトリストを複数の Control Manager サーバ間で同期できます。ハブ Control Manager サーバの不審オブジェクトリストは、すべてのノード Control Manager サーバとそれらのサーバに登録されているその他の管理下の製品からの不審オブジェクトリストを統合して、そのリストをノード Control Manager サーバに配信します。

管理者は、不審オブジェクトハブ Control Manager 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 Control Manager 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はノード Control Manager 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 Control Manager サーバ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 Control Manager 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 Control Manager から実行する必要があります。

不審オブジェクトノード Control Manager 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 Control Manager のサーバコンソールにログオンします。
2. [運用管理] > [不審オブジェクト] > [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 Control Manager サーバコンソールにログオンします。
5. [運用管理] > [不審オブジェクト] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。
6. [不審オブジェクトハブ Control Manager] タブで、不審オブジェクトハブ用の Control Manager でメモした内容を入力します。
   - サービス URL
   - API キー
7. [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 Control Manager 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。
8. 各不審オブジェクトノードの Control Manager サーバに対してこの処理を繰り返します。
9. 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。

不審オブジェクトハブ Control Manager から不審オブジェクトノードを登録解除する

注意

ノードの Control Manager 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 Control Manager 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 Control Manager サーバコンソールにログオンします。
2. [運用管理] > [不審オブジェクト] > [配信設定] に移動します。
3. [不審オブジェクトハブ Control Manager 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 Control Manager 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 Control Manager 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 Control Manager 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 Control Manager 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 Control Manager サーバの不審オブジェクトリストに残ります。

設定	不審オブジェクトハブ CONTROL MANAGER	ノードの CONTROL MANAGER
同期間隔	該当なし	5 分 (初期設定)

<table>
<tr><th>設定</th><th>不審オブジェクトハブ
Control Manager</th><th>ノードの Control Manager</th></tr>
<tr><td>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 Control Manager 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 Control Manager からハブ:
• 仮想アナライザリスト</td></tr>
<tr><td colspan="3">注意
• ハブの Control Manager 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 Control Manager 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 Control Manager 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 Control Manager サーバは両方のリストをノードの Control Manager サーバに配信します。
• ノードの Control Manager 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 Control Manager のユーザ指定リストにも存在する場合、ノードの Control Manager 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。
• 移行済みの Control Manager 6.0 のインストールから除外リストの自動同期を実行するには、移行前に Control Manager 6.0 サーバで不審オブジェクトハブおよびノードの Control Manager アーキテクチャを有効にしておく必要があります。
• Control Manager 7.0 では、Control Manager 6.0 から移行された不審オブジェクトハブおよびノードのアーキテクチャが保持されます。
• Control Manager 6.0 サーバの移行前に不審オブジェクトハブおよびノードの Control Manager アーキテクチャを有効にするには、<code>SystemConfiguration.xml</code> ファイルで <code>m_iTmcmSoDist_ForceSyncWhitelist</code> タグを検索し、値を「1」に変更します。</td></tr>
</table>

設定	不審オブジェクトハブ Control Manager	ノードの Control Manager
不審オブジェクトの設定	不審オブジェクトハブ Control Manager 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 Control Manager サーバ全体で一貫性が確保されます。	**重要** ノードの Control Manager サーバですべての不審オブジェクトリストを同期の取れた状態にしておくには、ノードの Control Manager サーバコンソールから不審オブジェクトリストに対して何の処理も実行しないでください (たとえば、オブジェクトの [追加] や [期限切れにする] など)。

第 22 章

不審オブジェクトリストエクスポート/インポートツールユーザガイド

このセクションでは、Control Manager の不審オブジェクトリストエクスポートツール (`SuspiciousObjectExporter.exe`) およびインポートツール (`ImportSOFromCSV.exe`) 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。

- 513 ページの「Control Manager を使用してユーザ指定リストをインポートする」

不審オブジェクトリストエクスポート/インポートツールユーザガイド

Trend Micro Control Manager™の不審オブジェクトリストエクスポート/インポートツールでは、Control Manager の不審オブジェクトリストをエクスポートおよびインポートできます。Control Manager 管理コンソールにサインインする必要はありません。

- 不審オブジェクトリストエクスポートツール: 不審オブジェクトリストを Control Manager サーバから複数のファイル形式でエクスポートします。
- 不審オブジェクトリストインポートツール: 適切な形式のコンマ区切り値 (CSV) の不審オブジェクトデータを Control Manager にインポートします。

エクスポート/インポートツールを使用して、不審オブジェクトデータを複数の Control Manager サーバや他社製アプリケーションで活用することにより、未知の脅威や発生しつつある脅威に対する保護を強化します。

不審オブジェクトリストエクスポートツールを使用する (SuspiciousObjectExporter.exe)

Control Manager 不審オブジェクトリストを複数のファイル形式でエクスポートするには、不審オブジェクトリストエクスポートツール (`SuspiciousObjectExporter.exe`) を使用します。初期設定では、不審オブジェクトリストエクスポートツールは不審オブジェクトデータを XML 形式でエクスポートします。

出力ファイル形式を変更する方法の詳細については、504 ページの「設定ファイルを変更する」を参照してください。

重要

不審オブジェクトエクスポートツールは、Control Manager7.0 以降で使用できます。

最新のインストールパッケージをダウンロードするには、http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp を参照してください。

手順

1. Control Manager 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、SuspiciousObjectExporter.exe ファイルが含まれるディレクトリを見つけます。

   ```
   cd <Control Manager インストールディレクトリ>\SOTools
   ```

3. 次のコマンドを使用して、SuspiciousObjectExporter.exe を実行します。

   ```
   SuspiciousObjectExporter.exe [/s <開始 ID> /e <終了 ID>] [/f <y | n>] [/d]
   ```

   注意

   パラメータなしで SuspiciousObjectExporter.exe を実行すると、詳細な使用方法が表示され、<開始 ID>と<終了 ID>の値を指定するように要求されます。

パラメータ	説明	例
/s <開始 ID>	エクスポートする最初のオブジェクトの ID を指定します。 **注意** • /e <終了 ID> 値を指定する必要があります。 • 値に 0 を指定するとリストの先頭を示します。	• `SuspiciousObjectExporter.exe /s 0 /e 0` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 3 /e 8` ID 3 から ID 8 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 0 /e 4` リストの先頭から ID 4 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。

パラメータ	説明	例
/e <終了 ID>	エクスポートする最後のオブジェクトの ID を指定します。 注意 • /s <開始 ID> 値を指定する必要があります。 • 値に 0 を指定するとリストの末尾を示します。	• `SuspiciousObjectExporter.exe /s 0 /e 0` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 3 /e 8` ID 3 から ID 8 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 4 /e 0` ID 4 からリストの末尾までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。

パラメータ	説明	例
/f <y | n>	エクスポート処理中にコマンドラインインタフェースをロックするかどうかを指定します。 **注意** オプションのパラメータです。指定しない場合の初期設定は「yes」です。 **重要** `SuspiciousObjectExporter.exe` ツール、PowerShell スクリプト、または Windows タスクスケジューラのバッチスクリプトを使用して自動エクスポートを予約する場合は、[引数の追加 (オプション)] フィールドで次のパラメータを指定する必要があります。 `/f n`	• `SuspiciousObjectExporter.exe /f y` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 0 /e 0 /f y` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /f n` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロック解除します。
/d	デバッグモードを有効にします。 **注意** サポートセンターから指示があった場合にのみ使用してください。	`SuspiciousObjectExporter.exe /d` すべての不審オブジェクトをエクスポートし、デバッグログを出力します。

4. エクスポートされた不審オブジェクトリストを確認するには、<**現在のディレクトリ**>¥SOTools¥ディレクトリに移動し、`SuspiciousObjectList.xml` ファイルを開きます。

注意

この手順は、<**現在のディレクトリ**>が<Control Manager **インストールディレクトリ**>であることを前提としています。

5. すべてのエクスポートログを確認するには、<**現在のディレクトリ**>¥SOTools¥ディレクトリに移動し、ExportRecord.txt ファイルを開きます。

注意

この手順は、<**現在のディレクトリ**>が<Control Manager **インストールディレクトリ**>であることを前提としています。

設定ファイルを変更する

不審オブジェクトリストインポートツールの初期設定の設定ファイルを変更するには、<Control Manager **インストールディレクトリ**>¥SOTools ディレクトリにある SuspiciousObjectExporter.exe.config ファイルを変更します。

ヒント

設定ファイルを変更する前にバックアップファイルを作成することをお勧めします。

キー	説明	例
outputRootFolderPath 場所: <appSettings>	SuspiciousObjectExporter.exe ツールの作業ディレクトリを指定します。	• <add key="outputRootFolderPath" value="."/> SuspiciousObjectExporter.exe プログラムが存在するディレクトリを使用してリストを処理します。 • <add key="outputRootFolderPath" value="C:\Program Files (x86)\Trend Micro\Control Manager"/> 指定したディレクトリ (C:¥Program Files (x86)¥Trend Micro¥Control Manager) を使用してリストを処理します。
outputFolderName 場所: <appSettings>	エクスポートする不審オブジェクトリストの出力ディレクトリを指定します。	• <add key="outputFolderName" value="SOTools"/> ファイルを<outputRootFolderPath>¥SOTools ディレクトリにエクスポートします。 • <add key="outputFolderName" value="SOList"/> ファイルを<outputRootFolderPath>¥SOList ディレクトリにエクスポートします。

キー	説明	例
styleSheetFile 場所: `<appSettings>`	エクスポートするリストに適用するスタイルシートを指定します。	• `<add key="styleSheetFile" value=""/>` `outputFile` キーで指定した`*.txt` または `*.xml` ファイルに、すべてのリストを XML 形式でエクスポートします。 • `<add key="styleSheetFile" value="ExportCSV.xslt"/>` 仮想アナライザで検出された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、または除外リストについて、列のサブセットを CSV 形式でエクスポートします。 **重要** `ExportCSV.xslt` スタイルシートを選択すると、このツールでエクスポートする列を設定できなくなります。スタイルシートで指定した列のみがエクスポートされます。 • `<add key="styleSheetFile" value="ExportSTIX.xslt"/>` すべての不審オブジェクトリストを STIX 形式でエクスポートします。 • `<add key="styleSheetFile" value="ExportCPL.xslt"/>` すべての不審オブジェクトリストを CPL 形式でエクスポートします。 **重要** スタイルシートを指定する場合は、`defaultSampleTemplates` キーに同じ値を設定する必要があります。

キー	説明	例
outputFile 場所: <appSettings>	エクスポートする不審オブジェクトリストのファイル名と拡張子を指定します。 出力ファイル形式を変更するには、新しいファイル拡張子を指定します。	• <add key="outputFile" value="SuspiciousObjectList.xml"/> 不審オブジェクトリストを SuspiciousObjectList.xml という名前の *.xml ファイルとしてエクスポートします。 • <add key="outputFile" value="SuspiciousObjectList.txt"/> 不審オブジェクトリストを SuspiciousObjectList.txt という名前の *.txt ファイルとしてエクスポートします。
defaultSampleTemplates 場所: <appSettings>	エクスポートするリストに適用するスタイルシートのソースファイルを指定します。	• <add key="defaultSampleTemplates" value="ExportCSV.xslt"/> 指定したスタイルシートファイルの場所を特定します。 **重要** 指定する値は、styleSheetFile キーまたは defaultSampleTemplates キー用に指定した値と一致する必要があります。 **注意** 初期設定値は"ExportCPL.xslt|ExportSTIX.xslt|ExportCSV.xslt"です。

キー	説明	例
<suspiciousObjectColumns> 場所: <soDataColumnSettings>	選択したリストのデータ列を指定します。 isEnable="true"に設定すると、指定したデータ列をエクスポートします。	• <add id="1" name="SeqID" isEnable="true"></add> 選択したリストから「SeqID」データ列をエクスポートします。 • <add id="1" name="MD5Key" isEnable="false"></add> 選択したリストから「MD5Key」データ列を明示的に除外します。 **重要** 「ExportCSV.xslt」スタイルシートを指定した場合、スタイルシートで指定した列のみがエクスポートされます。
<suspiciousObjectTypeList> 場所: <soTypeSettings>	選択したリストからエクスポートするオブジェクトの種類を指定します。 isEnable="true"に設定すると、指定したオブジェクトの種類をエクスポートします。	• <add value="0" description="IP" isEnable="true"></add> 選択したリストからすべての IP アドレスのオブジェクトをエクスポートします。 • <add value="1" description="Domain" isEnable="false"></add> エクスポートするリストからすべての「Domain」オブジェクトを明示的に除外します。

キー	説明	例
<suspiciousObjectSourceType> 場所: <soTypeSettings>	不審オブジェクトのソースの種類を指定します。 isEnable="true"に設定すると、指定したオブジェクトの種類をエクスポートします。	• <add value="0" description="SourceType" isEnable="true"/> 仮想アナライザの不審オブジェクトリストを選択します。 • <add value="1" description="SourceType" isEnable="true"/> ユーザ指定の不審オブジェクトリストを選択します。 • <add value="2" description="SourceType" isEnable="true"/> 仮想アナライザの除外リストを選択します。 重要 • ExportCSV.xslt スタイルシートを指定し、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を選択した場合、エクスポートされる列は [オブジェクト]、[種類]、[Scan Prefilter]、[メモ]、および [検出時の処理] です。 • ExportCSV.xslt スタイルシートを指定し、仮想アナライザの除外リストを選択した場合、エクスポートされる列は [オブジェクト]、[種類]、[Scan Prefilter]、および [メモ] です。

Control Manager を使用して仮想アナライザ不審オブジェクトの除外リストをエクスポートする

重要

Control Manager では、CSV 形式でのみ仮想アナライザで検出された不審オブジェクト除外リストをエクスポートできます。

手順

1. [運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] 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. [すべてエクスポート] をクリックします。

   進行状況の画面が表示されます。

4. エクスポートが完了したら、[ダウンロード] をクリックします。

   確認ボックスが表示されます。

5. [保存] をクリックします。

   [名前を付けて保存] 画面が表示されます。

6. (オプション) 新しい場所またはファイル名を指定します。

7. [保存] をクリックします。

Control Manager を使用してユーザ指定リストをエクスポートする

重要

Control Manager では、CSV 形式でのみユーザ指定の不審オブジェクトリストをエクスポートできます。

手順

1. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [すべてエクスポート] をクリックします。

   進行状況の画面が表示されます。

3. エクスポートが完了したら、[ダウンロード] をクリックします。

   確認ボックスが表示されます。

4. [保存] をクリックします。

   [名前を付けて保存] 画面が表示されます。

5. (オプション) 新しい場所またはファイル名を指定します。

6. [保存] をクリックします。

不審オブジェクトリストインポートツールを使用する (ImportSOFromCSV.exe)

適切な形式の不審オブジェクトデータファイル (`*.csv`) を Control Manager にインポートするには、不審オブジェクトリストインポートツール (`ImportSOFromCSV.exe`) を使用します。

重要

不審オブジェクトインポートツールは、Control Manager7.0 以降で使用できます。

最新の Control Manager インストールパッケージをダウンロードするには、http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp を参照してください。

手順

1. Control Manager 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、`ImportSOFromCSV.exe` ファイルが含まれるディレクトリを見つけます。

   `cd <Control Manager インストールディレクトリ>`

3. 次のコマンドを使用して、ImportSOFromCSV.exe を実行します。

   ```
   ImportSOFromCSV.exe "<フルパス>" {UserDefinedSO | ExceptionSO}
   ```

   ここでは次を意味します。

   - <**フルパス**>: 適切な形式の CSV ファイルのディレクトリとファイル名を指定します。
   - {UserDefinedSO}: ユーザ指定の不審オブジェクトリストデータが含まれるファイルを指定します。
   - {ExceptionSO}: 仮想アナライザ不審オブジェクトの除外リストデータが含まれるファイルを指定します。

   例:

   - `SuspiciousObjectImporter.exe "c:\Program Files (x86)\Trend Micro\Control Manager \importExceptionSample.csv" ExceptionSO`

     importExceptionSample.csv ファイルを c:¥Program Files (x86)¥Trend Micro¥Control Manager ディレクトリから Control Manager の仮想アナライザ不審オブジェクトの除外リストにインポートします。

Control Manager を使用して仮想アナライザ不審オブジェクトの除外リストをインポートする

重要

Control Manager でインポートできる仮想アナライザ不審オブジェクトの除外リストデータは、適切な形式の*.csv ファイルのみです。

手順

1. [運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] 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. [インポート] をクリックします。

   [除外設定のインポート] 画面が表示されます。
4. [参照] をクリックし、除外リストデータが含まれる*.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すると、詳細な手順が記載された*.csv ファイルをダウンロードできます。
5. [開く] をクリックします。
6. [インポート] をクリックします。

   [除外設定のインポート] 画面が閉じられ、インポートした除外設定が仮想アナライザで検出された不審オブジェクト除外リストに表示されます。

Control Manager を使用してユーザ指定リストをインポートする

重要

Control Manager でインポートできるユーザ指定の不審オブジェクトデータは、適切な形式の*.csv ファイルのみです。

手順

1. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [インポート] をクリックします。

   [ユーザ指定リストのインポート] 画面が表示されます。

3. [参照] をクリックし、ユーザ指定の不審オブジェクトデータが含まれる *.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すると、詳細な手順が記載された*.csv ファイルをダウンロードできます。

4. [開く] をクリックします。

5. [インポート] をクリックします。

   [ユーザ指定リストのインポート] 画面が閉じられ、インポートしたオブジェクトがユーザ指定の不審オブジェクトリストに表示されます。

第 23 章

Syslog 転送ツールの使用 (LogForwarder.exe)

このセクションでは、Control Manager Syslog 転送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。

概要

Syslog 転送ツール (`LogForwarder.exe`) は次世代の DataExport ツールで、複数の種類の製品ログを、Control Manager データベースから Syslog サーバへ、以下の形式で送信します。

- Common Event Format (CEF)
- Control Manager ログ形式

重要

- Trend Micro Control Manager 7.0 では、DataExport ツールのサポートが廃止されました。
  管理者は新しい Syslog 転送ツール (`LogForwarder.exe`) を使用する必要があります。

Syslog 転送ツールでは、ネットワークコンテンツ検査のログ、不審ファイルのログ、C&C コールバックログを含む新しいログの種類がサポートされています。管理者は、Control Manager サーバのバックグラウンドプロセスで実行されるようにこのツールを設定することもできます。

表 23-1. サポート対象のログの種類と形式

ログの種類	CEF ログ形式のサポート	CONTROL MANAGER ログ形式のサポート
Behavior Monitoring (挙動監視)	○	○
C&C Callback (C&C コールバック)	○	×
Data Loss Prevention (情報漏えい対策)	○	○
Data Loss Prevention (デバイスアクセス管理)	○	○
Engine Update Status (検索エンジンアップデートステータス)	○	○

ログの種類	CEF ログ形式のサポート	CONTROL MANAGER ログ形式のサポート
Suspicious File (不審ファイル)	○	×
Network Content Inspection (ネットワークコンテンツ検査)	○	×
Virus/Malware (ウイルス/不正プログラム)	○	×
Pattern Update Status (パターンファイルアップデートステータス)	○	○
Content Security (コンテンツセキュリティ)	○	×
Spyware/Grayware (スパイウェア/グレーウェア)	○	×
Web Security (Web セキュリティ)	○	×
Predictive Machine Learning (機械学習型検索)	○	×

システム要件

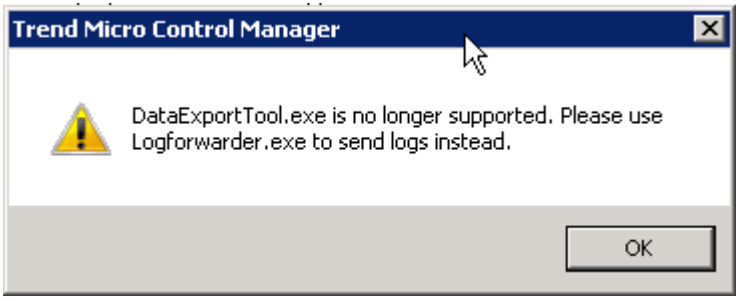
Syslog 転送ツールには Trend Micro Control Manager 7.0 が必要です。

制限事項

Trend Micro Control Manager 7.0 では、`DataExportTool.exe` ツールのサポートが廃止されました。

- Control Manager 7.0 の新規インストールでは、`DataExportTool.exe` ツールは提供されません。

- 以前のバージョンから Control Manager 7.0 に移行した場合は、`DataExportTool.exe` ツールを実行しようとすると、次の警告メッセージが表示されます。



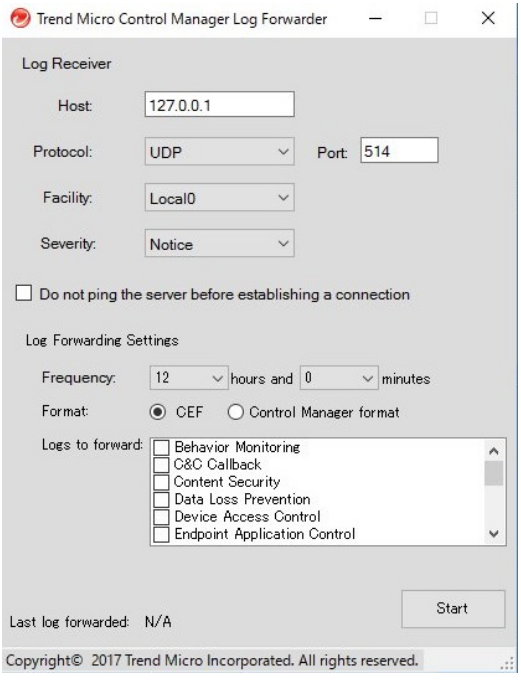
Syslog 転送ツールを設定する

手順

1. Control Manager のインストールディレクトリに移動します。

   初期設定では、インストールディレクトリは、`C:¥Program Files (x86)¥Trend Micro¥Control Manager` です。

2. 管理者権限 (管理者として実行) を使用して `LogForwarder.exe` ファイルを実行し、Syslog 転送ツールコンソールを開きます。



3. [Log Receiver] を設定します。
   - IP address: Syslog サーバの IP アドレス
   - Port: Syslog サーバのポート番号
   - Facility: Syslog メッセージのファシリティコード

     注意
     この設定は、Control Manager 形式のログにのみ適用されます。

   - Severity: Syslog メッセージの重大度レベル

     注意
     この設定は、Control Manager 形式のログにのみ適用されます。

   - (オプション) Do not ping the server before establishing a connection: 最初に対象サーバに ping することなく Syslog メッセージを送信する場合に選択します。

4. [Log Forwarding Settings] を設定します。
   - Frequency: ツールがログを送信する間隔です。
   - Format: CEF と Control Manager ログ形式のどちらを使用するか選択します。
   - Logs to forward: Control Manager に転送するログの種類を選択します。

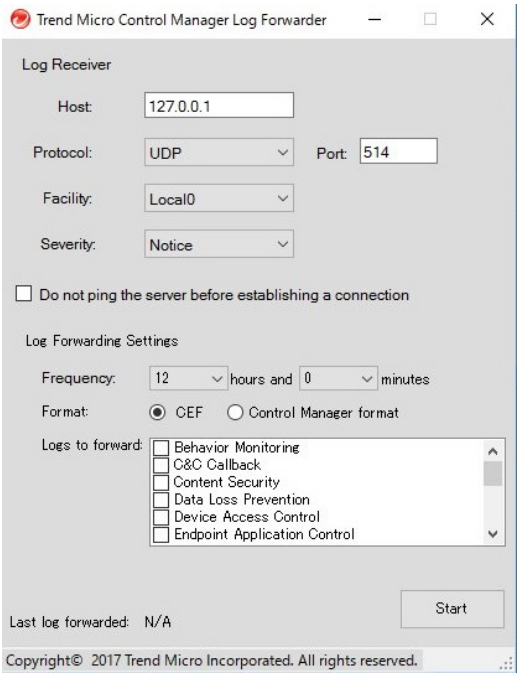
ログの転送を開始または停止する

手順

1. Control Manager のインストールディレクトリに移動します。

   初期設定では、インストールディレクトリは、`C:¥Program Files (x86)¥Trend Micro¥Control Manager` です。

2. 管理者権限 (管理者として実行) を使用して `LogForwarder.exe` ファイルを実行し、Syslog 転送ツールコンソールを開きます。



3. 次の処理のいずれかを実行します。

- ログの転送を開始するには、次の手順を実行します。

  a. [Start] をクリックします。

  注意

  Control Manager サービスがまだ開始していない場合、サービスが再開するのをしばらく待つよう指示するメッセージが表示されます。

  b. ログの転送を開始することを確認します。

  注意

  ログ転送を開始すると、Control Manager サービスが再開し、Syslog 転送ツールコンソールが閉じます。Control Manager サービスが正常に再開すると、ユーザが Syslog 転送ツールコンソールを再度開いて [Stop] をクリックするまで、ツールはバックグラウンドで実行を続けます。

- ログの転送プロセスを停止するには、次の手順を実行します。

  a. [Stop] をクリックします。

  注意

  Control Manager サービスがまだ開始していない場合、サービスが再開するのをしばらく待つよう指示するメッセージが表示されます。

  b. ログの転送を停止することを確認します。

  注意

  ログ転送を停止すると、Control Manager サービスが再開します。Control Manager サービスが正常に再開すると、ツールはバックグラウンドで実行されなくなります。

第 24 章

不審オブジェクト移行ツールユーザガイド

本章では、管理者が、Control Manager の不審オブジェクト移行ツールを使用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。

不審オブジェクト移行ツールユーザガイド

トレンドマイクロの不審オブジェクト移行ツールでは、不審オブジェクトデータを Control Manager サーバから他社製アプリケーションに移行できます。個々の Control Manager 不審オブジェクトリストを手動でエクスポート、形式設定、インポートする必要はありません。

本ユーザガイドでは、不審オブジェクト移行ツールをトレンドマイクロの不審オブジェクトリストエクスポートツールと Check Point Suspicious Activity Monitoring (SAM) Client ツールを連携する方法について説明します。

- 不審オブジェクト移行ツール: 不審オブジェクトリストエクスポートツールおよび Check Point SAM Client ツールをループ実行します。
- 不審オブジェクトリストエクスポートツール: 不審オブジェクトリストを Control Manager サーバから複数のファイル形式でエクスポートします。
- Check Point SAM Client: 不審オブジェクトデータを適切な形式で、Check Point サーバにインポートします。

個々の Control Manager 不審オブジェクトリストを Check Point サーバに手動で移行する場合は、不審オブジェクト移行ツールを実行せずに、不審オブジェクトリストエクスポートツールと Check Point SAM Client ツールを使用することもできます。

Check Point ファイアウォールサーバを準備する

注意

次の手順では、Gaia OS 搭載の Check Point Firewall R77.20 および SmartDashboard R77.20 を使用していることを前提としています。

重要

認証証明書の設定ファイルを準備する前に、Check Point ファイアウォールサーバを準備する必要があります。

手順

1. Check Point Open Platform for Security (OPSEC) 通信用に Check Point Suspicious Activity Monitoring (SAM) サーバポートを設定します。

   a. Check Point ファイアウォールサーバに expert モードでログオンします。

   b. 次のコマンドを使用して、vi エディタで `fwopsec.conf` ファイルを見つけて開きます。

      ```
      vi /var/opt/CPsuite-R77/fw1/conf/fwopsec.conf
      ```

   c. `sam_server auth_port` を探し、ポート番号を「18181」に変更します。

      ```
      sam_server auth_port 18181
      ```

   d. `sam_server port` を探し、ポート番号を「18180」に変更します。

      ```
      sam_server port 18180
      ```

   e. `<ESC>` キーを押して、vi エディタをコマンドモードに戻します。

   f. 次のコマンドを使用して、変更を保存します。

      ```
      :wq
      ```

   g. 次のコマンドを使用して、サーバをシャットダウンし、再起動します。

      ```
      shutdown -r -h 0
      ```

2. Check Point SmartDashboard コンソールにログオンします。

3. Check Point ファイアウォールを介して FW1_sam および FW1_ica_pull サービスを許可します。

   a. [Firewall] タブで [Policy] をクリックします。

   b. [Add Rule at the Top] をクリックします。

   c. 新しく作成したルールの [Service] 列で、(+) アイコンをクリックし、ドロップダウンリストから [FW1_sam] を選択します。

d. 新しく作成したルールの [Action] 列を右クリックし、プロパティを [Accept] に設定します。

e. [Add Rule at the Top] をクリックします。

f. 新しく作成したルールの [Service] 列で、(+) アイコンをクリックし、ドロップダウンリストから [FW1_ica_pull] を選択します。

g. 新しく作成したルールの [Action] 列を右クリックし、プロパティを [Accept] に設定します。

h. [Install Policy] をクリックします。

4. OPSEC アプリケーションおよびワンタイムパスワードを作成します。

a. [Manage] > [Servers and OPSEC Applications] に移動します。

b. [New] をクリックし、ドロップダウンメニューから [OPSEC Application] を選択します。

c. 次の項目を指定します。

- Name: OPSEC アプリケーションの名前を入力します。
- Host: ドロップダウンリストから Check Point ファイアウォールサーバを選択します。

d. [Client Entities] セクションで、[SAM] を選択します。

e. [Communication] をクリックします。

f. ワンタイムパスワードを作成し、確認します。

g. [Initialize] をクリックします。

確認ダイアログが表示されます。

h. [閉じる] をクリックします。

i. [OK] をクリックします。

認証証明書の設定ファイルを準備する

注意

- 次の手順では、認証証明書の設定ファイルを準備するために Control Manager 7.0 サーバを使用していることを前提としています。
- 不審オブジェクト移行ツールは、Control Manager7.0 以降で使用できます。

  最新の Control Manager インストールパッケージをダウンロードするには、http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp を参照してください。

重要

認証証明書の設定ファイルを準備する前に、Check Point ファイアウォールサーバを準備する必要があります。

詳細については、524 ページの「Check Point ファイアウォールサーバを準備する」を参照してください。

手順

1. Control Manager サーバでコマンドプロンプトを開きます。
2. Check Point ファイアウォールサーバから Secure Internal Communication (SIC) 証明書を準備します。
   a. 次のコマンドを実行します。

      ```
      opsec_pull_cert -h <host> -n <object> -p <password> -o <path>
      ```

      ここでは次を意味します。

      - `-h <host>`: Check Point ファイアウォールサーバの IP アドレスを指定します。
      - `-n <object>`: Check Point SmartDashboard コンソールで作成した OPSEC アプリケーションの名前を指定します。

        詳細については、524 ページの「Check Point ファイアウォールサーバを準備する」を参照してください。

- `-p <password>`: 指定した OPSEC アプリケーションのワンタイムパスワードを指定します。
- `-o <path>`: 出力される `opsec.p12` 証明書ファイルのフルパスを指定します。

`opsec_pull_cert` コマンドは、full entity sic name を次の形式で返します。

CN=*,O=*

b. `opsec_pull_cert` コマンドで返された full entity sic name をコピーします。

c. `opsec.p12` ファイルを`<Control Manager インストールディレクトリ>¥SOTools` ディレクトリに移動します。

3. `<Control Manager インストールディレクトリ>¥SOTools` ディレクトリに移動し、`sam.conf` ファイルを探します。

4. `sam.conf` ファイルをテキストエディタで開き、以下の表を使用して必要なキーを変更します。

キー	説明	例
sam_server auth_type	認証方法を指定します。	`sam_server auth_type sslca`
sam_server ip	Check Point ファイアウォールサーバの IP アドレスを指定します。	`sam_server ip 192.168.127.130`
sam_server auth_port	Check Point ファイアウォールサーバの OPSEC 通信ポートを指定します。	`sam_server auth_port 18181`
	重要 `fwopsec.conf` ファイルで設定したものと同じ `sam_server auth_port` 番号を指定する必要があります。	

キー	説明	例
sam_server opsec_entity_sic_name	Check Point ファイアウォールサーバの SIC 名を指定します。	sam_server opsec_entity_sic_name "cn=cp_mgmt,o=gw-1e9412..7ny9dn"
opsec_sic_name	opsec_pull_cert コマンドで返された SIC 名を指定します。	opsec_sic_name "CN=CMtest,O=gw-1e9412..7ny9dn"
	重要 opsec_pull_cert コマンドで返された正確な full entity sic name を指定する必要があります。	
opsec_sslca_file	認証証明書ファイルのファイル名を指定します。	opsec_sslca_file opsec.p12
opsec_sic_policy_file	SIC ポリシーファイルのファイル名を指定します。	opsec_sic_policy_file sic_policy.ini

5. <Control Manager インストールディレクトリ>¥SOTools ディレクトリに移動し、Customized.config ファイルを探します。

6. Customized.config ファイルをテキストエディタで開き、以下の表を使用して必要なキーを変更します。

キー	説明	例
場所: <SOMigrationTool>	値を「CKP_SAM_Client.exe」に変更します。	<add key="Sender" value="CKP_SAM_Client.exe" />

キー	説明	例
Arguments 場所: `<SOMigrationTool>`	値を「-t <timeout> -g <fw-ip> -c <conf_path> -A notify any <IP_address>」に変更します。 ここでは次を意味します。 • `-t <timeout>`: 不審オブジェクトが期限切れになるまで Check Point サーバが待機する時間 (秒数) を指定します。 • `-c <conf_path>`: `sam.conf` ファイルの相対パスを指定します。 • `-g <fw-ip>`: Check Point ファイアウォールサーバの IPv4 アドレスを指定します。 • `-A notify any <IP_address>`: Check Point ファイアウォールサーバに対し、有効な IPv4 アドレスを通知するように要求します。	`<add key="Arguments" value="-t 600 -g 192.168.127.130 -c sam.conf -A notify any 10.10.10.10" />`
	注意 Check Point `sam_client_action` 引数の使用の詳細については、Check Point サーバのドキュメントを参照してください。	
outputFolderName 場所: `<OutputSettings>`	値を「Check_Point」に変更します。	`<add key="outputFolderName" value="Check_Point" />`

キー	説明	例
outputFile 場所: `<OutputSettings>`	値を「SuspiciousObjectList.xml」に変更します。	`<add key="outputFile" value="SuspiciousObjectList.xml" />`
description="IP" 場所: `<suspiciousObjectTypeList>`	`isEnable="true"` に設定します。	`<add value="0" description="IP" isEnable="true"`
description="SourceType" 場所: `<suspiciousObjectSourceType>`	値を「0」に変更します。	`<add value="0" description="SourceType" isEnable="true"`
name="Entity" 場所: `<suspiciousObjectColumns>`	`isEnable="true"` に設定します。	`<add id="3" name="Entity" isEnable="true"`

不審オブジェクト移行ツールを使用する

Control Manager のすべての不審オブジェクトリストをエクスポートしたり、適切な形式の不審オブジェクトデータを Check Point サーバにインポートしたりするには、不審オブジェクト移行ツールを使用します。

注意

個々の Control Manager 不審オブジェクトリストを Check Point サーバに手動で移行する場合は、不審オブジェクト移行ツールを実行せずに、不審オブジェクトリストエクスポートツールと Check Point SAM Client ツールを使用できます。

詳細については、543 ページの「Check Point Suspicious Activity Monitoring Client ツールを使用する」参照してください。

重要

不審オブジェクト移行ツールを使用する前に、次の手順を実行する必要があります。

- Check Point ファイアウォールサーバを準備する。

  詳細については、524 ページの「Check Point ファイアウォールサーバを準備する」参照してください。

- 認証の設定ファイルを準備する。

  詳細については、527 ページの「認証証明書の設定ファイルを準備する」参照してください。

手順

1. Control Manager サーバにログオンします。
2. コマンドプロンプトを開きます。
3. 次のコマンドを使用して、`SOMigrationTool.exe` ファイルが含まれるディレクトリを見つけます。

   ```
   cd <Control Manager インストールディレクトリ>\SOTools
   ```

4. 次のコマンドを使用して、`SOMigrationTool.exe` を実行します。

   ```
   SOMigrationTool Check_Point
   ```

   コマンドの合計実行時間が表示され、不審オブジェクトデータの移行に成功したことが示されます。

5. Check Point ファイアウォールサーバでインポートした不審オブジェクトデータを確認するには、次の手順を実行します。

a. Check Point SmartView Monitor コンソールにログオンします。

b. [Tools] > [Suspicious Activity Rules] に移動します。

[Enforced Suspicious Activity Rules] 画面にインポートした不審オブジェクトデータが表示されます。

不審オブジェクトリストエクスポートツールを使用する (SuspiciousObjectExporter.exe)

Control Manager 不審オブジェクトリストを複数のファイル形式でエクスポートするには、不審オブジェクトリストエクスポートツール (`SuspiciousObjectExporter.exe`) を使用します。初期設定では、不審オブジェクトリストエクスポートツールは不審オブジェクトデータを XML 形式でエクスポートします。

出力ファイル形式を変更する方法の詳細については、504 ページの「設定ファイルを変更する」を参照してください。

重要

不審オブジェクトエクスポートツールは、Control Manager7.0 以降で使用できます。

最新のインストールパッケージをダウンロードするには、http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp を参照してください。

手順

1. Control Manager 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、`SuspiciousObjectExporter.exe` ファイルが含まれるディレクトリを見つけます。

   `cd <Control Manager インストールディレクトリ>\SOTools`

3. 次のコマンドを使用して、`SuspiciousObjectExporter.exe` を実行します。

```
SuspiciousObjectExporter.exe [/s <開始 ID> /e <終了 ID>] [/f
<y | n>] [/d]
```

注意

パラメータなしで SuspiciousObjectExporter.exe を実行すると、詳細な使用方法が表示され、<開始 ID>と<終了 ID>の値を指定するように要求されます。

パラメータ	説明	例
/s <開始 ID>	エクスポートする最初のオブジェクトの ID を指定します。 **注意** • /e <終了 ID> 値を指定する必要があります。 • 値に 0 を指定するとリストの先頭を示します。	• SuspiciousObjectExporter.exe /s 0 /e 0 すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • SuspiciousObjectExporter.exe /s 3 /e 8 ID 3 から ID 8 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • SuspiciousObjectExporter.exe /s 0 /e 4 リストの先頭から ID 4 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。

パラメータ	説明	例
/e <終了 ID>	エクスポートする最後のオブジェクトの ID を指定します。 注意 • /s <開始 ID> 値を指定する必要があります。 • 値に 0 を指定するとリストの末尾を示します。	• `SuspiciousObjectExporter.exe /s 0 /e 0` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 3 /e 8` ID 3 から ID 8 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 4 /e 0` ID 4 からリストの末尾までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。

パラメータ	説明	例
/f <y | n>	エクスポート処理中にコマンドラインインタフェースをロックするかどうかを指定します。 **注意** オプションのパラメータです。指定しない場合の初期設定は「yes」です。 **重要** `SuspiciousObjectExporter.exe` ツール、PowerShell スクリプト、または Windows タスクスケジューラのバッチスクリプトを使用して自動エクスポートを予約する場合は、[引数の追加 (オプション)] フィールドで次のパラメータを指定する必要があります。 `/f n`	• `SuspiciousObjectExporter.exe /f y` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 0 /e 0 /f y` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /f n` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロック解除します。
/d	デバッグモードを有効にします。 **注意** サポートセンターから指示があった場合にのみ使用してください。	`SuspiciousObjectExporter.exe /d` すべての不審オブジェクトをエクスポートし、デバッグログを出力します。

4. エクスポートされた不審オブジェクトリストを確認するには、**<現在のディレクトリ>**`¥SOTools¥`ディレクトリに移動し、`SuspiciousObjectList.xml` ファイルを開きます。

注意

この手順は、<**現在のディレクトリ**>が<Control Manager **インストールディレクトリ**>であることを前提としています。

5. すべてのエクスポートログを確認するには、<**現在のディレクトリ**>¥SOTools¥ディレクトリに移動し、ExportRecord.txt ファイルを開きます。

注意

この手順は、<**現在のディレクトリ**>が<Control Manager **インストールディレクトリ**>であることを前提としています。

設定ファイルを変更する

不審オブジェクトリストインポートツールの初期設定の設定ファイルを変更するには、<Control Manager **インストールディレクトリ**>¥SOTools ディレクトリにある SuspiciousObjectExporter.exe.config ファイルを変更します。

ヒント

設定ファイルを変更する前にバックアップファイルを作成することをお勧めします。

キー	説明	例
outputRootFolderPath 場所: <appSettings>	SuspiciousObjectExporter.exe ツールの作業ディレクトリを指定します。	• <add key="outputRootFolderPath" value="."/> SuspiciousObjectExporter.exe プログラムが存在するディレクトリを使用してリストを処理します。 • <add key="outputRootFolderPath" value="C:\Program Files (x86)\Trend Micro\Control Manager"/> 指定したディレクトリ (C:¥Program Files (x86)¥Trend Micro¥Control Manager) を使用してリストを処理します。
outputFolderName 場所: <appSettings>	エクスポートする不審オブジェクトリストの出力ディレクトリを指定します。	• <add key="outputFolderName" value="SOTools"/> ファイルを<outputRootFolderPath>¥SOTools ディレクトリにエクスポートします。 • <add key="outputFolderName" value="SOList"/> ファイルを<outputRootFolderPath>¥SOList ディレクトリにエクスポートします。

キー	説明	例
styleSheetFile 場所: <appSettings>	エクスポートするリストに適用するスタイルシートを指定します。	• <add key="styleSheetFile" value=""/> outputFile キーで指定した*.txt または *.xml ファイルに、すべてのリストを XML 形式でエクスポートします。 • <add key="styleSheetFile" value="ExportCSV.xslt"/> 仮想アナライザで検出された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、または除外リストについて、列のサブセットを CSV 形式でエクスポートします。 重要 ExportCSV.xslt スタイルシートを選択すると、このツールでエクスポートする列を設定できなくなります。スタイルシートで指定した列のみがエクスポートされます。 • <add key="styleSheetFile" value="ExportSTIX.xslt"/> すべての不審オブジェクトリストを STIX 形式でエクスポートします。 • <add key="styleSheetFile" value="ExportCPL.xslt"/> すべての不審オブジェクトリストを CPL 形式でエクスポートします。 重要 スタイルシートを指定する場合は、defaultSampleTemplates キーに同じ値を設定する必要があります。

キー	説明	例
outputFile 場所: `<appSettings>`	エクスポートする不審オブジェクトリストのファイル名と拡張子を指定します。 出力ファイル形式を変更するには、新しいファイル拡張子を指定します。	• `<add key="outputFile" value="SuspiciousObjectList.xml"/>` 不審オブジェクトリストを `SuspiciousObjectList.xml` という名前の `*.xml` ファイルとしてエクスポートします。 • `<add key="outputFile" value="SuspiciousObjectList.txt"/>` 不審オブジェクトリストを `SuspiciousObjectList.txt` という名前の `*.txt` ファイルとしてエクスポートします。
defaultSampleTemplates 場所: `<appSettings>`	エクスポートするリストに適用するスタイルシートのソースファイルを指定します。	• `<add key="defaultSampleTemplates" value="ExportCSV.xslt"/>` 指定したスタイルシートファイルの場所を特定します。 **重要** 指定する値は、`styleSheetFile` キーまたは `defaultSampleTemplates` キー用に指定した値と一致する必要があります。 **注意** 初期設定値は`"ExportCPL.xslt|ExportSTIX.xslt|ExportCSV.xslt"`です。

キー	説明	例
<suspiciousObjectColumns> 場所: <soDataColumnSettings>	選択したリストのデータ列を指定します。 isEnable="true"に設定すると、指定したデータ列をエクスポートします。	• <add id="1" name="SeqID" isEnable="true"></add> 選択したリストから「SeqID」データ列をエクスポートします。 • <add id="1" name="MD5Key" isEnable="false"></add> 選択したリストから「MD5Key」データ列を明示的に除外します。 重要 「ExportCSV.xslt」スタイルシートを指定した場合、スタイルシートで指定した列のみがエクスポートされます。
<suspiciousObjectTypeList> 場所: <soTypeSettings>	選択したリストからエクスポートするオブジェクトの種類を指定します。 isEnable="true"に設定すると、指定したオブジェクトの種類をエクスポートします。	• <add value="0" description="IP" isEnable="true"></add> 選択したリストからすべての IP アドレスのオブジェクトをエクスポートします。 • <add value="1" description="Domain" isEnable="false"></add> エクスポートするリストからすべての「Domain」オブジェクトを明示的に除外します。

キー	説明	例
<suspiciousObjectSourceType> 場所: <soTypeSettings>	不審オブジェクトのソースの種類を指定します。 isEnable="true"に設定すると、指定したオブジェクトの種類をエクスポートします。	• <add value="0" description="SourceType" isEnable="true"/> 仮想アナライザの不審オブジェクトリストを選択します。 • <add value="1" description="SourceType" isEnable="true"/> ユーザ指定の不審オブジェクトリストを選択します。 • <add value="2" description="SourceType" isEnable="true"/> 仮想アナライザの除外リストを選択します。 **重要** • ExportCSV.xslt スタイルシートを指定し、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を選択した場合、エクスポートされる列は [オブジェクト]、[種類]、[Scan Prefilter]、[メモ]、および [検出時の処理] です。 • ExportCSV.xslt スタイルシートを指定し、仮想アナライザの除外リストを選択した場合、エクスポートされる列は [オブジェクト]、[種類]、[Scan Prefilter]、および [メモ] です。

Check Point Suspicious Activity Monitoring Client ツールを使用する

注意

次の手順では、不審オブジェクトデータを Check Point ファイアウォールサーバにインポートする際に、Check Point によって提供される `CKP_SAM_Client.exe` ツールを使用していることを前提としています。

重要

Check Point SAM Client ツールを使用する前に、次の手順を実行する必要があります。

- Check Point ファイアウォールサーバを準備する。

  詳細については、524 ページの「Check Point ファイアウォールサーバを準備する」参照してください。

- 認証の設定ファイルを準備する。

  詳細については、527 ページの「認証証明書の設定ファイルを準備する」参照してください。

- 不審オブジェクトリストエクスポートツールを使用して、Control Manager 不審オブジェクトリストをエクスポートする。

  詳細については、499 ページの「不審オブジェクトリストエクスポートツールを使用する (SuspiciousObjectExporter.exe)」参照してください。

手順

1. Control Manager サーバにログオンします。
2. コマンドプロンプトを開きます。
3. 次のコマンドを使用して、`CKP_SAM_Client.exe` ファイルが含まれるディレクトリを見つけます。

   `cd <Control Manager インストールディレクトリ>/SOTools`

4. 次のコマンドを使用して、`CKP_SAM_Client.exe` を実行します。

```
CKP_SAM_Client.exe -t <timeout> -g <fw-ip> -c <conf_path> -A
notify any <IP_address>
```

ここでは次を意味します。

- `-t <timeout>`: 不審オブジェクトが期限切れになるまで Check Point サーバが待機する時間 (秒数) を指定します。
- `-c <conf_path>`: `sam.conf` ファイルの相対パスを指定します。
- `-g <fw-ip>`: Check Point ファイアウォールサーバの IPv4 アドレスを指定します。
- `-A notify any <IP_address>`: Check Point ファイアウォールサーバに対し、有効な IPv4 アドレスを通知するように要求します。

注意

- 引数を指定せずに `CKP_SAM_Client.exe` を実行すると、ツールの使用方法が表示されます。
- Check Point `sam_client_action` 引数の詳細については、Check Point ファイアウォールサーバのドキュメントを参照してください。

`CKP_SAM_Client.exe` ツールに、要求が正常に完了したことを示すメッセージが表示されます。

5. Check Point ファイアウォールサーバでインポートした不審オブジェクトデータを確認するには、次の手順を実行します。

   a. Check Point SmartView Monitor コンソールにログオンします。

   b. [Tools] > [Suspicious Activity Rules] に移動します。

      [Enforced Suspicious Activity Rules] 画面にインポートした不審オブジェクトデータが表示されます。

第 25 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。

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

トレンドマイクロでは、最新のセキュリティニュースをインターネットで公開しています。トレンドマイクロのセキュリティニュースでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティニュースは、次の URL からアクセスできます。

https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html

- ウイルス名やキーワードから検索できる脅威データベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティニュースに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

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専門のスタッフが解析し、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。

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

Control Manager 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 Control Manager (以下、Control Manager) 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
Control Manager 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	
Control Manager 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	

必要な情報	EXAMPLE	設定する値
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	
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

Control Manager 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	
ファイアウォール転送用 (任意: Control Manager のエージェントのインストール時に使用)	224	

Control Manager の入力規則

Control Manager 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
  - 最大長 —40 文字
  - 使用できない文字 —/ > & "

注意

Control Manager 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

Control Manager 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、Control Manager 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. Control Manager 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

設定ファイル	説明
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。
DMRegisterinfo.xml	CasProcessor.exe で使用されます。
DataSource.xml	Control Manager のプロセスの接続パラメータを保存します。
SystemConfiguration.xml	Control Manager 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. Control Manager プロセス

プロセス	説明
ProcessManager.exe	Control Manager 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、Control Manager データベースに保存します。
ReportServer.exe	Control Manager レポートを生成します。

プロセス	説明
MsgReceiver.exe	Control Manager 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	Control Manager サーバが他の Control Manager 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	Control Manager 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 (Control Manager 側) を管理します。
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実行するために、Control Manager 管理コンソールまたはその他のプロセスに発行元のジョブ 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 Control Manager 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

サービス	サービスポート
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、Control Manager 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。

- 562 ページの「データビュー: セキュリティログ」
- 656 ページの「データビュー: 製品情報」

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。

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-1. 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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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。

データ	説明
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: ウイルスバスター コーポレートエディションで、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-2. 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
送信元ホスト	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: ウイルスバスター Corp.で、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: ウイルスバスター Corp.で、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 件検出されたとします。 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: ウイルスバスター Corp.で、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 件検出されたとします。 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。

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-3. 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。
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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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-4. 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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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/不正プログラム詳細情報

このデータビューには、ネットワーク上に存在するウイルス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: ウイルスを検出した管理下の製品、ウイルスの名前、ウイルスに感染したエンドポイントの名前

表 B-5. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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。

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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター Corp.、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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの MAC アドレス。
管理サーバのエンティティ名	エンドポイントが登録されている管理下の製品サーバのエンティティ表示名が表示されます。
ドメイン	エンドポイントが登録されている管理下の製品サーバのドメインが表示されます。
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`
エンドポイントの感染経路	脅威の発生元のチャネル。
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。
送信元ホスト	ウイルスの感染元ソースの IP アドレスまたはホスト名が表示されます。

データ	説明
ユーザ (アカウント)	管理下の製品によってウイルスが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
結果	ウイルスに対して管理下の製品が実行した処理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処理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
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: ウイルスバスター Corp.で、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 件検出されたとします。 この場合、[検出数] は「10」になります。
エントリの種類	管理下の製品によって検出されたウイルス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)
詳細情報	ログクエリでのみ使用されます。選択項目に関する詳細情報が表示されます。 ログクエリ内で、この列には選択項目が下線付きで表示されます。下線付きの選択項目をクリックすると、その詳細が表示されます。 例: ホストの詳細、ネットワークの詳細、HTTP/FTP の詳細
ウイルスバスター Corp.ドメイン階層	ウイルスバスター Corp.ドメイン階層のパスが表示されます。
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。
OS:	エンドポイントで稼働している OS が表示されます。
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が表示されます。

データ	説明
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。

エンドポイントのウイルス/不正プログラム情報

エンドポイントで検出されたウイルス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: ウイルスを検出した管理下の製品、ウイルスを検出した検索の種類、検出されたウイルスへのエンドポイント上のファイルパス

表 B-6. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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/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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレス。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター Corp.、InterScan for Microsoft Exchange

データ	説明
管理サーバのエンティティ名	エンドポイントが登録されている管理下の製品サーバのエンティティ表示名が表示されます。
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
エンドポイント	ウイルスに感染したコンピュータの名前が表示されます。
ユーザ (アカウント)	管理下の製品によってウイルスが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
検索の種類	ウイルスを検出するために管理下の製品が使用する検索の種類が表示されます。例: リアルタイム、予約、手動
ファイル	管理下の製品が検出した、ウイルスに感染したファイルの名前が表示されます。
ファイルパス	管理下の製品がウイルスを検出したエンドポイントコンピュータのファイルパスが表示されます。
圧縮ファイル内のファイル	圧縮ファイル内の感染ファイルまたはウイルスの名前が表示されます。
結果	ウイルスに対して管理下の製品が実行した処理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処理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
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: ウイルスバスター Corp.で、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 件検出されたとします。 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: ウイルスを検出した管理下の製品、ウイルスが発生したトラフィックの方向、ウイルスをダウンロードしたインターネットブラウザまたは FTP エンドポイント

表 B-7. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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/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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
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`
エンドポイント	管理下の製品がウイルスを検出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。
感染元 URL	ウイルスの感染元である Web/FTP サイトの URL が表示されます。
ユーザ (アカウント)	管理下の製品によってウイルスが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
トラフィック/接続	ウイルスの侵入方向が表示されます。

データ	説明
ブラウザ/FTP クライアント	ウイルスの感染元のインターネットブラウザまたは FTP エンドポイントが表示されます。
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
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: ウイルスバスター コーポレートエディションで、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が表示されます。

メールのウイルス/不正プログラム情報

メールメッセージで検出されたウイルス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、ウイルスを含んでいるメールメッセージの送信者

表 B-8. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange

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
受信者	ウイルスを含んでいるメールメッセージの受信者が表示されます。
送信者	ウイルスを含んでいるメールメッセージの送信者が表示されます。
ユーザ (アカウント)	管理下の製品によってウイルスが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
件名	ウイルスを含んでいるメールメッセージの件名のコンテンツが表示されます。
ファイル	管理下の製品が検出した、ウイルスに感染したファイルの名前が表示されます。
圧縮ファイル内のファイル	圧縮ファイル内の感染ファイルまたはウイルスの名前が表示されます。
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
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: ウイルスバスター コーポレートエディションで、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が表示されます。

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が使用したプロトコル、ウイルスの感染元および感染先に関する具体的な情報

表 B-9. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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/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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
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`
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/ホスト名が表示されます。
感染元ホスト	ウイルスの感染元ソースの IP アドレスまたはホスト名が表示されます。
ユーザ (アカウント)	管理下の製品によってウイルスが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
トラフィック/接続	ウイルスの侵入方向が表示されます。

データ	説明
プロトコル	ネットワークへの侵入にウイルスが使用したプロトコルが表示されます。 例: HTTP、SMTP、FTP
エンドポイントコンピュータ	ウイルスに感染したコンピュータのコンピュータ名が表示されます。
エンドポイントポート	ウイルスに感染したコンピュータのポート番号が表示されます。
エンドポイント MAC	ウイルスに感染したコンピュータの MAC アドレスが表示されます。
感染元ソース	ウイルスの感染元ソースのコンピュータ名が表示されます。
感染元ポート	ウイルスの感染元ソースのポート番号が表示されます。
感染元 MAC	ウイルスの感染元ソースの MAC アドレスが表示されます。
ファイル	管理下の製品が検出した、ウイルスに感染したファイルの名前が表示されます。
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
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: ウイルスバスター コーポレートエディションで、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が表示されます。

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-10. 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。 ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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-11. 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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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-12. 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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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-13. 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。

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: ウイルスバスター コーポレートエディションで、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。
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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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-14. 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
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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、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/グレーウェア詳細情報

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の名前

表 B-15. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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/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。Control Manager 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。 • スパイウェア/グレーウェアに感染した、クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。例: ウイルスバスター Corp.、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。 • スパイウェア/グレーウェアに感染した、クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • スパイウェア/グレーウェアに感染した、クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの MAC アドレス。
管理サーバのエンティティ名	エンドポイントが登録されている管理下の製品サーバのエンティティ表示名が表示されます。
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。
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 IP アドレスまたはホスト名が表示されます。

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 IP アドレスまたはホスト名が表示されます。
ユーザ (アカウント)	管理下の製品によってスパイウェア/グレーウェアが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
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処理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
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: ウイルスバスター Corp.で、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 件検出されたとします。 この場合、[検出数] は「10」になります。
エントリの種類	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)
詳細情報	ログクエリでのみ使用されます。選択項目に関する詳細情報が表示されます。 ログクエリ内で、この列には選択項目が下線付きで表示されます。下線付きの選択項目をクリックすると、その詳細が表示されます。 例: ホストの詳細、ネットワークの詳細、HTTP/FTP の詳細
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。
ウイルスバスター Corp.ドメイン階層	ウイルスバスター Corp.クライアントが属しているクライアントツリードメインまたはサブドメインが表示されます。
ドメイン	エンドポイントが属するドメインの名前が表示されます。

データ	説明
OS	エンドポイントで稼働している OS 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。

エンドポイントのスパイウェア/グレーウェア

エンドポイント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-16. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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/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。Control Manager 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。 • スパイウェア/グレーウェアに感染した、クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
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。 • スパイウェア/グレーウェアに感染した、クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレス。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター Corp.、InterScan for Microsoft Exchange

データ	説明
管理サーバのエンティティ名	エンドポイントが登録されている管理下の製品サーバのエンティティ表示名が表示されます。
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。
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 IP アドレスまたはホスト名が表示されます。
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 IP アドレスまたはホスト名が表示されます。
ユーザ (アカウント)	管理下の製品によってスパイウェア/グレーウェアが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
検索の種類	スパイウェア/グレーウェアを検出するために管理下の製品が使用する検索の種類が表示されます。 例: リアルタイム、予約、手動
リソース	感染したリソースが具体的に表示されます。 例: `application.exe`、`H Key Local Machine\SOFTWARE\ACME`
リソースの種類	スパイウェア/グレーウェアに感染したリソースの種類が表示されます。 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	管理下の製品が検出したスパイウェア/グレーウェアの種類が具体的に表示されます。 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	スパイウェア/グレーウェアがネットワークにもたらすリスクのレベルが表示されます (トレンドマイクロによる定義)。 例: 高、中、低
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

データ	説明
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処理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
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。
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。

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インターネットブラウザまたは FTP エンドポイント

表 B-17. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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/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。Control Manager 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。 • スパイウェア/グレーウェアに感染した、クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター Corp.、InterScan for Microsoft Exchange

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。
IP	管理下の製品がスパイウェア/グレーウェアを検出したコンピュータの IP アドレスが表示されます。
感染元 URL	スパイウェア/グレーウェアの感染元である Web/FTP サイトの URL が表示されます。
トラフィック/接続	スパイウェア/グレーウェアの侵入方向が表示されます。
ブラウザ/FTP クライアント	ウイルスの感染元のインターネットブラウザまたは FTP エンドポイントが表示されます。
ユーザ (アカウント)	管理下の製品によってスパイウェア/グレーウェアが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
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処理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
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: ウイルスバスター Corp.で、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 件検出されたとします。 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が表示されます。

メールのスパイウェア/グレーウェア

メールメッセージ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、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-18. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
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。
受信者	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受信者が表示されます。
送信者	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が表示されます。
ユーザ (アカウント)	管理下の製品によってスパイウェア/グレーウェアが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
件名	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件名のコンテンツが表示されます。
ファイル	管理下の製品が検出した、スパイウェア/グレーウェアに感染したファイルの名前が表示されます。
圧縮ファイル内のファイル	圧縮ファイル内に存在するスパイウェア/グレーウェアのファイル名が表示されます。

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処理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
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: ウイルスバスター コーポレートエディションで、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が表示されます。

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具体的な情報

表 B-19. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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。

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。Control Manager 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。 • スパイウェア/グレーウェアに感染した、クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
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。
トラフィック/接続	スパイウェア/グレーウェアの侵入方向が表示されます。
プロトコル	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が表示されます。 例: HTTP、SMTP、FTP
エンドポイント IP	スパイウェア/グレーウェアに感染したコンピュータの IP アドレスが表示されます。
エンドポイント	スパイウェア/グレーウェア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。
エンドポイントポート	スパイウェア/グレーウェアに感染したコンピュータのポート番号が表示されます。
エンドポイント MAC	スパイウェア/グレーウェアに感染したコンピュータの MAC アドレスが表示されます。
送信元 IP	スパイウェア/グレーウェアの感染元ソースの IP アドレスが表示されます。
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ホスト名が表示されます。
感染元ポート	スパイウェア/グレーウェアの感染元ソースのポート番号が表示されます。

データ	説明
感染元 MAC	スパイウェア/グレーウェアの感染元ソースの MAC アドレスが表示されます。
ユーザ (アカウント)	管理下の製品によってスパイウェア/グレーウェアが検出されたとき、エンドポイントコンピュータにログオンしていたユーザの名前が表示されます。
ファイル	管理下の製品が検出した、スパイウェア/グレーウェアに感染したファイルの名前が表示されます。
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処理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
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: ウイルスバスター コーポレートエディションで、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が表示されます。

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-20. 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
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-21. 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。
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-22. 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。

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、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。
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-23. 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

データ	説明
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。

コンテンツ違反詳細情報

ネットワーク上のコンテンツ違反に関する具体的な情報が表示されます。例: コンテンツ違反を検出した管理下の製品、違反ポリシーの名前、ネットワーク上のコンテンツ違反の総数

表 B-24. コンテンツ違反詳細情報データビュー

データ	説明
受信	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター Corp.、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が表示されます。
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が表示されます。
件名	ポリシーに違反するメールの件名のコンテンツが表示されます。
ポリシー	メールが違反しているポリシーの名前が表示されます。
ポリシー設定	メールが違反しているポリシーの設定が表示されます。
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が表示されます。
ファイル	ポリシーに違反しているファイルの名前が表示されます。
URL	指定したポリシーに違反している URL が表示されます。

データ	説明
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)。 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が表示されます。 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が表示されます。
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が表示されます。 例: 駆除、隔離、削除
フィルタ処理結果	違反メールを検出したフィルタの処理結果が表示されます。
処理	コンテンツポリシーに違反するメール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: 配信、削除、通知
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。

高度な脅威を含むメールメッセージ

不正または疑わしい動作を示すすべてのメールメッセージが表示されます。疑わしい動作には、変則的な動作、誤データや偽データ、不審または不正な動作パターン、追加調査が必要なシステム侵入を疑わせる文字列などが含まれます。

データ	説明
受信日時	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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。Control Manager は、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。

データ	説明
製品	管理下の製品の名前が表示されます。例: ウイルスバスター Corp.、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が表示されます。
送信者	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が表示されます。
件名	ポリシーに違反するメールの件名のコンテンツが表示されます。
添付ファイル数	添付ファイルの数
添付ファイル	添付ファイルの名前
添付ファイルの種類	添付ファイルの種類
処理	コンテンツポリシーに違反するメール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: 配信、削除、隔離
脅威の種類	脅威の種類
脅威名	脅威の名前
リスクレベル	メールメッセージのリスクレベルの調査結果
送信元 IP	メール送信元に最も近い MTA の IP アドレス
メッセージ ID	管理者が設定した一意のメッセージ ID
リンク数	メッセージに含まれるリンクの数
リンク	リンクのリスト

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
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-25. 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-26. 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。
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。

スパムメール詳細情報

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。
例: スパムメール違反を検出した管理下の製品、違反ポリシーの名前、ネットワーク上のスパムメール違反の総数

表 B-27. スパムメール詳細情報データビュー

データ	説明
受信	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
受信者	スパムメールの受信者が表示されます。
送信者	スパムメールの送信者が表示されます。
件名	スパムメールの件名のコンテンツが表示されます。
ポリシー	メールが違反しているポリシーの名前が表示されます。
処理	メールで検出されたスパムメール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: 配信、通知、削除
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。例: スパムメール違反を検出した管理下の製品、スパムメール違反に対して管理下の製品が実行した具体的なアクション、ネットワーク上のスパムメール違反の総数

表 B-28. スパムメール接続情報データビュー

データ	説明
受信	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
送信元 IP	スパムメールの送信元のメールサーバの IP アドレスが表示されます。
フィルタの種類	違反メールを検出したフィルタの種類が表示されます。 例: Real-time Blackhole List (RBL+)、Quick IP リスト(QIL)
処理	メールサーバへのスパムメールの侵入を防ぐために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: 接続の破棄、接続の放置
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。

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。

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。例: ファイアウォール違反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、ネットワーク上のファイアウォール違反の総数

表 B-29. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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/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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
イベントの種類	違反をトリガしたイベントの種類が表示されます。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が表示されます (トレンドマイクロによる診断)。 例: 高、中、低
トラフィック/接続	通信方向が表示されます
プロトコル	侵入に使用されたプロトコルが表示されます。 例: HTTP、SMTP、FTP
送信元 IP	ネットワークに侵入を試みるコンピュータの IP アドレスが表示されます。

データ	説明
エンドポイントポート	攻撃されたコンピュータのポート番号が表示されます。
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。
ターゲットアプリケーション	侵入対象のアプリケーションが表示されます。
説明	トレンドマイクロによるイベントの詳細な説明が表示されます。
処理	ポリシー違反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: 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	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。

ネットワークコンテンツ検査情報

このデータビューには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-30. 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 Control Manager がデータを受信した時間が表示されます。
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。

データ	説明
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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター Corp.、InterScan for Microsoft Exchange
トラフィック/接続	通信方向が表示されます
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。
エンドポイントポート	攻撃されたコンピュータのポート番号が表示されます。
送信先 IP	攻撃対象になる可能性があるネットワーク上のコンピュータの IP アドレスが表示されます。
宛先ドメイン	攻撃対象になる可能性があるネットワーク上のコンピュータのドメインが表示されます。
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。
処理	ポリシー違反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。
パターンファイルの種類	違反を検出したパターンファイルの種類が表示されます。

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-31. 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 Control Manager がデータを受信した時間が表示されます。
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	管理下の製品のエンティティ表示名が表示されます。Control Manager は、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: ウイルスバスター Corp.、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が表示されます。
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 アドレスが表示されます。
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 アドレスが表示されます。
ポリシー/ルール	遵守ポリシー/ルールの名前が表示されます。
サービス	ポリシー/ルールを遵守しているサービス/プログラムの名前が表示されます。
ユーザ	管理下の製品によってポリシー/ルール遵守が検出されたとき、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。
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が表示されます。
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が表示されます。
説明	トレンドマイクロによるイベントの詳細な説明が表示されます。

データ	説明
検出数	管理下の製品によって検出されたポリシー/ルール遵守の総数が表示されます。 例: 管理下の製品が、1 台のコンピュータで同一の種類の遵守インスタンスが 10 件検出したとします。 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: セキュリティ遵守を検出した管理下の製品、遵守ポリシーの名前、ネットワーク上のセキュリティ遵守の総数

表 B-32. 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	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター コーポレートエディション、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が表示されます。
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 アドレスが表示されます。
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 アドレスが表示されます。
ポリシー/ルール	遵守ポリシー/ルールの名前が表示されます。

データ	説明
サービス	ポリシー/ルールを遵守しているサービス/プログラムの名前が表示されます。
ユーザ (アカウント)	管理下の製品によってポリシー/ルール遵守が検出されたとき、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。
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。
検出数	管理下の製品によって検出されたポリシー/ルール遵守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遵守インスタンスが 10 件検出されました。 この場合、[検出数] は「10」になります。

アプリケーションアクティビティの詳細

ネットワーク上のアプリケーションアクティビティの全般的な情報が表示されます。例: セキュリティ遵守を検出した管理下の製品、遵守ポリシーの名前、ネットワーク上のセキュリティ遵守の総数

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	Control Manager で管理下の製品からデータを受信した時刻。
生成	管理下の製品でデータが生成された時刻。
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。Control Manager 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。 例: ウイルスバスター コーポレートエディション、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) が表示されます。

データ	説明
検出元	脅威の兆候を検出したフィルタ、検索エンジン、管理下の製品が表示されます。
トラフィック/接続	ネットワークトラフィックの方向、または脅威の兆候が発生したネットワークの場所が表示されます。
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が表示されます。 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が表示されます。 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が表示されます。
送信元 IP	脅威の兆候の発生源である送信元の IP アドレスが表示されます。
感染元 MAC	脅威の兆候の発生源である送信元の MAC アドレスが表示されます。
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が表示されます。
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が表示されます。
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が表示されます。
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 アドレスが表示されます。
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が表示されます。
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 アドレスが表示されます。
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 アドレスのグループが表示されます。

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/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。
脅威の種類	管理下の製品が検出したセキュリティの脅威の種類が具体的に表示されます。
検出の重大度	インシデントの重大度レベルが表示されます。
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 アドレスが表示されます。 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 アドレスが表示されます。 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が表示されます。
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が表示されます。
ネットワークグループ	グループの名前が表示されます。
ホストへの影響の重大度	ホストへの影響の重大度が表示されます。
ログ ID	ログ ID が表示されます。

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-34. 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 Control Manager がデータを受信した時間が表示されます。
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。
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。

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-35. 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 Control Manager がデータを受信した時間が表示されます。
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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名
製品	管理下の製品の名前が表示されます。 例: ウイルスバスター Corp.
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。

エンドポイントアプリケーションコントロール違反詳細情報

ネットワーク上のアプリケーション違反に関する具体的な情報が表示されます。例: 違反しているポリシーやルールの名前、エンドポイントやアプリケーションに関する具体的な情報

表 B-36. エンドポイント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
受信日時	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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。
ユーザ名	アカウントのユーザ名が表示されます。
エンドポイント	影響を受けたコンピュータのホスト名が表示されます。
処理	処理の種類が表示されます。許可、ブロック、ロックダウンのいずれかです。
アプリケーション	ルールを起動するアプリケーションの名前が表示されます。
バージョン	バージョン情報が表示されます。
ポリシー	Trend Micro Endpoint Application Control ポリシーの名前が表示されます。
ルール	アプリケーションの使用に関するルールの名前が表示されます。
サーバ	Endpoint Application Control サーバのホスト名が表示されます。
接続ステータス	特定の Endpoint Application Control サーバの接続ステータスが表示されます。
エンドポイントの IP アドレス	ポリシー/ルールを遵守しているコンピュータの IP アドレスが表示されます。
SHA-1	ファイルの署名が表示されます。
コマンド	発行されたコマンドの種類が表示されます。
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が表示されます。

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ための情報が表示されます。

データ	説明
受信日時	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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。
サーバ	管理下の製品のサーバのホスト名が表示されます。
送信元 IP	侵入元の IP アドレス
送信元 MAC	侵入元の MAC アドレス
送信元ポート	侵入元のポート番号
送信先 IP	侵入先の IP アドレス
送信先 MAC	侵入先の MAC アドレス
送信先ポート	侵入先のポート番号
MAC (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 MAC アドレスが表示されます。ネットワーク内で侵入が確認された場合は侵入元の MAC アドレス、外部トラフィックの場合は侵入先の MAC アドレスが表示されます。
モード	インラインまたはタップ
処理	侵入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: 防御、検出
方向	通信方向
順位	侵入の順位
重大度	侵入の重大度
プロトコル	侵入時に利用されたプロトコル
アプリケーション	脆弱なアプリケーション
理由	パケットの拒否理由

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、コンピュータの特定の領域での変更を監視するための情報が表示されます。

データ	説明
受信日時	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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。
サーバ	管理下の製品のサーバのホスト名が表示されます。
変更	コンピュータの変更
ユーザ	コンピュータにログオンしているユーザ
プロセス	プロセスの変更
種類	レジストリキーの種類
キー	レジストリキー
順位	変更の順位
重大度	変更の重大度

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 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-37. 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。
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-38. 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。

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 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 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-39. 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

データ	説明
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。

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-40. 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-41. 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。
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-42. 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。
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 違反詳細情報

このデータビューには、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。たとえば、Web 違反を検出した管理下の製品、違反ポリシーの名前、ネットワーク上の Web 違反の総数が表示されます。

表 B-43. Web 違反詳細情報データビュー

データ	説明
受信	管理下の製品から Control Manager がデータを受信した時間が表示されます。
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。
管理サーバのエンティティ名	製品のエンティティ名を管理するサーバのエンティティ表示名が表示されます。
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。Control Manager 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: ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange
トラフィック/接続	通信方向が表示されます
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
URL	Web ポリシーに違反している URL の名前が表示されます。
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 アドレスが表示されます。
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が表示されます。
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 アドレスが表示されます。
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が表示されます。

データ	説明
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
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が表示されます。 例: URL ブロック
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。
ファイル	ポリシーに違反しているファイルの名前が表示されます。
プロセス	ポリシーに違反しているプロセスの名前が表示されます。
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が割合で表示されます (トレンドマイクロによる定義)。
処理	ポリシー違反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: 放置、ブロック
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 レピュテーション詳細情報

ネットワーク上のアプリケーションアクティビティの全般的な情報が表示されます。例: セキュリティ遵守を検出した管理下の製品、遵守ポリシーの名前、ネットワーク上のセキュリティ遵守の総数

表 B-44. 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	Control Manager で管理下の製品からデータを受信した時刻。
生成	管理下の製品でデータが生成された時刻。
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。Control Manager 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。 例: ウイルスバスター Corp.、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) が表示されます。
検出元	脅威の兆候を検出したフィルタ、検索エンジン、管理下の製品が表示されます。
トラフィック/接続	ネットワークトラフィックの方向、または脅威の兆候が発生したネットワークの場所が表示されます。
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が表示されます。 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が表示されます。 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が表示されます。
送信元 IP	脅威の兆候の発生源である送信元の IP アドレスが表示されます。
感染元 MAC	脅威の兆候の発生源である送信元の MAC アドレスが表示されます。
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が表示されます。
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が表示されます。

データ	説明
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が表示されます。
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 アドレスが表示されます。
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が表示されます。
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 アドレスが表示されます。
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 アドレスのグループが表示されます。
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が表示されます。
ポリシー/ルール	脅威の兆候が違反しているポリシー/ルールが表示されます。
URL	脅威の兆候と考えられる URL 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/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。 C&C リストのソース
C&C リストのソース	C&C サーバを特定した C&C リストのソースが表示されます。
C&C リスクレベル	C&C サーバのリスクレベルが表示されます。
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種類が具体的に表示されます。
検出の重大度	インシデントの重大度レベルが表示されます。

データ	説明
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 アドレスが表示されます。 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 アドレスが表示されます。 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が表示されます。
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が表示されます。
ネットワークグループ	グループの名前が表示されます。
ホストへの影響の重大度	ホストへの影響の重大度が表示されます。
ログ ID	ログ ID が表示されます。
攻撃フェーズ	攻撃が発生したフェーズが表示されます。
注釈	攻撃に関する説明が表示されます。
C&C サーバ	C&C サーバの名前、URL、または IP アドレスが表示されます。
C&C サーバの種類	サーバの種類が表示されます。
送信者	転送が開始された送信者のアドレスが表示されます。
受信者	転送先のアドレスが表示されます。
件名	URL を含んでいるメールメッセージの件名が表示されます。

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。

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-45. 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。
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。

データ	説明
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。
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-46. 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。

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-47. 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。

データ	説明
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-48. 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。

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-49. 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。
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-50. 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。
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。

データ	説明
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-51. 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。

データ	説明
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。

脅威の兆候の詳細情報

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: 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

表 B-52. 脅威の兆候の詳細情報データビュー

データ	説明
受信	管理下の製品から Control Manager がデータを受信した時間が表示されます。

データ	説明
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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター Corp.、InterScan for Microsoft Exchange
Mitigation ホスト	Mitigation Server (Network VirusWall Enforcer または Threat Mitigator) のホスト名が表示されます。
トラフィック/接続	ネットワークトラフィックの方向、または脅威の兆候が発生したネットワークの場所が表示されます。
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が表示されます。 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が表示されます。例: ARP、Bearshare、BitTorrent
送信先 IP アドレス	脅威の兆候が影響を与えるエンドポイントの IP アドレスが表示されます。
送信先ホスト	脅威の兆候が影響を与えるエンドポイントのホスト名が表示されます。
送信先ポート	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が表示されます。
送信先 MAC アドレス	脅威の兆候が影響を与えるエンドポイントの MAC アドレスが表示されます。
送信先 OS	対象ホストの OS が表示されます。
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が表示されます。 <x>はユーザ名です。
ログオン (送信先ユーザ<x>)	ログオンのタイムスタンプが表示されます。 <x>はログオン時間の数字と特定のタイムスタンプを表します。

データ	説明
送信元 IP アドレス	脅威の兆候の発生元の IP アドレスが表示されます。
送信元ホスト名	脅威の兆候の発生元のホスト名が表示されます。
送信元ポート	脅威の兆候の発生元のポート番号が表示されます。
送信元 MAC アドレス	脅威の兆候の発生元の MAC アドレスが表示されます。
送信元 OS	対象の侵入元ホストの OS が表示されます。
送信元ユーザ<x>	対象の感染元ホストへのログオンに使用された名前が表示されます。 <x>はユーザ名です。
ログオン (送信元ユーザ<x>)	侵入元のログオンのタイムスタンプが表示されます。 <x>はログオン時間の数字と特定のタイムスタンプを表します。
送信元ドメイン	脅威の兆候の発生元のドメインが表示されます。
セキュリティの脅威の種類	管理下の製品が検出したセキュリティの脅威の種類が具体的に表示されます。 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	脅威の兆候が違反しているポリシー/ルールが表示されます。
受信者	脅威の兆候の受信者が表示されます。
送信者	脅威の兆候の送信者が表示されます。
件名	スパイウェア/グレーウェアを含んでいるメールの件名のコンテンツが表示されます。
添付ファイル名	添付ファイルのファイル名と拡張子名が表示されます。
添付ファイルの種類	添付ファイルの種類が表示されます。
添付ファイルの SHA-1	添付ファイルの SHA-1 ハッシュが表示されます。
URL	脅威の兆候と考えられる URL が表示されます。

データ	説明
ユーザ (アカウント)	管理下の製品によって脅威の兆候が検出されたとき、感染先にログオンしていたユーザの名前が表示されます。
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が表示されます。
ブラウザ/FTP クライアント	脅威の兆候の発生元のインターネットブラウザまたは FTP エンドポイントが表示されます。
ファイル	不審なファイルの名前が表示されます。
圧縮ファイル内のファイル	脅威の兆候の発生元が圧縮ファイルかどうかが表示されます。
アーカイブの SHA-1	アーカイブファイルの SHA-1 ハッシュが表示されます。
アーカイブファイルタイプ	アーカイブファイルの種類が表示されます。
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が表示されます。
SHA-1	SHA-1 ハッシュが表示されます。
軽減処理	脅威の兆候に対して Mitigation Server が実行した処理の結果が表示されます。 例: ファイルはウイルス駆除されました、ファイル削除、ファイルは削除されました
軽減結果	脅威の兆候に対して Mitigation Server が実行した処理の結果が表示されます。
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が表示されます。
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が表示されます。
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 アドレスのグループが表示されます。
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。
C&C リストのソース	コールバックアドレスを含むリストの名前 • グローバルインテリジェンス (Trend Micro Smart Protection Network などのトレンドマイクログローバルインテリジェンスネットワーク) • 管理下の製品の仮想アナライザ • 管理下の製品で設定されたユーザ指定の C&C リスト
C&C リスクレベル	コールバックの重大度レベル
注釈	攻撃に関する説明が表示されます。
C&C サーバ	C&C サーバの名前、URL、または IP アドレスが表示されます。
C&C サーバの種類	サーバの種類が表示されます。
不正プログラムの種類	不正プログラムの種類が表示されます。

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-53. 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 Control Manager がデータを受信した時間が表示されます。
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。

データ	説明
Mitigation Server エンティティ名	Mitigation Server (Network VirusWall Enforcer または Threat Mitigator) のエンティティ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。例: ウイルスバスター Corp.、InterScan for Microsoft Exchange
エンドポイント IP	脅威が影響を与えるエンドポイントの IP アドレスが表示されます。
エンドポイント	脅威が影響を与えるエンドポイントのホスト名が表示されます。
データソース	脅威イベント情報を生成した Deep Discovery 製品またはタスクが表示されます。
データソースホスト	脅威イベント情報を生成した Deep Discovery 製品のホスト名が表示されます。
脅威イベント	Mitigation Server で記録された脅威関連イベントが表示されます。 http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm
軽減ステータス	脅威イベントがステータスグループ別に表示されます。 http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm
軽減の詳細	脅威イベントに関する詳細が表示されます。 http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/start.htm#help/info/mitigation_status.htm
検出数	管理下の製品が検出した脅威の総数が表示されます。
詳細情報	脅威に関する詳細が表示されます。

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-54. 相関の詳細情報データビュー

データ	説明
生成	管理下の製品がデータを生成した時間が表示されます。
IP アドレス	脅威の兆候が影響を与えるエンドポイントの IP アドレスが表示されます。
ネットワークグループ	監視対象のネットワークグループが表示されます。
プロトコル	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が表示されます。
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種類が表示されます。 例: ウイルス、スパイウェア/グレーウェア、不正行為
重大度	ホストへの影響の重大度が表示されます。
検出	検出の種類が相関ルールに基づいて表示されます。
詳細	検出に関する注釈やコメントが表示されます。
MAC アドレス	脅威の兆候が影響を与えるエンドポイントの MAC アドレスが表示されます。
ホスト名	脅威の兆候が影響を与えるエンドポイントのホスト名が表示されます。
相関ルール ID	ルール ID 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

ネットワークから検出された 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-55. 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 Control Manager がデータを受信した時間が表示されます。
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。
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
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
C&C リストのソース	C&C アドレスリストのソース • グローバルインテリジェンス (Trend Micro Smart Protection Network などのトレンドマイクログローバルインテリジェンスネットワーク) • 管理下の製品のアナライザ (仮想アナライザおよびネットワークコンテンツ検査エンジン) • Control Manager および管理下の製品 (Deep Discovery Inspector など) で設定したユーザ指定の C&C リスト
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
C&C リスクレベル	• 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
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
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
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

データ	説明
製品	管理下の製品の名前が表示されます。例: ウイルスバスター Corp.、InterScan for Microsoft Exchange
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。Control Manager は、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。

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-56. 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 Control Manager がデータを受信した時間が表示されます。
検出	管理下の製品が不審オブジェクトを検出した時間が表示されます。
エンドポイント	不審オブジェクトが検出されたエンドポイントが表示されます。
製品	管理下の製品の名前が表示されます。例: ウイルスバスター Corp.、InterScan for Microsoft Exchange
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。Control Manager は、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。
エンドポイントの IP アドレス	エンドポイントの IP アドレス
エンドポイントのホスト名	エンドポイントのホスト名
ファイルタイプ	不審オブジェクトのファイルタイプ
ファイル SHA-1	不審オブジェクトの SHA-1 ハッシュ値
ファイルパス	不審オブジェクトのファイルパスとファイル名

データ	説明
C&C リストのソース	C&C アドレスリストのソース • グローバルインテリジェンス (Trend Micro Smart Protection Network などのトレンドマイクログローバルインテリジェンスネットワーク) • 管理下の製品のアナライザ (仮想アナライザまたはネットワークコンテンツ検査エンジンの適合度ルール) • Control Manager および管理下の製品 (Deep Discovery Inspector など) で設定したユーザ指定の C&C リスト
処理	不審オブジェクトに対する処理
検索の種類	不審オブジェクトを検出した検索の種類
作成日時	不審オブジェクトがエンドポイントで作成された時間が表示されます。
変更日時	不審オブジェクトがエンドポイントで変更された時間が表示されます。

機械学習型検索の詳細情報

このデータビューには、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-57. 機械学習型検索の詳細情報

データ	説明
検出時刻	機械学習型検索で脅威が検出された時間が表示されます。
受信日時	管理下の製品から Control Manager がデータを受信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	次のいずれかの情報が表示されます。 • 管理下の製品のエンティティ表示名。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたエンドポイントの IP アドレスまたはホスト名。

データ	説明
製品/エンドポイント IP	次のいずれかの情報が表示されます。 • 管理下の製品のサーバの IP アドレス。 • エージェントがインストールされたエンドポイントの IP アドレス。
製品	管理下の製品の名前が表示されます。
サーバ	管理下の製品のサーバのホスト名が表示されます。
潜在的な脅威の種類	機械学習型検索が他の既知の脅威と分析を比較した後で、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	機械学習型検索エンジンによって判別されたセキュリティの脅威の名前。
ログオンユーザ	管理下の製品によって脅威が検出されたとき、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。
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」)。
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。
ファイル作成日時	検出されたオブジェクトのファイル作成日時が表示されます。
親プロセス	検出されたプロセスを開始したプロセス。
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。
プロセス所有者	検出されたプロセスが関連付けられたユーザ名が表示されます。
エンドポイントの感染経路	脅威の発生元のチャネル。
感染元	脅威の発生元が表示されます。
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が示されます。
処理結果	実行された処理の結果。
件名	検出を開始したメールメッセージの件名。

データ	説明
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時刻。
送信者	検出を開始したメールメッセージの送信者。
受信者	検出を開始したメールメッセージの受信者。

仮想アナライザによる検出情報

このデータビューには、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-58. 仮想アナライザによる検出情報

データ	説明
生成	管理下の製品が脅威を検出した時間が表示されます。
受信	管理下の製品から Control Manager がデータを受信した時間が表示されます。
製品	管理下の製品の名前が表示されます。
サーバ名	サーバの名前が表示されます。
ホスト	ホストの名前が表示されます。
エントリチャネル	感染経路が表示されます。
ソース	脅威の発生元が表示されます。
配信先	脅威の対象の場所が表示されます。
プロセス名	検出を開始したプロセスの名前。
SHA1	検出を開始したファイルの SHA-1 ハッシュ。
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」) が表示されます。
ファイル名	検出を開始したファイルの名前が表示されます。
ファイルタイプ	検出を開始したファイルの種類が表示されます。

データ	説明
URL	検出を開始した URL が表示されます。
送信ルール	仮想アナライザによって送信されたルールが表示されます。
作成要求日時	仮想アナライザがルールを送信した時間が表示されます。
完了日時	仮想アナライザの処理が完了した時間が表示されます。
セキュリティの脅威	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。
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が表示されます。
脅威のカテゴリ	セキュリティの脅威の種類が表示されます。
最も重大な脅威	重大度レベル別の最も重大な脅威が示されます。

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

このデータビューには、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	検出された不審オブジェクトの脅威の種類が表示されます。
オブジェクト	検出された不審オブジェクトの種類が表示されます。
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が表示されます。
リスクレベル	検出された不審オブジェクトのリスクレベルが表示されます。
有効期限	不審オブジェクトに設定された有効期限が表示されます。
初回サンプル送信日時	サンプルが仮想アナライザに送信された最初の日時が表示されます。
初回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初の製品が表示されます。

データ	説明
初回サンプル送信ホスト名	サンプルを仮想アナライザに送信した最初の製品のホスト名 (サーバ) が表示されます。
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) が表示されます。
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が表示されます。
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が表示されます。
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が表示されます。
最終サンプル送信日時	サンプルが仮想アナライザに送信された最後の日時が表示されます。
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が表示されます。
最終サンプル送信ホスト名	サンプルを仮想アナライザに送信した最後の製品のホスト名 (サーバ) が表示されます。
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) が表示されます。
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が表示されます。
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が表示されます。
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が表示されます。
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が表示されます。
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が表示されます。
エンドポイントのホスト名	検出を実行したエンドポイントのホスト名が表示されます。

データ	説明
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が表示されます。
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が表示されます。
エンドポイントのユーザ名	検出を実行した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。
エンドポイントの IP アドレス	検出を実行したエンドポイントの IP アドレスが表示されます。
不審オブジェクト初回使用日時	作成された不審オブジェクトをもとに、最初にそのハッシュ値のファイルを検出した日時が表示されます。
不審オブジェクト初回使用製品	作成された不審オブジェクトをもとに、最初にそのハッシュ値のファイルを検出した製品が表示されます。
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	作成された不審オブジェクトをもとに、最後にそのハッシュ値のファイルを検出した日時が表示されます。
不審オブジェクト最終使用製品	作成された不審オブジェクトをもとに、最後にそのハッシュ値のファイルを検出した製品が表示されます。
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が表示されます。
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が表示されます。

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-59. 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)
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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、2 台のコンピュータで 3 つの感染元からの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: ウイルスバスター コーポレートエディションで、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-60. 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: ウイルスバスター コーポレートエディション、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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、2 台のコンピュータで 3 つの感染元からの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: ウイルスバスター コーポレートエディションで、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-61. 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: ウイルスバスター コーポレートエディション、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
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: ウイルスバスター コーポレートエディションで、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: ウイルスバスター コーポレートエディションで、2 台のコンピュータで 3 つの感染元からの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。

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: ウイルスバスター コーポレートエディションで、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-62. 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。
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: ウイルスバスター コーポレートエディションで、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-63. 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。
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: ウイルスバスター コーポレートエディションで、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。

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

このデータビューには、情報漏えい対策イベント情報に関する情報が表示されます。

表 B-64. 情報漏えい対策イベント情報

データ	説明
受信	Control Manager がログを受信した時間が表示されます。
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。
イベント ID	イベントの ID が表示されます。
重大度	
ステータス	インシデントの検出ステータスが表示されます。
マネージャ	部門のマネージャの名前が表示されます。
部署	部門の名前が表示されます。
ポリシー	違反されたポリシーが表示されます。
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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。例: ウイルスバスター Corp.、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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの MAC アドレス。

データ	説明
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。Control Manager 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	クライアント (ウイルスバスター Corp.クライアントなど) がインストール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。
イベント発生元 (Active Directory の表示名)	イベント発生元の Active Directory の表示名が表示されます。
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 のアカウント名が表示されます。
イベント発生元 (送信者)	送信元のメールアドレスが表示されます。
Web サイト	イベントを開始した Web サイトの URL 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。
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が表示されます。
ルール	イベントを検出したルール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。
配信先	配信先が表示されます。
処理	イベントに対して実行された処理が表示されます。
イベント	イベント数が表示されます。

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が表示されます。

情報漏えい対策テンプレート一致情報

表 B-65. 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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの IP アドレスまたはホスト名。
製品	管理下の製品の名前が表示されます。例: ウイルスバスター コーポレートエディション、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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの MAC アドレス。

データ	説明
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。Control Manager 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	クライアント (ウイルスバスター Corp.クライアントなど) がインストール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。
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。

データ検出情報

データ検出情報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

表 B-66. データ検出の情報漏えい対策検出情報

データ	説明
受信	Control Manager がログを受信した時間が表示されます。
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。
ルール	イベントを検出したルールの名前が表示されます。

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。
ドメイン	管理下の製品が属するドメインが表示されます。
ユーザ	アクティビティを開始したユーザの名前が表示されます。
ユーザドメイン	ユーザが属するドメインの名前が表示されます。
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) が表示されます。
ファイル	完全なファイル名が表示されます。
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が表示されます。
処理	転送に対して実行された処理が表示されます。
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、追加情報が表示されます。

データ検出エンドポイント情報

表 B-67. 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。
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。

データビュー: 製品情報

Control Manager、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。

ライセンス情報

Control Manager 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-68. 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。Control Manager 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: ウイルスバスター コーポレートエディション、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: ウイルスバスター Corp. 11.0、Control Manager 6.0
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。

データ	説明
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。

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シート数、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-69. 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。
シート数	このアクティベーションコードで使用が許可されるシート数が表示されます。

製品ライセンス詳細情報

アクティベーションコードに関する情報、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: 管理下の製品の情報、評価版か製品版か、ライセンスの有効期限

表 B-70. 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	管理下の製品のエンティティ表示名が表示されます。Control Manager 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: ウイルスバスター Corp.、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: ウイルスバスター Corp.11.0、Control Manager 6.0
管理下のサービス	管理下のサービスの名前が表示されます。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
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。
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。
シート数	このアクティベーションコードで使用が許可されるシート数が表示されます。
説明	アクティベーションコードの説明が表示されます。

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。

製品配置の概要

Control Manager 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-71. 製品の配置概要データビュー

データ	説明
登録先 Control Manager	管理下の製品の登録先の Control Manager 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。
製品	管理下の製品の名前が表示されます。例: ウイルスバスター コーポレートエディション、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: ウイルスバスター コーポレートエディション 11.0、Control Manager 6.0
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。

製品のステータス情報

Control Manager に登録されている管理下の製品に関する詳細情報が表示されます。例: 管理下の製品のバージョンおよびビルド番号、オペレーティングシステム

表 B-72. 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	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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータのホスト名。
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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの MAC アドレス。
管理 Control Manager のエンティティ名	管理下の製品が登録されている Control Manager サーバのエンティティ表示名が表示されます。
管理サーバのエンティティ名	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。Control Manager 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。
ドメイン	管理下の製品が属するドメインが表示されます。

データ	説明
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 Control Manager への接続ステータス。例: 標準、異常、オフライン • エンドポイントクライアントの管理下の製品 (ウイルスバスター Corp) への接続ステータス。例: 標準、異常、オフライン
パターンファイルのステータス	管理下の製品またはクライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータが使用する各種パターンファイル/ルールのステータスが表示されます。例: 最新、期限切れ
検索エンジンのステータス	管理下の製品またはクライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータが使用する検索エンジンのステータスが表示されます。例: 最新、期限切れ
製品	管理下の製品の名前が表示されます。例: ウイルスバスター Corp.、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クライアントのバージョン番号が表示されます。例: ウイルスバスター Corp.11.0、Control Manager 6.0
製品のビルド	管理下の製品のビルド番号が表示されます。この情報は、製品の [バージョン情報] 画面に表示されます。例: バージョン: 5.0 (ビルド 1219)
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クライアント (ウイルスバスター Corp.クライアントなど) 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
OS	管理下の製品/エージェントがインストールされるコンピュータの OS が表示されます。
OS バージョン	管理下の製品/エージェントがインストールされるコンピュータの OS のバージョン番号が表示されます。
OS Service Pack	管理下の製品/エージェントがインストールされるコンピュータの OS の Service Pack 番号が表示されます。
アップデートエージェント	アップデートエージェントかどうか

データ	説明
前回の予約検索	前回の予約検索の日時
前回の手動検索	前回の手動検索の日時
前回の ScanNow	前回の ScanNow の日時
リアルタイム検索	リアルタイム検索が有効かどうか
ファイアウォール	ファイアウォールが有効かどうか
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が表示されます。
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
検索エンジンの配信ステータス	検索エンジンの配信のステータスが表示されます。
検索エンジンの配信	検索エンジンの配信の日時
ユーザ (アカウント)	管理下の製品サーバのエンドポイントに最後にログオンしたユーザの名前が表示されます。

製品のイベント情報

管理下の製品のイベントに関連する情報が表示されます。例: Control Manager 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. 製品のイベント情報データビュー

データ	説明
受信	管理下の製品のイベントのデータを Control Manager が受信した時間が表示されます。
生成	管理下の製品がイベントのデータを生成した時間が表示されます。

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。Control Manager 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: ウイルスバスター コーポレートエディション、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: ウイルスバスター コーポレートエディション 11.0、Control Manager 6.0
イベント重大度	イベントの重大度が表示されます。例: 情報、重大、警告
イベントの種類	発生したイベントの種類が表示されます。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
コマンドステータス	コマンドのステータスが表示されます。例: 成功、失敗、処理中
説明	管理下の製品がそのイベントに対して提示する説明が表示されます。

製品監査イベントログ

管理下の製品に関する監査情報が表示されます。たとえば、管理コンソールへのアクセスに関する情報などです。

表 B-74. 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	管理下の製品のイベントデータを Control Manager が受信した時間が表示されます。
生成	管理下の製品がイベントデータを生成した時間が表示されます。
ホスト	次のいずれかの情報が表示されます。 • 管理下の製品がインストールされたサーバのホスト名。 • エンジン (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータのホスト名。
ユーザ	アカウント情報が表示されます。

データ	説明
イベントのカテゴリ	発生したイベントのカテゴリが表示されます。例: 管理コンソールへのアクセス
イベントのレベル	イベントの重大度が表示されます。
イベントの説明	管理下の製品がそのイベントに対して提示する説明が表示されます。

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。

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-75. 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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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 Control Manager への接続ステータス。例: 標準、異常、オフライン • エンドポイントクライアントの管理下の製品 (ウイルスバスター Corp) 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: ウイルスバスター Corp.、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クライアントのバージョン番号が表示されます。例: ウイルスバスター Corp.11.0、Control Manager 6.0
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クライアント (ウイルスバスター Corp.クライアントなど) 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
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-76. 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。Control Manager 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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。 • クライアント (ウイルスバスター Corp.クライアントなど) がインストールされたコンピュータの 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 Control Manager への接続ステータス。例: 標準、異常、オフライン • エンドポイントクライアントの管理下の製品 (ウイルスバスター Corp) への接続ステータス。例: 標準、異常、オフライン

データ	説明
製品	管理下の製品の名前が表示されます。例: ウイルスバスター Corp.、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クライアントのバージョン番号が表示されます。例: ウイルスバスター Corp.11.0、Control Manager 6.0
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クライアント (ウイルスバスター Corp.クライアントなど) 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
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。
ウイルスバスター Corp.ドメイン階層	ウイルスバスター Corp.ドメイン階層のパスが表示されます。

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-77. 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。Control Manager 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。

データ	説明
製品	管理下の製品の名前が表示されます。例: ウイルスバスター コーポレートエディション、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: ウイルスバスター コーポレートエディション 11.0、Control Manager 6.0
接続ステータス	管理下の製品と Control Manager 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。
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-78. 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

データ	説明
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。

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-79. 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。

データ	説明
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。
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。

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-80. 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	クライアント (ウイルスバスター Corp.クライアントなど) がインストールされた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。

データ	説明
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-81. 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。

Control Manager 情報

Control Manager へのユーザアクセス、コマンド追跡情報、および Control Manager サーバのイベントに関する情報が表示されます。

ユーザアクセス情報

このデータビューには、Control Manager へのユーザアクセス、および Control Manager にログオン中にユーザが実行するアクティビティが表示されます。

表 B-82. ユーザアクセス情報データビュー

データ	説明
日時	アクティビティの開始時間が表示されます。
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が表示されます。
Active Directory グループ	Active Directory グループの名前が表示されます。
ユーザの役割	アカウントに割り当てられた Control Manager ユーザの役割の名前が表示されます。
アカウントの種類	Control Manager の管理者がユーザに割り当てたアカウントの種類が表示されます。例: root、Power User、Operator
アカウントの種類の説明	アカウントの種類の説明が表示されます。これは、初期設定のアカウントの種類については Control Manager から、カスタムのアカウントの種類についてはユーザ定義から取得されます。
アクティビティ	Control Manager でユーザが実行したアクティビティが表示されます。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が表示されます。
説明	アクティビティの説明があれば、それが表示されます。

Control Manager のイベント情報

Control Manager サーバのイベントに関連する情報が表示されます。例: Control Manager 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-83. Control Manager 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が表示されます。
イベントの種類	発生したイベントの種類が表示されます。例: TMI エージェントへの通知、サーバからのユーザ通知、レポートサービスからのユーザ通知
結果	イベントの結果が表示されます。例: 成功、失敗
説明	アクティビティの説明があれば、それが表示されます。

コマンド追跡情報

Control Manager が管理下の製品に配信するコマンドに関連する情報が表示されます。例: Control Manager 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-84. 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
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。
更新日	選択した Control Manager 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。
成功	成功したコマンドの数が表示されます。
失敗	失敗したコマンドの数が表示されます。
処理中	処理中のコマンドの数が表示されます。
すべて	コマンドの総数が表示されます (成功、失敗、処理中の合計)。

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: Control Manager 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-85. 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 Control Manager 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	Control Manager がそのイベントに対して提示する説明が表示されます。

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 Control Manager 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。

トークン変数について

トークン変数を使用して、[件名] フィールドおよび [メッセージ] フィールドにデータを表示することにより、イベント通知をカスタマイズします。

Control Manager は、以下のイベント通知のトークン変数をサポートします。

イベントのカテゴリ	説明
スタンダード	トークン変数はすべてのイベント通知に適用されます。 詳細については、677 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。
高度な脅威アクティビティ	トークン変数は高度な脅威アクティビティのイベント通知に適用されます。 詳細については、678 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。
C&C コールバック	トークン変数は C&C コールバックのイベント通知に適用されます。 詳細については、679 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。
コンテンツのポリシー違反	トークン変数は C&C コールバックのイベント通知に適用されます。 詳細については、680 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。
セキュリティレベル	トークン変数はセキュリティレベルのイベント通知に適用されます。 詳細については、680 ページの「セキュリティレベル違反トークン変数」を参照してください。
情報漏えい対策	トークン変数は情報漏えい対策のイベント通知に適用されます。 詳細については、681 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。

イベントのカテゴリ	説明
既知の脅威アクティビティ	トークン変数は既知の脅威アクティビティのイベント通知に適用されます。 詳細については、683 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。
ネットワークアクセス管理	トークン変数はネットワークアクセス管理のイベント通知に適用されます。 詳細については、684 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。

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。

変数	説明
%cmserver%	Control Manager サーバ名
%computer%	イベントが検出されたコンピュータのコンピュータ名
%entity%	イベントが発生した管理下の製品のディレクトリパス
%event%	通知をトリガしたイベント
%pname%	管理下の製品の名前
%pver%	管理下の製品のバージョン
%time%	イベントが発生した時刻 (hh:mm)
%vloginuser%	スパイウェアログ内のカスタマイズされたイベントのログオンユーザ情報
%act%	管理下の製品によって実行された処理。例: ファイルの駆除、削除、隔離

変数	説明
%actresult%	管理下の製品によって実行された処理の結果。例: 成功、処理が必要

高度な脅威アクティビティのトークン変数

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%	%hostIP%は、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 アドレスです。 • 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
%START_TIME%	開始時刻
%END_TIME%	終了時刻 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、Control Manager 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。

変数	説明
%detections%	検出数 例: Event: High risk Virtual Analyzer detections IP address: %hostIP% Host name: %computer% Group: %group% Time range: %START_TIME% - %END_TIME% Detections: %detections%

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。

変数	説明
%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
%CnC_LIST_SRC%	コールバックアドレスを含むリストの名前
%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
%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。

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

セキュリティレベル違反トークン変数

次の表は、セキュリティレベル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。

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

情報漏えい対策トークン変数

変数	説明
情報漏えい対策の変数 —予約イベント概要およびイベント詳細のアップデートイベントで使用されます。	
%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

変数	説明
%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
%SEVERITY%	イベントの重大度レベル
%POLICY%	Control Manager 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、Control Manager 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%	ユーザ別イベントの大幅な増加
%DLP_SENDER%	送信者別イベントの大幅な増加
%DLP_CHANNEL%	チャネル別イベントの大幅な増加
%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

変数	説明
ウイルス変数— アラートで使用されます。	
%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。
%ptnver%	• パターンファイル番号。 • 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。
%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 • アラートイベントカテゴリで使用されます。

変数	説明
%vfile%	感染ファイル名。アラートイベント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。

変数	説明
その他の変数 —Network VirusWall Enforcer タスク完了に関連するイベントで使用されます。	
%action%	ネットワークウイルスに対する Network VirusWall Enforcer の処理 (通過、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。

付録 D

IPv6 のサポート

この付録には、Control Manager 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。

Control Manager サーバの要件

Control Manager 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	Control Manager 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	Control Manager では、%文字を IPv6 サーバアドレスに使用できません。
Control Manager 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
Control Manager 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。

- Control Manager 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。Control Manager 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、Control Manager 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

- 管理下のサーバ
- 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、Control Manager 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。

Control Manager の MIB ファイルを使用する

Control ManagerMIB 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://<Control Manager サーバ IP アドレス>:<ポート番号>/TVCSDownload/tools/cm2_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

次のテーブルは、Control Manager ログ出力と CEF Syslog の種類の間で Syslog コンテンツをマッピングします。

次のトピックがあります。

- 751 ページの「CEF ネットワークコンテンツ検査のログ」

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
ヘッダ (vendor)	アプライアンスベンダ	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	イベント ID	700106
ヘッダ (eventName)	ログ名	情報漏えい対策
ヘッダ (severity)	重大度	3
cs1Label	「cs1」フィールドに対応するラベル	「ポリシー 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	「製品」
cn1	製品の種類の値	例: 15
rt	ログ生成日時 (UTC)	例: Feb 14 2017 11:14:08 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

CEF キー	説明	値
要求	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;」
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」
cs5Label	「cs5」フィールドに対応するラベル	「ルール」
cs5	ルール名	例: SAMPLE RULE SET
cs6Label	「cs6」フィールドに対応するラベル	「テンプレート」
cs6	テンプレート名	例: 「PSG Policy」
cn3Label	「cn3」フィールドに対応するラベル	「チャネル」
cn3	チャネルの種類	例: 「3」 詳細については、697 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	「処理」
cn2	処理結果	例: 「4」 詳細については、695 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。

CEF キー	説明	値
cs2Label	「cs2」フィールドに対応するラベル	「ポリシー」
cs2	ポリシー名	例: 「OfficeScan」
cs3Label	「cs3」フィールドに対応するラベル	「製品のエンティティ名/エンドポイント」
cs3	エンドポイントのホスト名	例: 「Sample_OSCE」
dvchost	サーバのホスト名	例: 「localhost」
deviceFacility	製品名	例: 「OfficeScan」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|700106|Data Loss Preve
ntion|3|cs3Label=Product_Entity/Endpoint cs3=Sample_OSCE 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=PSG Policy cn3Label=Channel cn3=0 cn2Label=Action c
n2=4 deviceFacility=OfficeScan
```

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

値	説明
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)
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)

値	説明
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)
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

値	説明
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
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)

値	説明
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)
211	ドキュメント管理 (SharePoint)

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)	アプライアンスベンダ	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	挙動監視: ポリシー ID	BM:1000
ヘッダ (eventName)	ログ名	挙動監視
ヘッダ (severity)	重大度	3
rt	ログ生成日時 (UTC)	例: 「Feb 14 2017 11:14:08 GMT+00:00」
dvchost	ホスト名	例: 「localhost」

CEF キー	説明	値
cn1Label	「cn1」フィールドに対応するラベル	「リスクレベル」
cn1	リスクレベル	• 0: 低 • 1: 高
cs2Label	「cs2」フィールドに対応するラベル	「ポリシー ID」

CEF キー	説明	値
cs2	ポリシー ID	• 0: 感染実行可能ファイル • 1: スタートアッププログラムの追加 • 2: ホストファイルの変更 • 3: DLL (プログラムライブラリ) インジェクション • 4: Internet Explorer プラグインの追加 • 5: Internet Explorer の設定の変更 • 6: シェル設定の変更 • 7: サービスの追加 • 8: セキュリティポリシー設定の変更 • 9: ファイアウォールポリシー設定の変更 • 10: システムファイルの変更 • 11: システムファイルの複製 • 13: レイヤードサービスプロバイダ • 14: システムプロセスの変更 • 16: 不審な挙動 • 100: 新しく検出されたプログラム • 200: 不正なファイル暗号化 • 1000: 脅威の挙動分析 • 9999: ユーザ定義ポリシー

CEF キー	説明	値
sproc	Aegis の件名	例:「C:\\Windows\\SysWOW64\ \rundll32.exe」
cn2Label	「cn2」フィールドに対応するラベル	「イベントの種類」
cn2	イベントの種類	• 1: プロセス • 2: プロセスイメージ • 4: レジストリ • 8: ファイルシステム • 16: ドライバ • 32: SDT • 64: システム API • 128: ユーザモード • 2048: 攻撃コード • 65535: すべて
cs1Label	「cs1」フィールドに対応するラベル	「対象」
cs1	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	• 0: 許可 • 1: 確認 • 2: 拒否 • 3: 強制終了 • 4: 読み取りのみ許可 • 5: 読み取り/書き込みのみ許可 • 6: 読み取り/実行のみ許可 • 7: フィードバック • 8: 駆除 • 1002: 不明 • 1003: 診断 • 1004: 強制終了。ファイルは復元されました。 • 1005: 強制終了。一部のファイルは復元されませんでした。 • 1006: 強制終了。ファイルは復元されませんでした。 • 1007: 強制終了。再開結果: ファイルは復元されました。 • 1008: 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。 • 1009: 強制終了。再開結果: ファイルは復元されませんでした。
cn3Label	「cn3」フィールドに対応するラベル	「TranslatedAegisOperation」

CEF キー	説明	値
cn3	変換された Aegis オブジェクトに対する操作	• 101: プロセス作成 • 102: 開く • 103: 強制終了 • 104: 強制終了 • 301: 削除 • 302: 書き込み • 303: アクセス • 401: ファイル作成 • 402: 閉じる • 403: 実行 • 501: 起動 • 601: 攻撃コード • 9999: 未処理のオペレーション
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	製品名	例: 「OfficeScan」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|BM:1000|Behavior Monit
oring|3|rt=Aug 16 2017 05:00:40 GMT+00:00 dvchost=localhost
cn1Label=Risk_Level cn1=1 cs2Label=Policy cs2=1000 sproc=C:\
\Windows\\SysWOW64\\rundll32.exe cn2Label=Event_Type cn2=4 c
s1Label=Target cs1=HKCU\\Software\\Microsoft\\Windows\\Curre
ntVersion\\Run\\COM+ act=3 cn3Label=Operation cn3=302 shost=
shost1 src=10.0.76.40 deviceFacility=OfficeScan
```

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	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	イベント ID	700107
ヘッダ (eventName)	ログ名	デバイスアクセス管理
ヘッダ (severity)	重大度	3
rt	ログ生成日時 (UTC)	例: 「Feb 14 2017 11:14:08 GMT+00:00」
cs1Label	「cs1」フィールドに対応するラベル	「製品のエンティティ名/エンドポイント」
cs1	サーバのホスト名	例: 「Sample_OSCE」
shost	送信元ホスト名	例: 「shost1」
dvchost	対象ホスト名	例: 「localhost」
cn1Label	「cn1」フィールドに対応するラベル	「製品」
cn1	製品 ID	例: 「OfficeScan」 詳細については、707 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	「デバイスの種類」

CEF キー	説明	値
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	「権限」
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: 「ウイルスバスター Corp.」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|700107|Device Access C
ontrol|3|rt=Aug 16 2017 04:49:15 GMT+00:00 cs1Label=Product_
Entity/Endpoint cs1=Sample_OSCE 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=OfficeScan
```

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
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	ウイルスバスター Corp.
16	OfficeScan for Microsoft SBS
18	ServerProtect for Windows
19	ServerProtect for Windows (SOHO)
20	Control Manager サーバ
21	汎用
22	InterScan VirusWall for UNIX

値	説明
23	InterScan VirusWall for Windows
24	MOCA
25	Golden Gate
26	ActiveUpdate
27	IS_Y2K_SCANNER
28	Y2K VIRUS TECH SUPPORT SRV
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

値	説明
47	InterScan Messaging Security Virtual Appliance
50	InterScan Gateway Security Appliance
51	ServerProtect for Linux
52	ServerProtect for EMC
53	ServerProtect for NetApp
56	Control Manager サーバ
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

値	説明
100	Control Manager エージェント
200	eDoctor Server
300	eDoctor Agent
1000	InterScan eManager
1001	InterScan AppletTrap
1002	InterScan VirusWall Java
1003	IS_SEMAIL
132	InterScan Messaging Security Suite Solaris 版
120	Threat Discovery Appliance
131	Database Protect for Linux
151	Total Discovery Mitigation Server
154	Deep Discovery Inspector
155	InterScan for IBM Domino
156	Deep Discovery Email Inspector
31004	Trend Micro Deep Security
31005	Trend Micro Mobile Security
31003	Trend Micro Endpoint Application Control
1004	InterScan WebProtect for ICAP
10001	NEC StarOffice
20001	Dr. Soloman Anti-virus
20002	Inoculan
20003	Norton Anti-virus
20004	Sophos SWEEP

値	説明
20005	Intel LANProtect
20006	McAfee Virus Scan
20007	FProt
21000	その他のサードパーティ製品
55555	デモ製品
31104	Cloud App Security
31008	Deep Discovery Analyzer
31009	Trend Micro Endpoint Sensor
31101	Hosted Email Security
31006	Vulnerability Protection
31103	InterScan Web Security as a Service
31001	Trend Micro Security (for Mac)
31002	Trend Micro Endpoint Encryption
31007	Trend Micro Safe Mobile Workforce
31102	ウイルスバスター ビジネスセキュリティサービス

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)	アプライアンスベンダ	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0

CEF キー	説明	値
ヘッダ (eventid)	イベント ID	800102
ヘッダ (eventName)	ログ名	検索エンジンアップデートステータス
ヘッダ (severity)	重大度	3
rt	ログ生成日時 (UTC)	例:「Apr 20 2017 12:04:34 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	「製品/エンドポイント 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	「接続ステータス」
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	「検索エンジン」
cn2	検索エンジン	例:「4096」
cn5Label	「cn5」フィールドに対応するラベル	「検索エンジンバージョン」
cs5	検索エンジンバージョン	例:「9.950.1006」

CEF キー	説明	値
cn3Level	「cn3」フィールドに対応するラベル	「検索エンジンのステータス」
cn3	検索エンジンのステータス	例: 「1」 • 0: 未使用 • 1: 使用中
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	製品名	例: 「OfficeScan」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|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=OfficeScan .[0]
```

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)	アプライアンスベンダ	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	PML: 処理結果	PML: ファイルはウイルス駆除されました

CEF キー	説明	値
ヘッダ (eventName)	検出名	virusa
ヘッダ (severity)	重大度	3
rt	検出日時 (UTC)	例: 「Feb 14 2017 11:14:08 GMT+00:00」
dvchost	製品サーバ	例: 「Sample_OSCE」
cn1Label	「cn1」フィールドに対応するラベル	「潜在的な脅威の種類」
cn1	潜在的な脅威の種類	例: 「35.143」 詳細については、716 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	「セキュリティの脅威」
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」
cn2Label	「cn2」フィールドに対応するラベル	「種類」
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」

CEF キー	説明	値
cn4Label	「cn4」フィールドに対応するラベル	「プロセスコマンド」
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	「感染元」
cs3	感染元	例: 「http://10.0.0.1/」
dst	製品/エンドポイント IP	例: 「10.0.35.49」
c6a3Label	「c6a3」フィールドに対応するラベル	「製品/エンドポイント IP」
c6a3	製品/エンドポイント IP	例: 「10.0.17.6」
cn3Label	「cn3」フィールドに対応するラベル	「脅威の可能性」
cn3	脅威の可能性	例: 「82」
act	処理結果	例: 「21」 詳細については、695 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。

CEF キー	説明	値
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: 「OfficeScan」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|PML:File cleaned|virus
a|3|deviceFacility=1 cs2Label=DetectionName cs2=virusa suser
=Sample-OSCE\\Administrator cn2Label=DetectionType cn2=0 fil
ePath=C:\\WindowsFILENAME deviceCustomDate1Label=FileCreatio
nDate deviceCustomDate1=Nov 03 2016 08:58:03 GMT+00:00 sproc
=notepad.exe cs4Label=ProcessCommandLine cs4=notepad.exe -te
st duser=admin app=2 cs3Label=InfectionLocation cs3=http://1
0.0.0.1/ dst=10.0.174.28 cn3Label=Confidence cn3=82 act=21
```

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

値	説明
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
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 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)	アプライアンスベンダ	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	イベント ID	800101

CEF キー	説明	値
ヘッダ (eventName)	ログ名	パターンファイルアップデートステータス
ヘッダ (severity)	重大度	3
rt	ログ生成日時 (UTC)	例: 「Nov 02 2017 12:46:44 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	「製品/エンドポイント IP」
cs2	製品/エンドポイント IP	例: 「10.0.7.20」
cs3Label	「cs3」フィールドに対応するラベル	「アップデートエージェント」
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	「ドメイン」
cs4	ドメイン	例: 「初期設定」
cn1Label	「cn1」フィールドに対応するラベル	「接続ステータス」

CEF キー	説明	値
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	「パターンファイル/ルール」
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	「パターンファイル/ルールのバージョン」
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	「パターンファイル/ルールのステータス」
cn3	パターンファイル/ルールのステータス	例: 「1」 • 0: 未使用 • 1: 使用中
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	製品名	例: 「OfficeScan」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|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=OfficeScan .[0]
```

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	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	MS: フィルタ処理	MS:1
ヘッダ (eventName)	ポリシー名	ポリシー
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

CEF キー	説明	値
act	フィルタ処理	例: 「2」 • 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
cs1Label	「cs1」フィールドに対応するラベル	例: 「SL_PolicyContent」
cs1	ポリシー設定	例: 「Default_policy」
cs2Label	「cs2」フィールドに対応するラベル	例: 「CLF_ProductVersion」
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: 「SL_FilterType」

CEF キー	説明	値
cs3	フィルタの種類	例: 「2」 • 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: 「SL_MessageAction」

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: 「OSCEClient01」
rt	ログ生成日時 (UTC)	例: 「Nov 15 2017 08:45:57 GMT+00:00」
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: 「5」

CEF キー	説明	値
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	製品名	例: 「OfficeScan」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|MS:5|This is a policy
name|3|deviceExternalId=6 rt=Nov 15 2017 08:46:23 GMT+00:00
cntLabel=AggregatedCount cnt=1 dhost=employee_a1@Acompany.co
m;employee_a2@Acompany.com duser=employee_a1@Acompany.com ac
t=5 cs1Label=SL_PolicyContent cs1=Default_policy cs2Label=CL
F_ProductVersion cs2=5.6 cs3Label=SL_FilterType cs3=5 cs4Lab
el=CLF_ReasonCode cs4=access violation cs5Label=CLF_ReasonCo
deSource cs5=20 cs6Label=SL_MessageAction cs6=5 cat=1705 dvc
host=OSCEClient01 cn1Label=CLF_ServerityCode cn1=0 fname=2_f
ile_D2AF1F1DB8857744AFFD6C85BDEF86FBEDCE5C35 msg=Open this e
mail to win a free phone shost=bear@abc.mail.com;yumi@abc.ma
il.com suser=bear@abc.mail.com deviceFacility=OfficeScan
```

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	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager

CEF キー	説明	値
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	デバイスイベントクラス ID	スパイウェア検出
ヘッダ (eventName)	イベント名	スパイウェア検出
ヘッダ (severity)	重大度	3
cnt	検出数	例: 「10」
rt	ログ生成日時 (UTC)	例: 「Oct 06 2017 8:39:46 GMT +00:00」
cn1Label	「cn1」フィールドに対応するラベル	例: 「パターンファイルの種類」
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:「システムの再起動が必要です」 詳細については、727 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」

CEF キー	説明	値
dvchost	エンドポイントのホスト名	例: 「OSCEClient01」
deviceExternalId	ID	例: 「3」
fname	リソース	例: 「C:\\Users\\abc\\Desktop\\cdbxp_\\cdbxp_.notanexe」
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: 「OSCEClient01」
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: 「OfficeScan 」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|Spyware Detected|Spywa
re Detected|3|deviceExternalId=3 rt=Oct 06 2017 08:39:46 GMT
+00:00 cnt=1 dhost=OSCEClient01 cn1Label=PatternType cn1=107
3741840 cs1Label=VirusName cs1=ADW_OPENCANDY cs2Label=Engine
Version cs2=6.2.3027 cs5Label=ActionResult cs5=Reboot system
 successfully cs6Label=PatternVersion cs6=1297 cat=1727 dvch
ost=OSCEClient01 fname=C:\\Users\\abc\\Desktop\\cdbxp_\\cdbx
p_.notanexe filePath=F:\\Malware\\psas\\rsrc2.bin dst=50.8.1
.1 deviceFacility=OfficeScan
```

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。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	ブロックの成功
36	隔離の成功
37	スタンプの成功
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
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	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。

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

CEF キー	説明	値
ヘッダ (vendor)	アプライアンスベンダ	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	AV: 処理	AV: ファイル名が変更されました
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: 「OSCEClient01」
duser	ユーザ	例: 「Admin004」
act	処理	例:「ファイル名が変更されました」 詳細については、727 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 8:39:46 GMT +00:00
cn1Label	「cn1」フィールドに対応するラベル	例: 「VLF_PatternNumber」
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、734 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。

CEF キー	説明	値
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: 「手動検索」 • 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」
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」

CEF キー	説明	値
cs5	1 次処理結果	例:「ファイルのウイルス駆除不能」 詳細については、727 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:「2 次処理結果」
cs6	2 次処理結果	例:「ファイルのウイルス駆除不能放置」 詳細については、727 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	エンドポイントのホスト名	例:「OSCEClient01」
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」
filePath	ファイルパス	例:「C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\Rar$DR01.046\\」

CEF キー	説明	値
msg	圧縮ファイル内のファイル	例: 「BMAC Schedule of Events.xls」
shost	送信元ホスト	例: 「ABC-OSCE-WKS12」
suser	送信元ホスト	例: 「ABC-OSCE-WKS12」
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: 「OfficeScan 」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|AV:File renamed|JS_EXP
LOIT.SMDN|3|deviceExternalId=104 rt=Feb 18 2016 14:34:00 GMT
+00:00 cnt=1 dhost=OSCE_Client-4 duser=Admin004 act=File ren
amed cn1Label=VLF_PatternNumber cn1=920500 cn2Label=VLF_Seco
ndAction cn2=3 cs1Label=VLF_FunctionCode cs1=Manual Scan cs2
Label=VLF_EngineVersion cs2=9.500.1005 cs3Label=CLF_ProductV
ersion cs3=10.6 cs4Label=CLF_ReasonCode cs4=virus log cs5Lab
el=VLF_FirstActionResult cs5=File renamed cs6Label=VLF_Secon
dActionResult cs6=N/A cat=1703 dvchost=OSCEClient04 cn3Label
=CLF_ServerityCode cn3=2 fname=0348C693056617D34FC5B5BAB4643
885FEE5FEDF;0xD5D56AC2 filePath=C:\\Users\\Administrator\\De
sktop\\trend_test_virus\\Trojans\\ msg=BMAC Schedule of Even
ts.xls shost=ABC-OSCE-WKS12 suser=ABC-OSCE-WKS12 dst=10.201.
129.24 deviceFacility=OfficeScan
```

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	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
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、740 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	ログ生成日時 (UTC)	例:「Nov 15 2017 8:43:57 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:「外部ユーザポリシー」
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、738 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:「OSCEClient08」

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」
要求	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	製品名	例: 「OfficeScan 」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|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=OSCEClient08 fname=test.txt request=http://www.viol
etsoft.net/counter/insert.php?dbserver\=db1&c_pcode\=25&c_pi
d\=funpop1&c_kind\=4&c_mac\=FE-ED-BE-EF-0C-E1 deviceFacility
=OfficeScan
```

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
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

値	説明
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
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
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

値	説明
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
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

値	説明
54	RTMP
68	DNS 要求
256	BitTorrent
257	Kazaa
258	LimeWire
259	BearShare
260	Bluester
261	eDonkey eMule
262	Edonkey2000
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

値	説明
277	iMesh
278	Skype
279	Google Talk
317	Cabos
318	Zultrax
319	Foxy
320	eDonkey
321	Ares
322	Miranda
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

値	説明
641	Chikka SMS Messenger
642	eBuddy
643	ICQ2Go
644	ILoveIM Web Messenger
645	IMUnitive
646	Mabber
647	Meebo
648	Yahoo!Web Messenger
848	SIP2
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

値	説明
10009	ND
10010	RAW

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	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	CnC: 処理	CnC: ブロック
ヘッダ (eventName)	名前	CnC コールバック
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: 「OfficeScan」
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	ログ生成日時 (UTC)	例:「Oct 11 2017 06:34:09 GMT +00:00」
shost	エンドポイントのホスト名	例: 「OSCEClient01」
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: 「Web レピュテーション サービスデータベース内の C&C サーバの URL - HTTP (要求)」
act	処理	例: 「ブロック」 • 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」

CEF キー	説明	値
cn3	コールバックアドレスの形式	例: 「1」 • 0: IP • 1: IP • 2: HTTP • 3: SMTP
要求	URL	例: 「http://CC13.jojo.com」
deviceCustomDate1 Label	「deviceCustomDate1」フィールドに対応するラベル	例: 「SLF_FirstSeen」
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」
deviceCustomDate2 Label	「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」
deviceProcessNam e	プロセス名	例: 「C:\\Program Files (x86)\ \Internet Explorer\\iexplore.exe」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|CnC:Block|CnC Callback
|3|deviceExternalId=12 rt=Oct 11 2017 06:34:09 GMT+00:00 cat
=1756 deviceFacility=OfficeScan cs2Label=EI_ProductVersion c
```

```
s2=11.0 shost=OSCEClient01 src=10.201.86.187 cs3Label=SLF_Do
mainName cs3=DOMAIN act=Block cn1Label=SLF_CCCA_RiskLevel cn
1=1 cn2Label=SLF_CCCA_DetectionSource cn2=1 cn3Label=SLF_CCC
A_DestinationFormat cn3=1 dst=10.201.86.195 deviceProcessNam
e=C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe
```

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	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	FH: 処理	FH: ログ
ヘッダ (eventName)	名前	不審ファイル
ヘッダ (severity)	重大度	3
deviceExternalId	ID	例: 「1」
cat	ログの種類	例: 「1766」
deviceFacility	製品名	例: 「OfficeScan」
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	検出日時	例:「Nov 15 2017 2:47:21 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」

CEF キー	説明	値
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: 「OSCE-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」
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: 「Log」 • 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」

CEF キー	説明	値
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

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|FH:Log|Suspicious File
s|3|deviceExternalId=1 rt=Nov 15 2016 02:47:21 GMT+00:00 cat
=1766 deviceFacility=OfficeScan cn1Label=SLF_ProductVersion
cn1=11 dst=10.201.86.151 dhost=OSCE-CLIENT-1 cs2Label=SLF_Tr
ueFileType cs2=SLF_TrueFileType fileHash=D6712CAE5EC821F910E
14945153AE7871AA536CA cs3Label=SLF_FileSource cs3=C:\\Users\
\Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\017
545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE cn2Label=SL
F_SourceType cn2=0 act=Log cn3Label=SLF_ScanType cn3=1
```

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	トレンドマイクロ
ヘッダ (pname)	アプライアンス製品	Control Manager
ヘッダ (pver)	アプライアンスバージョン	7.0
ヘッダ (eventid)	NCIE: 処理	NCIE: 放置
ヘッダ (eventName)	名前	不審接続
ヘッダ (severity)	重大度	3
deviceExternalId	ID	例: 「1」

CEF キー	説明	値
cat	ログの種類	例: 「1756」
deviceFacility	製品名	例: 「OfficeScan」
rt	ログ生成日時 (UTC)	例: 「Oct 11 2017 6:34:06 GMT +00:00」
deviceProcessName	対象プロセス	例: 「C:\\Windows\\system32\\svchost-1.exe」
src	送信元 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	送信元 IPv6 アドレス	例: 「2620:101:4003:7a0:fd4b:52ed:53bd:ae3d」
spt	送信元ポート	例: 「54594」
dst	送信先 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	送信先 IPv6 アドレス	例:「fe80::38ca:cd15:443c:40bb%11」
dpt	送信先ポート	例: 「80」

CEF キー	説明	値
act	処理	例: 「放置」 • 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/接続	例: 「受信」 • 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」

ログの例:

```
CEF:0|Trend Micro|Control Manager|7.0|NCIE:Pass|Suspicious C
onnection|3|deviceExternalId=1 rt=Oct 11 2017 06:34:06 GMT+0
0:00 cat=1756 deviceFacility=OfficeScan deviceProcessName=C:
\\Windows\\system32\\svchost-1.exe act=Pass src=10.201.86.15
2 dst=10.69.81.64 spt=54594 dpt=80 deviceDirection=None cn1L
abel=SLF_PatternType cn1=2 cs2Label=NCIE_ThreatName cs2=Mali
cious_identified_CnC_querying_on_UDP_detected
```

索引

さ

た

は

わ