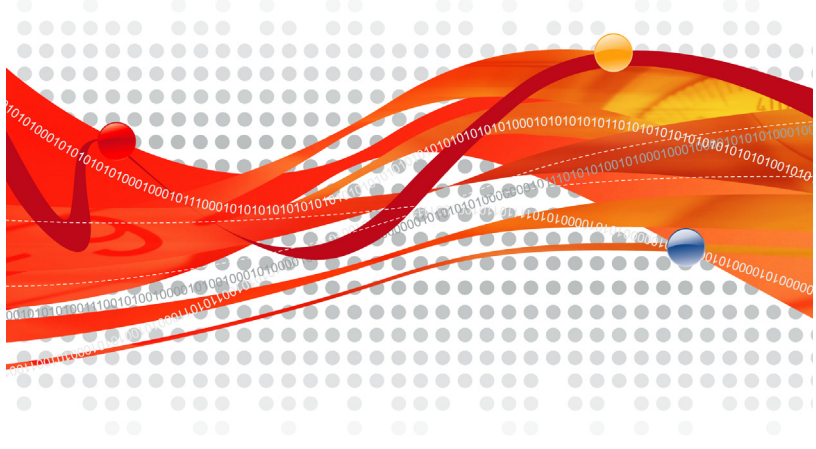
Trend Micro
Control Manager™



安心を、ひとつ上のステージへ。

TREND MICRO™

管理者ガイド

トレンドマイクロへのお客様情報の送信について

「フィッシング詐欺対策」「URLフィルタ」では、Webサイトが安全かどうかの判定のために、お客様がアクセスしたURLの情報を暗号化してトレンドマイクロのサーバに送信します。

サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。

また、これらの機能を有効にしたうえで、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されているWebサイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスしたWebページのURLにお客様が入力したID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。

「ソフトウェア安全性評価サービス」では、プログラムが安全かどうかの判定のために、プログラムの情報をトレンドマイクロのサーバに送信します。
「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
「迷惑メール対策ツール」では、弊社製品の改良目的および迷惑メールの撲滅のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のウェブサイトから見つけることができます。

「http://www.treas.gov/ofac/」、および「http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm」

2008年12月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

あなたは本製品に関連した米国輸出管理法令の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

お客様が複数年契約（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://jp.trendmicro.com/jp/support/lifecycle/index.html

著作権について

商標について

P/N: TMCMFF-AE0300_R1 (2009/04)

目次

はじめに

本書では、Trend Micro Control Manager (以下、Control Manager) 5.0 の概要、インストールの計画とインストール手順、さらに運用環境に応じて機能するように設定する方法について説明します。

本章は次の内容で構成されています。

バージョン 5.0 の新機能

Control Manager 5.0 は、ウイルス対策 / コンテンツセキュリティ製品を監視および管理するソフトウェアとして大幅に強化されました。新バージョンでは優れたアーキテクチャにより、Control Manager の柔軟性と拡張性がこれまで以上に高まりました。

バージョン 5.0 での新機能は次のとおりです。

- 18 ページの「レポート機能およびログ機能の向上」
- 18 ページの「ユーザアクセス管理の向上」
- 19 ページの「製品ディレクトリの管理および監視の向上」
- 19 ページの「インテリジェントなコンポーネント監視」
- 20 ページの「製品ライセンスの配信のサポート」

レポート機能およびログ機能の向上

Control Manager 5.0 では、アドホッククエリの機能が用意されています。ユーザは、データビューを介して Control Manager データベースに対してクエリを実行することで、管理下の製品または Control Manager に関する情報を取得できます。

ユーザが独自のレポートテンプレートを作成できるようになりました。列、行、棒グラフ、円グラフのドラッグアンドドロップ機能により、テンプレートを迅速、簡単、効率的に作成できます。

ユーザアクセス管理の向上

Control Manager 5.0 では、次の方法によりユーザアクセス管理が向上しています。

- アカウントの種類をカスタマイズすることで、Control Manager 管理者は、ユーザが Control Manager 管理コンソールからアクセスできるメニュー項目を指定できます。

  例: Control Manager 管理者が、管理コンソールの製品ツリーとログ / レポートセクションにのみアクセス可能なアカウントの種類を作成したとします。このアカウントの種類が割り当てられたユーザには、Control Manager 管理コンソールの他の領域は表示されません。

- ユーザアカウントをカスタマイズすることで、Control Manager 管理者は、ユーザがアクセス可能な製品 / ディレクトリと、それらの製品 / ディレクトリに対してユーザが実行可能な操作を指定できます。

  例 : Bob と Jane は、ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) の管理者です。両者のアカウントの種類が持つ権限は同じです (管理コンソールの同じメニュー項目にアクセスできます)。Jane は、すべてのウイルスバスター Corp. サーバに対する操作を監視しています。一方、Bob は、マーケティング部門のデスクトップを保護するウイルスバスター Corp. サーバに対する操作のみを監視しています。この場合、両者が管理コンソールに表示できる情報は異なります。Bob がログオンして参照できる情報は、Bob の Control Manager ユーザアカウントでアクセス可能なウイルスバスター Corp. サーバ (マーケティング部門用のウイルスバスター Corp. サーバ) に関する情報のみです。一方、Jane の Control Manager ユーザアカウントには Control Manager に登録済みのすべてのウイルスバスター Corp. サーバに対するアクセス権が付与されているため、Jane はログオン時に、すべてのウイルスバスター Corp. サーバに関する情報を参照できます。

製品ディレクトリの管理および監視の向上

Control Manager 5.0 では、製品ディレクトリによる製品の管理および監視が向上しています。向上した機能は以下のとおりです。

- 複数のクライアントを持つ製品に対するウイルスバスター Corp. 形式のビュー
- 下位の Control Manager サーバによって管理されている製品の、上位の Control Manager サーバによる管理
- 管理下の製品または製品クライアントに対する名前による検索
- 製品ツリーでの管理下の製品の移動時における、移動前の場所からのアクセス権の継承

インテリジェントなコンポーネント監視

Control Manager 5.0 では、ユーザがアクセス権を持ち、Control Manager に登録されている管理下の製品のコンポーネントのみが表示されます。これまでのバージョンでは、すべての製品のすべてのコンポーネントが表示されました。

製品ライセンスの配信のサポート

管理下の製品に対するアクティベーションコードの配信および再配信が可能になりました。Control Manager のライセンス管理では、次の操作がサポートされます。

- 管理下の製品は、自己のアクティベーションコードを Control Manager に登録できます。
- Control Manager 管理者は、登録済みの管理下の製品のすべてのアクティベーションコードのステータス、または他のユーザが入力したアクティベーションコードのステータスを表示できます。また、アクティベーションコードを使用する管理下の製品を表示できます。
- Control Manager 管理者は、新しいアクティベーションコードを追加して、そのアクティベーションコードを特定の管理下の製品に配信できます。
- Control Manager 管理者は、既存のアクティベーションコードを選択して、そのアクティベーションコードを特定の管理下の製品に配信できます。
- Control Manager 管理者は、アクティベーションコードを更新してから、古いアクティベーションコードを使用していた管理下の製品に新しいアクティベーションコードを配信できます。
- Control Manager 管理者は、管理下の製品によってまったく使用されなくなったアクティベーションコード、または配信プロセス中のアクティベーションコードを削除できます。

ログ集約のサポート

管理下の製品に対するログの集約コマンドの送信がサポートされました。これにより、不要と思われる情報が管理下の製品において削除され、集約されたログが Control Manager に送信されます。

管理下の製品に対するサポートの向上

Control Manager では、次の管理下の製品が新たにサポート対象製品になりました。

注意： 本トピックには 2008 年 5 月現在、日本ではリリース / サポートされていない製品も記載されています。

表 -1. サポートされる管理下の製品

管理下の製品の名前	バージョン
ウイルスバスター コーポレートエディション	8.0
InterScan for Microsoft Exchange	6.0
Portalprotect for Microsoft SharePoint Portal Server	2007 および x64 OS 上でサポート
InterScan for Lotus Domino	OS/AS 400 サポート
ServerProtect for Linux	3.0
ServerProtect for Microsoft Windows/Novell NetWare	X64 OS
InterScan Gateway Security Appliance	• 1.5 • 1.5+SP1
InterScan Messaging Security Suite	• 7.0 • 7.0+SP1
InterScan Web Security Appliance	3.0
InterScan Web Security Suite	3.0
InterScan WebProtect for ISA	• 5.0 • 5.01
Network VirusWall Enforcer 2500	2.0
Network VirusWall Enforcer 1200	2.0
InterScan Messaging Security Appliance 5000	• 1.0 • 7.0

表 -1. サポートされる管理下の製品

管理下の製品の名前	バージョン
Total Discovery Appliance	• 1.0 • 2.0 (開発中)
ServerProtect for Linux	2.5

Control Manager のドキュメント

Control Manager のドキュメント構成は次のとおりです。

表 -2. **Control Manager のドキュメント**

ドキュメント	説明
オンラインヘルプ	Web ベースのヘルプです。Control Manager の管理コンソールからアクセスできます。 オンラインヘルプには、Control Manager のコンポーネントと機能の説明に加えて、Control Manager の設定手順が記載されています。
製品 Q&A	問題解決およびトラブルシューティングに関する情報のデータベースです。製品の既知の問題に関する最新の情報が提供されます。製品 Q&A にアクセスするには、次の Web サイトに移動してください。 http://esupport.trendmicro.co.jp/
Readme ファイル	Readme ファイルには、オンラインドキュメント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ます。新機能の説明、インストールのヒント、既知の問題、製品リリースの履歴などのトピックがあります。
インストールガイド	印刷版は製品パッケージに同梱されています。PDF 版は製品 DVD からアクセスするか、トレンドマイクロの Web サイトからダウンロードできます。 インストールガイドには、Control Manager のインストール方法と、すぐに稼働できるようにするための基本的な設定方法が詳しく記載されています。
管理者ガイド	PDF 版は、Control Manager の製品 CD からアクセスするか、トレンドマイクロの Web サイトからダウンロードできます。 管理者ガイドには、Control Manager と管理下の製品の配置、インストール、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ています。本書の各章の内容については、「本書について」を参照してください。
チュートリアル	PDF 版は、トレンドマイクロの Web サイトからダウンロードできます。 チュートリアルには、Control Manager と Control Manager に登録されている管理下の製品の配置、インストール、設定、および管理方法の手順が記載されています。

注意： Control Manager の最新のマニュアルおよび最新のコンポーネントは、トレンドマイクロの Web サイト(http://www.trendmicro.co.jp/download/) に随時公開されます。

本書について

Trend Micro Control Manager 管理者ガイドは次の内容で構成されています。

表 -3. 管理者ガイドの概要

タスク	説明
インストール前	第 1 章 製品の概要 — Control Manager の概要、製品のアーキテクチャ、およびすべての機能について説明します。
	第 2 章 配置計画 — 配置および製品アプリケーションに関する情報と、Control Manager の最適な配置を実現するための推奨事項について説明します。
インストール	第 3 章 新規インストール — Control Manager サーバのインストール手順について説明します。
	第 4 章 サーバのアップグレードおよびエージェントの移行 — 旧バージョンの Control Manager から Control Manager 5.0 へのアップグレードについて説明します。

表 -3. 管理者ガイドの概要

タスク	説明
インストール後	第 5 章 Control Manager システムの管理 — 基本的な管理コンソールのナビゲーション、ユーザの作成およびインポート、サーバと管理下の製品のアップデートについて説明します。
	第 6 章 Control Manager システムの監視 — 通知の設定、レポートの生成、ログの収集などの、Control Manager 環境の解析と監視について説明します。
	第 7 章 管理下の製品の管理 — Control Manager システムと管理下の製品の管理について説明します。
	第 8 章 トレンドマイクロのサービスの使用 — トレンドマイクロ エンタープライズ プロテクション ストラテジーや大規模感染予防サービスなどの Control Manager サービスの使用方法について説明します。
	第 9 章 ツールの使用 — エージェント移行ツール、階層管理ツールなどの Control Manager ツールの使用方法について説明します。
	第 10 章 アンインストール — Control Manager のアンインストール方法について説明します。
	第 11 章 製品サポート情報 — 質問が生じたりサポートが必要となった場合のトレンドマイクロへの問い合わせ方法について説明します。
付録	• 「システムチェックリスト」— Control Manager の各種タスクのチェックリストです。印刷して使用できます。 • 「データビューについて」— アドホッククエリおよびレポートテンプレートで使用するデータ列について説明します。

対象読者

本書では、読者がセキュリティシステムについて基本的な知識を持っていることを前提としています。旧バージョンの Control Manager を使用している管理者および担当者のために、旧バージョンの Control Manager に関する説明も含まれています。Control Manager を使用した経験がない読者には、Control Manager の概念をより深く理解するために役立ちます。

ドキュメントの規則

情報の検索と解釈を簡単にするために、Control Manager のドキュメントでは次の規則を使用しています。

表 -4. ドキュメントの規則

規則	説明
注意 :	設定上の注意と推奨設定を記載
ヒント :	最適な設定と推奨設定を記載
警告 :	障害の原因となるプロセスについての警告を記載

第 1 章

製品の概要

Trend Micro Control Manager (以下、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管理するための集中管理コンソールです。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ヵ所から監視できます。

Control Manager を通して、システム管理者はウイルス感染やセキュリティ違反といった活動やウイルス / 不正プログラムの侵入ポイントを監視し把握できます。また、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アップデートコンポーネントを手動または事前予約によりダウンロードし、ネットワーク全体に配信することで、ウイルス対策を最新で一貫した状態に保つことができます。Control Manager では、製品を個別に、または製品グループ別に柔軟に設定できます。

本章は次の内容で構成されています。

スタンダード版およびアドバンス版

Control Manager には、スタンダート版とアドバンス版の 2 つのバージョンがあります。アドバンス版には、スタンダード版にはない機能が組み込まれています。たとえば、アドバンス版では階層管理構造がサポートされます。これは、上位の Control Manager アドバンス版サーバが複数の下位の Control Manager アドバンス版サーバから情報を受け取ることで、Control Manager システム全体を、1 つの上位 Control Manager アドバンス版サーバで管理できることを意味します。この上位サーバは、システム全体のハブとしての役割を果たします。

注意： Control Manager 5.0 アドバンス版では、次のサーバを下位の Control Manager サーバとしてサポートします。

- Control Manager 5.0 アドバンス版
- Control Manager 3.5 スタンダード版またはエンタープライズ版

Control Manager 5.0 スタンダード版サーバを下位サーバとすることはできません。

スタンダード版とアドバンス版の Control Manager サーバによってサポートされる機能の一覧は、425 ページの「Control Manager のバージョン別機能比較」を参照してください。

Control Manager の使用方法

Control Manager は、組織のローカルエリアネットワークおよび広域ネットワーク上に配置されているウイルス対策 / コンテンツセキュリティ製品およびサービスを管理するための機能を提供するように設計されています。

表 1-1. Control Manager の機能

機能	説明
設定の一元化	製品ディレクトリと階層管理構造を通して、単一の管理コンソールからウイルスに対する処理やコンテンツセキュリティ対策を調整できます。 これにより、組織内で一貫したセキュリティポリシーを実施できます。
大規模感染予防対策	大規模感染予防サービスにより、ネットワーク上でのウイルス / 不正プログラムの大規模感染を食い止めるための予防措置を実施します。
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います。 指定されているセキュリティレベルに応じて、メッセージを暗号化、または認証付きで暗号化できます。
HTTPS による通信の保護	この機能により、管理コンソールへのアクセスを保護できます。
タスク委任機能	システム管理者は、Control Manager 管理コンソールの各ユーザに異なる権限を持つアカウントを付与できます。 ユーザアカウントにより、ユーザが Control Manager システムで参照および実行できる内容が定義されます。アカウントの利用状況は、アクセスログによって確認できます。
コマンド追跡	この機能により、実行されたコマンドを Control Manager 管理コンソールから監視できます。 たとえば、パターンファイルのアップデートや配信など、時間がかかるコマンドが正常に終了されたかどうかを確認したい場合に役立ちます。

表 1-1. Control Manager の機能

機能	説明
リアルタイム / オンデマンドでの製品管理	管理下の製品をリアルタイムで管理します。 Control Manager は、管理コンソールで変更された設定を即座に管理下の製品に送信します。システム管理者は管理コンソールから手動検索を実行できます。このような機能はウイルスの大規模感染発生時には欠かせないものです。
コンポーネントの集中管理	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アップデートして、すべての管理下の製品を最新の状態にします。
レポートの一元化	包括的なログおよびレポートを使用して、ウイルス対策およびコンテンツセキュリティ製品のパフォーマンスの概要を調べることができます。 Control Manager を通じて管理下のすべての製品からログを収集できるため、製品別にログをチェックする必要がありません。

Trend Micro Management Communication Protocol について

Trend Micro Management Communication Protocol (以下、MCP) は、トレンドマイクロが提供する、管理下の製品用の次世代エージェントです。MCP は Trend Micro Management Infrastructure (以下、TMI) の代替として、Control Manager と管理下の製品間の通信に使用されます。MCP には次の新機能があります。

- ネットワーク負荷とパッケージサイズの削減
- NAT およびファイアウォール環境のサポート
- HTTPS サポート
- 一方向および双方向の通信サポート
- シングルサインオン (SSO) サポート

ネットワーク負荷とパッケージサイズの軽減

TMI では、XML ベースのアプリケーションプロトコルを使用します。XML は、プロトコルデザインにおいて一定の拡張性と柔軟性を提供しますが、XML を通信プロトコルのデータ形式の標準として使用すると次のような短所があります。

CGI の名前 / 値ペアやバイナリ構造体などの他のデータ形式と比べて、XML の解析には、より多くのシステムリソースが必要となります (プログラムが、サーバまたはデバイスのリソースをより多く消費します)。

XML では、情報の伝送に必要なエージェントの負荷が、他のデータ形式と比べて大幅に大きくなります。

データが必要とするリソースが大きくなるため、データ処理のパフォーマンスが低下します。

他のデータ形式よりも、パケット伝送に時間がかかり、伝送速度が遅くなります。

上記のような問題に対して、MCP のデータ形式では問題解決の工夫が実装されています。MCP のデータ形式は BLOB (バイナリ) ストリームで、各項目は名前 ID、型、長さ、および値によって構成されます。この BLOB 形式には次の利点があります。

- **XML よりもデータ転送サイズが小さい** — データ型を使用することで、情報の格納に使用されるバイト数を制限できます。データ型には、整数型、符号なし整数型、ブール型、浮動小数点型があります。
- **解析速度がより速い** — 固定バイナリ形式を使用して、各データ項目を 1 つずつ簡単に解析できます。解析パフォーマンスは、XML よりも数倍速くなります。
- **設計の柔軟性の強化** — 各項目が名前 ID、型、長さ、および値から構成されることで、設計の柔軟性も考慮に入れられています。項目の順序は任意で、補助項目は必要な場合にのみ通信プロトコルに含めることができます。

MCP では、データ伝送にバイナリストリーム形式が採用されたことに加えて、圧縮 / 非圧縮に関係なく、異なる種類のデータを接続にパックすることができます。このデータ伝送方式によって、ネットワーク帯域幅の維持が可能になると同時に、スケーラビリティが向上します。

NAT およびファイアウォールトラバーサルサポート

IPv4 ネットワーク上の限定された IP アドレスを使用して、より多くのエンドポイントコンピュータをインターネットに接続するために、NAT (ネットワークアドレス変換) デバイスが広く使用されています。NAT デバイスは、NAT デバイスに接続するコンピュータへのプライベート仮想ネットワークを形成することによりこれを可能にします。NAT デバイスに接続された各コンピュータには、専用のプライベート仮想 IP アドレスが 1 つ割り当てられます。NAT デバイスは、このプライベート IP アドレスを実際の IP アドレスに変換してから、インターネットに要求を送信します。これにより問題が起こる場合があります。接続している各コンピュータは仮想 IP アドレスを使用していますが、多くのネットワークアプリケーションがそのことを認識していないためです。通常、予期しないプログラムの誤動作やネットワークの接続の問題を引き起こします。

Control Manager 2.5/3.0 エージェントと連携する製品には、1 つの前提条件があります。サーバは、サーバからエージェントへの接続を開始することでエージェントに到達できるという事実に依存しています。どちら側からでも相互にネットワーク接続を開始できるので、これは双方向通信製品と呼ばれます。この前提条件は、エージェントが NAT デバイスの背後にあるときや、Control Manager サーバが NAT デバイスの背後にあるときには当てはまりません。この接続は NAT デバイスにのみルーティング可能で、NAT デバイスの背後にある製品や、NAT デバイスの背後にある Control Manager サーバにはルーティングできないためです。この問題の一般的な解決策の 1 つとして、NAT デバイス上に特定のマップ関係を構築し、受信要求を関連エージェントに自動ルーティングする方法があります。ただし、この解決方法ではユーザの関与が必要となり、大規模な製品配置が必要な場合はうまく機能しません。

MCP では、一方向の通信モデルを採用することでこの問題に対応します。一方向通信では、エージェントのみがサーバへのネットワーク接続を開始できます。サーバは、エージェントへの接続を開始できません。一方向通信はログのデータ転送に適しています。一方、サーバからのコマンド発行は、受動モードでの実行となります。つまり、コマンド配信は、エージェント側からサーバに対して使用可能なコマンドのポーリングが行われてはじめて実現します。

HTTPS サポート

MCP 統合プロトコルでは、業界標準の通信プロトコル (HTTP/HTTPS) が採用されています。HTTP/HTTPS には TMI と比べて、次の利点があります。

- IT 部門の大多数のスタッフが HTTP/HTTPS に精通しているため、通信に関する問題の特定やその解決方法の選別が容易になります。
- ほとんどの企業環境では、パケットを通過させるためにファイアウォールに新しいポートを開く必要がありません。
- SSL/TLS や HTTP ダイジェスト認証など、HTTP/HTTPS 用に構築された既存のセキュリティメカニズムを使用できます。

MCP を使用することで、次の 3 つのセキュリティレベルを Control Manager に適用できます。

- **低** — HTTP 通信が使用されます。
- **中** — HTTPS がサポートされている場合は HTTPS 通信が使用され、HTTPS がサポートされていない場合は HTTP 通信が使用されます。
- **高** — HTTPS 通信が使用されます。

一方向および双方向通信のサポート

MCP では、一方向の通信と双方向の通信がサポートされます。

一方向通信

NAT トラバーサルは、現在のネットワーク環境において、より重要な問題になっています。この問題に対応するために、MCP では一方向通信を使用します。一方向通信では、MCP クライアントがサーバへの接続を開始し、サーバからコマンドをポーリングします。それぞれの要求は CGI に類似したコマンドクエリまたはログの送信です。ネットワークへの影響を軽減するために、接続は可能な限り開かれたまま維持されます。以降の要求では既存の開かれた接続が使用されます。接続が閉じられた場合でも、同じホストへの SSL 対応のすべての接続は、セッション ID のキャッシュ機能によって、再接続にかかる時間が大幅に短縮されます。

双方向通信

双方向通信は、一方向通信に代わる方法です。双方向通信では、一方向通信を基本としながら、サーバからの通知を受信するチャネルが追加されています。この追加チャネルもHTTP プロトコルに基づいています。双方向通信では、MCP エージェントによるサーバからのコマンド受信とその処理のリアルタイム性が向上します。MCP エージェント側では、Control Manager サーバからの通知を受信するために、CGI に類似した要求を処理できる Web サーバまたは CGI 互換のプログラムが必要です。

シングルサインオン (SSO) サポート

MCP を使用することにより、Control Manager では、トレンドマイクロ製品へのシングルサインオン (SSO) 機能がサポートされるようになりました。この機能を使用すると、ユーザは Control Manager にログオンするだけで、他のトレンドマイクロ製品にログオンしなくてもそのリソースにアクセスできるようになります。

Control Manager のアーキテクチャ

Control Manager は、トレンドマイクロの製品やサービスを 1ヵ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。Control Manager が使用するコンポーネントのリストについては、35 ページの表 1-2、「Control Manager コンポーネント」を参照してください。

表 1-2. Control Manager コンポーネント

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。スタンダード版とアドバンス版では機能が異なります。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、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 管理コンソールのホストとなる 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サーバ 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。メールメッセージ、Windows イベントログ、MSN Messenger、SNMP、Syslog、ポケットベル、またはアプリケーションを経由して通知を送信するように [イベントセンター] を設定できます。 • 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 (アドバンス版のみ) Control Manager レポートは、Control Manager システム上で発生したウイルス / 不正プログラム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。

表 1-2. Control Manager コンポーネント

コンポーネント	説明
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、Control Manager システムの新しいバックボーンとなります。 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。
Trend Micro Infrastructure	Control Manager サーバと管理下の製品間の通信を処理します。 コミュニケータ (メッセージルーティングフレームワークとも呼ばれます) は、Control Manager システムの通信バックボーンであり、コミュニケータは、TMI の 1 コンポーネントです。コミュニケータは Control Manager サーバと管理下の製品間のすべての通信を処理しています。コミュニケータは管理下の製品と通信するために Control Manager エージェントと対話します。
Control Manager 2.x エージェント	Control Manager サーバからコマンドを受け取り、ステータス情報やログを Control Manager サーバに送信します。 Control Manager エージェントは、管理下の製品サーバにインストールされ、Control Manager から製品を管理するために必要な機能を提供します。エージェントは、管理下の製品およびコミュニケータと対話します。エージェントは、管理下の製品とコミュニケータとの間をつなぐブリッジとして機能します。そのため、管理下の製品と同じコンピュータにエージェントをインストールする必要があります。
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 Microsoft Internet Explorer を利用して、事実上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。

第 2 章

配置計画

Trend Micro Control Manager (以下、Control Manager) をネットワークに配置する前に管理者が考慮すべきいくつかの点があります。本章では、Control Manager の配置計画の作成とテストインストールの実施について説明します。

本章は次の内容で構成されています。

インストール形態の決定

Control Manager サーバをネットワーク環境に戦略的に分散して、ウイルス対策 / コンテンツセキュリティ製品を適切に管理するためのインストール形態を決定します。

Control Manager のような企業規模のクライアントサーバ製品を同機種または異機種環境に導入するためには、入念な計画と評価が必要になります。

計画を容易に作成できるように、次の 2 種類のインストール形態を推奨します。

- **集中管理** — 集中管理では、メインオフィスにある単一の Control Manager から、下位サーバと管理下の製品を分散および管理します。組織が複数のオフィスを持っていても、拠点間に高速で信頼性の高いローカルおよびワイドエリア接続がある場合は、集中管理を適用できます。
- **分散管理** — 分散管理は、地理的に離れた複数のメインオフィスがある組織において、複数の Control Manager サーバから管理します。

注意： 初めて Control Manager をお使いになる場合は、アドバンス版の Control Manager の上位サーバを使用して、集中管理および分散管理を処理することをお勧めします。

集中管理について

集中管理では、メインオフィスにある 1 つの Control Manager から、下位サーバと管理下の製品を管理します。

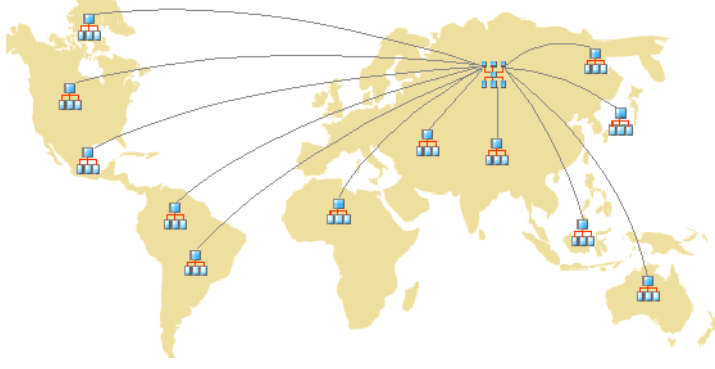


図 2-1.　Control Manager アドバンス版の上位サーバおよび複数の下位サーバ

Control Manager の集中管理を実施する前に、次の作業を実行する必要があります。

- 管理下の製品および階層構造の数の決定
- サーバと管理下の製品 / 階層構造の最適な比率の計画
- スタンダード版、アドバンス版のどちらを使用するかの指定

注意： Control Manager 5.0 アドバンス版では、次のサーバを下位の Control Manager サーバとしてサポートします。

- Control Manager 5.0 アドバンス版
- Control Manager 3.5 スタンダード版またはエンタープライズ版

Control Manager 5.0 スタンダード版サーバを下位サーバとすることはできません。

管理下の製品および階層構造の数の決定

Control Manager で管理しようとする、管理下の製品および階層構造の数を決定します。この情報は、最適な通信や管理のために配置すべき Control Manager サーバの種類と数、またそれらのサーバをネットワーク上のどこに配置するのかを決定する上で必要になります。

異機種ネットワーク環境で、Windows や UNIX などの異なる OS を使用している場合、Windows ベースと UNIX ベースの製品の数を確認します。この情報により、Control Manager の階層管理を実施するかどうかを決定します。

サーバと管理下の製品 / 階層構造の最適な比率の計画

1 台の Control Manager サーバで管理可能な、ローカルネットワーク上の管理下の製品と階層構造の数を決定する上で最も重要な要素は、エージェントとサーバ間の通信、または上位サーバと下位サーバ間の通信です。

Control Manager システムの CPU および RAM の要件を決める際には、推奨システム要件を参考にしてください。

Control Manager サーバの指定

必要な管理下の製品と階層構造の数に基づいて、Control Manager サーバを決定および指定します。アドバンス版とスタンダード版のどちらの Control Manager サーバを指定するかを決めます。

さらに、Windows サーバの中から、Control Manager サーバとして設定するものを選択します。専用サーバをインストールする必要があるかどうかについても検討します。

Control Manager をインストールするサーバを選択するときは、次の点を考慮します。

- CPU 負荷の程度
- サーバが実行している他の機能

アプリケーションサーバなどの他の用途にも使用されているサーバに Control Manager をインストールする場合、基幹アプリケーションやリソースを大量に消費するアプリケーションを実行していないサーバへのインストールを推奨します。

注意： ウイルスバスター Corp. と Control Manager はどちらも IIS を使用して、クライアント、エージェント / 下位サーバと通信しています。2 つのアプリケーション間で競合が生じることはありませんが、どちらも IIS リソースを使用することから、Control Manager を他のコンピュータにインストールし、サーバの負荷を軽減することをお勧めします。

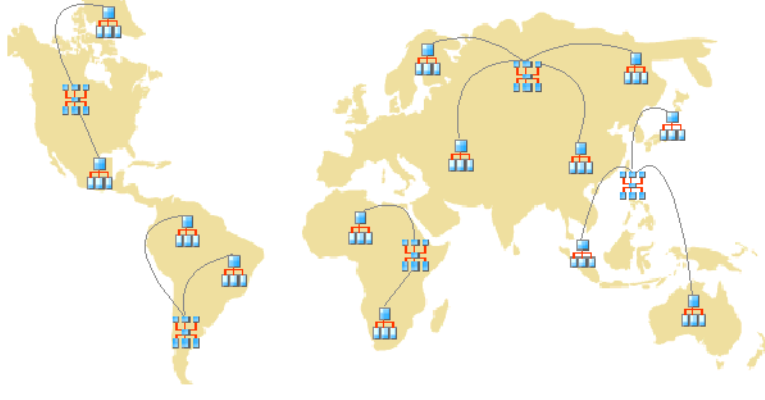
各ネットワークの構成に応じて、上記以外に処置すべきことが発生する場合もあります。

分散管理について

集中管理と同様に、関連するネットワーク情報を収集して、この情報が Control Manager サーバの分散管理にどのように関わるかを判別する必要があります。

それぞれのネットワークの特性を考慮して、Control Manager サーバの最適な数を決定してください。

DMZ や専用ネットワークを含む、さまざまな場所に Control Manager サーバを配置できます。インターネット上で Internet Explorer を使用して管理下の製品または下位サーバを管理し、Control Manager 管理コンソールにアクセスするには、公開されたネットワーク上の DMZ に Control Manager サーバを配置します。



nb

図 2-2. Control Manager アドバンス版の上位サーバおよび複数の下位サーバ (アドバンス版とスタンダード版) を使用した分散管理

分散管理においては次の点を考慮します。

- 管理下の製品または下位サーバのグループ化
- 拠点数の決定
- 管理下の製品および下位サーバの数の決定
- ネットワークトラフィックの計画
- サーバと管理下の製品 / 階層構造の最適な比率の計画
- Control Manager サーバのインストール場所の決定

管理下の製品または下位サーバのグループ化

管理下の製品または下位サーバをグループ化する場合、次の点に注意してください。

表 2-1. 管理下の製品または下位サーバのグループ化の注意点

注意点	説明
社内のネットワークポリシーおよびセキュリティポリシー	社内のネットワークにアクセス権や共有権を適用する場合、社内のネットワークポリシーとセキュリティポリシーに従って管理下の製品および下位サーバをグループ化します。
組織と機能	会社の組織上および機能上の分割に従って、管理下の製品および下位サーバをグループ化します。たとえば、2 台の Control Manager サーバで製品グループとテスト担当グループを管理します。
所在地	管理下の製品 / 下位サーバの位置が Control Manager サーバと管理下の製品 / 下位サーバ間の通信に影響する場合には、グループ化の判断基準として地理的な位置を考慮します。
管理責務	管理下の製品および下位サーバを、それぞれのシステムまたはセキュリティの担当者に合わせてグループ化します。これにより、グループ設定が可能になります。

拠点数の決定

Control Manager 配置内の拠点の数を決定します。この情報は、インストールが必要なサーバの数とサーバのインストール先を決定する上で必要になります。

以上の情報は、組織の WAN または LAN 構成図から取得します。

管理下の製品および下位サーバの数の決定

Control Manager で管理しようとする、管理下の製品および下位サーバの総数についても知る必要があります。拠点ごとに管理下の製品または下位サーバの総数に関するデータを収集することをお勧めします。この情報を取得できない場合は、概算の数でも役立ちます。この情報は、インストールが必要になるサーバの数を決定する上で必要になります。

ネットワークトラフィックの計画

Control Manager では、サーバと管理下の製品 / 下位サーバの通信時にネットワークトラフィックが発生します。組織のネットワークへの影響を最小限に抑えるように、Control Manager のネットワークトラフィックを計画します。

Control Manager 関連のネットワークトラフィックの発生元として、次のものがあります。

- 接続ステータス
- ログ
- コミュニケータスケジュール設定
- Control Manager サーバへの管理下の製品の登録

  初期設定では、Control Manager サーバには、リリース時の製品情報が含まれます。しかし、新バージョンの製品を Control Manager に登録するときに、そのバージョンが既存の製品プロファイルに対応しない場合は、その新しい製品の製品情報が Control Manager サーバにアップロードされます。
- Control Manager 上位サーバへの下位サーバの登録
- 最新コンポーネントのダウンロードと配信

サーバと管理下の製品 / 階層構造の最適な比率の計画

WAN 上に Control Manager を配置する場合、メインオフィスの Control Manager サーバによって、リモートオフィスの下位サーバおよび管理下の製品が管理されます。リモートオフィスの管理下の製品または下位サーバが WAN を通じメインオフィスにレポートを送信する場合には、WAN 上のネットワーク帯域幅の多様性について考慮する必要があります。WAN 環境のネットワーク帯域幅に多様性を持たせることは、Control Manager にとって有益です。同じサーバにレポートを送信する管理下の製品 / 下位サーバが LAN 上と WAN 上の双方にある場合、レポートは自動的に交互交替的に送信されます。つまり、Control Manager サーバによって、接続が速い方の管理下の製品または下位サーバが優先されます。優先されるのはほとんどの場合、LAN 上の管理下の製品または下位サーバです。

Control Manager システムの CPU および RAM の要件を決める際には、推奨システム要件を参考にしてください。

Control Manager サーバの指定

必要な管理下の製品と階層構造の数に基づいて、Control Manager サーバを決定および指定します。

さらに、Windows サーバの中から、Control Manager サーバとして設定するものを選択します。専用サーバをインストールする必要があるかどうかについても検討します。

Control Manager をインストールするサーバを選択するときは、次の点を考慮します。

- CPU 負荷の程度
- サーバが実行している他の機能

アプリケーションサーバなどの他の用途にも使用されているサーバに Control Manager をインストールする場合、基幹アプリケーションやリソースを大量に消費するアプリケーションを実行していないサーバへのインストールを推奨します。

注意： ウイルスバスター Corp. と Control Manager はどちらも IIS を使用して、クライアント、エージェント / 下位サーバと通信しています。2 つのアプリケーション間で競合が生じることはありませんが、どちらも IIS リソースを使用することから、Control Manager を他のコンピュータにインストールし、サーバの負荷を軽減することをお勧めします。

Control Manager サーバのインストール場所の決定

クライアントの数とインストールが必要なサーバの数を把握できたので、次に Control Manager サーバのインストール先を決定します。メインオフィスにすべてのサーバをインストールする必要があるか、一部をリモートオフィスにインストールする必要があるかを判断します。

通信の速度を高め、管理下の製品および下位サーバを最も効果的に管理するためには、環境内の特定の場所に戦略的にサーバを配置します。

- **メインオフィス** メインオフィスとは、組織内の管理下の製品および下位サーバの大部分が配置されている施設です。メインオフィスは、「本社」、「本店」などとも呼ばれます。メインオフィスは、他の場所に小規模なオフィスや支店を持つこともあります。ここでは、「リモートオフィス」と呼びます。

ヒント： メインオフィスに上位サーバをインストールすることをお勧めします。

- **リモートオフィス** リモートオフィスは、大規模な組織の一部である小規模で専門的なオフィスのことで、メインオフィスとの WAN 接続があります。リモートオフィスの管理下の製品または下位サーバから中央オフィスの Control Manager サーバにレポートが送信される場合、この Control Manager サーバへの接続が難しい場合があります。帯域幅の制限により、Control Manager サーバと適切に通信できない場合があります。

  メインオフィスとリモートオフィス間のネットワーク帯域幅が、設定の変更の通知やステータスの送信といったルーチン的なクライアントサーバ通信には十分でも、コンポーネント配信や他の作業には不十分である場合があります。

インストールの流れ

Control Manager システムのセットアップには、次の作業に関連する複数の手順が必要です。

手順 1: Control Manager システムのインストールの計画 (サーバの分散、ネットワークトラフィック、データストレージ、および Web サーバの検討)

手順 2: Control Manager サーバのインストール — Control Manager サーバのインストール中に、バックアップおよび復元ファイルの場所を指定します。

手順 3: Control Manager エージェントのインストール

対応 OS

Control Manager サーバおよびエージェントは、次の OS 上にインストールできます。

Control Manager サーバ

- Windows 2000 Server (Service Pack 3 または Service Pack 4)
- Windows 2000 Advanced Server (Service Pack 3 または Service Pack 4)
- Windows 2003 Server Standard Edition (Service Pack 1 または Service Pack 2)
- Windows 2003 Server Standard Edition R2 パッチなしまたは Service Pack 2
- Windows 2003 Server Enterprise Edition (Service Pack 1 または Service Pack 2)
- Windows 2003 Server Enterprise Edition R2 パッチなしまたは Service Pack 2
- WOW (Windows 2003 Standard または Enterprise の 64 ビット構造)

従来の Control Manager エージェント

表 2-2.　従来の Control Manager エージェント対応 OS

MICROSOFT	その他
・Windows XP Professional バージョン ・Windows 2000 Server ・Windows 2000 Advanced Server ・Windows NT 4.0 + Service Pack 3 ・Windows NT Server 4.0 (Service Pack 6a 以上) ・Microsoft Windows Server 2003 Standard Edition/Enterprise Edition	・Novell Desktop 9 ・AIX ・Red Hat Linux 6.2、7.1、7.2 ・RedHat Enterprise Linux 4.3 ・Turbolinux 6.5、7.0 ・SuSE Linux 6.3、7.2、7.3 ・SuSE Enterprise 9.2 ・AS/400 ・OS390 ・その他 GateLock、Linux 6.x kernel、 Solaris 2.6、2.7、2.8、Debian 3.1 4

テストインストール

テストインストールによって、各機能がどのように動作するか、完全な導入後にどのようなレベルのサポートが必要になるかを判断するためのフィードバックを得ることができます。

ヒント： Control Manager を全面的にインストールする前に、限定的な環境で試験的にインストール (テストインストール) することを推奨します。

Control Manager のテストインストールにより、次のことを実現できます。

- Control Manager および管理下の製品に対する理解
- 社内のネットワークポリシーの策定または改善

テストインストールは、改良の必要な設定箇所を判断するために便利です。これにより、IT 部門またはインストールチームは導入手順を事前に実践して改善したり、組織の業務上の要件を満たすかどうかをテストする機会を得ることができます。

Control Manager のテストインストールを行うには、次のタスクを実行します。

テストインストールの準備

準備段階では、次の処理を完了します。

手順 1: テスト環境における、Control Manager サーバとエージェントの構成を決定します。

- 異機種間のテスト構成におけるすべてのシステム間で TCP/IP 接続を確立させます。
- Control Manager システムから各エージェントシステムに、またその逆方向に ping コマンドを発行することにより、双方向の TCP/IP 通信を確認します。

手順 2: どのような配置が環境に適しているかを知るために、さまざまな配置方法を評価します。

手順 3: テストインストールに使用するシステムチェックリストに記入します。

テストサイトの選定

実際の稼働環境に類似したテスト用のサイトを選定します。構成をできるかぎり実稼働環境に近い形に近づけます。

ロールバック計画の作成

インストール時またはアップグレード時に何か問題が発生した場合に備え、災害復旧計画またはロールバック計画を用意する必要があります (Control Manager 3.5 にロールバックする方法など)。このプロセスには、IT リソースだけでなく、ローカルな企業ポリシーも反映する必要があります。

テストインストールの開始

準備作業とシステムチェックリストの記入が完了したら、Control Manager サーバとエージェントをインストールし、テストインストールを開始します。

テストインストールの評価

試験の開始から終了までに確認された成功点と失敗点のリストを作成します。潜在的な問題を特定し、導入を成功させるための対応策を検討します。

このテスト評価計画は、実際のインストールおよび配置計画全体に組み込むことができます。

サーバの配置計画

管理計画について

Control Manager の配信の初期段階で、ControlManager サーバへのアクセスを許可するユーザ数を決定しておきます。ユーザの数は、管理をどの程度集中させるかによって異なります。集中化の度合いは、ユーザ数と反比例するという法則を考慮してください。

次の管理モデルのいずれかに従います。

- **集中管理計画** — 集中管理モデルでは、Control Manager へのアクセス権を必要最低限のユーザにのみ与えます。高度な集中管理においては、管理者は 1 人だけです。ネットワーク上のウイルス対策サーバやコンテンツセキュリティサーバはすべて、1 人の管理者によって管理されます。

  集中管理では、ネットワーク上のウイルス対策ポリシーやコンテンツセキュリティポリシーの管理が最も厳密になります。しかし、ネットワークが複雑になるに従って、管理者の作業負荷が大きくなり、1 人では対応できなくなる可能性があります。

- **分散管理計画** — この計画は、システム管理者の責任範囲が明確に定義、確立されている大規模なネットワークの場合に便利です。たとえば、メールサーバ管理者がメール関連のウイルス対策製品を担当したり、ある支店の管理者がその支店全体のウイルス対策を担当するというように、製品別や拠点別に責任を分担します。

  分散管理モデルを選択した場合でも、Control Manager の主となる管理者を設定する必要がありますが、管理者間で責任を分担することができます。

  各管理者には、担当する製品や拠点の設定のみを表示したり変更できるように権限を与えます。

上記のいずれかの管理モデルを土台とし、製品ディレクトリと必要なユーザアカウントを設定することによって Control Manager システムを管理することができます。

Control Manager サーバの配置について

Control Manager は実際のインストール場所に関係なく製品を管理できます。したがって、1 つの Control Manager サーバからすべてのウイルス対策製品やコンテンツセキュリティ製品を管理することができます。

しかし、Control Manager システムの管理を何台かのサーバ間で (アドバンス版ユーザの場合) 分割する方が好都合な場合もあります。各ネットワークの特徴に基づいて、Control Manager サーバの最適な数を決定する必要があります。

単一サーバによる運用

単一サーバによる運用は、中小規模の、1 つのサイトからなる企業に適しています。この構成では、1 人の管理者による管理が容易になりますが、管理計画に応じて必要とされる追加の管理者アカウントを作成することも可能です。

さらに、この構成では、エージェントポーリング、データ転送、アップデート配信などのネットワークトラフィック負荷が 1 つのサーバ、およびこのサーバを収容する LAN に集中します。ネットワークの規模が拡大すると、パフォーマンスへの影響も大きくなります。

複数サーバによる運用

複数の拠点からなる大規模な企業では、Control Manager サーバを地域ごとに設置して、ネットワーク負荷を分散しなければならない場合があります。

Control Manager システムで発生するトラフィックの詳細については、52 ページの「Control Manager のネットワークトラフィックについて」を参照してください。

ネットワークトラフィックの計画

ネットワークへの Control Manager の影響を最小限に抑える計画を作成するには、Control Manager システムで発生するトラフィックについて理解することが重要です。

ここでは、Control Manager システムで発生するネットワークトラフィックを理解し、ネットワークに負荷のかからない運用を計画するために必要な情報について説明します。さらに、トラフィックの発生間隔に関する項では、Control Manager システム上にトラフィックを頻繁に生じさせる発生元について説明します。

Control Manager のネットワークトラフィックについて

ネットワークへの Control Manager の影響を最小限に抑える計画を作成するには、Control Manager システムで発生するトラフィックについて理解することが重要です。

ネットワークトラフィックの発生元

Control Manager のネットワークトラフィックを生じさせる発生元を次に示します。

- ログのトラフィック
- Trend Micro Management Infrastructure (TMI) ポリシー
- 製品登録
- 最新コンポーネントのダウンロードと配信

トラフィックの発生間隔

Control Manager システムでは、次の要因によりトラフィックが頻繁に発生します。

- ログ
- MCP ポーリングおよびコマンド
- Trend Micro Management Infrastructure ポリシー

ログ

管理下の製品は、それぞれのログの設定に従ったさまざまな間隔で Control Manager にログを送信します。

管理下の製品エージェントの接続ステータス

初期設定では、管理下の製品のエージェントは 60 分ごとに接続ステータスメッセージを送信します。管理者はこの値を 5 分から 480 分までの間で指定することができます。コミュニケータ接続ステータスの実行間隔を指定するときは、コミュニケータのステータス情報の更新頻度と、システムリソースの消費の抑制の両方を考慮する必要があります。

多くの場合、初期設定で十分な結果が得られますが、これらの設定を変更する必要がある場合には、次の点を考慮に入れておいてください。

- **長い間隔の接続ステータス (60 分以上)** — 接続ステータスの実行間隔を長く設定するほど、Control Manager サーバの管理コンソールにステータスが表示されるまでに発生するイベントの数が多くなります。

  たとえば、次の送信時間に達するまでの間にエージェントとの接続の問題が解決された場合、ステータスが「停止中」または「異常」と表示されていたとしても、エージェントとの通信が回復している可能性があります。

- **短い間隔の接続ステータス (60 分未満)** — 接続ステータスの実行間隔を短く設定すると、Control Manager サーバの管理コンソールに、より最新のステータスが表示されるようになります。ただし、消費されるネットワークの帯域幅が増加します。

注意 : 間隔を 15 分以下に設定したい場合には、まず既存のネットワークトラフィックを調べて、ネットワーク帯域幅の使用が増えることによる影響について理解する必要があります。

ネットワークプロトコル

Control Manager の通信は、主に UDP プロトコルと TCP プロトコルに基づいて行われます。

ネットワークトラフィックの生成源

ログのトラフィック

Control Manager サーバと管理下の製品間には、常に「製品ログ」によるネットワークトラフィックが存在します。製品ログは、各管理下の製品が Control Manager サーバに対して定期的に送信するログです。

表 2-3. Control Manager ログトラフィック

ログの種類	含まれる情報
ウイルス / スパイウェアのログ	検出されたウイルス / 不正プログラム、スパイウェア / グレーウェアなどのセキュリティ上の脅威
セキュリティログ	コンテンツセキュリティ製品から報告された違反
Web セキュリティログ	Web セキュリティ製品から報告された違反
イベントログ	コンポーネントのアップデート、一般的なセキュリティ違反などのイベント
ステータス	管理下の製品の環境。この情報は製品ディレクトリのステータス概要ページに表示されます。
ネットワークウイルスログ	ネットワークパケット内で検出されたウイルス
パフォーマンス測定	旧バージョンの製品で使用
URL アクセス	Web セキュリティ製品から報告された違反
セキュリティ違反	Network VirusWall 製品から報告された違反
セキュリティ遵守	Network VirusWall 製品から報告されたクライアントのセキュリティ遵守
セキュリティ統計	Network VirusWall 製品から計算、報告されたクライアントのセキュリティ遵守数とセキュリティ違反数の差異
エンドポイント	Web セキュリティ製品から報告された違反

Trend Micro Management Communication Protocol ポリシー

Trend Micro Management Communication Protocol (MCP) は、Control Manager の通信用コンポーネントの最も新しい部分です。MCP は次のポリシーを適用します。

MCP 接続ステータス — Control Manager への MCP 接続ステータスにより、Control Manager に最新の情報が表示されるようにし、管理下の製品と Control Manager サーバ間の接続が正常に保たれます。

MCP コマンドポーリング — MCP エージェントが Control Manager へのコマンドポーリングを開始すると、Control Manager はエージェントに管理下の製品のログを送信するよう通知するか、管理下の製品にコマンドを発行します。また、Control Manager ではコマンドポーリングを、Control Manager と管理下の製品の間の接続を確認するパッシブな接続ステータスとして解釈します。

Trend Micro Management Infrastructure ポリシー

Trend Micro Management Infrastructure (TMI) — Control Manager の通信用コンポーネントの一環であり、維持管理を目的としたトラフィックを継続的に発生させます。TMI は次のポリシーを実施しています。

- **コミュニケータ接続ステータス** — コミュニケータは、TMI のメッセージルーティングフレームワークであり、Control Manager サーバに定期的な間隔でポーリングします。これにより、Control Manager コンソールに最新の情報が表示されるようにし、管理下の製品と Control Manager サーバ間の接続が正常に保たれます。
- **稼働時間ポリシー** — 稼働時間ポリシーでは、コミュニケータが Control Manager サーバに情報を送信する時間帯を定義します。このポリシーはコミュニケータスケジュール設定を使用して定義されます。ユーザは、送信を停止する時間帯を 3 つ設定することができます。ただし、次の 2 種類の情報には、コミュニケータスケジュール設定が適用されません。
    - 緊急時のメッセージ
    - 禁止されたメッセージ

TMI は、コミュニケータが稼働時間外であっても、緊急時メッセージを Control Manager サーバに送信します。一方、コミュニケータが稼働時間内であっても、TMI は禁止されたメッセージを Control Manager に送信しません。

製品登録によるトラフィック

製品情報は、特定の製品をどのように管理するかに関する情報を Control Manager に提供します。管理下の製品をはじめて Control Manager サーバに登録するときに、製品情報はサーバに送信されます。

製品情報は製品ごとにあり、通常、複数のバージョンがある製品の場合、バージョン別の製品情報があります。製品情報には次の情報が含まれます。

- カテゴリ (ウイルス対策など)
- 製品名
- 製品バージョン
- メニューバージョン
- ログ形式
- コンポーネント情報 — この製品で使用されるコンポーネントの情報 (パターンファイルなど)
- コマンド情報

初期設定では、Control Manager サーバはリリースの時点の管理下の製品情報を保持しています。ただし、Control Manager に新しいバージョンの製品が登録されると、その新しい製品情報が Control Manager サーバに送信されます。

アップデートの配信

最新コンポーネントの配信について

Control Manager のアップデート作業は、次の 2 つの手順に分かれます。

手順 1: トレンドマイクロから最新コンポーネントを取得します。Control Manager で、トレンドマイクロのアップデートサーバから直接または別の場所からコンポーネントをダウンロードできます。

手順 2: これらのコンポーネントを管理下の製品に配信します。

Control Manager で、次のコンポーネントを管理下の製品に配信できます。

- パターンファイル / テンプレート
- 各種エンジン (検索エンジン、ダメージクリーンナップエンジン)
- スパムメール判定ルール
- 製品プログラム (製品によって異なる)
- ネットワークウイルスパターンファイル (Network VirusWall 製品のみ)

注意： Control Manager でダメージクリーンナップテンプレートまたはダメージクリーンナップエンジンをアップデートするには、まずトレンドマイクロ ダメージクリーンナップ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。

トレンドマイクロでは、管理下の製品が新たなウイルスの脅威に対応できるよう、それらのコンポーネントを定期的にアップデートすることをお勧めします。製品プログラムのアップデートについては、それぞれの製品のマニュアルを参照してください。

管理下の製品へのコンポーネントの配信によって、帯域幅が多く消費されます。可能な場合は、ネットワークへの影響が最小限に抑えられる時間帯に配信することが重要です。

配信計画を使用して、コンポーネントをスケジュールに従って配信することができます。

また、Control Manager サーバと管理下の製品とのネットワーク接続がアップデートに対処できることを確認します。これは、ネットワークに必要な Control Manager サーバの数を決定する際に考慮される要素です。

データベースの計画

Control Manager のデータは SQL データベースに格納する必要があります。Control Manager がインストールされているサーバに専用のデータベースがない場合、インストールプログラムから Microsoft SQL Express をインストールするためのオプションが提示されます。ただし、SQL Express の制約により、大規模なネットワークでは SQL Server を使用する必要があります。

注意： Control Manager は SQL Server へのアクセスに、SQL Server 認証と Windows 認証を使用します。

データベースの推奨設定

Control Manager と SQL Server を同じコンピュータにインストールする場合、固定メモリサイズがサーバ上の総メモリの 3 分の 2 になるように SQL Server を設定します。たとえば、サーバの RAM が 256MB の場合、SQL サーバの固定メモリサイズを 150MB に設定します。

Control Manager サーバ、または SQL Server 専用サーバなど別のサーバに、Control Manager SQL データベースをインストールします。Control Manager が管理する製品が 1000 を超える場合、専用のコンピュータにインストールした SQL Server を使用することをお勧めします。

注意： SQL リソースの管理方法やデータベースのサイズに関するその他の推奨事項については、Microsoft SQL Server に付属するドキュメントを参照してください。

ODBC ドライバ

Control Manager では、ODBC ドライバを使用して、SQL Server と通信します。基本的には、ODBC バージョン 3.7 で動作します。ただし、SQL 2000/2005 の名前付きインスタンスに接続する場合、SQL ODBC ドライバは、バージョン 2000.80.194.00 が必要になります。

Control Manager のセットアッププログラムは、適切なバージョンの ODBC ドライバが使用されているかどうか、また Control Manager のインストール先コンピュータに SQL Server がインストールされているかどうかをチェックします。Control Manager サーバと別のコンピュータ上の SQL Server については、これらを手動で確認し、Control Manager が確実にデータベースにアクセスできることを保証する必要があります。

認証

Control Manager では SQL データベースへのアクセスに、Windows 認証ではなく、混合モード認証 (Windows 認証と SQL Server 認証) が使用されます。

Web サーバの設定

Web サーバの設定

Control Manager セットアッププログラムの [Web サーバ情報の指定] 画面では、Web サーバをホスト名、FQDN、IP アドレスのいずれかで指定します。Web サーバ名を決定する上での考慮事項は、次と同じです。

- ホスト名または FQDN を使用すると、Control Manager サーバの IP アドレスの変更に容易に対応できますが、システムは DNS サーバに依存するようになります。
- IP アドレスを使用する場合、固定 IP アドレスが必要です。

この Web サーバアドレスを使用し、コンポーネントのアップデートサーバを識別します。この情報は「SystemConfiguration.xml」ファイルに保存され、Control Manager サーバからアップデートを取得できるようにエージェントへの通知の一部に含められます。アップデートサーバは次のように記述されます。

Value=http://<Web サーバの IP アドレス >:< ポート >/TvcsDownload/ActiveUpdate/< コンポーネント >

ここで、

- **ポート** — アップデート元に接続するポート。Web サーバアドレス画面で指定することもできます。初期設定のポート番号は 80 です。
- TvcsDownload/ActiveUpdate — Control Manager セットアッププログラムは、対応するこの仮想ディレクトリを IIS 指定の Web サイトに作成します。
- **コンポーネント** — アップデートされたコンポーネントに応じて異なります。たとえば、パターンファイルがアップデートされる場合、ここには次の値が含められます。

  Pattern/Vsapixxx.zip

  「Pattern」は、<Control Manager のインストールフォルダ >¥WebUI¥download¥activeupdate¥pattern フォルダに対応します。「Vsapi.zip」は圧縮形式でのウイルスパターンです。

第 3 章

新規インストール

本章では、Trend Micro Control Manager (以下、Control Manager) のサーバのインストール方法を説明します。Control Manager のサーバのシステム要件をリストアップすると共に、インストール後の設定や、製品のアクティベーション手順を示します。

本章は次の内容で構成されています。

システム要件

企業のネットワークは企業自身と同様、1 つ 1 つ異なります。したがって、ネットワークごとに要求されるものが異なり、複雑さのレベルもさまざまです。本章では、最低限必要なシステム要件と推奨されるシステム要件の両方を説明し、一般的な推奨事項とネットワーク規模に応じた推奨事項についても示します。

注意： システム要件に記載されている OS の種類やハードディスク容量などは、OS のサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

最小システム要件

次の表は、Control Manager サーバに最低限必要なシステム要件をまとめたものです。

注意： Control Manager 5.0 アドバンス版では、次のサーバを下位の Control Manager サーバとしてサポートします。

- Control Manager 5.0 アドバンス版
- Control Manager 3.5 スタンダード版またはエンタープライズ版

Control Manager 5.0 スタンダード版サーバを下位サーバとすることはできません。

エージェントのシステム要件については、各製品のドキュメントを参照してください。

表 3-1. Control Manager サーバのハードウェアの最小システム要件

ハードウェア	最小要件
CPU	Intel Pentium III 600MHz 以上 (Intel IA64 プロセッサを除く) ・シングル CPU ・デュアル CPU ・クワッド CPU

表 3-1. Control Manager サーバのハードウェアの最小システム要件

ハードウェア	最小要件
メモリ	・最小 2GB の RAM ・4GB 推奨
ディスク空き容量	・790MB 以上 (Control Manager スタンダード / アドバンス版) ・300MB 以上 (SQL 2005 Express 用、任意)

表 3-2. Control Manager サーバのソフトウェアの最小システム要件

ソフトウェア	最小要件
OS	・Microsoft Windows 2000 Server (Service Pack 3 または Service Pack 4) ・Windows 2000 Advanced Server (Service Pack 3 または Service Pack 4) ・Windows Server 2003 Standard Edition (Service Pack 1 または Service Pack 2) ・Windows Server 2003 Standard Edition R2 (パッチなしまたは Service Pack 2) ・Windows Server 2003 Enterprise Edition (Service Pack 1 または Service Pack 2) ・Windows Server 2003 Enterprise Edition R2 (パッチなしまたは Service Pack 2) ・Windows Server 2008 Standard Edition ・Windows Server 2008 Enterprise Edition ・WOW (Windows 2003/2008 Standard または Enterprise の 64 ビット構造)
Web サーバ	・Microsoft IIS サーバ 5.0 (2000 プラットフォーム用) ・Microsoft IIS サーバ 6.0 (2003 プラットフォーム用) ・Microsoft IIS サーバ 7.0 (2008 プラットフォーム用)
データベース	・Microsoft Data Engine (MSDE) 2000 (Service Pack 3 以上を推奨) ・Microsoft SQL Server 2000 (Service Pack 3 以上を推奨) ・Microsoft SQL Server 2005

表 3-2.　Control Manager サーバのソフトウェアの最小システム要件

ソフトウェア	最小要件
その他	・Microsoft .NET Framework 2.0 (Control Manager のパッケージに同梱) ・Windows Installer 3.1 (Control Manager のパッケージに同梱) ・Microsoft Visual C++ 2005 SP1 再頒布可能パッケージ (Control Manager のパッケージに同梱) ・SQL Express 用 Microsoft Data Access Components (MDAC) 2.8 SP1 以上 (Control Manager のパッケージに同梱されていません) ・Microsoft Windows Server 2008 環境において、次にあげる Microsoft IIS 7.0 サーバのロールサービス (役割サービス) が必要です。 [HTTP 基本機能] - Static Content (静的なコンテンツ) - Default Document (既定のドキュメント) - Directory Browsing (ディレクトリの参照) - HTTP Errors (HTTP エラー) [アプリケーション開発] - ASP.NET - .Net Extensibility (.NET 拡張性) - ASP - CGI - ISAPI Extensions (ISAPI 拡張) - ISAPI Filters (ISAPI フィルタ) [セキュリティ] - Request Filtering (要求フィルタ) [管理ツール] - IIS 6 Management Compatibility (IIS6 管理互換)
管理コンソール	・ブラウザ — Windows Internet Explorer 6 以上 ・Java VM — Microsoft 版 5.0.0.3805 以上

表 3-3.　連携する運用管理ツール

	連携する運用管理ツール
Fujitsu	・Systemwalker Centric Manager (システムウォーカーセントリックマネージャー) V13.2
Hitachi	・統合システム運用管理 JP1 Version 8
NEC	・WebSAM System Navigator Ver3.1

Control Manager エージェントの最新情報については、次の URL を参照してください。

http://jp.trendmicro.com/jp/products/enterprise/tmcm/related/index.html

推奨システム要件

Control Manager の最適なパフォーマンスを得るには、次のシステム要件を参考にしてください。

全般的な推奨要件

- Control Manager をプライマリドメインコントローラ (PDC)、バックアップドメインコントローラ (BDC)、またはその他のトレンドマイクロ製品を実行するサーバにインストールしないでください。著しいパフォーマンスの低下を引き起こす可能性があります。

- 物理メモリはシステムのリソースであり、サーバ上のすべてのアプリケーションで共有されます。プロセッサに合わせてメモリも拡張します。メモリを消費し尽くさないようにしてください。

表 3-4. Control Manager サーバの一般的な推奨事項

ハードウェア / ソフトウェア	推奨される要件
ネットワークアダプタ	100Mbps、32 ビットのアダプタ (Control Manager サーバと管理下の製品の両方に必要)。バスマスタリング、ダイレクトメモリアクセス (DMA) 型のものを推奨
ファイルシステム	NT File System (NTFS) パーティション
モニタ	解像度が 1024 x 768、256 色以上出力可能な VGA モニタ

Control Manager サーバのインストール

Control Manager のインストール計画を作成したら、Control Manager サーバのインストールを開始できます。418 ページの「サーバアドレスチェックリスト」を確認してください。このリストにはインストールに必要なシステム関連情報を記録することができます。

インストールには次の情報が必要です。

- 関連するサーバアドレスとポート情報
- サーバ / エージェント間の通信で使用するセキュリティのレベル

データベースに関連して、あらかじめ次の情報を確認してください。

- Control Manager で SQL Server を使用するかどうか Control Manager サーバと異なるサーバに SQL Server がある場合は、そのサーバの IP アドレス、FQDN (Fully Qualified Domain Name)、または NetBIOS 名が必要です。SQL Server のインスタンスが複数存在する場合は、使用するインスタンスについての情報が必要です。

- Control Manager で使用する SQL データベースの認証情報
  - データベースのユーザ名
  - パスワード

注意： Control Manager は SQL Server へのアクセスに、Windows 認証と SQL Server 認証の両方を使用します。

- Control Manager が扱う管理下の製品の数を決定します。サーバ上に SQL Server が検出されない場合、Control Manager は SQL 2005 Express SP2 をインストールします。SQL Express では、一定の数の接続しか扱うことができません。

Control Manager をインストールするには、次の手順に従ってください。

手順 1: すべての必須コンポーネントのインストール

手順 2: インストール先の指定

手順 3: 使用許諾契約書への同意、および製品とサービスのアクティベーション

手順 4: Control Manager のセキュリティと Web サーバ設定の指定

手順 5: バックアップ設定の指定とデータベース情報の設定

手順 6: root アカウントのセットアップと通知の設定

ヒント： 新規インストールよりも、バージョン 5.0 にアップグレードすることをお勧めします。

Control Manager サーバをインストールするには

手順 1: すべての必須コンポーネントのインストール

1. Windows のタスクバーで、[スタート]→[ファイル名を指定して実行] の順に選択し、Control Manager インストールプログラム (Setup.exe) を探します。製品 DVD からインストールする場合は、製品 DVD の Control Manager フォルダに移動します。ソフトウェアをトレンドマイクロの Web サイトからダウンロードした場合は、コンピュータ上の該当するフォルダに移動してください。インストールプログラムにより、システム上の必須コンポーネントのチェックが行われます。

   インストールプログラムによりサーバ上で次のコンポーネントが検出されなかった場合、見つからないコンポーネントをインストールするよう指示するダイアログボックスが表示されます。

   - Windows Installer 3.1 — このコンポーネントは Control Manager のインストールパッケージに同梱しています。
   - Microsoft Data Access Components (MDAC) 2.8 SP1 以上 — このコンポーネントは Control Manager のインストールパッケージに含まれていません。
   - Microsoft .Net Framework 2.0 — このコンポーネントは Control Manager のインストールパッケージに同梱しています。
   - Microsoft Visual C++ 2005 SP1 再頒布可能パッケージ — このコンポーネントは Control Manager のインストールパッケージに同梱しています。

2. すべての未検出のコンポーネントのインストール IIS 確認ダイアログボックスが表示されます。

3. インストールを続行するには [はい] をクリックします。[ようこそ] 画面が表示されます。

インストールプログラムにより、システム上に現在あるコンポーネントのチェックが行われます。インストールを進める前に、Microsoft Management Console のすべてのインスタンスを停止します。移行の詳細については、104 ページの「Control Manager エージェントの移行計画」を参照してください。

4. [次へ] をクリックします。ソフトウェア使用許諾契約書が表示されます。

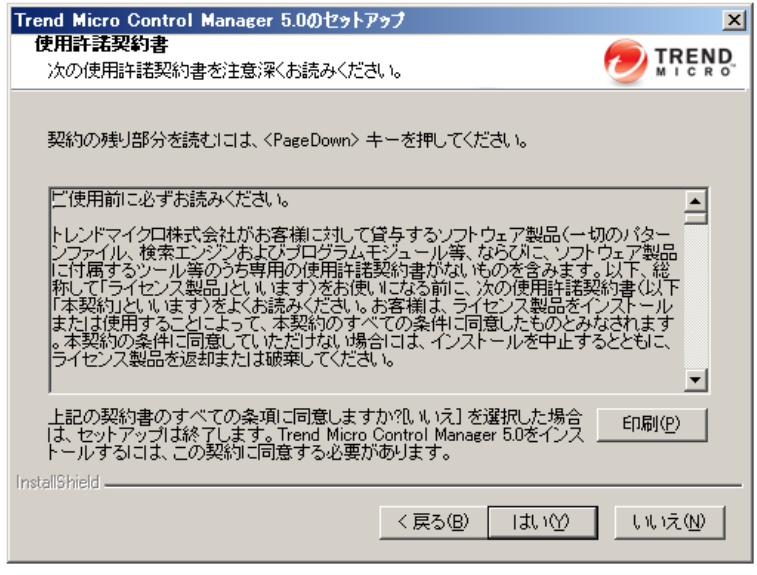


図 3-1. 契約事項に同意する場合は [はい] をクリックします。

契約事項に同意する場合は [はい] を、同意しない場合は [いいえ] をクリックします。[いいえ] をクリックした場合、インストールはこの時点で中止されます。[はい] をクリックすると、インストールが続行されます。検出されたコンポーネントの一覧が表示されます。

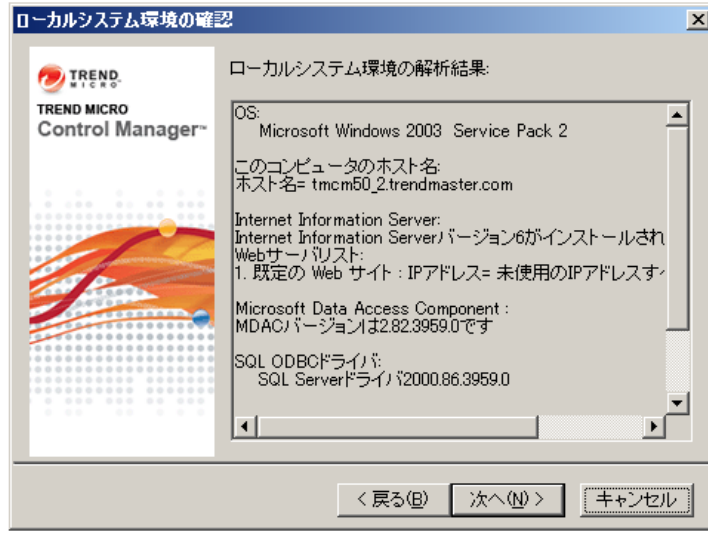


図 3-2.　インストール先のシステム環境情報の表示

手順 2: インストール先の指定

1. [次へ] をクリックします。[インストール先フォルダの選択] 画面が表示されます。

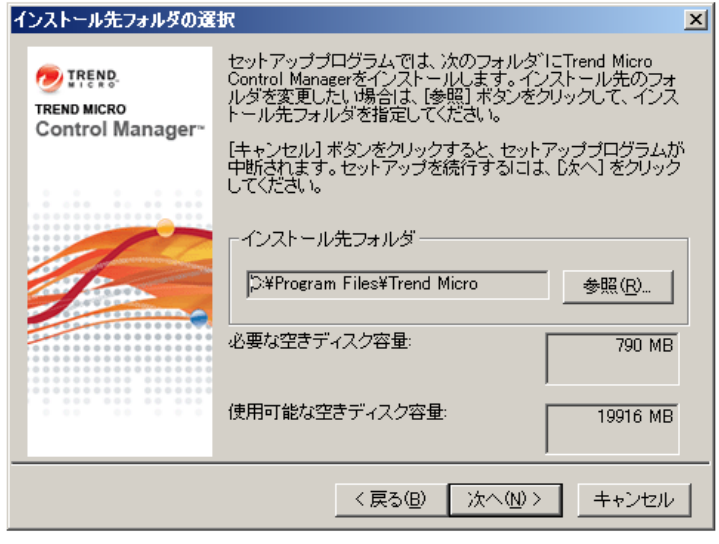


図 3-3. インストール先フォルダの選択

2. Control Manager のインストールディレクトリを指定します。初期設定では、C:¥Program Files¥Trend Micro にインストールされます。この場所を変更する場合は、[参照] をクリックして、場所を指定します。

注意： 初期設定以外のディレクトリを選択した場合でも、Control Manager の通信 (Trend Micro Management Infrastructure および MCP) 関連のファイルは Program Files フォルダ内の既定の場所にインストールされます。

手順 3: 製品とサービスのアクティベーション

1. [次へ] をクリックします。[製品のアクティベーション] 画面が表示されます。

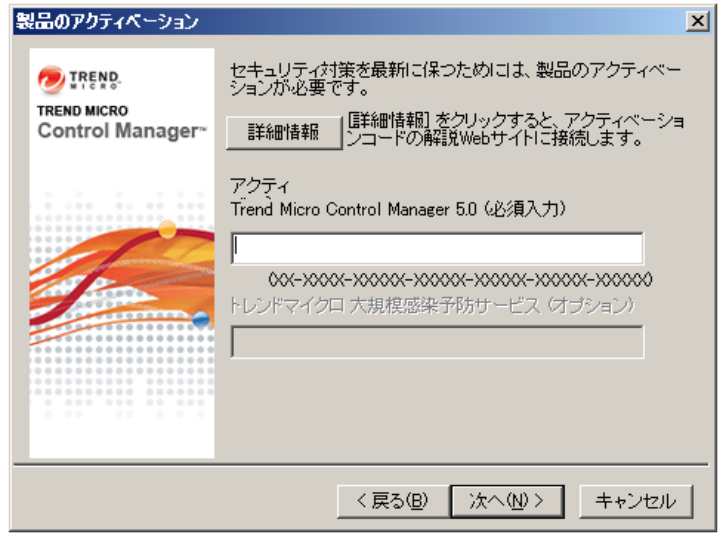


図 3-4. Control Manager およびサービスを有効にするアクティベーションコードの入力

2. Control Manager および購入したその他の追加サービスのアクティベーションコードを入力します。オプションのサービスのアクティベーションは、Control Manager コンソールから実行することもできます。Control Manager 5.0 およびその他のサービス (大規模感染予防サービス) の全機能を利用するには、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。

3. [次へ] をクリックします。[ウイルストラッキング] 画面が表示されます。

図 3-5. ウイルストラッキングセンターへのウイルス情報送信

4. [情報を送信する] を選択し、ウイルストラッキングセンターへのウイルス情報の送信を設定します。Control Manager では、管理下の製品で検出されたウイルスの情報をウイルストラッキングセンターに送信することができます。ウイルストラッキングセンターに送信されるのは、Control Manager システムで検出されたウイルスの名前と件数のみです。その他の情報 (コンピュータ名、サイト名、IP アドレスなど) は一切送信されません。ウイルス情報の送信はインストール時に設定しますが、インストール後も管理コンソールを使用していつでも設定を変更することができます。

手順 4: Control Manager のセキュリティと Web サーバ設定の指定

1. [次へ] をクリックします。[セキュリティレベルとホストアドレスの選択] 画面が表示されます。

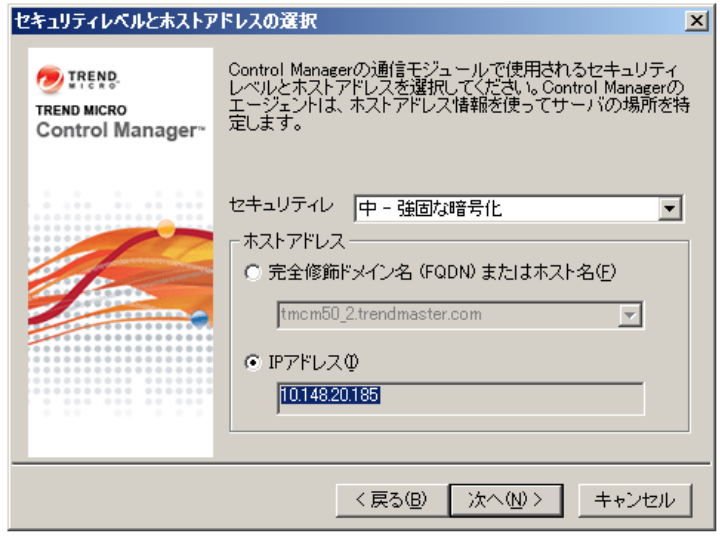


図 3-6. セキュリティレベルの選択

2. [セキュリティレベル] リストから、Control Manager がエージェントと通信する際のセキュリティレベルを選択します。次のオプションがあります。

   - **高 — 強固な暗号化と認証** — Control Manager と管理下の製品との間のすべての通信に認証付きの 128 ビット暗号化を使用します。Control Manager と管理下の製品との間の通信として最も安全な通信方法です。
   - **中 — 強固な暗号化** — 128 ビット暗号化がサポートされる場合は、Control Manager と管理下の製品との間のすべての通信に 128 ビット暗号化を使用します。これは、Control Manager インストール時の初期設定です。
   - **低 — 普通の暗号化** — Control Manager と管理下の製品との間のすべての通信に 40 ビット暗号化を使用します。Control Manager と他の製品との間の通信として最も安全性が低い通信方法です。

3. Control Manager と通信するエージェントのホストアドレスを選択します。

ヒント： ホスト名を使用して Control Manager をインストールすることをお勧めします。IP アドレスを使用してインストールを実行すると、Control Manager サーバの IP アドレスを変更する必要が生じた場合に問題が発生する可能性があります。Control Manager では、インストールに使用した IP アドレスの変更をサポートしていません。そのため、サーバの IP アドレスを変更しなければならない場合、管理者が Control Manager を再インストールする必要が生じます。ホスト名を使用してインストールすれば、この問題を回避できます。

FQDN/ ホスト名を使用する場合 :

a. [完全修飾ドメイン名 (FQDN) またはホスト名] を選択します。

b. 表示されているフィールドで、FQDN またはホスト名を選択または入力します。

IP アドレスを使用する場合 :

a. [IP アドレス] を選択します。

b. [IP アドレス] に IP アドレスを入力します。IP アドレスの各エントリはセミコロン (;) で区切ります。

4. [次へ] をクリックします。[Web サーバ情報の指定] 画面が表示されます。

   [Web サーバ情報の指定] 画面の設定では、通信のセキュリティ設定とサーバの識別方法を指定します。

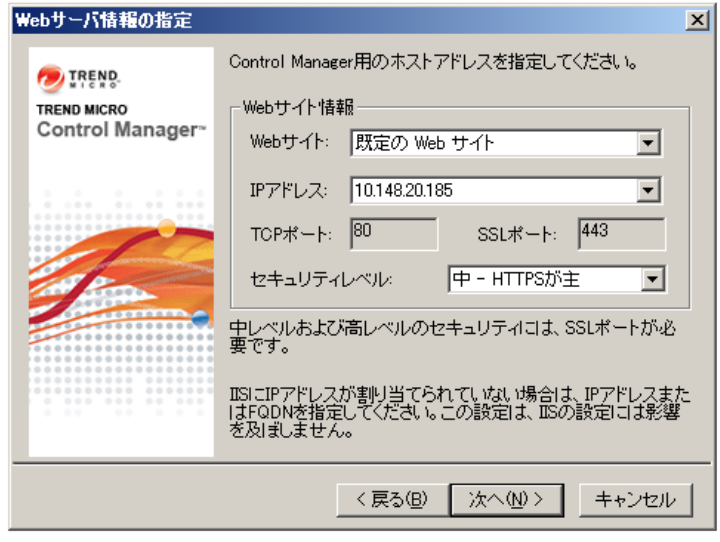


図 3-7.　Web サーバ情報の指定

5. [Web サイト] リストから、Control Manager にアクセスする Web サイトを選択します。

6. [IP アドレス] リストから、Control Manager の管理コンソールで使用する、IP アドレスまたは FQDN/ ホスト名を選択します。この設定では、Control Manager の通信システムにおける Control Manager サーバの識別方法を指定します。セットアッププログラムは、サーバの FQDN と IP アドレスの両方を検索し、検出された場合は、これらをフィールドに表示します。

   サーバで複数のネットワークインタフェースカードが使用されている場合、またはサーバに複数の FQDN が割り当てられている場合は、その名前と IP アドレスが表示されます。リストを使用して、最適なアドレスまたは名前を選択します。

   サーバの識別にホスト名または FQDN を使用する場合、製品がインストールされているコンピュータ上でこの名前を解決できることを確認してください。解決できない場合、製品は Control Manager サーバと通信することができません。

7. [セキュリティレベル] リストから、Control Manager が通信する際のセキュリティレベルを選択します。次のオプションがあります。

   - **高 — HTTPS のみ** — すべての Control Manager の通信に HTTPS プロトコルを使用します。Control Manager と他の製品との間の通信として最も安全な通信方法です。
   - **中 — HTTPS が主** — HTTPS がサポートされている場合は、すべての Control Manager の通信に HTTPS プロトコルを使用します。HTTPS が利用できない場合は、エージェントは HTTP を使用します。これは、Control Manager インストール時の初期設定です。
   - **低 — HTTP が基本** — すべての Control Manager の通信に HTTP プロトコルを使用します。Control Manager と他の製品との間の通信として最も安全性が低い通信方法です。

8. [低 — HTTP が基本] を選択した場合、および ISS 管理コンソールで SSL ポート値を指定していない場合は、[SSL ポート] で Control Manager の通信に使用するアクセスポートを指定します。

手順 5: バックアップ設定の指定とデータベース情報の設定

1. [次へ] をクリックします。[インストール先の選択] 画面が表示されます。

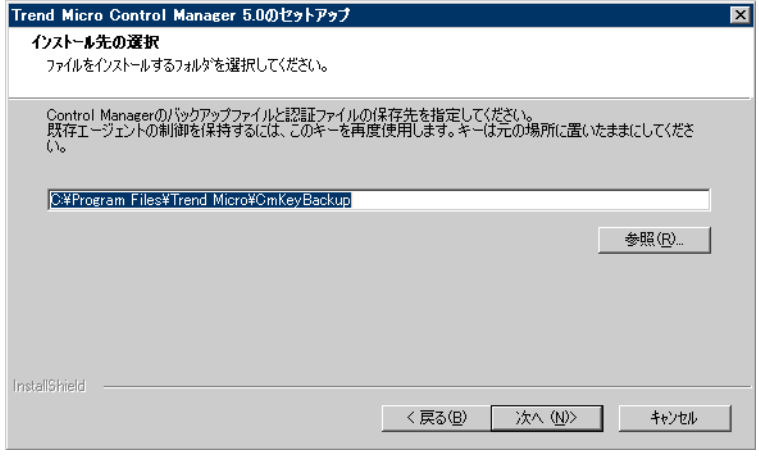


図 3-8. バックアップファイルと認証ファイルの保存場所の選択

2. Control Manager のバックアップファイルと認証ファイルの保存場所を指定します (詳細については、100 ページの「バックアップする必要がある Control Manager ファイル」を参照)。別の場所を指定するには、[参照] をクリックします。

3. [次へ] をクリックします。[Control Manager データベースのセットアップ] 画面が表示されます。

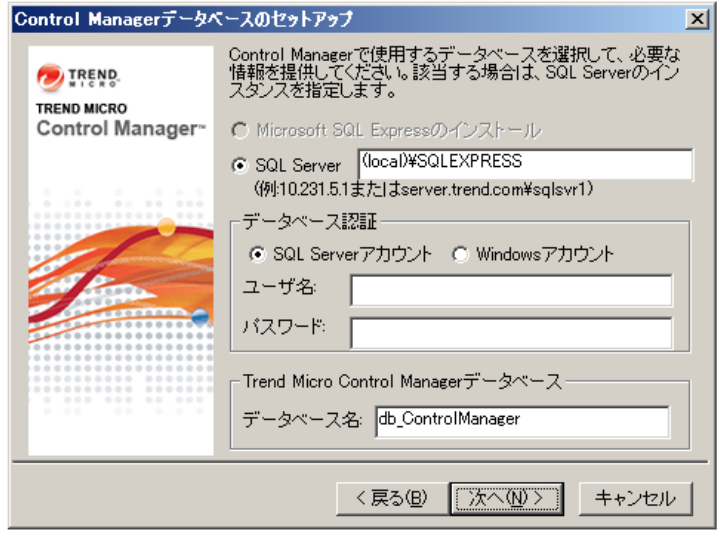


図 3-9. Control Manager データベースの選択

4. Control Manager で使用するデータベースを選択します。

- Microsoft SQL Express のインストール — SQL Server がこのコンピュータにインストールされていない場合、このオプションが自動的に選択されます。データベースには必ずパスワードを指定してください。

ヒント： Microsoft SQL Express は、管理下のネットワーク規模が小さい場合に適しています。大規模な Control Manager システムの場合、SQL Server の使用をお勧めします。

- SQL Server — サーバ上で SQL Server が検出された場合、このオプションが自動的に選択されます。次の項目を入力してください。
    - SQL Server (¥Instance) — Control Manager で使用する SQL Server のホストサーバです。使用しているサーバに SQL Server が存在する場合は、このオプションが自動的に選択されます。

      別のサーバを指定する場合は、FQDN、IP アドレス、または NetBIOS 名を指定してください。

      SQL Server のホストサーバは、Control Manager がインストールされているサーバ、または別のサーバのどちらでも指定することができますが、パフォーマンスを考慮し、別のサーバにインストールすることをお勧めします。複数の SQL Server インスタンスが存在する場合は、特定のインスタンスを指定する必要があります。たとえば、次のように指定します。
      your_sql_server.com¥instance
    - データベース認証 — SQL Server にアクセスするための認証情報を入力します。初期設定のユーザ名は「sa」です。

警告： セキュリティ保護のため、SQL データベースには必ずパスワードを設定してください。

5. [Trend Micro Control Manager データベース] に Control Manager データベースの名前を入力します。初期設定では「db_ControlManager」です。

6. データベースを作成するには、[次へ] をクリックします。既存の Control Manager データベースが検出された場合には、次のオプションを使用できます。

- 既存のデータベースに新しいレコードを追加 — インストールする Control Manager ではそれまでのサーバで使用されていた設定、アカウント、およびエンティティが使用されます。また、前回のインストールに指定した root アカウントがそのまま使用されます。root アカウントを新しく作成することはできません。

注意： Control Manager 5.0 のインストール時に、旧バージョンの Control Manager データベースに対して [既存のデータベースに新しいレコードを追加する] を選択することはできません。

- 既存のレコードを削除して、新しいデータベースを作成 — 既存のデータベースは削除され、同じ名前の新しいデータベースが作成されます。
- 別名で新規データベースを作成 — 前の画面に戻ります。ここで Control Manager データベースの名前を変更することができます。

注意： 既存のデータベースにレコードを追加する場合、root アカウントを変更することはできません。root アカウントの設定画面が表示されます。

手順 6: root アカウントのセットアップと通知の設定

1. [次へ] をクリックします。次の画面が表示されます。

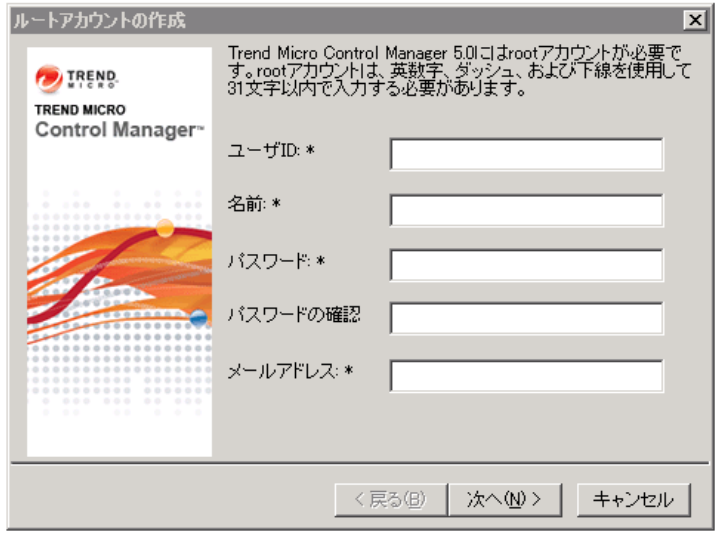


図 3-10.　root アカウントのセットアップとプロキシサーバの設定

2. 次の情報を入力してください。

   - ユーザ ID
   - 名前
   - パスワード
   - パスワードの確認
   - メールアドレス

3. [次へ] をクリックします。[メッセージルーティングパスの指定] 画面が表示されます。この画面は、ホストサーバに TMI がインストールされていない場合にのみ表示されます。

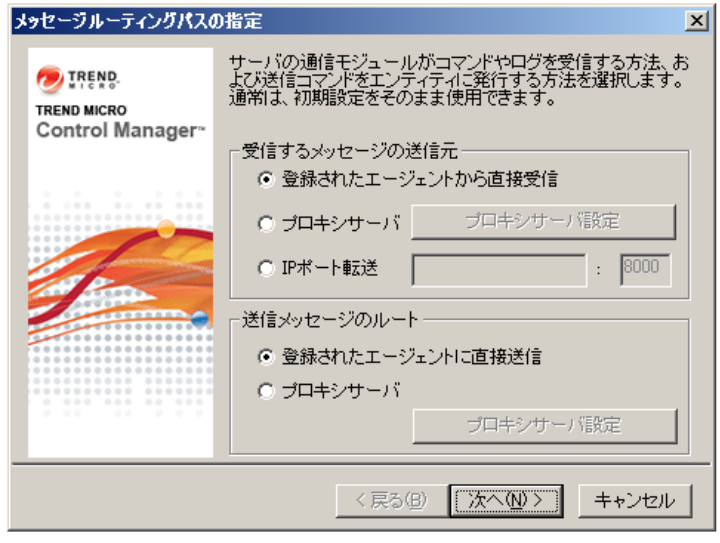


図 3-11. メッセージまたは要求のルートの定義

4. 送信メッセージと受信メッセージの送信経路を指定します。この設定によって、Control Manager は既存のセキュリティシステムを使用できるようになります。適切な送信経路を選択してください。

注意： メッセージの送信経路を設定できるのはインストール中だけです。インストール中に設定するプロキシはインターネット接続で使用されるプロキシ設定とは関係ありませんが、初期設定では同じ設定が使用されます。

受信するメッセージの送信元

- 登録されたエージェントから直接受信 — エージェントは到着したメッセージを直接受信します。
- プロキシサーバ — メッセージの受信にプロキシサーバを使用する場合は、このオプションを選択します。
- IP ポート転送 — Control Manager でファイアウォールの IP ポート転送機能が使用されるように設定します。ファイアウォールサーバの FQDN、IP アドレス、または NetBIOS 名を指定してから、通信のために開かれているポート番号を入力します。

送信メッセージのルート

- 登録されたエージェントに直接送信 — 送信メッセージはエージェントに直接送信されます。
- プロキシサーバ — 送信メッセージはプロキシサーバ経由で送信されます。

5. [完了] をクリックしてインストールを終了します。

図 3-12. セットアップの完了

正常なインストールの確認

以下の手順に従って、Control Manager サーバが正常にインストールされたかどうかを確認します。

Control Manager サーバの正常なインストールの確認

Control Manager サーバが正常にインストールされたかどうかを確認するには、次をチェックします。

Program Files¥Trend Micro ディレクトリの下に次のフォルダ構造が含まれていること

- COMMON¥TMI
- COMMON¥ccgi
- Control Manager

セットアッププログラムにより、次のサービスが作成されたこと

- Trend Micro Control Manager
- Trend Micro Common CGI
- Trend Micro Management Infrastructure
- Trend Micro Network Time Protocol

次のプロセスが実行されていること

Trend Micro Common CGI プロセス :

- jk_nt_service.exe
- java.exe

Microsoft Internet Information Server プロセス :

- inetinfo.exe

ISAPI フィルタ :

- CCGIRedirect
- ReverseProxy
- TmcmRedirect

Trend Micro Management Infrastructure プロセス :

- cm.exe (TMI-CM)
- mrf.exe (メッセージルーティングフレームワークモジュール)
- DMServer.exe (TMI-DM 全機能)

Control Manager プロセス :

- ProcessManager.exe
- LogReceiver.exe
- MsgReceiver.exe
- LogRetriever.exe
- CmdProcessor.exe
- UIProcessor.exe
- ReportServer.exe
- ntpd.exe
- DCSProcessor.exe
- CasProcessor.exe

インストール後の設定

Control Manager のインストールが完了したら、次の作業を実行することをお勧めします。

1. Control Manager のアクティベーション
2. ユーザアカウントとアカウントタイプの設定
3. 最新コンポーネントのダウンロード
4. 通知の設定

Control Manager の登録およびアクティベーション

Control Manager のインストールが正常に終了したら、管理コンソールでライセンスのステータスと有効期限をチェックしてください。これには、[運用管理]→[ライセンス管理]→[Control Manager] の順に選択します。ステータスが [アクティベート済み] でない、または期限切れの場合は、アクティベーションコードを取得して製品をアクティベートしてください (管理コンソールで [運用管理]→[ライセンス管理]→[Control Manager]→[新しいアクティベーションコードを入力してください] の順に選択します)。アクティベーションコードに関して問題がある場合は、購入先にお問い合わせください。詳細については、89 ページの「製品のアクティベーション」を参照してください。

ユーザアカウントの設定

必要と思われる Control Manager のユーザアカウントを作成します。アカウントを作成するときは次の点を考慮します。

- ユーザタイプの数 (Administrator、Power User、Operator)
- 各ユーザタイプへの適切な許可および権限の割り当て
- ユーザが階層管理構造を利用するためには、「Power User」以上の権限が必要になります。

詳細については、122 ページの「Control Manager へのユーザアクセスの設定」を参照してください。

最新コンポーネントのダウンロード

インストール完了後、トレンドマイクロのアップデートサーバから手動で最新のコンポーネントをダウンロードします。トレンドマイクロのアップデートサーバは、最新のセキュリティ保護を継続できるよう最新のコンポーネントを提供しています。Control Manager サーバとインターネットの間にプロキシサーバがある場合には、プロキシサーバを設定する必要があります (管理コンソールで [運用管理]→[設定]→[プロキシの設定] の順に選択します)。詳細については、155 ページの「新規コンポーネントのダウンロードと配信」を参照してください。

通知の設定

インストール完了後、通知を送信するイベントを設定し、重大なウイルス攻撃やセキュリティに関わるアクティビティを監視できるようにします。通知の受信者を指定するほか、通知チャネルを選択し、通知の送信が期待どおりに実行されるかどうかをテストします。管理コンソールから [運用管理]→[イベントセンター] の順に選択します。詳細については、193 ページの「イベントセンターの使用」を参照してください。

製品のアクティベーション

セキュリティアップデートファイルや製品アップデートファイルを常に最新のものにするために、Control Manager サーバのアクティベーションを実行します。

Control Manager のアクティベーション

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。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、Control Manager 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を含む全機能を使用できるようにします。

注意： Control Manager のアクティベーション実行後、変更を有効にするには、ログオフして再びログオンしてください。

Control Manager の登録およびアクティベーションを行うには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [ライセンス管理] の上にカーソルを置きます。サブメニューが表示されます。
3. [Control Manager] をクリックします。[ライセンス情報] 画面が表示されます。
4. [製品のアクティベーション] または [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。
5. [新しいアクティベーションコード] に、アクティベーションコードを入力します。
6. [アクティベート]→[OK] の順に選択します。

製品版へのアップグレード

体験版の試用期間が過ぎた後も Control Manager を引き続き使用するには、Control Manager を製品版にアップグレードしてアクティベーションを実行します。アップデート済みのプログラムコンポーネントのダウンロードを含む、全機能を使用するためには、Control Manager のアクティベーションを実行してください。

製品版にアップグレードするには

1. 製品版を購入します。購入については、トレンドマイクロの営業部または販売代理店にお問い合わせください。
2. 製品版パッケージに付属のアクティベーションコードを用意します。
3. 上記の手順に従って Control Manager のアクティベーションを実行します。

サポート契約の更新

Control Manager と、それに統合されている関連製品およびサービス (大規模感染予防サービス) のサポート契約の更新は、次のいずれかの方法で行います。

お使いの製品またはサービスのサポート契約を更新するには、新しいアクティベーションコードが必要です。アクティベーションコードについては、トレンドマイクロの営業部または販売代理店にお問い合わせください。

サポート契約の更新手順は、使用している製品が体験版か製品版かによって異なります。

[オンラインでステータスを確認] を使用して製品のサポート契約を更新するには

1. 上部のメニューで [運用管理] の上にマウスカーソルを置きます。ドロップダウンメニューが表示されます。
2. [ライセンス管理] の上にマウスカーソルを置きます。サブメニューが表示されます。
3. [Control Manager] をクリックします。[ライセンス情報] 画面が表示されます。
4. [ライセンス情報] で、[ステータス更新]→[OK] の順に選択します。
5. 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。

更新済みのアクティベーションコードを手動で入力してサポート契約を更新するには

1. 上部のメニューで [運用管理] の上にマウスカーソルを置きます。ドロップダウンメニューが表示されます。
2. [ライセンス管理] の上にマウスカーソルを置きます。サブメニューが表示されます。
3. [Control Manager] をクリックします。[ライセンス情報] 画面が表示されます。
4. 作業領域の [Control Manager ライセンス情報] で、[新しいアクティベーションコードを入力してください] リンクをクリックします。

5. [製品のアクティベーション] 画面が表示されます。
6. [新しいアクティベーションコード] に、アクティベーションコードを入力します。
7. [アクティベート] をクリックします。
8. [OK] をクリックします。

第 4 章

サーバのアップグレードおよびエージェントの移行

既存の Trend Micro Control Manager (以下、Control Manager) 3.5 を Control Manager 5.0 にアップグレードする場合には、あらかじめ慎重に検討し入念な計画を立てる必要があります。MCP または以前の Control Manager エージェントを Control Manager 5.0 サーバに移行する場合も同様です。

本章は次の内容で構成されています。

Control Manager 5.0 へのアップグレード

次の表は、スタンダード版またはアドバンス版にアップグレードする際に留意すべき点をまとめたものです。

表 4-1. Control Manager 5.0 へのアップグレード時の注意点

サポート内容	スタンダード版	アドバンス版
Control Manager 3.5 からのアップグレード	可	可
レポートの保持	不可	可
スタンダード版からアドバンス版への変更 スタンダード版からアドバンス版に変更するには、アドバンス版用のアクティベーションコードを使用して Control Manager を上書きインストールしてください。インストール中にアドバンス版用アクティベーションコードの入力が要求されます。	可	適用外
エンタープライズ / アドバンス版からスタンダード版への変更	適用外	可

Control Manager 3.5 サーバのアップグレード

Control Manager 3.5 の既存のインストールの上に Control Manager 5.0 をインストールすることをお勧めします。そうすることで、以前のすべての設定、ログ、レポート、および製品ディレクトリがそのままの状態に保たれます。ただし、アップグレードする前に、Control Manager がインストールされるサーバに十分なシステムリソースがあることを確認してください。

警告： アップグレードを実行する前に、必ず既存のサーバをバックアップしてください。

アップグレードと移行のシナリオ

Control Manager のアップグレードまたは移行では、次の 3 つのシナリオがサポートされています。

- 「シナリオ 1: Control Manager 3.5 サーバの Control Manager 5.0 へのアップグレード」
- 「シナリオ 2: エージェント移行ツールを使用した Control Manager 5.0 の新規インストールへの移行」
- 「シナリオ 3: 階層管理環境のアップグレードまたは移行」

シナリオ 1: Control Manager 3.5 サーバの Control Manager 5.0 へのアップグレード

Control Manager 3.5 を Control Manager 5.0 に直接アップグレードする場合、管理者は Control Manager をバックアップするか、または Control Manager をインストールするサーバの OS 全体をバックアップするかを選択できます。OS のバックアップにはより多くの作業が必要になりますが、データの損失を防止する上でより高度なセキュリティを提供します。

既存の Control Manager サーバとデータベースをバックアップしてアップグレードするには

1. 既存の Control Manager 3.5 データベースをバックアップします。
2. ¥Trend Micro¥CmKeyBackup¥*.* 以下のすべてのファイルをバックアップします。
3. 現在の Control Manager 3.5 サーバのすべてのフォルダをバックアップします。
4. 現在の Control Manager 3.5 サーバのレジストリをバックアップします。
5. 必要に応じて Windows Installer 3.1 をインストールします。
6. 必要に応じて MDAC 2.8 SP1 をインストールします。
7. Control Manager 3.5 上に Control Manager 5.0 を上書きインストールします。

注意： 手順 2 ～ 4 については 100 ページの表 4-3、「バックアップする必要がある Control Manager ファイル」を参照してください。

サーバの OS 全体と Control Manager データベースをバックアップしてアップグレードするには

1. 既存の Control Manager 3.5 サーバの OS をバックアップします。
2. 既存の Control Manager 3.5 データベースをバックアップします。
3. 必要に応じて Windows Installer 3.1 をインストールします。
4. 必要に応じて MDAC 2.8 SP1 をインストールします。
5. Control Manager 3.5 上に Control Manager 5.0 を上書きインストールします。

シナリオ 2: エージェント移行ツールを使用した Control Manager 5.0 の新規インストールへの移行

このシナリオには、既存の Control Manager サーバとは別のサーバに Control Manager 5.0 をインストールする作業が含まれます。これにより、以前のサーバの使用を徐々に停止することができます。エージェントの移行の詳細については、104 ページの「Control Manager エージェントの移行計画」を参照してください。

Control Manager 3.5 サーバを Control Manager 5.0 の新規インストールに移行するには

1. 既存の Control Manager 3.5 データベースをバックアップします。
2. 別のコンピュータに Control Manager 5.0 を新規インストールします。
3. エージェント移行ツールを使用して、Control Manager 3.5 サーバから Control Manager 5.0 サーバにエンティティを移行します。

注意： エージェント移行ツールは、管理下の製品の移行のみをサポートします。エージェント移行ツールでは、以前のサーバからのログ、レポート、または製品ディレクトリの移行はサポートしません。

シナリオ 3: 階層管理環境のアップグレードまたは移行

Control Manager では、2 つの方法で階層管理環境をアップグレードできます。1 つ目の方法では、Control Manager の下位サーバを登録解除し、その後再登録します。2 つ目の方法では、ファイル (CascadingUpgrade.ini) を作成して下位サーバに挿入します。

表 4-2. CascadingUpgrade.ini 変数

変数	[上位 CONTROL MANAGER の設定] 画面	説明
上位 CONTROL MANAGER の設定		
Host	サーバの FQDN または IP アドレス	Control Manager 上位サーバのホスト名または IP アドレス。
Port	ポート	プロキシサーバとの通信に使用されるポート番号。
Protocol	HTTPS による接続	Control Manager 上位サーバとの通信に使用されるプロトコル。
WebServerUser	Web サーバ認証	Web サーバ認証に必要なユーザ名。
WebServerPassword		Web サーバ認証に必要なパスワード。

表 4-2. CascadingUpgrade.ini 変数

変数	[上位 CONTROL MANAGER の設定] 画面	説明
MCP プロキシの設定		
Enable	上位 Control Manager サーバとの通信にプロキシサーバーを使用する	プロキシサーバを使用するには「1」を指定します。プロキシサーバを使用しない場合は「0」を指定します。
Type	プロキシのプロトコル	プロキシサーバとの通信に使用されるプロトコル。
Host	サーバの名前または IP アドレス	プロキシサーバのホスト名または IP アドレス。
Port	ポート	プロキシサーバとの通信に使用されるポート番号。
ProxyServerUser	プロキシサーバ認証	プロキシサーバ認証に必要なユーザ名。
ProxyServerPassword		プロキシサーバ認証に必要なパスワード。

下位サーバの登録解除により階層管理環境をアップグレードまたは移行するには

1. Control Manager 上位サーバから、すべての下位サーバを登録解除します。
2. Control Manager 上位サーバをバックアップします。
3. Control Manager のすべての下位サーバをバックアップします。
4. Control Manager 上位サーバをアップグレードします。
5. Control Manager のすべての下位サーバをアップグレードします。
6. Control Manager のすべての下位サーバを上位サーバに登録します。

CascadingUpgrade.ini を使用して階層管理環境をアップグレードまたは移行するには

1. Control Manager 上位サーバをバックアップします。
2. Control Manager のすべての下位サーバをバックアップします。
3. テキストエディタを使用して次のファイルを作成します。

   CascadingUpgrade.ini ファイル
   CascadingUpgrade.ini ファイルには次の形式を使用します。

```
[Common]
Host=
Port=
Protocol=
WebServerUser=
WebServerPassword=

[Proxy]
Enable=
Type=
Host=
Port=
ProxyServerUser=
ProxyServerPassword=
```

4. Control Manager の各下位サーバの Control Manager フォルダに、CascadingUpgrade.ini ファイルを挿入します。
5. Control Manager 上位サーバをアップグレードします。
6. Control Manager のすべての下位サーバをアップグレードします。

表 4-3.　バックアップする必要がある Control Manager ファイル

CONTROL MANAGER 3.5 情報	パス
データベース	SQL Enterprise Manager または osql を使用して Control Manager データベースをバックアップします。詳細については、Control Manager のオンラインヘルプを参照してください。
認証情報 (Control Manager が復元された場合に、特定の Control Manager サーバに通知していた管理下の製品が、同じサーバに通知するように指定します)	¥Program Files¥Trend Micro¥CmKeyBackup
設定ファイル	¥Program Files¥Trend Micro¥Control Manager¥Settings¥*.* ¥Program Files¥Trend Micro¥Control Manager¥DataSource.xml ¥Program Files¥Trend Micro¥Control Manager¥CascadingLogConfiguration.xml ¥Program Files¥Trend Micro¥Control Manager¥Settings¥DMregisterinfo.xml ¥Program Files¥Trend Micro¥Control Manager¥EntityEmulator.xml ¥Program Files¥Trend Micro¥Control Manager¥ProductUIHandler.xml ¥Program Files¥Trend Micro¥Control Manager¥SystemConfiguration.xml
GUID 情報	¥Program files¥Trend Micro¥COMMON¥TMI¥TMI.cfg の GUID の値
管理下の製品情報	¥Program Files¥Trend Micro¥COMMON¥TMI¥mrf_entity.dat ¥Program Files¥Trend Micro¥COMMON¥TMI¥mrf_entity.bak
アップデート関連ファイル	¥Program Files¥Trend Micro¥Control Manager¥webui¥download¥activeupdate

表 4-3.　バックアップする必要がある Control Manager ファイル

CONTROL MANAGER 3.5 情報	パス
Control Manager レジストリ	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥TVCS HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥TMI HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥CommonCGI HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥TMCM HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥TMI HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥MSDE HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥MSDE HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥MSSQLServer HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TMCM HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendMicro_NTP HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendMicro Infrastructure HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendCCGI HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥MSSQLServer

Control Manager 3.5 へのロールバック

Control Manager 5.0 へのアップグレードに失敗した場合、次の手順で Control Manager 3.5 システムに戻します。

シナリオ 1: Control Manager 5.0 サーバから Control Manager 3.5 へのロールバック

Control Manager サーバおよびデータベースのバックアップからロールバックするには

1. Control Manager 5.0 サーバを削除します。
2. Control Manager 3.5 サーバをインストールします。
3. バックアップしたデータベースで、Control Manager 3.5 データベースを復元します。
4. バックアップしたフォルダで、Control Manager3.5 のすべてのフォルダを復元します。
5. バックアップしたレジストリで、Control Manager 3.5 レジストリを復元します。
6. ¥Trend Micro¥CmKeyBackup¥*.* 以下のすべてのファイルを復元します。
7. Control Manager 3.5 の Service Pack と HotFix を適用します。
8. 以前の証明書をインポートします。

サーバの OS 全体と Control Manager データベースのバックアップからロールバックするには

1. バックアップしたデータベースで、Control Manager 3.5 データベースを復元します。
2. バックアップした OS で、サーバの OS を復元します。

シナリオ 2: エージェント移行ツールを使用した Control Manager 5.0 の新規インストールからのロールバック

エージェントの移行の詳細については、104 ページの「Control Manager エージェントの移行計画」を参照してください。

Control Manager 5.0 の新規インストールから Control Manager 3.5 サーバにロールバックするには

1. バックアップしたデータベースで、Control Manager 3.5 データベースを復元します。
2. エージェント移行ツールを使用して、Control Manager 5.0 サーバから Control Manager 3.5 サーバにエンティティを移行します。

シナリオ 3: 階層管理環境のロールバック

下位サーバの登録解除により階層管理環境をロールバックするには

1. Control Manager 上位サーバから、すべての下位サーバを登録解除します。
2. Control Manager 上位サーバをロールバックします。
3. Control Manager のすべての下位サーバをロールバックします。
4. Control Manager の Service Pack と HotFix を適用します。
5. Control Manager のすべての下位サーバを上位サーバに登録します。

アップグレードに CascadingUpgrade.ini を使用した階層管理環境をロールバックするには

1. Control Manager 上位サーバから、すべての下位サーバを登録解除します。
2. Control Manager 上位サーバをロールバックします。
3. Control Manager のすべての下位サーバをロールバックします。
4. Control Manager の Service Pack と HotFix を適用します。
5. Control Manager のすべての下位サーバを上位サーバに登録します。

Control Manager エージェントの移行計画

Control Manager 5.0 サーバにエージェントを移行するには、次の 2 つの方法があります。

- 一括アップグレード

  一括アップグレードは、次の方法で行われます。

  表 4-4.　一括アップグレード

移行元	処理
サーバ : Control Manager 3.5/5.0 **エージェント** : MCP	MCP エージェントを Control Manager 5.0 サーバに登録します。MCP エージェントは移行前の製品ディレクトリ構造を維持します。
サーバ : Control Manager 3.5/5.0 **エージェント** : **エージェントの混在**	Control Manager エージェント : Control Manager 2.5x エージェントが Control Manager 5.0 サーバに登録されます。移行前の Control Manager の製品ディレクトリ構造は、移行後も維持されます。 MCP MCP エージェントを Control Manager 5.0 サーバに登録します。MCP エージェントは移行前の製品ディレクトリ構造を維持します。

  この方法は、出荷時の設定で使用している場合や比較的小規模なネットワークで運用しているエージェントの移行 (できれば、テスト環境) に推奨します。48 ページの「テストインストール」を参照してください。しかし、一度開始した移行処理は中止できないため、この方法は小規模の配信に最適で、ネットワークの規模が大きいほど難度も高くなります。

- 段階的アップグレード

  単一サーバを大規模な Control Manager 3.5 システムで運用している場合、段階的なアップグレードをお勧めします。また、複数のサーバが存在するネットワークの

場合にはこの方法が必須です。この方法では、より体系的にシステムを移行することができます。移行作業は、次の方針に基づいて進めます。

- 既存のネットワークの中で最も移行の影響が小さいと思われるシステムで、まず移行を実施します。その後、より影響が大きいシステムの移行を順次実行します。
- 十分に計画を立てた後、1 度にすべての移行手順を実行するのではなく、1 つずつ手順を実行します。

  そうすることによって、移行中に問題が発生した場合に問題解決のための作業を最小限にすることができます。

段階的アップグレードを実施するには、次の手順に従ってください。

a. 以前の Control Manager バージョンがインストールされていないサーバに Control Manager 5.0 をインストールします。

b. Control Manager 5.0 サーバの AgentMigrateTool.exe を実行します。

Control Manager エージェントインストールと「エージェント移行ツール (AgentMigrateTool.exe) の使用」を合わせて利用し、既存の Control Manager システム上でのエージェントアップグレード計画を立ててください。エージェント移行ツールの利用により、Control Manager エージェントが登録されているサーバのリストを生成することができます。これにより、移行元サーバを手動で選択する必要がなくなります。

Control Manager 2.x エージェントの移行シナリオ

次のようなエージェントの移行シナリオが考えられます。

- 単一サーバの移行

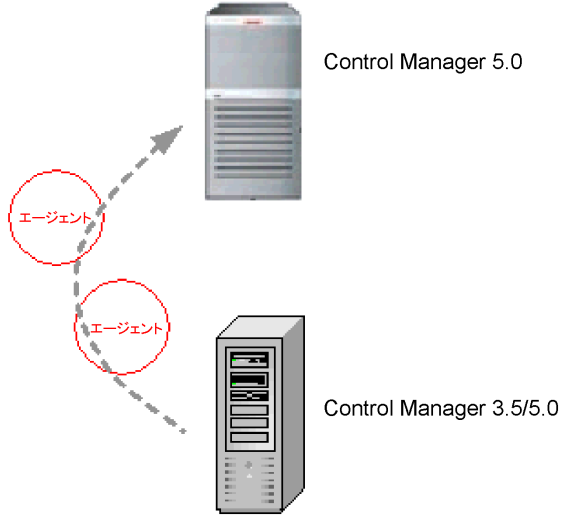


図 4-1.　単一サーバに属するエージェントの移行

この場合は、高速または段階的な移行モードを使用できます。94 ページの「Control Manager 5.0 へのアップグレード」を参照してください。

- さまざまなサーバ / エージェントの統合

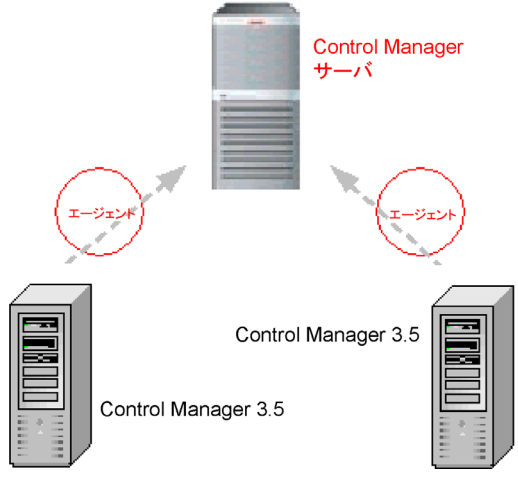


図 4-2.　複数のサーバに属するエージェントの移行

Control Manager のユーザ管理機能を使用して、Control Manager 管理下のシステムへのアクセス権をユーザごとに設定することができます。以前は拠点ごとにユーザのアクセスを限定する場合、各拠点に Control Manager サーバを配置することが必要でしたが、1 台の Control Manager サーバで、管理下のシステム全体のユーザアクセスを管理できるようになりました。

Control Manager 2.5 エージェントの移行フロー

Control Manager 2.5 エージェントの移行にあたり、エージェント移行ツールは次のことを実行します。

1. Trend Micro Management Infrastructure サービスの停止
2. Control Manager 3.5 サーバから製品ディレクトリ情報の取得
3. Control Manager 3.5 データベースおよび TMI.cfg からエージェント情報の削除
4. アップグレードが行われていない Control Manager 2.5x エージェントバージョンの保持

5. Control Manager 5.0 データベースおよび TMI.cfg へのエージェント情報の書き込み
6. Trend Micro Management Infrastructure サービスの再起動

Control Manager 2.5x エージェントの移行に失敗した場合、AgentMigrateTool.exe は Control Manager 5.0 データベースと TMI.cfg からエージェント情報を削除し、Control Manager 3.5 データベースにそれらを再び書き込みます。

MCP エージェント移行フロー

MCP の移行中にエージェント移行ツールは以下を実行します。

1. 移行先サーバの Trend Micro Management Infrastructure (TMI) サービスを停止します。
2. Control Manager サーバから製品ディレクトリ情報を取得します。
3. アップグレードが行われていない Control Manager エージェントバージョンを保持します。
4. エージェントの情報を移行先サーバのデータベースに書き込みます。
5. 移行先サーバの Trend Micro Management Infrastructure (TMI) サービスを再起動します。
6. 移行先サーバの Trend Micro Control Manager サービスを停止してから再起動します。
7. 移行元サーバに Change Server コマンドの発行を要求し、MCP エージェントによるポーリングを待機します。

Control Manager 2.5x および MCP エージェントの移行

AgentMigrateTool.exe を使用し、Control Manager 3.5 サーバ、または Control Manager 5.0 サーバが管理していた Windows ベースのエージェントを移行します。エージェントを移行する際は、2.5x エージェントを先に移行し、次に MCP を移行します。

エージェントの移行が失敗すると以下のことが起こります。

- エージェントは引き続き移行元のサーバに管理されます。
- エージェントのログが移行元と移行先の両方のサーバに記録されます。

移行されたログは、エージェントが移行先のサーバに登録されるまでログを表示しません。移行先の Control Manager サーバは、削除がトリガされると移行ログを削除します。

注意： エージェントの移行先となる Control Manager 5.0 サーバで直接、AgentMigrateTool.exe を実行します。

Control Manager 2.5x または MCP エージェントを移行するには

1. Windows エクスプローラを使用して、Control Manager 5.0 のインストールフォルダを開きます。次に例を示します。

   ```
   C:¥Program Files¥Trend Micro¥Control Manager¥
   ```

2. AgentMigrateTool.exe をダブルクリックします。

注意： 移行先の Control Manager サーバの Remote Registry サービスを起動することを覚えておいてください。そうでないと移行は成功しません。

3. 上部のメニューで [移行元サーバの設定] を選択します。
4. [移行元サーバの設定] 画面で、移行元サーバの IP アドレスを入力します (移行するエージェントがホストされている、Control Manager 3.5、または Control Manager 5.0 のいずれかのサーバ)。

5. [システム管理者のアカウント] に移行先サーバへのアクセスに使用される管理者ユーザ名とパスワードを入力し、[接続] をクリックします。

6. メイン画面で [追加] か [すべて追加] をクリックし、エージェントを移行元から移行先のリストに移します。

7. 次のオプションのすべてまたはいずれかを選択します。

   - **ツリー構造を保持する** — 移行先サーバ、つまり Control Manager 5.0 サーバで、選択された管理下の製品の移行前の製品ディレクトリ構造が保持されます。
   - **ログを移行する** — AgentMigrateTool.exe により、選択した管理下の製品のログが移行元から移行先のサーバにコピーされます。
   - **HTTPS を有効にする** — AgentMigrateTool.exe により、HTTPS を使用して Control Manager に登録するよう移行エージェントに通知されます。このオプションを選択しない場合、エージェントは Control Manager の登録に HTTP を使用します。

     これらのオプションは、移行先リストに一覧表示されるエージェントに適用できます。

ヒント： 移行元サーバのすべてのエージェントを移行しようとする場合には、[ツリー構造を保持する] と [ログを保持する] のオプションを両方とも選択することをお勧めします。

Control Manager 2.1 エージェントを使用する管理下の製品を移行すると、移行先のサーバでは、移行された管理下の製品の古いログを検索することができません。AgentMigrateTool.exe を実行する前に、Control Manager 2.5 エージェントにアップグレードすることを推奨します。

InterScan Messaging Security Suite 5.1 Windows 版は、Control Manager 2.1 エージェントを使用しています。

- InterScan eManager 3.50 (適用可能なすべてのプラットフォーム)
- InterScan eManager 3.52 (適用可能なすべてのプラットフォーム)

- ScanMail eManager 5.0 (適用可能なすべてのプラットフォーム)
- ScanMail eManager 5.1 (適用可能なすべてのプラットフォーム)
- InterScan Messaging Security Suite 5.1 for Windows

8. [移行] をクリックします。

確認メッセージが表示されたら [OK] をクリックします。移行先のリストに並んでいるエージェントが移行されます。

Control Manager データベースの移行

Control Manager データベースを移行するには、次の 2 つの方法があります。

- Control Manager 3.5 サーバに Control Manager 5.0 をインストール。トレンドマイクロの推奨する方法です。

  Control Manager 5.0 セットアップにより、データベースは自動的にバージョン 5.0 にアップグレードされます。詳細については、-107 ページの「Control Manager 2.5 エージェントの移行フロー」を参照してください。

- Control Manager 3.5 データベースを Control Manager 5.0 サーバに手動で移行

Control Manager SQL 2005 データベースの他の SQL 2005 Server への移行

TMI.cfg ファイル内の設定を変更することで、SQL 2005 Server 間で Control Manager データベースを移動できます。

既存のデータベースを他の SQL 2005 Server に移行するには

1. Windows サービスを使用し、次の Control Manager サービスを停止します。
   - Trend Micro Management Infrastructure
   - Trend Micro Common CGI
   - Control Manager
2. 現在の SQL Server から新しい SQL Server に Control Manager データベースをコピーします。

   注意： Control Manager はデータベース認証用のユーザ名およびパスワードを暗号化します。db_ControlManager へのアクセスに使用するアカウントと同じ認証アカウントを新しい SQL Server に設定し、同じ ID とパスワードの組み合わせをそのまま使用することをお勧めします。
3. [スタート] メニューから、[プログラム]→[管理ツール]→[データソース (ODBC)] の順に選択し、ODBC データソースアドミニストレータを開きます。
4. [システム DSN] タブをクリックし、[ControlManager_DataBase] データソースを選択し、[構成] をクリックします。
5. [Microsoft SQL Server 用の DSN の設定] で、移行先サーバを選択して [接続する SQL Server サーバー名を入力してください。] の値を変更し、[次へ] をクリックします。

   移行先サーバがリストになければ、「サーバ名」を入力します。
6. 次の画面で、[ユーザーが入力する SQL Server 用のログイン ID とパスワードを使う] オプションと [SQL Server に接続して追加の構成オプションの既定設定を取得する] オプションを選択します。

7. Control Manager のインストール時 (P.78: 図 3-9. Control Manager データベースの選択) に登録した「ID」(ユーザ名) と「パスワード」を入力し、[次へ] をクリックします。
8. [完了] をクリックして新しい設定を保存し、[Microsoft SQL Server DSN 設定] 画面を閉じます。
9. [OK] をクリックし、ODBC データソースアドミニストレータを閉じます。
10. Windows サービスを使用し、すべての Control Manager サービスを再起動します。

管理コンソールにログオンして製品ディレクトリを参照し、すべての管理下の製品が登録されているか確かめます。問題なく登録されていれば、データベースは新しい SQL Server に正常に移行されています。

第 5 章

Control Manager システムの管理

Trend Micro Control Manager (以下、Control Manager) では、Web ベースの管理コンソールを使用して、管理下の製品と他の Control Manager サーバを管理できます。

本章は次の内容で構成されています。

管理コンソールの使用

管理コンソールは、次の要素で構成されています。

- **上部のメニュー** — Control Manger および管理下の製品を管理するための [ホーム]、[製品]、[サービス]、[ログ / レポート]、[アップデート]、および [運用管理] メニューへのリンクを提供します。また、Control Manager のオンラインヘルプ、トレンドマイクロの製品 Q & A、セキュリティ情報、および Control Manager の [バージョン情報] 画面へのリンクを提供します。
- **作業領域 (右側の画面)** — 管理下の製品または下位サーバ設定の管理、タスクの起動、またはシステムステータス、ログ、およびレポートの表示を実行する領域です。

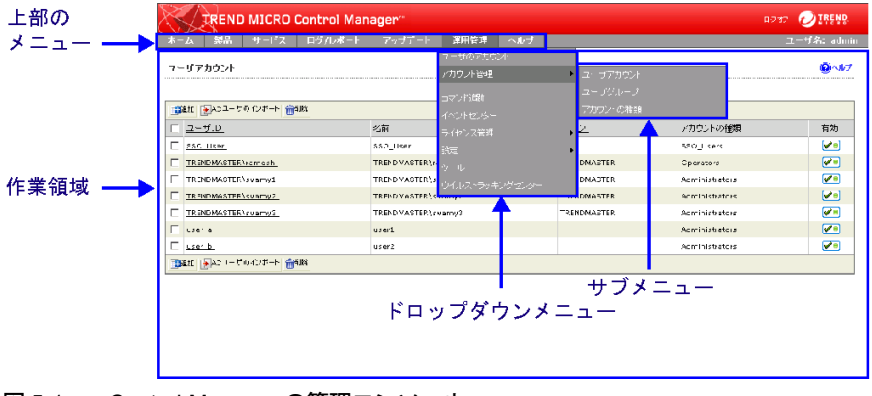


図 5-1.　Control Manager の管理コンソール

表 5-1.　上部のメニューの項目

上部のメニュー	
ホーム	ネットワークの概要が表示されます。また、詳細情報画面およびレポートへのショートカットが提供されます。
製品	管理下の製品、コミュニケータ、および下位サーバを管理するためのオプションが含まれています。
サービス	トレンドラボからのメッセージと使用可能なサービス (大規模感染予防サービスおよび脆弱性診断サービス) の概要が表示されます。

表 5-1.　上部のメニューの項目

上部のメニュー	
ログ / レポート	Control Manager 管理下の製品と下位サーバのレポートを管理するためのオプションと、Control Manager サーバに登録されているすべての製品のログを表示するためのオプションが含まれています。
アップデート	手動アップデート、事前予約アップデート、およびコンポーネント配信の各計画を設定するためのオプションが含まれています。
運用管理	コマンド追跡、イベントセンター、アカウント管理設定、ライセンス管理設定、接続設定、およびツールの各オプションが含まれています。
ヘルプ	次の各情報が提供されます。 ・機能および設定方法についての詳細な説明 ・トレンドマイクロのサポートチームが提供する技術的な製品情報と対処方法 ・最新のウイルスプログラムに関する警告と、現在危険性の高い上位 10 のウイルスプログラムのリスト ・Control Manager のバージョン、ビルド番号、および著作権情報

ロックのメカニズムについて

管理コンソールは、2 人のユーザが同時に同じ画面と機能にアクセスできないようにする、ロックのメカニズムを備えています。次の表は、管理コンソールのあるオプションが使用中のときに、Control Manager によってロックされる機能を示しています。

表 5-2.　ロックのメカニズム

使用中の機能	ロックされる機能
アカウント管理	アカウント管理 ディレクトリ管理
ディレクトリ管理	アカウント管理 ディレクトリ管理
エージェント通信スケジュール	エージェント通信スケジュール
接続ステータス設定	接続ステータス設定

つまり、ユーザ a がディレクトリ管理を使用して管理下の製品を編成しているときには、管理コンソールにログオンしている別のユーザ b は、ディレクトリ管理オプションとユーザ管理オプションにアクセスできません。

ロックされたオプションにアクセスしようとすると、そのオプションの情報画面が表示されます。その画面には、次の情報が表示されています。

- ユーザ ID
- アクセスしているユーザが Control Manager サーバにログオンした日付と時刻
- Control Manager の管理コンソールへのアクセスに使用したコンピュータの IP アドレス

アクセスしようとした機能が使用中であるかどうかを確認するには、定期的に [表示更新] をクリックしてください。

注意： Administrator 権限のアカウントは、他のユーザが使用している機能をロック解除して強制的にログオフさせることができます。これを実行するには、ロックされたオプションの情報画面で [解除] をクリックしてください。

ロックされた機能からログオフされたユーザが再びアクセスしようとした場合は、「ログオンセッションが無効になりました」というダイアログボックスが表示されます。[OK] をクリックすると、管理コンソールのログオン画面が表示されます。

管理コンソールへのアクセス

管理コンソールにアクセスするには、次の 2 つの方法があります。

- Control Manager サーバから直接アクセス

Control Manager サーバから管理コンソールに直接アクセスするには

a. Windows の [スタート] メニューから、[プログラム]→[Trend Micro Control Manager]→[Trend Micro Control Manager] の順に選択します。

b. ユーザ ID とパスワードを入力します。

c. [ログオン] をクリックします。

- リモートアクセス

Internet Explorer を使用して管理コンソールにリモートアクセスするには

a. ブラウザのアドレスフィールドに次の URL を入力して、[ログオン] 画面を開きます。

   http(s)://{ ホスト名 }/WebApp/

   { 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。

b. ユーザ ID とパスワードを入力します。

c. [ログオン] をクリックします。

コンソールを開くと、使用している Control Manager システム全体のステータスの概要が、初期画面に表示されます。この概要は、製品ディレクトリで生成されるステータスの概要と同じものです。ユーザの権限によって、アクセスできる Control Manager 機能が決まります。

注意 : アクセスできる管理コンソールのインスタンスは 1 つだけです。Control Manager では、1 つのコンピュータ上で 2 つ以上のブラウザを使用して同じ Control Manager 管理コンソールにアクセスすることはできません。

管理コンソールへの HTTPS アクセスの設定

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。

Control Manager 管理コンソールへの HTTPS アクセスを設定するには

1. 証明書発行機関 (http://www.VeriSign.com など) から「Web サイト証明書」を取得します。

2. [スタート] メニューから、[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。
3. 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。
4. [既定の Web サイト] を選択して、[プロパティ] を右クリックします。
5. [既定の Web サイト] で [ディレクトリセキュリティ] タブを選択して [サーバ証明書] をクリックし、新しいサーバ証明書を使ってサーバ証明書要求を作成します。

   a. [次へ] をクリックします。
   b. [サーバ証明書] 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。
   c. 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。
   d. キーのパスワードを指定し、[次へ] をクリックします。
   e. [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。

6. [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。
7. [既定の Web サイト] リストから「Control Manager」仮想ディレクトリを選択して、[プロパティ] を右クリックします。
8. [ディレクトリセキュリティ] タブを選択して、[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] ウィンドウが開きます。

   a. [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。
   b. [OK] をクリックして、[セキュリティ保護された通信] ウィンドウを閉じます。

9. [OK] をクリックして、[既定の Web サイト] リストに戻ります。

次回 HTTPS 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、セキュリティチャンネルを通して表示される必要があります。

HTTPS 管理コンソールへのアクセス

Web ベースのコンソールから Control Manager サーバに、設定データを暗号化して渡す場合は、Control Manager での Web アクセスに HTTP を指定してから、ポート 443 経由で HTTPS プロトコルを使用するように管理コンソールの URL を変更します。暗号化通信用 (HTTPS) の URL は、次の形式で入力してください。

https://{ホスト名}:443/ControlManager

ここで、

{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。

443 は、HTTPS セッション中に割り当てられるポートです。

安全な Control Manager サイトにアクセスすると、そのサイトから自動的に証明書が送信され、Internet Explorer のステータスバーにロックアイコン ( ) が表示されます。

管理コンソールからのログオフ

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。

- ヘッダ上の [ログオフ] をクリックします。
- <Ctrl>+<W> キーを押します。

Control Manager へのユーザアクセスの設定

Control Manager のユーザ管理が変更され、次の 4 つのセクション構成になりました。

表 5-3.　Control Manager ユーザアカウントのオプション

セクション	説明
ユーザのアカウント	[ユーザのアカウント] 画面には、特定のユーザに対して Control Manager が持っているすべての情報が表示されます。 [ユーザのアカウント] 画面に表示される情報は、ユーザごとに異なります。
ユーザアカウント	[ユーザアカウント] 画面には、Control Manager のすべてのユーザが表示されます。また、この画面では、Control Manager のユーザアカウントを作成および管理するための機能が提供されます。 これらの機能を使用して、アクセス権を設定し、ユーザが実行できる処理を制限することによって、ユーザの責任範囲を明確に定義できます。機能は次のとおりです。 ・実行 ・設定 ・ディレクトリ編集
ユーザグループ	[ユーザグループ] 画面には Control Manager のグループが表示され、グループを作成するためのオプションが提供されます。 Control Manager では、ユーザグループは、個々にユーザを選別することなく、複数のユーザに対して効率的に通知を送信するための方法として使用されます。Control Manager では、同じアクセス権限を共有するグループを作成することはできません。
アカウントの種類	[アカウントの種類] 画面には、Control Manager のすべてのユーザの役割が表示されます。また、Control Manager のユーザの役割を作成および管理するための機能が提供されます。 ユーザの役割により、ユーザがアクセス可能な Control Manager 管理コンソールの領域が定義されます。

ヒント：ユーザごとに異なるアクセス権と権限を割り当てることにより、セキュリティを損なうことなく、特定の管理タスクを委任することができます。

アカウントの種類について

これまでのバージョンの Control Manager には、次の 4 種類のユーザアカウントがありました。Control Manager 5.0 では、これらのアカウントの種類は初期設定のアカウントの種類として使用されます。

- Operator
- Power User
- Administrator/Root

Control Manager 5.0 では、アカウントの種類のカスタマイズが導入されます。アカウントの種類のカスタマイズにより、Control Manager 管理者は上記以外のユーザにアクセスを許可する Control Manager 管理コンソールのメニュー項目を指定できます。初期設定のアカウントの種類が持つアクセス権限は変更できません。

ヒント： アカウントの種類の設定とユーザアカウントの設定は、次の順序で実行することををお勧めします。

1. ユーザがアクセス可能な製品 / ディレクトリを指定します (138 ページの「ユーザアカウントを編集するには」の手順 8 を参照)。

2. ユーザがアクセス可能なメニュー項目を指定します (初期設定のアカウントの種類が適切でない場合、126 ページの「アカウントの種類を追加するには」または 128 ページの「アカウントの種類を編集するには」を参照)。

3. 各ユーザのアカウントのアカウントの種類を指定します (138 ページの「ユーザアカウントを編集するには」の手順 7 を参照)。

次の表は、初期設定の各アカウントで使用できる機能についてまとめたものです。

表 5-4.　ユーザアカウントのアクセス

メニュー項目			OPERATOR	POWER USER	ADMINISTRATOR
ホーム			●	●	●
製品			●	●	●
サービス					●
ログ / レポート	新規アドホッククエリ			●	●
	保存されたアドホッククエリ			●	●
	ユーザのレポート		●	●	●
	1 回限りのレポート			●	●
	予約レポート			●	●
	設定	ログ集約			●
		ログ管理			●
		レポート管理		●	●
アップデート	手動ダウンロード			●	●
	予約ダウンロード			●	●
	コンポーネントリスト			●	●
	配信計画			●	●
	設定	予約ダウンロードの除外設定		●	●
		アップデート / 配信の設定		●	●

表 5-4.　ユーザアカウントのアクセス

メニュー項目			OPERATOR	POWER USER	ADMINISTRATOR
運用管理	ユーザのアカウント		●	●	●
	アカウント管理	ユーザアカウント			●
		ユーザグループ		●	●
		アカウントの種類			●
	コマンド追跡			●	●
	イベントセンター				●
	ライセンスの管理	管理下の製品			●
		Control Manager			●
	設定	エージェントの通信スケジュール			●
		上位 Control Manager の設定			●
		イベントセンターの設定			●
		接続ステータスの設定			●
		プロキシ設定			●
		タイムアウトの設定			●
		製品エージェントの追加 / 削除	●	●	●
	ツール				●
	ウイルストラッキングセンター				●

root アカウントについて

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 権限および Administrator 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、管理下の製品に対してエージェントをインストールできます。

root アカウントには、他にも次の権限があります。

- サーバ上のすべてのユーザアカウントを表示できるのは、root アカウントだけです。その他のアカウントは、子アカウントのみ表示できます。
- root アカウントは、他のユーザが使用している機能をロック解除して、強制的にログオフさせることができます。

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。

アカウントの種類の追加

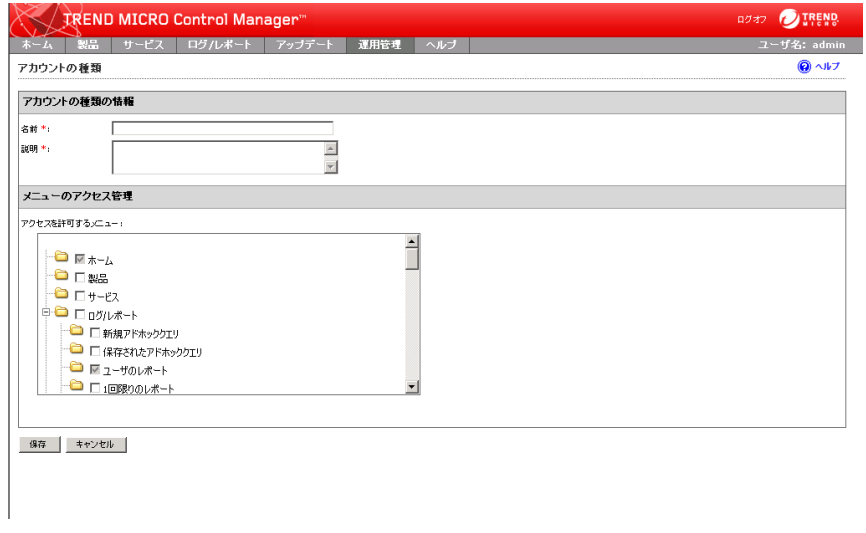
初期設定のアカウントの種類が管理者の要件を満たさない場合は、独自のアカウントの種類を作成できます。アカウントの種類をユーザ定義することにより、Control Manager 管理コンソールのすべての要素に対して権限を設定できます。

アカウントの種類を追加するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューの [アカウントの種類] をクリックします。[アカウントの種類] 画面が表示されます。

4. [追加] をクリックします。[アカウントの種類] 画面が表示されます。



5. [名前] に一意のアカウントの種類の名前を入力します。

6. [説明] にアカウントの種類の説明を入力します。

ヒント： この説明は [アカウントの種類] リストに表示されます。アカウントの種類の名前が、対象とするユーザを完全に表していない場合、意味がわかるような説明を入力することで、アカウントの種類の識別に役立てることができます。

7. そのアカウントの種類がアクセス可能なメニュー項目を選択します。[ホーム]、[ユーザのレポート]、および [ユーザのアカウント] のメニュー項目は、どのアカウントの種類でもアクセスできます。

8. [保存] をクリックします。[アカウントの種類] 画面が表示され、[アカウントの種類] リストに新しいアカウントの種類が表示されます。

アカウントの種類の編集

アカウントの種類が要件に合わず、いくつかの変更が必要になったときは、アカウントの種類を編集します。

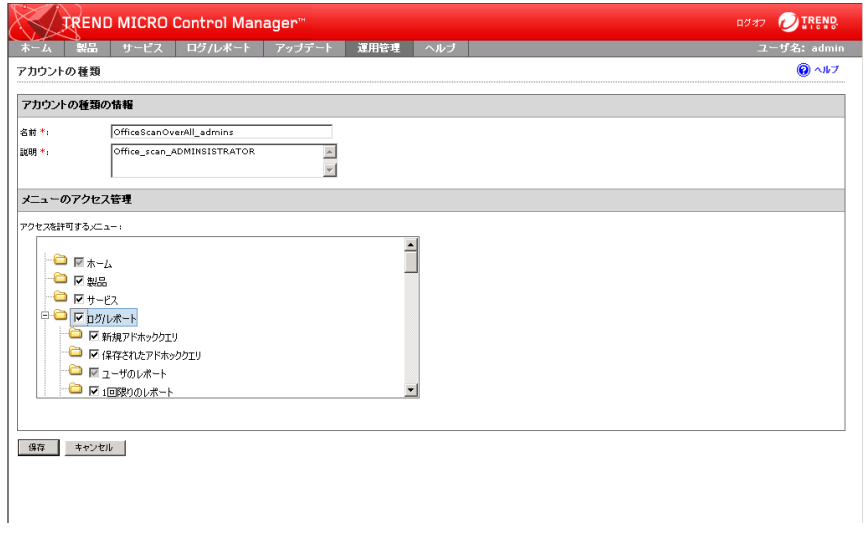
アカウントの種類を編集するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューの [アカウントの種類] をクリックします。[アカウントの種類] 画面が表示されます。

4. [名前] 列で、編集するアカウントの種類をクリックします。対応する [アカウントの種類] 画面が表示されます。



5. 必要に応じて、アカウントの種類の情報を編集します。

6. [保存] をクリックします。[アカウントの種類] 画面が表示され、[アカウントの種類] リストに編集したアカウントの種類が表示されます。

ユーザアカウントについて

管理者は、[ユーザアカウント] 画面の機能を使用して、特定の管理下の製品へのアクセス権を制限し実行できるアクションを限定することで、ユーザの責任範囲を明確に定義できます。

ヒント：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が該当します。

例 : Bob と Jane は、ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) の管理者です。両者のアカウントの種類が持つ権限は同じです (管理コンソールの同じメニュー項目にアクセスできます)。Jane は、すべてのウイルスバスター Corp. サーバに対する操作を監視しています。一方、Bob は、マーケティング部門のデスクトップを保護するウイルスバスター Corp. サーバに対する操作のみを監視しています。この場合、両者が管理コンソールに表示できる情報は異なります。Bob がログオンして参照できる情報は、Bo b の Control Manager ユーザアカウントでアクセス可能なウイルスバスター Corp. サーバ (マーケティング部門用のウイルスバスター Corp. サーバ) に関する情報のみです。一方、Jane の Control Manager ユーザアカウントには Control Manager に登録済みのすべてのウイルスバスター Corp. サーバに対するアクセス権が付与されているため、Jane はログオン時に、すべてのウイルスバスター Corp. サーバに関する情報を参照できます。

アクセス権の設定

ユーザのアクセス権によって、製品ディレクトリ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、実行権のみをユーザに与えた場合には、実行権に関連するオプションのみが製品ディレクトリに表示されます。

各ユーザアカウントには、次のアクセス権を設定することができます。

表 5-5. Control Manager ユーザアカウントのオプション

セクション	説明
実行	指定されたフォルダ内の管理下の製品に対して、[ScanNow] などのコマンドを実行するための権限です。この権限には、次のオプションが関連付けられています。 ・ScanNow ・パターンファイル / テンプレートの配信 ・リアルタイム検索 ・プログラムファイル配信 ・エンジンの配信 ・ライセンスプロファイルの配信
設定	指定されたフォルダ内の管理下の製品の設定用コンソールにアクセスするための権限です。この権限を持っているユーザに対しては、< 管理下の製品 > の一般的な設定機能、および製品固有のオプション (たとえば、ウイルスバスター Corp. のパスワード設定機能) がメニュー上に表示されます。
ディレクトリ編集	ユーザがアクセス可能な管理下の製品 / ディレクトリの構成を変更するための権限です。

注意： これらのオプションが表示されるかどうかは、製品のプロファイルによっても異なります。たとえば、eManager のように、製品に検索機能がない場合には、[ScanNow] オプションは製品ツリーのタスクメニューに表示されません。

ユーザアカウントの追加

次のタスクを実行するときは、ユーザアカウントを追加します。

- 他のユーザに対して、アクセスできる製品 / ディレクトリを指定するとき
- 他のユーザに対して、Control Manager 管理コンソールへのログオンを許可するとき
- 特定のユーザを通知受信者リストに指定するとき
- 特定のユーザをユーザグループに追加するとき

ヒント： アカウントの種類の設定とユーザアカウントの設定は、次の順序で実行することををお勧めします。

1. ユーザがアクセス可能な製品 / ディレクトリを指定します (138 ページの「ユーザアカウントを編集するには」の手順 8 を参照)。

2. ユーザがアクセス可能なメニュー項目を指定します (初期設定のアカウントの種類が適切でない場合、126 ページの「アカウントの種類を追加するには」または 128 ページの「アカウントの種類を編集するには」を参照)。

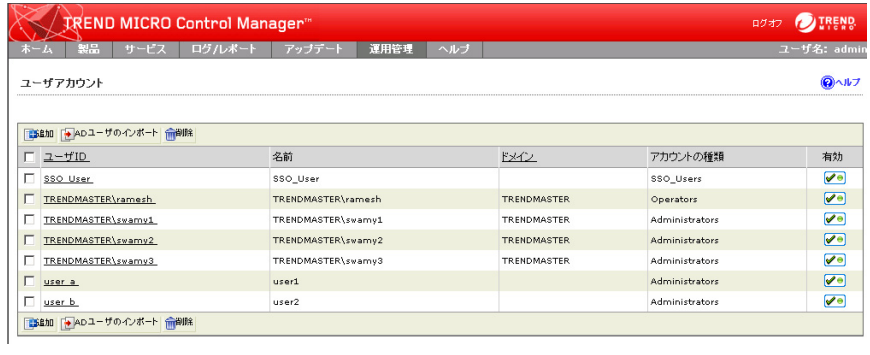
3. ユーザのアカウントのアカウントの種類を指定します (138 ページの「ユーザアカウントを編集するには」の手順 7 を参照)。

ユーザアカウントを追加するときは、ユーザの識別情報を入力し、アカウントの種類を割り当て、フォルダへのアクセス権を設定する必要があります。

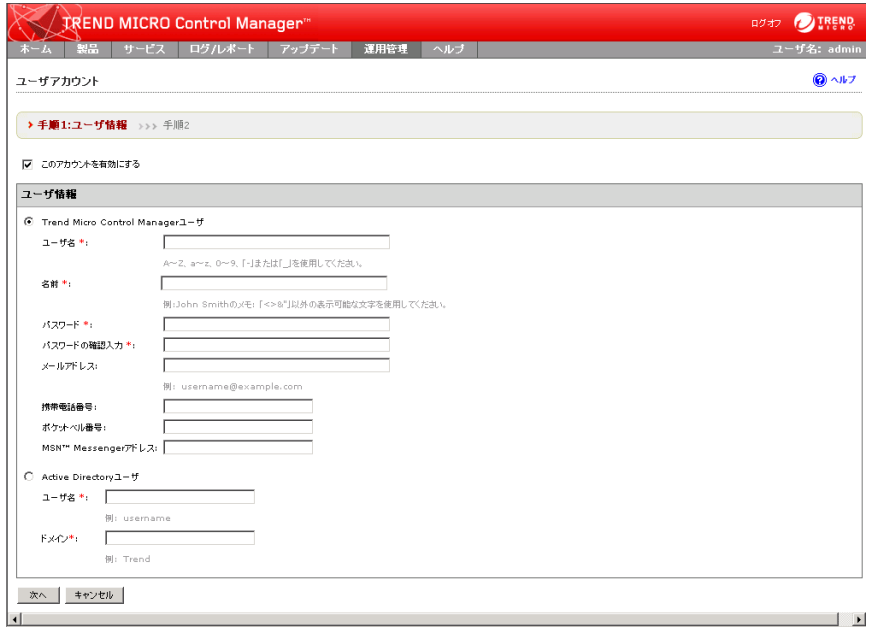
注意： Active Directory ユーザのアカウントを、Control Manager から無効にすることはできません。Active Directory ユーザを無効にするには、Active Directory サーバからアカウントを無効にする必要があります。

ユーザアカウントを追加するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューの [ユーザアカウント] をクリックします。[ユーザアカウント] 画面が表示されます。



4. [追加] をクリックします。[ユーザアカウント 手順 1:ユーザ情報] 画面が表示されます。



5. [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、Control Manager ユーザを有効にします。

6. 追加するユーザの種類を選択します。

Trend Micro Control Manager ユーザを追加する場合

a. [Trend Micro Control Manager ユーザ] を選択します。

b. 次の情報は必須項目です。

- ユーザ名 — Control Manager 管理コンソールへのログオン時にユーザが使用する名前。たとえば、OfficeScan_Admin。
- 名前 — ユーザのフルネーム。たとえば、John Smith。
- パスワード — パスワードは確認入力が必要です。ユーザは [ユーザのアカウント] 画面で各自のログオンパスワードを変更できます。

c. 次の情報は任意です。これらの情報も [ユーザのアカウント] 画面で変更できます。

- メールアドレス — 通知の受信に使用するメールアドレス
- 携帯電話番号 — 通知の受信に使用する携帯電話番号
- ポケットベル番号 — 通知の受信に使用するポケットベル番号
- MSN アカウント — 通知の受信に使用する MSN Messenger のアドレス

Active Directory ユーザを追加する場合

注意 : Active Directory ユーザのアカウントを、Control Manager から無効にすることはできません。

Active Directory ユーザを無効にするには、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。

---

a. [Active Directory ユーザ] を選択します。

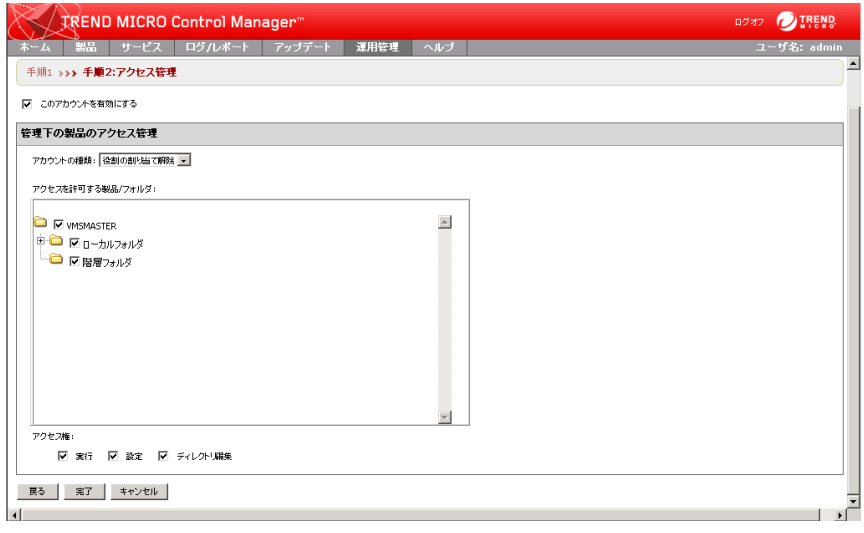
b. 次の情報は必須項目です。

- ユーザ名 : ユーザの Active Directory での識別名
- ドメイン : ユーザが所属するドメイン

注意 : ユーザ名およびドメイン名は、32 文字までの長さで指定できます。

---

7. [次へ] をクリックします。[ユーザアカウント 手順 2:アクセス管理] 画面が表示されます。



8. [アカウントの種類] リストからアカウントの種類を選択します。

   初期設定のオプションは [Operator]、[Power User]、および[Administrator] ですが、独自のアカウントの種類を作成することもできます。

9. [アクセスを許可する製品 / フォルダ] から、ユーザがアクセスできる製品またはディレクトリを選択します。

ヒント： 製品ディレクトリは、使いやすさを考慮に入れて構成することが重要です。

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。

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。

---

10. ユーザに割り当てる権限を選択します。これらの権限により、製品に対してユーザが実行できる処理が決まります。

注意： 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。つまり、自分自身のアクセス権より上位のユーザアクセス権を割り当てることはできません。さらに、アカウントの権限を制限すると、下位アカウントの権限も制限されます。

11. [完了] をクリックします。

ユーザアカウントの編集

アカウント情報、アカウントの種類、フォルダへのアクセス権などの、ユーザアカウントに関する情報を変更します。設定側のアカウントの権限を制限すると、そのすべての下位アカウントの権限も制限されます。

アカウントを編集する際には、次の点に留意してください。

- root 権限のユーザは、システム上のすべてのアカウントを編集できます。ただし、Administrator アカウントを持つユーザが編集できるのは、自分が作成したアカウントだけです。
- アカウントの権限は、その親アカウントの権限のサブセットです。したがって、親アカウントの権限が縮小されると、子アカウントの権限もそれに応じて縮小されます。
- アカウントの権限を変更すると、そのアカウントを使用しているセッションがすべて終了します。親アカウントの変更によって権限が減らされる場合には、子アカウントにその変更が反映されると共に、子アカウントもログアウトされます。
- 既存アカウントのユーザ名を変更することはできません。

ユーザアカウントを編集するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューの [ユーザアカウント] をクリックします。[ユーザアカウント] 画面が表示されます。
4. 編集するアカウントの [ユーザ ID] をクリックします。[ユーザアカウント 手順 1：ユーザ情報] 画面が表示されます。
5. アカウント情報を変更し、[次へ] をクリックします。
6. アクセス可能なフォルダとアクセス権を変更します。
7. [完了] をクリックします。

ユーザアカウントの無効化

一時的にユーザを Control Manager システムにアクセスできないようにするには、ユーザアカウントを無効にします。無効にしても、ユーザアカウント情報は保持されるので、いつでもそのユーザアカウントを有効にすることができます。

ユーザアカウントを無効にするには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。別のメニューが表示されます。
3. [ユーザアカウント] をクリックします。[ユーザアカウント] 画面が表示されます。
4. [ユーザアカウント] 表の [有効] 列で、ステータスアイコン (緑色のチェック) をクリックします。ステータスアイコンが赤色のダッシュに変わります。

ユーザアカウントの削除

Control Manager システムからユーザアカウントを完全に削除することもできます。ユーザアカウントを削除すると、そのユーザは所属していたグループからも削除され、ユーザアカウントが追加されていた受信者リストのイベント通知を受け取ることができなくなります。

ユーザアカウントを削除するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。別のメニューが表示されます。
3. [ユーザアカウント] をクリックします。[ユーザアカウント] 画面が表示されます。

4. 削除するアカウントに該当するチェックボックスをオンにします。
5. [削除] をクリックします。

ユーザグループの追加

ユーザグループを使用すると、個々のユーザではなく 1 つのユーザグループに一度に通知を送信できるため、管理が容易になります。ユーザの種類、場所、受信通知の種類などの類似した特性を持つユーザを、グループに追加できます。ユーザが Control Manager のユーザアカウントを持っていない場合は、そのユーザのメールアドレスを入力すれば、ユーザグループに追加することができます。ただし、通知を受信できるのは、そのグループが特定のイベントの受信者リストに追加されている場合だけです。

ユーザグループを追加するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。サブメニューが表示されます。
3. [ユーザグループ] をクリックします。[ユーザグループ] 画面が表示されます。

4. 右側の画面で、[新規グループの追加] をクリックします。

5. [グループ名] にグループの名前を入力します。

6. [グループメンバー] では、ユーザをグループリストに追加または削除します。

ユーザの追加

a. [追加メンバー] リストからユーザを選択します。複数のユーザを選択するときは、<Ctrl> キーを押しながら選択します。

b. [>>] をクリックして、選択したユーザを [グループユーザリスト] に追加します。

ユーザアカウントの設定時に指定した連絡先情報に基づいて、通知がユーザに送信されます。

ユーザの削除

a. [グループユーザリスト] からユーザを選択します。複数のユーザを選択するときは、<Ctrl> キーを押しながら選択します。

b. [<<] をクリックして、ユーザを削除します。

7. Control Manager のアカウントを持っていないユーザをグループユーザリストに追加するには、必要に応じて [追加メンバー] に次の項目を入力します。
   - メールアドレス
   - ポケットベル番号

   複数の項目を入力するときは、各項目をセミコロン (;) で区切ります。
8. [保存] をクリックします。
9. [OK] をクリックします。

ユーザグループの編集

Control Manager のユーザアカウントを持たないユーザを含め、いつでもユーザをグループに追加したりグループから削除したりできます。

ユーザグループを編集するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューの [ユーザグループ] をクリックします。[ユーザグループ] 画面が表示されます。
4. 右側の画面で、変更するグループの隣にある [編集] をクリックします。
5. 必要に応じてエントリを変更します。
6. [保存] をクリックします。
7. [OK] をクリックします。

ユーザグループの削除

ユーザグループが不要になった場合は、Control Manager システムからユーザグループを完全に削除します。ユーザグループを削除すると、メンバーは、そのユーザグループが追加されていた受信者リストのイベント通知を受け取ることができなくなります。

ユーザグループを削除するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [アカウント管理] の上にカーソルを置きます。別のメニューが表示されます。
3. [ユーザグループ] をクリックします。[ユーザグループ] 画面が表示されます。
4. 削除するグループの横にある [削除] をクリックします。
5. [OK] をクリックして、ユーザグループを削除します。
6. [OK] をクリックします。

製品ディレクトリについて

管理下の製品とは、Control Manager から管理されるウイルス対策製品、コンテンツセキュリティ製品、または Web セキュリティ対策製品のことです。管理下の製品は、Control Manager 管理コンソールの製品ディレクトリでは、アイコン (たとえば、  や ) で表示されます。これらのアイコンは、トレンドマイクロのウイルス対策製品、コンテンツセキュリティ製品、および Web セキュリティ対策製品を表します。Control Manager では、管理下の製品のステータスによって変化する、動的なアイコンがサポートされるようになりました。管理下の製品のアイコンおよび関連付けられているステータスに関する詳細については、管理下の製品に付属するドキュメントを参照してください。

管理下の製品は、製品ディレクトリを通して、製品単位またはグループ単位で管理します。次の表は、[製品ディレクトリ] 画面のメニュー項目とボタンをまとめたものです。

表 5-6.　[製品ディレクトリ] 画面のオプション

メニュー項目	説明
詳細検索	1 つ以上の管理下の製品に対して検索を実行するときは、このボタンをクリックして検索条件を指定します。
設定	Web ベースのコンソールにログオンし管理下の製品を設定するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。
タスク	特定の管理下の製品または管理下の製品グループ、あるいは特定の下位サーバまたは下位サーバグループに対して、最新コンポーネントの配信などの特定の機能を実行するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。 ディレクトリまたは Control Manager からタスクを開始すると、そのディレクトリに属するすべての管理下の製品に対して要求が送信されます。
ログ	製品ログを検索または表示するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。 特定の管理下の製品を選択した場合は、その製品のログのみを検索できます。それ以外の場合は、ディレクトリ内で使用可能なすべての製品のログを検索できます。
ディレクトリ管理	[ディレクトリ管理] 画面を開くときにクリックします。この画面から、ドラッグアンドドロップによるエンティティ / ディレクトリの移動や、新しいディレクトリの作成などを実行できます。
ボタン	**説明**
検索	特定の管理下の製品に対して検索を実行するときは、目的の管理下の製品名を入力してから、このボタンをクリックします。
ステータス	ディレクトリ内の 1 つまたは複数の管理下の製品についてのステータス概要を取得するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。

表 5-6.　[製品ディレクトリ] 画面のオプション

メニュー項目	説明
フォルダ	ディレクトリ内の管理下の製品および管理下の製品クライアントについてのステータス概要を取得するときは、目的のディレクトリを選択してから、このボタンをクリックします。

注意： 下位の Control Manager サーバに属する管理下の製品に対して、上位の Control Manager サーバによるタスクを適用することはできません。

ディレクトリ管理を使用した管理下の製品のグループ化

ディレクトリ管理を使用して、管理モデルのニーズに合うように、製品ディレクトリ構成をカスタマイズします。たとえば、製品の場所で分類したり、メッセージングセキュリティ対策製品、Web セキュリティ対策製品、ファイルサーバ対策製品などの種類別に分類できます。

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 5-7.　管理下の製品をグループ化する際の利点と欠点

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造の推奨設定

管理下の製品および下位サーバの製品ディレクトリ構造を計画するときは、次の推奨設定を適用することをお勧めします。

表 5-8. 管理下の製品または下位サーバのグループ化の注意点

構造	説明
社内のネットワークポリシーおよびセキュリティポリシー	社内のネットワークにアクセス権や共有権を適用する場合、社内のネットワークポリシーとセキュリティポリシーに従って管理下の製品および下位サーバをグループ化します。
組織と機能	会社の組織上および機能上の分割に従って、管理下の製品および下位サーバをグループ化します。たとえば、2 台の Control Manager サーバで製品グループとテスト担当グループを管理します。
所在地	管理下の製品 / 下位サーバの位置が Control Manager サーバと管理下の製品 / 下位サーバ間の通信に影響する場合には、グループ化の判断基準として地理的な位置を考慮します。
管理責務	管理下の製品および下位サーバを、それぞれのシステムまたはセキュリティの担当者に合わせてグループ化します。これにより、グループ設定が可能になります。

製品ディレクトリを使用することで、管理下の製品のグループ化をユーザが指定可能になり、それらのグループに対して次のような管理タスクを実行できるようになります。

- 管理下の製品の設定
- 製品への ScanNow の実行要求 (製品でサポートされている場合のみ)
- 製品情報および製品のインストール環境の詳細情報 (製品バージョン、パターンファイルのバージョン、検索エンジンのバージョン、OS など) の表示
- 製品レベルのログの表示
- 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、製品プログラムの配信

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。

- **ユーザのアクセス**

  アカウントを作成するときに、ユーザに対してアクセスを許可する、製品ディレクトリ内の特定の範囲を指定します。たとえば、root ディレクトリを選択すると、製品ディレクトリ全体へのアクセス権を付与することになります。管理下の特定の製品を選択した場合には、その製品へのアクセス権だけが付与されます。

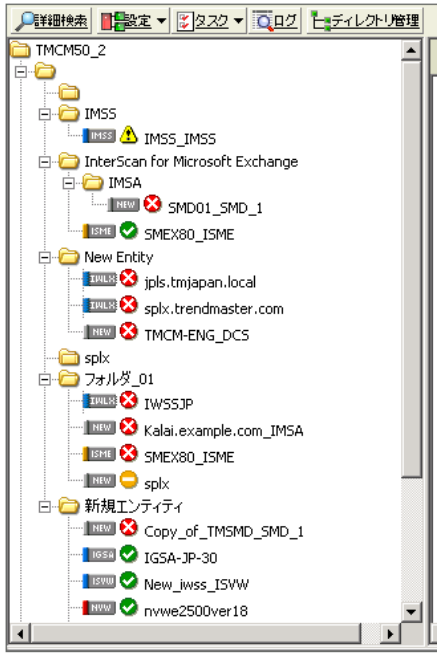
- **配信計画**

  配信計画に基づいて、最新のパターンファイル、検索エンジン、スパムメール判定ルール、製品プログラム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できます。したがって、製品ディレクトリを適切に構成することで、配信先の指定を簡略化できます。

- **大規模感染予防ポリシーとダメージクリーンナップテンプレートの配信**

  大規模感染予防ポリシーとダメージクリーンナップテンプレートを効率的に配信できるかどうかは、配信計画に依存します。

次に製品ディレクトリの例を示します。



管理下の製品は、登録済みウイルス対策製品またはコンテンツセキュリティ製品として識別され、接続ステータスも表示されます。

製品ディレクトリのアイコンのリストについては、Control Manager のオンラインヘルプの「製品ディレクトリについて」を参照してください。

図 5-2.　製品ディレクトリの例

ディレクトリ管理機能を使用して、製品ディレクトリを配置します。製品の種類を表すフォルダ名を使用して、保護の種類や Control Manager システムの管理モデルに従って、管理下の製品をグループ化します。たとえば、ファイルサーバ管理者にアクセス権を付与して、Server protection フォルダを設定できるようにします。

製品ディレクトリの初期設定フォルダ

Control Manager の新規インストール直後の製品ディレクトリは、次のディレクトリで構成されます。

表 5-9. 製品ディレクトリの初期設定フォルダ

構造	説明
root	すべての管理下の製品と下位の Control Manager サーバが、root ディレクトリに配置されます。
階層フォルダ	階層管理環境では、上位サーバに対するすべての下位サーバが [階層フォルダ] に格納されます。
ローカルフォルダ	Control Manager エージェントによって処理される、新規に登録された管理下の製品が、[新規エンティティ] フォルダに格納されます。
検索結果	基本検索または拡張検索を実行すると、その検索条件に合致するすべての管理下の製品が検索結果フォルダに格納されます。

下位サーバの管理

Control Manager アドバンス版には階層管理構造が用意されています。これによって、下位サーバと呼ばれる複数の Control Manager サーバを 1 台の上位サーバから制御できます。

上位サーバは、下位サーバと呼ばれる Control Manager スタンダード版またはアドバンス版サーバを管理する Control Manager サーバです。下位サーバは、上位サーバの管理下にある Control Manager サーバです。

注意： Control Manager 5.0 アドバンス版では、次のサーバを下位の Control Manager サーバとしてサポートします。

- Control Manager 5.0 アドバンス版
- Control Manager 3.5 スタンダード版またはエンタープライズ版
- Control Manager 3.0 SP6 スタンダード版またはエンタープライズ版

Control Manager 5.0 スタンダード版サーバを下位サーバとすることはできません。

上位サーバは、自身の管理下の製品を除き、下位サーバが直接操作する管理下の製品に対しては、間接的な管理を行います。

次の表は、上位サーバと下位サーバの相違点をまとめています。

表 5-10. 上位サーバと下位サーバの機能比較

機能	上位サーバで提供	下位サーバで提供
階層構造のサポート	可	不可
管理下の製品の管理	可	可
複数の下位サーバの操作	可	不可
広域タスクの発行	可	不可
広域レポートの作成	可	不可

注意： 上位サーバを別の上位サーバに登録することはできません。また、1 つのサーバが同時に上位サーバと下位サーバになることはできません。

下位サーバの設定

階層管理構造では、Control Manager の管理コンソールを使用して、上位サーバに属するすべての下位サーバを管理および監視するとともに、次の処理を実行できます。

- ウイルス対策、コンテンツセキュリティ対策、および Web セキュリティ対策の概要の監視
- イベントログやセキュリティログのクエリ
- タスクの開始
- レポートの表示
- 下位サーバの管理コンソールへのアクセス

階層構造を使用すると、企業のウイルス対策およびコンテンツセキュリティ対策製品を広範囲にわたって効果的に管理することが可能です。

ヒント： 1 台の Control Manager 上位サーバの管理対象が、200 台以下の下位サーバと 9,600 台以下の管理下の製品となるように構成することをお勧めします。

下位サーバの登録または登録解除

下位サーバを登録または登録解除しても、下位サーバを有効または無効にした場合と同じ結果は得られません。登録または登録解除では、上位サーバと下位サーバの接続が完全に切断され、有効化または無効化では両サーバ間の接続が一時的に停止します。

たとえば、下位サーバ xyz が上位サーバ a に登録されていた場合に、下位サーバ xyz を上位サーバ a から登録解除し、この下位サーバ xyz を上位サーバ b に登録します。すると、上位サーバ b がこの下位サーバ xyz を管理することになり、上位サーバ a の階層構造ツリーから下位サーバ xyz は削除されます。

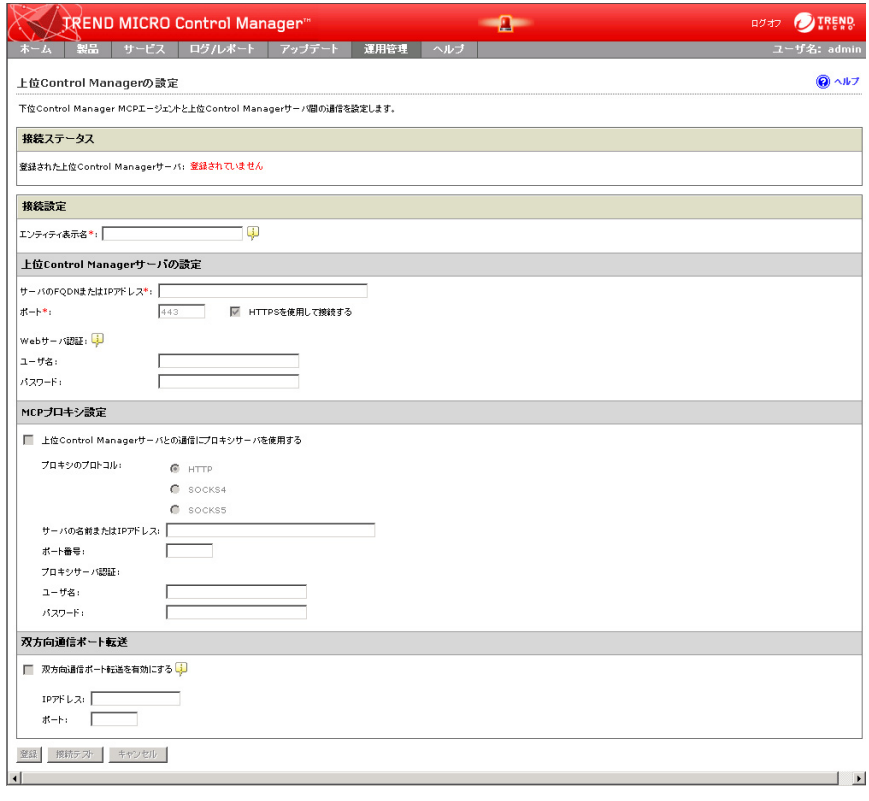
上位サーバである a と b 間で負荷を分散させる場合、一般的には次の場合に負荷分散を実行します。

- 上位サーバ a が、上位サーバ b より多数の下位サーバを管理している場合。

- 上位サーバ a が過負荷状態になったために、上位サーバ a の負荷を軽減し、一部の下位サーバを上位サーバ b に移行させる場合。

下位サーバを登録するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューの [上位 Control Manager の設定] を選択します。[上位 Control Manager の設定] 画面が表示されます。



4. [接続の設定] を設定します。

   - 上位の Control Manager に表示される下位サーバ名を [エンティティ表示名] に入力します。

5. [上位 Control Manager サーバの設定] を設定します。

   a. 上位の Control Manager サーバの FQDN または IP アドレスを [サーバの FQDN または IP アドレス] に入力します。

   b. 上位の Control Manager が MCP との通信に使用するポート番号を [ポート] に入力します。

   ヒント： セキュリティを増すためには、[HTTPS を使用して接続する] を選択します。

   c. Control Manager の IIS Web 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。

6. [MCP プロキシ設定] を設定します。

   a. Control Manager サーバとの接続にプロキシサーバを使用する場合、[上位 Control Manager サーバの設定] を選択し、次の設定を完了する必要があります。

   b. プロキシが使用するプロトコルを選択します。

      - HTTP
      - SOCKS 4
      - SOCKS 5

   c. [サーバの名前または IP アドレス] にプロキシサーバの FQDN または IP アドレスを入力します。

   d. [ポート] にプロキシサーバのポート番号を入力します。

   e. プロキシサーバでユーザ認証が必要な場合は、ユーザ名およびパスワードを入力します。

7. [双方向通信ポート転送] を設定します。

   a. MCP エージェントでポート転送を使用する場合は、[双方向通信ポート転送を有効にする] を選択して次の設定を完了する必要があります。

   b. [IP アドレス] に転送 IP アドレスを入力します。

   c. [ポート] にポート番号を入力します。

8. 下位サーバが上位の Control Manager サーバに接続していることを確認するには、[接続テスト] をクリックします。

9. [登録] をクリックして上位の Control Manager サーバに接続します。

下位の Control Manager サーバを登録解除するには

1. 下位サーバから上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. [設定] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューの [上位 Control Manager の設定] を選択します。[上位 Control Manager の設定] 画面が表示されます。

4. 画面の下部にある [登録解除] をクリックします。

新規コンポーネントのダウンロードと配信

トレンドマイクロでは、最新のウイルスおよび不正プログラムの脅威に対して保護された状態を保てるように、ウイルス対策およびコンテンツセキュリティコンポーネントのアップデートをお勧めしています。初期設定では、Control Manager サーバに管理下の製品が登録されていない場合でも、Control Manager でウイルスパターンファイル、ダメージクリーンナップテンプレート、および脆弱性診断パターンファイルがダウンロードされます。

アップデートできるのは、次のコンポーネントです。ここでは、頻繁にアップデートすることが推奨されるものから記載してあります。

- **パターンファイル / テンプレート** : パターンファイル / テンプレートには、ウイルス、トロイの木馬など、不正プログラムを識別するためのパターンが数多く含まれています。管理下の製品による、ウイルスに感染したファイルの検出および駆除能力を決定付けるものです。
- **スパムメール判定ルール** : スパムメール判定ルールは、トレンドマイクロが提供するファイルで、スパムメール判定およびコンテンツフィルタに使用されます。
- **エンジン** : エンジンには、ウイルス / 不正プログラム検索エンジン、ダメージクリーンナップエンジン、ネットワークウイルス検索エンジン、スパイウェア検索エンジンなどがあります。これらのコンポーネントでは、検索および駆除機能が実行されます。
- **製品プログラム** : 製品固有のコンポーネント (Service Pack など)。

注意 : コンポーネントをアップデートできるのは、製品のアクティベーションが完了している場合だけです。

Control Manager システムのトラフィックを最小限に抑えるには、管理下の製品に適用する必要がないコンポーネントのダウンロードを無効にしてください。

[コンポーネントリスト] 画面には、管理下の製品に対して使用可能なすべての Control Manager コンポーネントの完全なリストが表示されます。また、このリストでは、コンポーネントと、そのコンポーネントを使用する管理下の製品が対応付けられています。[コンポーネントリスト] 画面を開くには、[アップデート]→[コンポーネントリスト] の順に選択します。

図 5-3.　[コンポーネントリスト] 画面

ヒント： 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。管理下の製品を登録した場合、または後からサービスを有効にした場合、該当するコンポーネントの手動ダウンロードまたは予約ダウンロードを設定してください。

コンポーネントの手動ダウンロード

Control Manager を最初にインストールするとき、ネットワークが攻撃されているとき、または新しいコンポーネントをネットワークに配信する前にテストするときに、最新コンポーネントを手動でダウンロードします。

トレンドマイクロの推奨する手動ダウンロードの構成方法を、次に説明します。コンポーネントを手動でダウンロードするには、複数の手順を実行する必要があります。

ヒント：配信計画およびプロキシ設定を既に設定してある場合は、手順 1 および 2 は無視してください。

手順 1: コンポーネントの配信計画の設定

手順 2: プロキシの設定　(プロキシサーバを使用する場合)

手順 3: アップデートするコンポーネントの選択

手順 4: ダウンロード方法の設定

手順 5: 自動配信の設定

手順 6: 手動ダウンロードの完了

手動でコンポーネントをダウンロードするには

手順 1 — コンポーネントの配信計画の設定

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [配信計画] をクリックします。[配信計画] 画面が表示されます。

3. [追加] をクリックします。[新規配信計画の追加] 画面が表示されます。

4. [新規配信計画の追加] 画面で、[名前] に配信計画名を入力します。

5. [追加] をクリックして、配信計画の詳細を入力します。[新規スケジュールの追加] 画面が表示されます。

6. [新規スケジュールの追加] 画面で、次のいずれかのオプションを選択して、配信スケジュールを選びます。

   - 保留時間 — Control Manager で最新コンポーネントをダウンロードした後、指定した間隔に従って、配信を遅らせます。

     メニューを使用して、時間または分単位で保留期間を指定します。

   - 開始時刻 — 指定した時刻に配信を実行します。

     メニューを使用して、時間または分単位で配信時刻を指定します。

7. スケジュールを適用する製品ディレクトリのフォルダを選択します。選択したフォルダに含まれるすべての製品に対して、スケジュールが適用されます。
8. [保存] をクリックします。
9. さらに、[保存] をクリックして、新規配信計画を適用します。

手順 2 — プロキシの設定 (プロキシサーバを使用する場合)

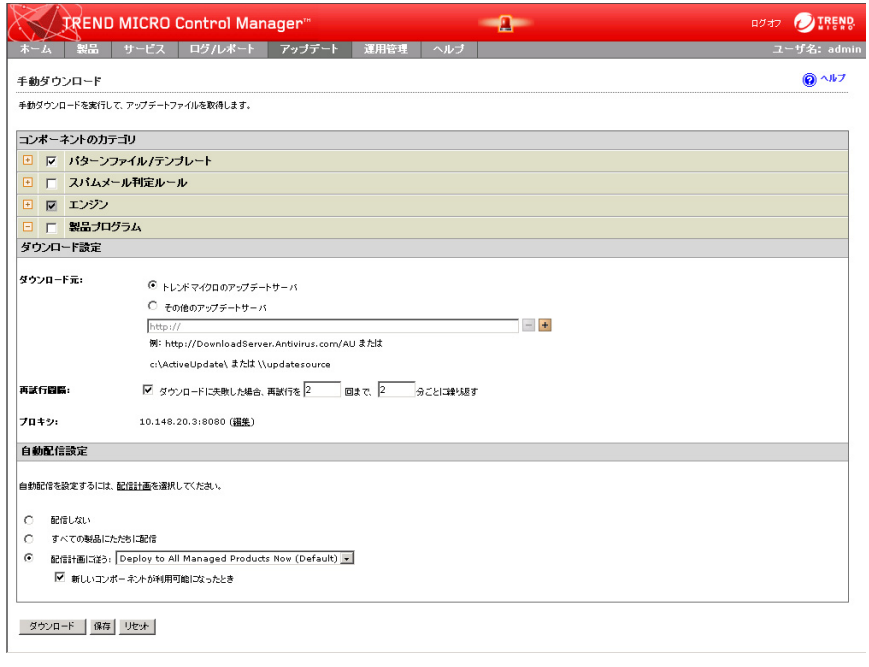
1. [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [プロキシの設定] をクリックします。[接続の設定] 画面が表示されます。

4. [プロキシサーバを使用してパターンファイル、エンジン、およびライセンスをアップデートする] チェックボックスをオンにします。
5. プロトコルを選択します。
   - HTTPS
   - SOCKS 4
   - SOCKS 5
6. [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。

7. [ポート] に、ポート番号を入力します。
8. サーバで認証が必要な場合は、ログオン名とパスワードを入力します。
9. [保存] をクリックします。

手順 3 — アップデートするコンポーネントの選択

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [手動ダウンロード] をクリックします。[手動ダウンロード] 画面が表示されます。



3. [コンポーネントのカテゴリ] で、ダウンロードするコンポーネントを選択します。

   a. 各コンポーネントグループのコンポーネントリストを展開するには [+] アイコンをクリックします。

b. ダウンロードするコンポーネントを選択します。グループのすべてのコンポーネントを選択するには、次を選択します。

- **パターンファイル / テンプレート**
- **スパムメール判定ルール**
- **各種エンジン**
- **製品プログラム**

手順 4 — ダウンロード方法の設定

1. ダウンロード元を選択します。

   - **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をダウンロードします。
   - **その他のアップデートサーバ** — 指定のフィールドにダウンロード元の URL を入力します。

     [その他のアップデートサーバ] を選択すると、複数のダウンロード元を指定できます。ダウンロード元を追加するには、[+] アイコンをクリックします。ダウンロード元は 5 つまで設定できます。

2. [再試行間隔] を選択して、コンポーネントのダウンロードに適用する再試行回数と再試行間隔を指定します。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

---

3. ネットワーク上で HTTP プロキシサーバを使用している場合 (Control Manager サーバがインターネットに直接アクセスできない場合) は、[編集] をクリックして、[接続の設定] 画面でプロキシを設定します。

手順 5 — 自動配信の設定

1. [自動配信設定] で、ダウンロードしたコンポーネントをいつ配信するかを選択します。次のオプションがあります。

   - **配信しない** — コンポーネントは Control Manager にダウンロードされますが、管理下の製品には配信されません。このオプションは次の場合に使用します。
     - 管理下の製品に個々に配信する場合
     - アップデートしたコンポーネントを配信前にテストする場合
   - **すべての製品にただちに配信** — コンポーネントは Control Manager にダウンロードされ、管理下の製品に配信されます。
   - **配信計画に従う** — コンポーネントは Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。
   - **新しいコンポーネントが利用可能になったとき** — コンポーネントはアップデート元で新しいコンポーネントが利用可能になったときに Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。

注意： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

2. コンポーネントが Control Manager にダウンロードされたら、[配信計画に従う :] のリストから配信計画を選択します。
3. [保存] をクリックします。

手順 6 — 手動ダウンロードの完了

1. [ダウンロード] をクリックし、[OK] をクリックして確認します。ダウンロードの応答画面が表示されます。進捗バーにダウンロードの進行状況が表示されます。
2. [コマンド詳細] をクリックして、[コマンド詳細] 画面にダウンロードの詳細を表示します。

3. [OK] をクリックして [手動ダウンロード] 画面に戻ります。

手動ダウンロードへのアクセス

ただちに新しいコンポーネントをダウンロードするときは、[手動ダウンロード] 画面を使用します。

[手動ダウンロード] 画面にアクセスするには

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [手動ダウンロード] をクリックします。[手動ダウンロード] 画面が表示されます。

手動ダウンロードの設定

[ダウンロード設定] グループでは、Control Manager で手動でダウンロードするコンポーネントとダウンロード方法を定義します。

手動ダウンロードを設定するには

1. [手動ダウンロード] 画面にアクセスします。
2. 右側の画面の [ダウンロード設定] で、次の操作を行います。

   a. ダウンロードするコンポーネントを選択します。

   b. ダウンロード元を選択します。

      - **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をダウンロードします。
      - **その他のアップデートサーバ** — 指定のフィールドにダウンロード元の URL を入力します。

        [その他のアップデートサーバ] を選択すると、複数のダウンロード元を指定できます。ダウンロード元を追加するには、[+] アイコンをクリックします。ダウンロード元は 5 つまで設定できます。

c. [再試行間隔] を選択して、コンポーネントのダウンロードに適用する再試行回数と再試行間隔を指定します。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

d. ネットワーク上で HTTP プロキシサーバを使用している場合 (Control Manager サーバがインターネットに直接アクセスできない場合) は、[編集] をクリックして、[接続の設定] 画面でプロキシを設定します。

3. [保存] をクリックします。

手動ダウンロード自動配信の設定

[自動配信設定] グループを使用して、Control Manager による最新コンポーネントの配信方法を設定します。

手動ダウンロード自動配信を設定するには

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [手動ダウンロード] をクリックします。[手動ダウンロード] 画面が表示されます。
3. [自動配信設定] で、ダウンロードしたコンポーネントをいつ配信するかを選択します。
   - **配信しない** — コンポーネントは Control Manager にダウンロードされますが、管理下の製品には配信されません。このオプションは次の場合に使用します。
     - 管理下の製品に個々に配信する場合
     - アップデートしたコンポーネントを配信前にテストする場合
   - **すべての製品にただちに配信** — コンポーネントは Control Manager にダウンロードされ、管理下の製品に配信されます。

- **配信計画に従う** — コンポーネントは Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。
- **新しいコンポーネントが利用可能になったとき** — コンポーネントはアップデート元で新しいコンポーネントが利用可能になったときに Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

4. コンポーネントが Control Manager にダウンロードされたら、[配信計画に従う:] のリストから配信計画を選択します。
5. [保存] をクリックします。

注意： [自動配信設定] の設定は、管理下の製品によって使用されるコンポーネントにのみ適用されます。

ダメージクリーンナップサービスおよび脆弱性診断の場合は、最新バージョンが利用可能になると、Control Manager によってコンポーネント (ダメージクリーンナップテンプレート、ダメージクリーンナップエンジン、脆弱性診断パターンファイル、および脆弱性診断エンジン) が自動的に配信されます。

予約ダウンロードの除外設定

[予約ダウンロードの除外設定] 画面を使用して、予約ダウンロードを実行しない時間帯や曜日を指定できます。

休日や業務時間外に Control Manager でダウンロードが実行されるのを避けたい場合に、この設定が役立ちます。

注意： 曜日の設定は選択した日に適用し、時間の設定はすべての曜日に適用します。

例 : 管理者は、Control Manager で週末または平日の稼働時間外にコンポーネントをダウンロードしないようにします。管理者は [曜日の設定] を有効にして [土曜日] および [日曜日] を選択します。次に、管理者は [時間の設定] を有効にして [00:00 から 9:00] および [18:00 から 24:00] の時間を指定します。

予約ダウンロードの除外スケジュールを設定するには

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [予約ダウンロードの除外設定] をクリックします。[予約ダウンロードの除外設定] 画面が表示されます。

4. 次の設定を行います。

   - **曜日の設定** — 予約ダウンロードを実行しない曜日を設定するには、[指定した曜日を除外する] チェックボックスをオンにし、曜日を指定します。指定された曜日のすべてのダウンロードが毎週ブロックされます。
   - **時間の設定** — 予約ダウンロードを実行しない時間帯を設定するには、[指定した時間を除外する] チェックボックスをオンにし、時間を指定します。指定された時間のすべてのダウンロードが毎日ブロックされます。

5. [保存] をクリックします。

予約ダウンロードについて

コンポーネントの予約ダウンロードを設定して、ネットワークの安全のためにコンポーネントが最新の状態に保たれるようにします。Control Manager では、コンポーネントを細かく分けてダウンロードできます。コンポーネントグループおよび個々のコンポーネントのダウンロードスケジュールを指定できます。すべてのスケジュールは、それぞれ独立して実行されます。コンポーネントグループのダウンロードをスケジュールすると、グループ内のすべてのコンポーネントがダウンロードされます。

現在の Control Manager システムに設定されている、次のコンポーネント情報を入手するときは、[予約ダウンロード] 画面を使用します。

- **実行間隔** : コンポーネントごとに、ダウンロードの実行間隔が表示されます。
- **有効** : 予約ダウンロードが有効であるか無効であるかが表示されます。
- **ダウンロード元** : 最新コンポーネントの場所を示す URL またはパスが表示されます。

コンポーネントの予約ダウンロードを設定するには、複数の手順を実行する必要があります。

手順 1: コンポーネントの配信計画の設定

手順 2: プロキシの設定 (プロキシサーバを使用する場合)

手順 3: アップデートするコンポーネントの選択

手順 4: ダウンロードスケジュールの設定

手順 5: ダウンロード方法の設定

手順 6: 自動配信の設定

手順 7: スケジュールの有効化と設定の保存

予約ダウンロードの設定とコンポーネントの予約ダウンロードの有効化

手順 1 — コンポーネントの配信計画の設定

1. 上部のメニューで [アップロード] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [配信計画] をクリックします。[配信計画] 画面が表示されます。

3. [追加] をクリックします。[新規配信計画の追加] 画面が表示されます。

4. [新規配信計画の追加] 画面で、[名前] に配信計画名を入力します。

5. [追加] をクリックして、配信計画の詳細を入力します。[新規スケジュールの追加] 画面が表示されます。

6. [新規スケジュールの追加] 画面で、次のいずれかのオプションを選択して、配信スケジュールを選びます。

   - 保留時間 — Control Manager で最新コンポーネントをダウンロードした後、指定した間隔に従って、配信を遅らせます。

     メニューを使用して、時間または分単位で保留期間を指定します。

   - 開始時刻 — 指定した時刻に配信を実行します。

     メニューを使用して、時間または分単位で配信時刻を指定します。

7. スケジュールを適用する製品ディレクトリのフォルダを選択します。選択したフォルダに含まれるすべての製品に対して、スケジュールが適用されます。
8. [OK] をクリックします。
9. [保存] をクリックして、新規配信計画を適用します。

手順 2 — プロキシの設定 (プロキシサーバを使用する場合)

1. [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [プロキシの設定] をクリックします。[接続の設定] 画面が表示されます。

4. [プロキシサーバを使用してパターンファイル、エンジン、およびライセンスをアップデートする] チェックボックスをオンにします。
5. プロトコルを選択します。
   - HTTPS
   - SOCKS 4
   - SOCKS 5
6. [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。
7. [ポート] にプロキシサーバのポート番号を入力します。

8. サーバで認証が必要な場合は、ログオン名とパスワードを入力します。

9. [保存] をクリックします。

手順 3 — アップデートするコンポーネントの選択

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. [予約ダウンロード] をクリックします。[予約ダウンロード] 画面が表示されます。

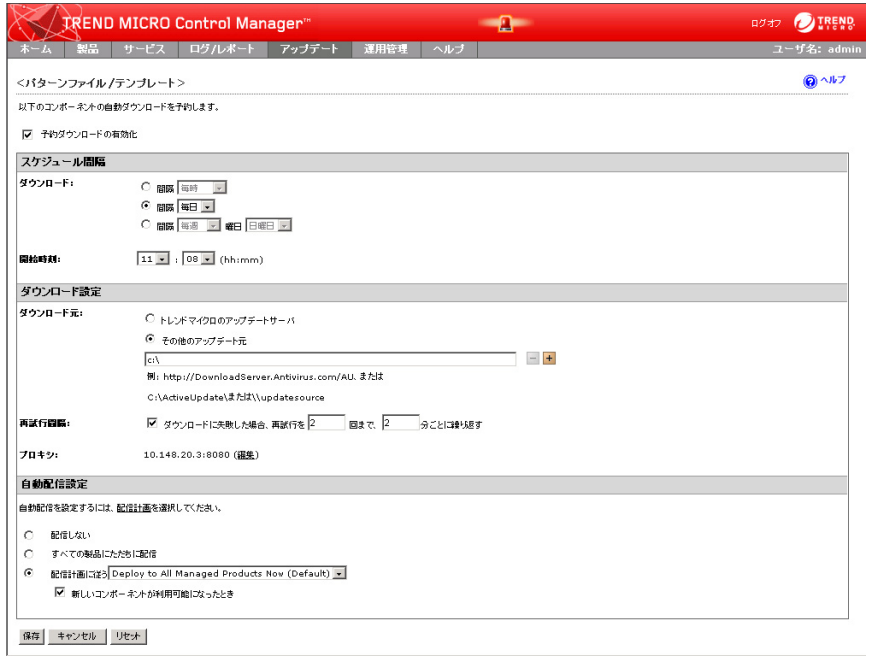
3. [コンポーネントのカテゴリ] で、ダウンロードするコンポーネントを選択します。

   a. 各コンポーネントグループのコンポーネントリストを展開するには [+] アイコンをクリックします。

   b. ダウンロードするコンポーネントを選択します。グループのすべてのコンポーネントを選択するには、次を選択します。

      - **パターンファイル / テンプレート**
      - **スパムメール判定ルール**
      - **エンジン**
      - **製品プログラム**

[< コンポーネント名 >] 画面が表示されます。ここで、< コンポーネント名 > は選択したコンポーネントの名前です。



手順 4 — ダウンロードスケジュールの設定

1. [予約ダウンロードの有効化] チェックボックスをオンにして、コンポーネントの予約ダウンロードを有効にします。
2. ダウンロードのスケジュールを設定します。[間隔] を選択し、該当するリストボックスを使用して、適切なスケジュールを指定します。ダウンロードの実行間隔には、分、時間、日、週のいずれかの時間単位を選択できます。
3. [開始時刻] メニューを使用して、スケジュールが開始される日付と時刻を指定します。

手順 5 — ダウンロード方法の設定

1. ダウンロード元を選択します。

   - **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をダウンロードします。
   - **その他のアップデート元** — 指定のフィールドにダウンロード元の URL を入力します。

     [その他のアップデート元] を選択すると、複数のダウンロード元を指定できます。ダウンロード元を追加するには、[+] アイコンをクリックします。ダウンロード元は 5 つまで設定できます。

2. [再試行間隔] を選択し、コンポーネントのダウンロードを再試行する回数と間隔を指定します。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

---

3. ネットワーク上で HTTP プロキシサーバを使用している場合 (Control Manager サーバがインターネットに直接アクセスできない場合) は、[編集] をクリックして、[接続の設定] 画面でプロキシを設定します。

手順 6 — 自動配信の設定

1. [自動配信設定] で、ダウンロードしたコンポーネントをいつ配信するかを選択します。次のオプションがあります。

   - **配信しない** — コンポーネントは Control Manager にダウンロードされますが、管理下の製品には配信されません。このオプションは次の場合に使用します。
     - 管理下の製品に個々に配信する場合
     - アップデートしたコンポーネントを配信前にテストする場合
   - **すべての製品にただちに配信** — コンポーネントは Control Manager にダウンロードされ、管理下の製品に配信されます。

- **配信計画に従う** — コンポーネントは Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。
- **新しいコンポーネントが利用可能になったとき** — コンポーネントはアップデート元で新しいコンポーネントが利用可能になったときに Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

2. コンポーネントが Control Manager にダウンロードされたら、[配信計画に従う:] のリストから配信計画を選択します。
3. [保存] をクリックします。

手順 7 — スケジュールの有効化と設定の保存

1. [有効] 列のステータスボタンをクリックします。
2. [保存] をクリックします。

予約ダウンロードのスケジュール間隔の設定

最新コンポーネントをダウンロードするスケジュールを [スケジュール (実行間隔)] で設定します。

[スケジュール (実行間隔)] を設定するには

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [予約ダウンロード] をクリックします。[予約ダウンロード] 画面が表示されます。
3. [コンポーネントのカテゴリ] で、ダウンロードするコンポーネントを選択します。

a. 各コンポーネントグループのコンポーネントリストを展開するには [+] アイコンをクリックします。

b. ダウンロードするコンポーネントを選択します。グループのすべてのコンポーネントを選択するには、次を選択します。

- **パターンファイル / テンプレート**
- **スパムメール判定ルール**
- **エンジン**
- **製品プログラム**

[< コンポーネント名 >] 画面が表示されます。ここで、< コンポーネント名 > は選択したコンポーネントの名前です。

4. [スケジュール間隔] で次の項目を指定します。

a. ダウンロードのスケジュールを設定します。[間隔] を選択し、該当するリストボックスを使用して、適切なスケジュールを指定します。ダウンロードの実行間隔には、分、時間、日、週のいずれかの時間単位を選択できます。

b. [開始時刻] リストボックスを使用して、スケジュールが開始される日付と時刻を指定します。

5. [保存] をクリックします。

予約ダウンロードの設定

[ダウンロード設定] グループでは、Control Manager により自動的にダウンロードされるコンポーネントのダウンロード方法を指定します。

[ダウンロード設定] を設定するには

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. [予約ダウンロード] をクリックします。[予約ダウンロード] 画面が表示されます。

3. [コンポーネントのカテゴリ] で、ダウンロードするコンポーネントを選択します。

   a. 各コンポーネントグループのコンポーネントリストを展開するには [+] アイコンをクリックします。

   b. ダウンロードするコンポーネントを選択します。グループのすべてのコンポーネントを選択するには、次を選択します。

      - **パターンファイル / テンプレート**
      - **スパムメール判定ルール**
      - **エンジン**
      - **製品プログラム**

   [< コンポーネント名 >] 画面が表示されます。ここで、< コンポーネント名 > は選択したコンポーネントの名前です。

[ダウンロード設定] で、次の操作を行います。

4. [ダウンロード元] で、次のダウンロード元のいずれかを選択します。

   - **トレンドマイクロのアップデートサーバ** — (初期設定) トレンドマイクロのアップデートサーバから最新コンポーネントがダウンロードされます。
   - **その他のアップデート元** — 別のサーバから最新コンポーネントをダウンロードする場合に、ダウンロード元の URL を指定します。たとえば、会社のイントラネットサーバに最新コンポーネントがある場合はこのオプションを指定します。

     [その他のアップデート元] を選択すると、複数のダウンロード元を指定できます。ダウンロード元を追加するには、[+] アイコンをクリックします。ダウンロード元は 5 つまで設定できます。

5. [再試行間隔] を選択し、最新コンポーネントのダウンロードを再試行する間隔を指定します。試行回数を 1 ～ 3、試行間隔 (分) を 1 ～ 10 の範囲で指定してください。

注意： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

6. ネットワーク上でプロキシサーバを使用している場合 (Control Manager サーバがインターネットに直接アクセスできない場合) は、[編集] をクリックして、[接続の設定] 画面でプロキシを設定します。

7. [保存] をクリックします。

予約ダウンロード自動配信の設定

[自動配信設定] グループを使用して、Control Manager による最新コンポーネントの配信方法を設定します。

[自動配信設定] を設定するには

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. [予約ダウンロード] をクリックします。[予約ダウンロード] 画面が表示されます。

3. [コンポーネントのカテゴリ] で、ダウンロードするコンポーネントを選択します。

   a. 各コンポーネントグループのコンポーネントリストを展開するには [+] アイコンをクリックします。

   b. ダウンロードするコンポーネントを選択します。グループのすべてのコンポーネントを選択するには、次を選択します。

      - **パターンファイル / テンプレート**
      - **スパムメール判定ルール**
      - **エンジン**
      - **製品プログラム**

   [< コンポーネント名 >] 画面が表示されます。ここで、< コンポーネント名 > は選択したコンポーネントの名前です。

[自動配信設定] で、次の操作を行います。

4. [自動配信設定] で、ダウンロードしたコンポーネントをいつ配信するかを選択します。次のオプションがあります。

   - **配信しない** — コンポーネントは Control Manager にダウンロードされますが、管理下の製品には配信されません。このオプションは次の場合に使用します。
     - 管理下の製品に個々に配信する場合
     - アップデートしたコンポーネントを配信前にテストする場合
   - **すべての製品にただちに配信** — コンポーネントは Control Manager にダウンロードされ、管理下の製品に配信されます。
   - **配信計画に従う** — コンポーネントは Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。
   - **新しいコンポーネントが利用可能になったとき** — コンポーネントはアップデート元で新しいコンポーネントが利用可能になったときに Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。

注意： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

5. コンポーネントが Control Manager にダウンロードされたら、[配信計画に従う:] のリストから配信計画を選択します。
6. [保存] をクリックします。

注意： [自動配信設定] の設定は、管理下の製品によって使用されるコンポーネントにのみ適用されます。

ダメージクリーンナップサービスおよび脆弱性診断の場合は、最新バージョンが利用可能になると、Control Manager によってコンポーネント (ダメージクリーンナップテンプレート、ダメージクリーンナップエンジン、脆弱性診断パターンファイル、および脆弱性診断エンジン) が自動的に配信されます。

配信計画について

配信計画を使用すると、管理下の製品グループをアップデートする順序を設定できます。Control Manager では、さまざまな管理下の製品に対して、複数の配信計画を異なるスケジュールで実行することができます。たとえば、メールメッセージからのウイルス感染が拡大しているときは、InterScan for Microsoft Exchange の最新パターンファイルなど、メールウイルス検索ソフトウェアのアップデート処理を優先させることができます。

Control Manager をインストールすると、2 つの配信計画が作成されます。

- すべての製品にただちに配信 (通常時) — コンポーネントのアップデート時に使用される初期設定の配信計画です。
- すべての製品にただちに配信 (大規模感染時) — 大規模感染予防サービスの予防措置ステージでの初期設定の配信計画です。

これらの配信計画の初期設定では、製品ディレクトリ内のすべての製品に最新コンポーネントが即座に配信されます。

手動ダウンロードおよび予約ダウンロードページから計画を選択または作成します。これらの計画を必要に応じてカスタマイズしたり、新しい配信計画を作成することが可能です。たとえば、次のような大規模感染の性質に応じて、配信計画を作成してください。

- メールからのウイルス
- ファイル共有ウイルス

製品ディレクトリへの最新コンポーネントの配信は、ダウンロード処理とは別のものです。

Control Manager では、最新コンポーネントをダウンロードし、手動または予約ダウンロード設定に従って配信計画を実行します。

配信計画を作成または実施するときは、次の点に注意してください。

- 配信スケジュールは、特定の製品に対してではなく、フォルダに対して割り当てます。

  このことを考慮して、あらかじめディレクトリのフォルダを構成する必要があります。

- 1 つの配信計画スケジュールにつき、1 つのフォルダのみを含めることができます。

  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したい 3 つのフォルダがある場合、最初のフォルダを 5 分後、2 番めのフォルダを 10 分後、3 番めのフォルダを 15 分後に配信することができます。

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [配信計画] をクリックします。[配信計画] 画面が表示されます。

3. [追加] をクリックします。[新規配信計画の追加] 画面が表示されます。

4. [新規配信計画の追加] 画面で、[名前] に配信計画名を入力します。

5. [追加] をクリックして、配信計画の詳細を入力します。[新規スケジュールの追加] 画面が表示されます。

6. [新規スケジュールの追加] 画面で、次のいずれかのオプションを選択して、配信スケジュールを選びます。

   - 保留時間 — Control Manager で最新コンポーネントをダウンロードした後、指定した間隔に従って、配信を遅らせます。

     メニューを使用して、時間または分単位で保留期間を指定します。

   - 開始時刻 — 指定した時刻に配信を実行します。

     メニューを使用して、時間または分単位で配信時刻を指定します。

7. スケジュールを適用する製品ディレクトリのフォルダを選択します。選択したフォルダに含まれるすべての製品に対して、スケジュールが適用されます。
8. [OK] をクリックします。
9. [保存] をクリックして、新規配信計画を適用します。

プロキシの設定

コンポーネントのダウンロードおよびライセンスのアップデートに使用するプロキシサーバ接続を設定します。

プロキシサーバを設定するには

1. [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [プロキシの設定] をクリックします。[接続の設定] 画面が表示されます。

4. [プロキシサーバを使用してパターンファイル、エンジン、およびライセンスをアップデートする] チェックボックスをオンにします。

5. プロトコルを選択します。
   - HTTPS
   - SOCKS 4
   - SOCKS 5
6. [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。
7. [ポート] に、ポート番号を入力します。
8. サーバで認証が必要な場合は、ログオン名とパスワードを入力します。
9. [保存] をクリックします。

アップデート / 配信の設定

ネットワークの共有フォルダからコンポーネントをダウンロードするには、ローカル環境の Windows 認証と、リモート環境の UNC 認証を設定する必要があります。

「ローカル環境の Windows 認証」は、Control Manager サーバの Active Directory におけるユーザアカウントのことです。このアカウントには、次のものが必要です。

- 管理者権限
- 「バッチジョブとしてログオン」ポリシー設定

「リモート環境の UNC 認証」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許可を得ている、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です。

UNC パスからのダウンロードを有効にするには

1. 上部のメニューで [アップデート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。

3. [アップデート / 配信の設定] をクリックします。[アップデート / 配信の設定] 画面が表示されます。
4. [ローカル環境の Windows 認証] および [リモート環境の UNC 認証] に、ユーザ名とパスワードを入力します。
5. [保存] をクリックします。
6. [手動ダウンロード] または [予約ダウンロード] にアクセスします。
7. [ダウンロード設定]→[ダウンロード元] グループで、[その他のアップデートサーバ]を選択して、共有ネットワークフォルダを指定します。
8. [保存] をクリックします。

「バッチジョブとしてログオン」ポリシーの設定

「ローカル環境の Windows 認証」は、Control Manager サーバの Active Directory におけるユーザアカウントのことです。このアカウントには、次のものが必要です。

- 管理者権限
- 「バッチジョブとしてログオン」ポリシー設定

ユーザが「バッチジョブとしてログオン」リストに登録されていることを確認するには

1. [スタート]→[設定]→[コントロール パネル] の順にクリックします。
2. [管理ツール] をクリックします。
3. [ローカルセキュリティポリシー] を開きます。[ローカル セキュリティ設定] 画面が表示されます。
4. [ローカル ポリシー]→[ユーザー権利の割り当て] をクリックします。
5. [バッチ ジョブとしてログオン] をダブルクリックします。[バッチ ジョブとしてログオンのプロパティ] ダイアログボックスが表示されます。
6. 対象ユーザがリストに表示されない場合は、そのユーザを追加します。

第 6 章

Control Manager システムの監視

Trend Micro Control Manager (以下、Control Manager) には、Control Manager システムを監視するためのオプションがいくつかあります。概要画面、通知、ログ、およびレポートは、いずれも、ネットワークの監視に使用できます。

本章は次の内容で構成されています。

Control Manager の概要画面の表示

Control Manager には、管理下の製品コンポーネントとネットワーク保護に関する各種情報を要約表示する便利な概要画面が用意されています。

注意： 本トピックには 2008 年 5 月現在、日本ではリリース / サポートされていない製品も記載されています。

[ホーム] 画面

[ホーム] 画面を使用して、Control Manager によって管理される製品ネットワークの概要を一覧表示します。[ホーム] 画面には、次の各セクションがあります。

表 6-1. [ホーム] 画面の情報

セクション	説明
ウイルス対策概要	Control Manager に登録されている、ウイルス対策保護 / 検出機能を持つすべての管理下の製品の概要情報が表示されます。ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.)、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS)、Total Discovery Appliance などが該当します。
スパイウェア概要	Control Manager に登録されている、スパイウェア対策保護 / 検出機能を持つすべての管理下の製品の概要情報が表示されます。ウイルスバスター Corp.、InterScan MSS、Total Discovery Appliance などが該当します。
コンテンツ対策概要	Control Manager に登録されている、コンテンツ対策保護 / 検出機能を持つすべての管理下の製品の概要情報が表示されます。InterScan MSS、Total Discovery Appliance などが該当します。
Web セキュリティ概要	Control Manager に登録されている、Web 対策保護 / 検出機能を持つすべての管理下の製品の概要情報が表示されます。ウイルスバスター Corp.、Trend Micro InterScan Web Security Suite (以下、IWSS)、Total Discovery Appliance などが該当します。

表 6-1.　[ホーム] 画面の情報

セクション	説明
ネットワークウイルス概要	Control Manager に登録されている、ネットワークウイルス対策保護 / 検出機能を持つすべての管理下の製品の概要情報が表示されます。Trend Micro Network VirusWall Enforcer (以下、Network VirusWall Enforcer) 、Total Discovery Appliance などが該当します。
違反ステータス	管理者によって作成された Network VirusWall Enforcer のポリシーに違反したすべてのクライアントの概要情報が表示されます。
コンポーネントステータス	登録されているすべての管理下の製品のコンポーネントの概要情報が表示されます。Control Manager サーバに登録されている製品のコンポーネントに関する情報のみが表示されます。 たとえば、Control Manager サーバにウイルスバスター Corp. サーバのみ登録されている場合は、ウイルスバスター Corp. のコンポーネントのみが表示されます。

ヒント： 各表の右側の列に表示されている下線付きの数字をクリックすると、詳細情報画面が開き、その行の項目に関する詳細情報が表示されます。

例 : [ウイルス対策概要] 表で [駆除] 行に対応する数字をクリックすると、詳細情報画面が開きます。この詳細情報画面には、駆除されたすべてのコンポーネントに関する情報が表示されます。

コマンド追跡の使用

Control Manager サーバでは、管理下の製品と下位サーバに対して発行されたすべてのコマンドのレコードを保持しています。コマンドとは、管理下の製品または下位サーバに対して、コンポーネントのアップデートなどの特定のタスクを実行するように送られる指示のことです。コマンド追跡を使用すると、すべてのコマンドの進行状況を監視することができます。

たとえば、終了するまでに数分間かかることがある ScanNow 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を参照して結果を調べることができます。

[コマンド追跡] 画面には、次の項目の詳細が表示されます。

表 6-2. コマンド追跡の詳細

情報	説明
発行日時	Control Manager サーバが管理下の製品または下位サーバに対してコマンドを発行した日付と時刻
コマンド	発行されたコマンドの種類
成功	コマンドを完了した管理下の製品または下位サーバの台数
失敗	コマンドを実行できなかった管理下の製品または下位サーバの台数
処理中	現在コマンドを実行している管理下の製品または下位サーバの台数
すべて	Control Manager がコマンドを発行した管理下の製品または下位サーバの合計台数

[成功]、[失敗]、[処理中]、または [すべて] の列のリンクをクリックすると、[コマンド詳細] 画面が表示されます。

コマンド詳細について

[コマンド詳細] 画面には、コマンドの結果に関する詳細な情報が表示されます。Control Manager では、次の単位でコマンド詳細が記録およびグループ化されます。

- 関連する管理下の製品またはサービス
- 開始日時 — Control Manager サーバによって管理下の製品または下位サーバに対してコマンドが発行された日時が追加コマンド情報とともに示されます。

  たとえば、手動ダウンロードを実行すると、発行されたフィールドには、Control Manager がダウンロードできた、またはできなかったコンポーネントに関するパラメータ情報が表示されます。手動ダウンロードコマンド詳細に、「エンジン」というパラメータが含まれる場合があります。これによって、Control Manager が検索エンジンコンポーネントをダウンロードしたことがわかります。追加の詳細が適用されないコマンドの場合、パラメータは「該当なし」です。

- 前回のレポート日時 — Control Manager サーバで、管理下の製品または下位サーバからの応答が受信された日時が示されます。
- ユーザ (アカウント) — 管理下の製品または下位サーバに対してタスクを発行したユーザアカウントが示されます。
- 成功 — コマンドを完了した管理下の製品または下位サーバの数が示されます。
- 失敗 — コマンドを実行できなかった管理下の製品または下位サーバの数が示されます。
- 処理中 — 現在コマンドを実行中の管理下の製品または下位サーバの数が示されます。

個々の製品またはサービスの詳細について

- 前回のレポート日時 — 管理下の製品から Control Manager サーバに応答が送信された日時が示されます。
- サーバ / エンティティ — 下位サーバまたは管理下の製品サーバのホスト名が示されます。
- ステータス — 発行されたコマンドのステータスが示されます。

  たとえば、下位サーバに対してパターン / ルールの配信を実行するときに、下位サーバにすでに最新のパターンファイルが格納されている場合、[ステータス] は [スキップ] となります。

  次に、[ステータス] の値を示します。

表 6-3. [コマンド詳細] のステータス

成功	処理中	失敗
スキップ	送信	タイムアウト
サポートなし	追跡	キャンセル
成功	要求送信完了	使用不可
		失敗

- 説明 — ステータスの説明です。

[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、[クエリ (コマンド追跡)] 画面を使用します。

24 時間以内に発行されたコマンドをクエリおよび表示するには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [コマンド追跡] を選択します。[コマンド追跡] 画面が表示されます。

3. 作業領域で、[クエリ] をクリックします。[クエリ (コマンド追跡)] 画面が表示されます。

4. [クエリ (コマンド追跡)] で、次のパラメータの値を指定します。

- 対象期間 — クエリの範囲を指定します。

  あらかじめ設定されている範囲から選択するか、または独自の範囲を指定します。範囲を指定する場合は、年、月、日を指定します。

- コマンド — 監視するコマンドを選択します。
- ユーザ (アカウント) — 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 — コマンドのステータスを選択します。
- ソートの種類 — 結果をどのように [クエリ結果 (コマンド追跡)] 画面に表示するか指定します。

  時間、コマンド、またはユーザによってクエリ結果が配置されます。

- 表示順序 — 結果を昇順と降順のどちらで [クエリ結果 (コマンド追跡)] 画面に表示するか指定します。

5. [コマンドの表示] をクリックします。[クエリ結果 (コマンド追跡)] 画面に、コマンドを実行した製品数とその実行結果が表示されます。

[成功]、[失敗]、[処理中]、または [すべて] の列のリンクをクリックして、[コマンド詳細] 画面を表示します。

イベントセンターの使用

イベントとは、管理下の製品によって検出されて、Control Manager サーバに転送されるアクションのことです。イベントセンターを使用すると、さまざまなイベントの通知を設定できます。

イベントセンターでは、次の種類に従ってイベントを分類します。

表 6-4. イベントセンターのイベント

情報	説明
アラート	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、194 ページの表 6-5「アラートイベント」を参照してください。
大規模感染予防サービス	ポリシーの適用に関する情報と、大規模感染予防サービスに関するアップデート情報を提供します。 大規模感染予防サービスの通知タイプでは、次のサービスイベントがグループ化されます。 ・アクティブ大規模感染予防ポリシー受信 ・大規模感染予防モード開始 ・大規模感染予防モード停止 ・大規模感染予防ポリシーアップデート失敗 ・大規模感染予防ポリシーアップデート成功
脆弱性診断サービス	「脆弱性診断タスク完了」のイベントに関する通知を送信します。
統計	Network VirusWall 製品の「違反の統計」のイベントに関する通知を送信します。
アップデート	ウイルス対策コンポーネントとコンテンツセキュリティコンポーネントのアップデート結果 (成功か失敗か) を通知します。詳細については、194 ページの表 6-6「アップデートアラートイベント」を参照してください。
異常	製品オプションや、サービスのアクティベーションとアクティベーション解除に関する情報を提供します。詳細については、195 ページの表 6-7「異常アラートイベント」を参照してください。
セキュリティ違反	メールメッセージのコンテンツ違反およびクライアントの Web 違反について、警告を発します。詳細については、194 ページの表 6-5「アラートイベント」を参照してください。

表 6-5.　アラートイベント

アラート	説明
ウイルスアウトブレークアラート	管理下のウイルス対策製品に適用されます。
特定ウイルス用アラート	管理下のウイルス対策製品に適用されます。
ウイルス検出	• 1 次処理 /2 次処理失敗 — 管理下のウイルス対策製品に適用されます。 • 1 次処理成功 — 管理下のウイルス対策製品に適用されます。 • 2 次処理成功 — 管理下のウイルス対策製品に適用されます。
特定スパイウェア用アラート	管理下のスパイウェア対策製品に適用されます。
スパイウェア検出	• スパイウェア検出 — 処理成功 — 管理下のスパイウェア対策製品に適用されます。 • スパイウェア検出 — 1 次および 2 次処理失敗 / 使用不可 — 管理下のスパイウェア対策製品に適用されます。
ネットワークウイルスアラート	Network VirusWall などのパケット検索製品に適用されます。
脆弱性に対する攻撃の兆候	Network VirusWall などのパケット検索製品に適用されます。

表 6-6.　アップデートアラートイベント

アラート	説明
エンジンアップデート失敗	管理下のウイルス対策製品に適用されます。
エンジンアップデート成功	管理下のウイルス対策製品に適用されます。
パターンファイル / テンプレートアップデート失敗	管理下のウイルス対策製品に適用されます。
パターンファイル / テンプレートアップデート成功	管理下のウイルス対策製品に適用されます。
スパムメール判定ルールアップデート失敗	管理下のコンテンツセキュリティ製品に適用されます。
スパムメール判定ルールアップデート成功	管理下のコンテンツセキュリティ製品に適用されます。

表 6-7.　異常アラートイベント

アラート	説明
リアルタイム検索開始	管理下のウイルス対策製品に適用されます。
リアルタイム検索停止	管理下のウイルス対策製品に適用されます。
サービス開始	管理下のウイルス対策製品およびコンテンツセキュリティ製品に適用されます。
サービス停止	管理下のウイルス対策製品およびコンテンツセキュリティ製品に適用されます。

表 6-8.　セキュリティ違反イベント

アラート	説明
コンテンツセキュリティ違反	管理下のコンテンツセキュリティ製品に適用されます。InterScan MSS などが該当します。
Web セキュリティ違反	管理下の Web セキュリティ製品に適用されます。IWSS などが該当します。

通知メッセージのカスタマイズ

イベントの通知をカスタマイズするには変数を使用します。通知の設定時にこれらの変数を挿入して、通知の受信者に詳細を連絡できるようにします。

使用可能な変数には次のものがあります。

表 6-9.　一般的な変数

タグ	説明
すべてのイベント通知で使用される一般変数	
%cmserver%	Control Manager サーバのホスト名
%computer%	イベントが検出されたクライアントコンピュータのネットワーク名
%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

表 6-9.　一般的な変数

タグ	説明
%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)
%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
%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

表 6-10.　ウイルス関連の通知メッセージの変数

タグ	説明
ウイルス変数 — アラートまたは大規模感染予防サービスイベントの通知で使用されます。	
%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、およびアクティブ大規模感染予防ポリシー受信と大規模感染予防サービス開始の通知タイプで使用されます。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。 • アクティブ大規模感染予防ポリシー受信および大規模感染予防サービス開始の通知タイプとしては、この変数は必要な大規模感染予防ポリシーを示します。
%ptnver%	• パターンファイル番号。 • アラートイベントカテゴリ、およびアクティブ大規模感染予防ポリシー受信と大規模感染予防サービス開始の通知タイプで使用されます。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。 • アクティブ大規模感染予防ポリシー受信および大規模感染予防サービス開始の通知タイプとしては、この変数は必要な大規模感染予防ポリシーを示します。
%threat_info%	• 大規模感染予防ポリシーによって提供されるウイルス / 不正プログラムの脅威情報。 • アクティブ大規模感染予防ポリシー受信および大規模感染予防サービス開始で使用されます。

表 6-10. ウイルス関連の通知メッセージの変数

タグ	説明
%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。 • たとえば、管理下のウイルス対策製品によってメールメッセージからウイルス / 不正プログラムが検出された場合、宛先のユーザ名が %vdest% の値となります。 • アラートイベントカテゴリで使用されます。
%vfile%	感染ファイル名。アラートイベント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。

表 6-11. その他の通知メッセージの変数

タグ	説明
その他の変数 — ダメージクリーンナップサービス、Network VirusWall、および脆弱性診断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 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、ダメージクリーンナップタスク完了、および脆弱性診断タスク完了のイベントで使用されるエラーの説明。

Control Manager では、Control Manager システムで発生したイベント通知を、個人の受信者や受信者グループに送信できます。次の方法で通知が送信されるようにイベントセンターを設定します。

表 6-12. 通知の送信方法

送信方法	説明
メール通知	企業のメールメッセージシステムまたは SMTP アカウント (たとえば、Yahoo や Hotmail) に属するメールボックスに送信されるメッセージです。
Windows イベントログ通知	Windows Event Viewer アプリケーションのログに、Control Manager によって記録されたイベントが格納されます。
SNMP トラップ通知	SNMP (Small Network Management Protocol) トラップは、SNMP プロトコルをサポートする管理コンソールを使用しているネットワーク管理者に、通知を送信する方法です。 通知は、MIB (Management Information Base) に格納されます。SNMP トラップ通知を表示するときは、MIB ブラウザを使用します。
ポケットベル通知	数字からなるメッセージを送信できます。
アプリケーション通知	通知の送信に使用するアプリケーションを指定できます。 たとえば、組織で net send コマンドを呼び出すバッチファイルを使用しているとします。この場合、[パラメータ] を使用して、トリガアプリケーションによって適用されるコマンドを定義します。
MSN™ Messenger 通知	オンラインの MSN Messenger アカウントに通知が送信されます。 Control Manager から、オンラインの MSN Messenger アカウントに通知が送信されます。オフラインの MSN Messenger アカウントは Control Manager からの通知を受信することはできません。
Syslog	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、他のサポート対象製品に直接 syslog を転送できます。たとえば、Cisco Security Monitoring、Analysis and Response System (MARS) などに対応しています。

通知の有効化または無効化

[イベントセンター] 画面から通知を有効または無効にします。

通知を有効または無効にするには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [イベントセンター] を選択します。[イベントセンター] 画面が表示されます。

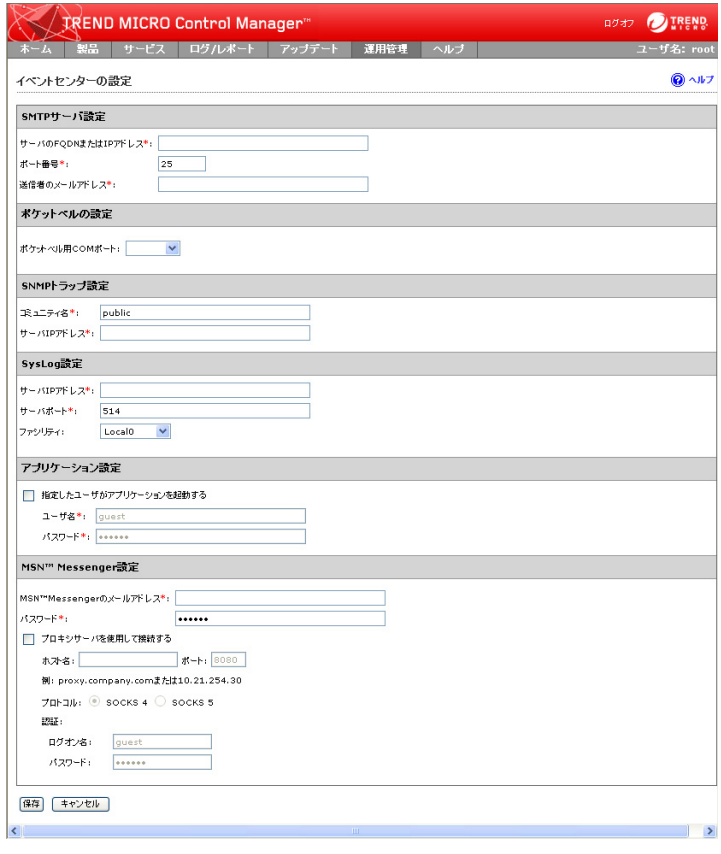
3. 有効または無効にするイベント通知に対応するイベントカテゴリを展開します。
4. 次のいずれかを実行します。
   - 個々のイベントのチェックボックスをオンまたはオフにします。
   - [イベント] チェックボックスをオンまたはオフにして、セクション全体のすべての通知を選択します。
5. [保存] をクリックします。

通知方法の設定

[イベントセンター] 画面を使用して、各種通知方法の詳細を設定します。

通知方法を設定するには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [イベントセンターの設定] サブメニューを選択します。[イベントセンターの設定] 画面が表示されます。



4. 通知方法を設定します。

メール通知を設定する場合

a. 作業領域の [SMTP サーバ設定] で、SMTP サーバのホスト名とポート番号を入力します。proxy.company.com などの完全修飾ドメイン名 (FQDN) を使用するか、SMTP サーバの IP アドレスを使用します。

b. Control Manager 送信者のメールアドレスを入力します。このアドレスは、一部の SMTP サーバで必要となる送信者のアドレスとして使用されます。

ポケットベル通知を設定する場合

- 作業領域の [ポケットベル用 COM ポート] で、リストから該当する COM ポートを選択します。

SNMP 通知を設定する場合

a. 右側の画面の [SNMP トラップ設定] で、コミュニティ名を指定します。

b. SNMP トラップサーバの IP アドレスを指定します。

syslog 通知を設定する場合

a. 右側の画面の [SysLog 設定] で、syslog サーバのホスト名とポート番号を入力します。proxy.company.com などの完全修飾ドメイン名 (FQDN) を使用するか、syslog サーバの IP アドレスを使用します。

b. syslog に使用するファシリティを指定します。

アプリケーション通知を設定する場合

a. 右側の画面の [アプリケーション設定] で、[指定したユーザがアプリケーションを起動] を選択します。

b. 通知の送信に使用するアプリケーションを起動するユーザのユーザ名とパスワーを入力します。

MSN Messenger 通知を設定する場合

a. 作業領域の [MSN™ Messenger 設定] で、MSN Messenger のメールアドレスを指定します。これは、MSN Messenger のユーザ名です。

b. .Net Passport のメールアドレスのパスワードを入力します。

c. インターネット接続にプロキシサーバを使用する場合、[プロキシサーバを使用して接続する] をオンにします。

   i. プロキシサーバのホスト名とポートを指定します。

   ii. プロキシサーバのプロトコルとして [SOCKS 4] または [SOCKS 5] を選択します。

   iii. プロキシ認証に使用するログオン名とパスワードを入力します。

5. [保存] をクリックします。

通知の受信者の設定と通知の配信のテスト

[ユーザおよびグループの選択] 画面を使用して、イベントごとの通知の受信者を設定します。

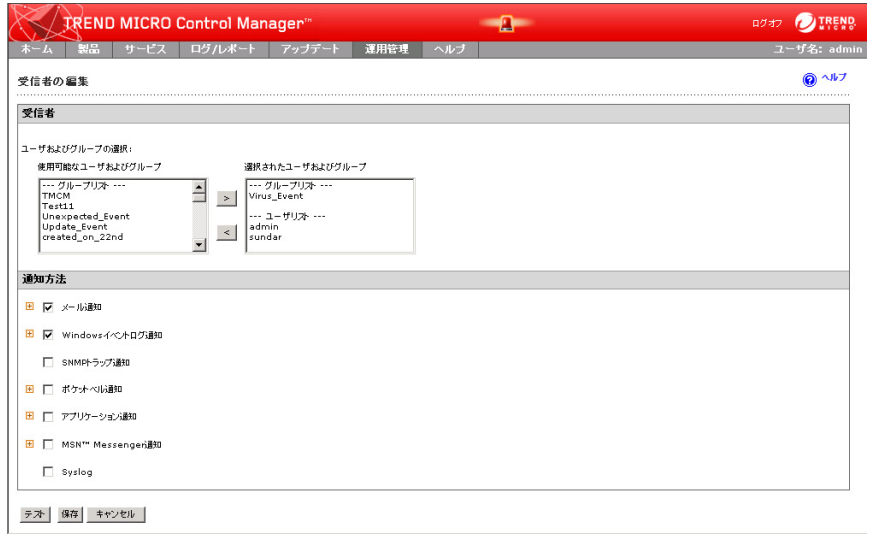
通知の受信者を設定し通知の配信をテストするには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. ドロップダウンメニューから [イベントセンター] を選択します。[イベントセンター] 画面が表示されます。

3. 設定対象のイベント通知に対応するイベントカテゴリを展開します。

4. 設定するイベントの [受信者] リンクをクリックします。[ユーザおよびグループの選択] 画面が表示されます。



5. [受信者] で [選択されたユーザおよびグループ] リストにユーザを指定または削除して、通知の受信者を設定します。

受信者をリストに追加する場合

a. [使用可能なユーザおよびグループ] リストのユーザまたはグループをクリックします。複数の受信者を選択するときは、<Ctrl> キーを押しながら選択します。

b.  をクリックして、[受信者] リストにエントリを追加します。

受信者をリストから削除する場合

a. [受信者] リストからユーザまたはグループをクリックします。複数の受信者を選択するときは、<Ctrl> キーを押しながら選択します。

b.  をクリックして、[受信者] リストからエントリを削除します。

6. 設定する通知方法のチェックボックスをオンにします。

   [イベントセンターの設定] 画面で、通知方法を設定します。199 ページの「通知方法の設定」を参照してください。

7. 設定した通知方法を展開して、対応するメッセージフィールドに通知内容を入力します。

8. [テスト] をクリックして、システムから通知を配信できるかどうかテストします。

9. [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の設定

アウトブレークアラートにより、管理下のシステム全体のウイルス / 不正プログラムの感染状況を把握できます。

ウイルスアウトブレークアラートを設定するには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. ドロップダウンメニューから [イベントセンター] を選択します。[イベントセンター] 画面が表示されます。

3. [アラート] イベントカテゴリを展開し、ウイルスアウトブレークアラートに対する [設定] リンクをクリックします。[ウイルスアウトブレークアラートの設定] 画面が表示されます。

4. [アラートの設定] で、次の項目を指定します。
   - **検出** — アウトブレークアラートをトリガするウイルスの件数
   - コンピュータまたはユーザ — 感染したコンピュータまたはユーザの数
   - **期間** — ウイルス検出パラメータの対象となる期間
5. [保存] をクリックします。

特定ウイルス用アラートの設定

システムでウイルス / 不正プログラムが検出されたら、必ず通知を送信するように Control Manager を設定します。特定ウイルス用アラートを設定すると、ウイルス / 不正プログラムの大規模感染の危険性に対して早期に警告を発することができます。

特定ウイルス用アラートを設定するには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [イベントセンター] を選択します。[イベントセンター] 画面が表示されます。
3. [アラート] イベントカテゴリを展開し、特定ウイルス用アラートに対する [設定] リンクをクリックします。

4. 監視対象のウイルス名を指定します。最大 10 件のウイルスを指定します。

5. [アラートの設定] で、ドロップダウンリストボックスを使用して [期間] を時間単位で指定します。

6. [保存] をクリックします。

特定スパイウェア用アラートの設定

システムでスパイウェアが検出されたら、必ず通知を送信するように Control Manager を設定します。特定スパイウェア用アラート通知を設定すると、スパイウェアの危険性に対して早期に警告を発することができます。

特定スパイウェア用アラートを設定するには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. ドロップダウンメニューから [イベントセンター] を選択します。[イベントセンター] 画面が表示されます。

3. [アラート] イベントカテゴリを展開し、特定スパイウェア用アラートに対する [設定] リンクをクリックします。

4. 監視対象のスパイウェア名を指定します。スパイウェアを 10 件まで指定できます。

5. [アラートの設定] で、ドロップダウンリストボックスを使用して [期間] を時間単位で指定します。

6. [保存] をクリックします。

ネットワークウイルスアラートの設定

ネットワークウイルスアラートでは、システム全体におけるネットワークウイルスの大規模感染の危険性について警告します。

ネットワークウイルスアラートを設定するには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [イベントセンター] を選択します。[イベントセンター] 画面が表示されます。
3. [アラート] イベントカテゴリを展開し、ネットワークウイルスアラートに対する [設定] リンクをクリックします。

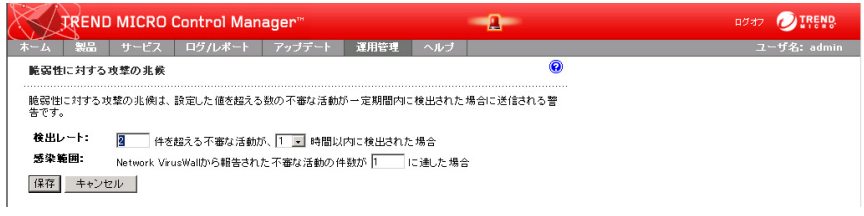
4. [アラートの設定] で、次の項目を指定します。
   - **検出** — アウトブレークアラートをトリガするウイルスの件数
   - コンピュータまたはユーザ — 感染したコンピュータまたはユーザの数
   - **期間** — ウイルス検出パラメータの対象となる期間
5. [保存] をクリックします。

脆弱性に対する攻撃の兆候の設定

脆弱性に対する攻撃の兆候では、システムの脆弱性に対する攻撃の危険性を警告します。

脆弱性に対する攻撃の兆候通知を設定するには

1. 上部のメニューの [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [イベントセンター] を選択します。[イベントセンター] 画面が表示されます。
3. [アラート] イベントカテゴリを展開し、脆弱性に対する攻撃の兆候に対する [設定] リンクをクリックします。



4. [アラートの設定] で、次の項目を指定します。
   - **検出数** — アウトブレークアラートをトリガするウイルスの件数
   - コンピュータまたはユーザ — 感染したコンピュータまたはユーザの数
   - **期間** — ウイルス検出パラメータの対象となる期間
5. [保存] をクリックします。

ログの使用

Control Manager ではさまざまな種類のログからデータを受け取りますが、ユーザが Control Manager データベースに対してログデータを直接検索できるようになりました。ユーザはフィルタ条件を指定することで、必要なデータのみを収集できます。

また、ログの集約機能が Control Manager に導入されました。ログの集約により、クエリのパフォーマンスが向上します。また、管理下の製品から Control Manager へのログの送信時に必要となるネットワーク帯域幅の消費を低減できます。その反面、集約により、データの一部が失われることになります。Control Manager データベースにないデータは検索できません。

Control Manager で生成されるログについて

Control Manager サーバでは、アクセスとシステムイベントの 2 種類のサーバログが作成されます。

表 6-13. Control Manager サーバログ

サーバログ	説明
アクセスログ	このログには、Control Manager 管理コンソールへのログオンから製品ディレクトリのフォルダ名の変更にいたるまで、ユーザが Control Manager 管理コンソールを使用して実行した処理がすべて記録されます。
サーバイベントログ	このログには、Control Manager サーバで発生したイベントのうち、ユーザによる処理以外のイベントがすべて記録されます。

管理下の製品のログについて

管理下の製品のログには、Control Manager 管理下の製品のパフォーマンスに関する情報が記録されます。クライアントログからは、上位サーバまたは下位サーバによって管理される特定の製品や製品のグループに関する情報を取得できます。Control Manager のデータクエリ機能とフィルタ機能により、管理者は必要な情報のみに焦点を当てることが可能となります。

管理下の製品では、Windows イベントログのほか、製品の機能に応じて、さまざまな種類のログが作成されます。

表 6-14. 管理下の製品のログ

サーバログ	説明
イベントログ	ユーザまたはコンピュータによって開始された処理が記録されます。次のいずれかまたはすべてのイベントをクエリできます。 ・ウイルスアウトブレーク ・モジュールアップデート ・サービス開始 ・サービス停止 ・セキュリティ違反 ・脆弱性に対する攻撃の兆候
セキュリティログ — ウイルス /Web セキュリティ	ウイルス感染やコンテンツセキュリティ違反の発生源についての情報が記録されます。この発生源は、「経路」とも呼ばれます。次の経路の種類に従って、ログを確認できます。 ・コンテンツセキュリティ違反 ・ダウンロードトラフィックからのウイルス検出 ・メールメッセージからのウイルス検出 ・ファイルからのウイルス検出 ・Web セキュリティ違反 ・ネットワークセキュリティ違反
ステータスログ	管理下の製品または下位サーバの環境に関する情報が記録されます。[ステータス] タブでこの情報が使用されます。

次の表に、管理下の製品から Control Manager に送信されるログを示します。

注意： 本トピックには 2008 年 5 月現在、日本ではリリース / サポートされていない製品も記載されています。

表 6-15. Control Manager 管理下の製品のログ

管理下の製品	イベントログ	ウイルス / スパイウェアログ	セキュリティログ	Web セキュリティログ	ネットワークウイルスログ	ステータスログ	URL アクセスログ	パフォーマンス測定ログ	エンドポイントログ	セキュリティ違反ログ	セキュリティ遵守ログ	セキュリティ統計ログ
InterScan eManager	●		●			●						●
InterScan Messaging Security Suite	●	●	●			●						●
InterScan Web Security Suite	●	●		●		●	●					●
InterScan for Cisco CSC SSM	●	●	●	●	●	●	●					
ウイルスバスター コーポレートエディション	●	●				●			●			●
ServerProtect	●	●				●						●
ServerProtect for Linux												
ScanMail eManager	●		●			●						●
InterScan for Domino/Lotus Notes	●	●				●						●
InterScan for Microsoft Exchange	●	●				●						●
Network VirusWall 2500	●				●	●				●	●	●
Network VirusWall Enforcer 2500	●				●	●				●	●	●

表 6-15. Control Manager 管理下の製品のログ

管理下の製品	イベントログ	ウイルス / スパイウェアログ	セキュリティログ	Web セキュリティログ	ネットワークウイルスログ	ステータスログ	URL アクセスログ	パフォーマンス測定ログ	エンドポイントログ	セキュリティ違反ログ	セキュリティ遵守ログ	セキュリティ統計ログ
Network VirusWall 1200	●				●	●				●	●	
Network VirusWall Enforcer 1200	●				●	●				●	●	

ヒント： 多くのログを保管すると、Control Manager システムのパフォーマンスに関する豊富な情報を参照できるようになります。ただし、ディスクの容量を消費する原因にもなります。したがって、あまり多くのディスク領域が消費されないように、ログサイズを制限する必要があります。

ログ集約について

Control Manager のログ集約機能を使用すると、管理下の製品によって消費されるネットワーク帯域幅が低減されます。管理者は、ログ集約を設定することにより、管理下の製品から Control Manager に送信されるログ情報を選択できます。

警告： ログ集約には代償があります。管理下の製品から Control Manager に送信されない情報は失われます。Control Manager では、サーバにない情報に対してレポートやクエリを作成できません。これによって問題が生じる場合があります。たとえば、ある情報を重要でないと判断し管理下の製品で破棄した後に、その情報が重要となり、破棄した情報を復元できない場合です。

ログ集約を設定するには

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [ログ集約の設定] サブメニューを選択します。[ログ集約ルールの編集] 画面が表示されます。

4. [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。
5. 管理下の製品から Control Manager に送信しないデータに対応するチェックボックスをオフにします。
6. [保存] をクリックします。

ログデータの検索

Control Manager では、Control Manager のログと管理下の製品のログから、管理者が必要とする情報のみを収集できるようになりました。この機能は、アドホッククエリの使用により実現されます。アドホッククエリにより、管理者は、直接 Control Manager データベースから情報をすばやく取得できるようになります。データベースには、Control Manager サーバに登録されたすべての製品から収集された情報がすべて格納されています (ログ集約によりクエリが可能なデータに影響を与えます)。アドホッククエリによるデータベースからのデータの直接取得は、管理者にとって非常に強力なツールとなります。

管理者は、データの検索時に、クエリ条件にフィルタを適用することで、必要なデータのみが返されるように指定できます。データを取得したら、管理者は、それらを今後の解析用に CSV 形式または XML 形式にエクスポートすることも、クエリを保存して再利用することもできます。また、Control Manager では、保存したクエリをユーザ間で共有できるため、他のユーザがクエリを有効に活用することもできます。

アドホッククエリの使用手順は、次のとおりです。

手順 1: クエリ先として管理下の製品またはログオン中の Control Manager サーバを選択する

手順 2: クエリ用のデータビューを選択する

手順 3: フィルタ条件と表示する情報を指定する

手順 4: クエリを保存および実行する

手順 5: 取得したデータを CSV 形式または XML 形式にエクスポートする

注意： Control Manager では、保存したアドホッククエリをユーザ間で共有できます。保存して共有されるクエリは、[ログ / レポート]→[保存されたアドホッククエリ] 画面に表示されます。

データビューについて

データビューは、関連付けられたデータセルのクラスタによって構成されるテーブルです。データビューは、Control Manager データベースに対してアドホッククエリを実行するための基盤となります。

Control Manager のデータビューは、製品情報とセキュリティ上の脅威情報の 2 つの主要なカテゴリに分類されます。データベースの詳細については、429 ページの「データビューについて」を参照してください。2 つの主要なカテゴリは、さらにいくつかのサブカテゴリに分類され、各サブカテゴリには概要情報と詳細情報があります。

Control Manager の管理コンソールには、データビューと、各データビューで使用可能な情報が表示されます。

表 6-16. Control Manager データビューの主要カテゴリ

主要カテゴリ	説明
製品情報	次の項目に関する情報が表示されます。 ・Control Manager ・管理下の製品 ・管理下の製品コンポーネント ・製品ライセンス
セキュリティ上の脅威情報	管理下の製品によって検出された次のセキュリティ上の脅威に関する情報が表示されます。 ・全体的な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 ・コンテンツ違反 ・スパムメール ・Web コンテンツ違反 ・ポリシー/ ルール違反 ・脅威の兆候

注意： Control Manager によってサポートされる使用可能なデータビューの詳細については、429 ページの「データビューについて」を参照してください。

アドホッククエリの実行

アドホッククエリは、Control Manager データベースに対して、情報を直接要求する手段です。アドホッククエリでは、要求の対象範囲を絞り込みパフォーマンスを向上させる目的で、データビューが使用されます。データビューの指定に加えて、要求に対してフィルタ条件を指定することで、さらに検索を絞り込むことができます。

アドホッククエリを実行するときは、最初に、現在ログオン中の Control Manager サーバにクエリを実行するか、Control Manager が管理する管理下の製品にクエリを実行するかを指定します。管理下の製品には、他の Control Manager 下位サーバも含まれます。

データの取得元とする管理下の製品 / ディレクトリを選択したら、クエリに使用するデータビューを選択します。データビューの詳細については、214 ページの「データビューについて」を参照してください。

データビューを選択した、クエリのフィルタ条件、クエリ結果として表示する情報、および情報の表示順序を指定します。

注意： アドホッククエリのデータフィルタには、最大で 20 件の条件を指定できます。

最後に、将来の再利用に備えてクエリを保存するかどうかを指定します。Control Manager では、保存したクエリをユーザ間で共有できるため、他のユーザがクエリを有効に活用することもできます。

たとえば、ウイルスバスター Corp. の管理者である Chris が、自分が担当するウイルスバスター Corp. サーバのパターンファイルのステータスをチェックする必要があるとします。最初に、Chris は管理下の製品を選択します。次に、[製品情報]→[コンポーネント情報] の順に選択し、そこでデータビューの [管理下の製品のパターンファイル / ルールステータス] を選択します。プロセスの次の手順に進む前に、フィルタ条件として、「製品の種類 : ウイルスバスター Corp、パターンファイルのステータス : 期限切れ」を指定します。[列の表示を変更する] をクリックします。また、クエリの完了後にクエリ結果として表示するフィールドを選択します。表示情報として、パターンファイルのバージョン、ホスト名、および IP アドレスを選択します。製品名とパターンファイルのステータスはフィルタ条件として絞り込まれているため、選択の必要はありません。

アドホッククエリを実行するには

1. 上部のメニューで [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [新規アドホッククエリ] をクリックします。[アドホッククエリ] 画面が表示されます。

手順 1: 情報の発生元の指定

1. [アドホッククエリ] 画面から、検索情報の発生元を指定します。
   - Control Manager の選択 — 情報の発生元となる、ユーザがログオン中の Control Manager サーバを指定します。

     このオプションを指定すると製品ツリーが無効になります。ユーザがログオンしている Control Manager サーバからの情報のみが検索対象になるためです。
   - 製品ツリーの選択 — 情報の発生元となる、Control Manager サーバが管理している管理下の製品を指定します。

このオプションを指定すると、情報の発生元となる防御策カテゴリを選択する必要があります。製品ディレクトリから管理下の製品 / ディレクトリを選択すれば、このカテゴリは選択されます。

注意： この画面で管理下の製品 / ディレクトリを選択すると、次の画面で表示されるデータビューが変わります。

たとえば、製品ディレクトリでウイルスバスター Corp. を選択すると、デスクトップ保護に関連付けられたデータビューのみが [使用可能なデータビュー] リストに表示されます。

2. [次へ] をクリックします。[データビュー] 画面が表示されます。

手順 2: クエリ用のデータビューの指定

1. [使用可能なデータビュー] リストから、必要なデータビューを選択します。データビューの詳細については、214 ページの「データビューについて」を参照してください。

2. [次へ] をクリックします。[クエリ条件] 画面が表示されます。

手順 3: 表示順序の指定

1. クエリ結果として返される情報の表示と順序を指定します。

   a. [列の表示を変更する] をクリックします。[表示順序の選択] 画面が表示されます。

b. クエリから情報が返されたときに表示するデータビューの列を、[使用可能なフィールド] リストから選択します。選択した列が反転表示します。

ヒント： 列は 1 度に 1 列ずつ選択するか、<Shift> または <Ctrl> キーを使用して複数列を選択します。

1 度に 1 列ずつ選択し追加すると、情報がその順序で表示され、表示順序の指定にもなります。

---

c. [追加] ボタンをクリックして、選択した列を [選択されたフィールド] リストに移動させます。選択した列が [選択されたフィールド] リストに表示されます。

d. 列の選択と追加を、必要に応じて繰り返します。

e. [選択されたフィールド] リストで列を選択してから、[上に移動] または [下に移動] ボタンを使用して、情報の表示順序を指定します。リストの一番上にある列が、クエリ結果では左端の列として表示されます。

f. [戻る] をクリックします。[クエリ条件] 画面が表示されます。

手順 4: フィルタ条件の指定

概要データ (タイトルに「概要」という単語のあるデータビュー) に対してクエリを実行するときは、[必要な条件] で項目を指定する必要があります。

1. [必要な条件] を指定します。
   - データの [集計日時] を指定するか、COOKIE をレポートに表示するかどうかを指定します。
2. [カスタム条件] を指定します。
   a. [カスタム条件] を選択します。カスタム条件オプションが表示されます。
   b. [キーワード] でデータカテゴリ用の条件フィルタルールを指定します。
      - すべての条件 — これを選択すると、論理積 (AND) として機能します。レポートに表示されるデータは、すべてのフィルタ条件に適合する必要があります。
      - いずれかの条件 — これを選択すると、論理和 (OR) として機能します。レポートに表示されるデータは、いずれかのフィルタ条件に適合する必要があります。
   c. データ用のフィルタ条件を指定します。Control Manager では、データのフィルタ用に最大 20 個の条件がサポートされています。

注意: フィルタ条件を指定しないと、アドホッククエリでは該当する列の結果がすべて返されます。フィルタ条件を指定して、クエリから返された情報のデータ分析を簡単にすることをお勧めします。

      i. 左側のドロップダウンリストから、フィルタ対象となる列を選択します。
      ii. 中央のドロップダウンリストから、フィルタに適用する一致条件を選択します。

iii. 右側のフィールドに、フィルタ条件を入力します。ここには、フィルタ対象として選択した列に応じて、リストボックスまたはテキストボックスが表示されています。

iv. データビューのフィルタ条件をさらに追加するには、[+] アイコンをクリックします。

手順 5: クエリの保存と実行

1. [クエリ設定の保存] の [保存されたアドホッククエリリストにこのクエリを保存します。] をクリックして、作成したアドホッククエリを保存します。

2. [クエリ名] に、保存するアドホッククエリの名前を入力します。

注意： Control Manager では、保存したアドホッククエリをユーザ間で共有できます。保存したクエリは、[ログ / レポート]→[ユーザのレポート] 画面に表示されます。

3. [クエリ] をクリックします。クエリの結果を表示する [アドホッククエリの結果] 画面が表示されます。

画面上の項目の詳細については、各項目の下線リンクをクリックしてください。

手順 6: クエリ結果の CSV 形式または XML 形式へのエクスポート

1. 次のオプションをクリックすると、[ファイルのダウンロード] ダイアログボックスが表示されます。

   - CSV 形式で出力 — クエリ結果を CSV ファイル形式でエクスポートできます。
   - XML 形式で出力 — クエリ結果を XML ファイル形式でエクスポートできます。

2. 次のいずれかを実行します。

   - [開く] をクリックし、クエリ結果を CSV 形式または XML 形式でただちに表示します。
   - [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。ファイルを保存する場所を指定します。

3. クエリ用の設定を保存するには

   a. [クエリ設定の保存] をクリックします。確認画面が表示されます。

b. 保存するクエリの名前を [クエリ名] に入力します。

c. [OK] をクリックします。保存したクエリが [保存されたアドホッククエリ] 画面に表示されます。

アドホッククエリの保存と共有

Control Manager では、ユーザが作成したアドホッククエリを保存できます。保存したアドホッククエリは、[ログ / レポート]→[保存されたアドホッククエリ] 画面に表示されます。[保存されたアドホッククエリ] 画面には、[ユーザのクエリ] と [使用可能なクエリ] の 2 つのタブがあります。

[保存されたアドホッククエリ] 画面の [ユーザのクエリ] タブには、ログオン中のユーザによって作成されたすべてのアドホッククエリが表示されます。[ユーザのクエリ] 画面では、クエリの追加、編集、表示、削除、エクスポート、共有化 / 共有解除の各タスクを実行できます。保存したクエリを共有化すると、そのクエリが他のユーザに対して公開されます。

注意： Control Manager のアクセス管理は、ユーザアカウントとユーザの種類を通じて実行されますが、これによりユーザがアクセス可能な情報が制限されます。これは、すべてのユーザ共有クエリを表示できても、アクセス管理によってクエリの実効性が制限されることを意味します。

例 : たとえば、ウイルスバスター Corp. の管理者である Chris が、ウイルスバスター Corp. の情報を対象としたアドホッククエリを作成し共有化したとします。InterScan for Microsoft Exchange の管理者である Sam 共有クエリにアクセス可能ですが、Chris のクエリを使用して独自のアドホッククエリを作成し、それを実行すると、空白の結果が返されます。これは、Sam にはウイルスバスター Corp. の情報へのアクセス権がないためです。この例では、Chris がウイルスバスター Corp. に対してのみアクセス権を持ち、Sam が InterScan for Microsoft Exchange サーバにのみアクセス権を持っていることが前提となります。

保存したアドホッククエリの編集

Control Manager では、[保存されたアドホッククエリ] 画面の [ユーザのクエリ] タブを使用して、保存したアドホッククエリを編集できます。保存したアドホッククエリを編集するには、次の手順を実行する必要があります。

手順 1: クエリ先として管理下の製品またはログオン中の Control Manager サーバを選択する

手順 2: クエリ用のデータビューを選択する

手順 3: フィルタ条件と表示する情報を指定する

手順 4: クエリを保存して実行する

手順 5: 取得したデータを CSV 形式または XML 形式にエクスポートする

保存したアドホッククエリを編集するには

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. [保存されたアドホッククエリ] をクリックします。[保存されたアドホッククエリ] 画面が表示されます。

3. 編集対象の保存したアドホッククエリの名前をクリックします。[製品ツリーの選択] 画面が表示されます。

手順 1: 情報の発生元の指定

1. [新規アドホッククエリ] 画面から、レポートの生成元となるネットワーク防御策カテゴリ (管理下の製品またはディレクトリ) を指定します。

   - Control Manager の選択 — 情報の発生元となる、ユーザがログオン中の Control Manager サーバを指定します。

     このオプションを指定すると製品ツリーが無効になります。ユーザがログオンしている Control Manager サーバからの情報のみが検索対象になるためです。

   - 製品ツリーの選択 — 情報の発生元となる、Control Manager サーバが管理している管理下の製品を指定します。

     このオプションを指定する場合は、情報の発生元となる防御策カテゴリを選択する必要があります。製品ディレクトリから管理下の製品 / ディレクトリを選択することにより、このカテゴリは選択されます。

   注意： この画面で管理下の製品 / ディレクトリを選択すると、表示されるデータビューが変わります。たとえば、製品ディレクトリでウイルスバスター Corp. を選択すると、デスクトップ保護に関連付けられたデータビューのみが [データビュー] リストに表示されます。

2. [次へ] をクリックします。[データビュー] 画面が表示されます。

手順 2: クエリ用のデータビューの指定

1. [使用可能なデータビュー] リストから、必要なデータビューを選択します。データビューの詳細については、214 ページの「データビューについて」を参照してください。
2. [次へ] をクリックします。[クエリ条件] 画面が表示されます。

手順 3: 表示順序の指定

1. クエリ結果として返される情報の表示と順序を指定します。

   a. [列の表示を変更する] をクリックします。[表示順序の選択] 画面が表示されます。

   b. クエリから情報が返されたときに表示するデータビューの列を、[使用可能なフィールド] リストから選択します。選択した列が反転表示します。

   ヒント： 列は 1 度に 1 列ずつ選択するか、<Shift> または <Ctrl> キーを使用して複数列を選択します。

   1 度に 1 列ずつ選択し追加すると、情報がその順序で表示され、表示順序の指定にもなります。

   c. [追加] ボタンをクリックして、選択した列を [選択されたフィールド] リストに移動させます。選択した列が [選択されたフィールド] リストに表示されます。

   d. 列の選択と追加を、必要に応じて繰り返します。

   e. [選択されたフィールド] リストで列を選択してから、[上に移動] または [下に移動] ボタンを使用して、情報の表示順序を指定します。リストの一番上にある列が、クエリ結果では左端の列として表示されます。

   f. [戻る] をクリックします。[クエリ条件] 画面が表示されます。

手順 4: フィルタ条件の指定

概要データ (タイトルに「概要」という単語のあるデータビュー) に対してクエリを実行するときは、[必要な条件] で項目を指定する必要があります。

1. [必要な条件] を指定します。

   - データの [集計日時] を指定するか、COOKIE をレポートに表示するかどうかを指定します。

2. [カスタム条件] を指定します。

   a. [カスタム条件] を選択します。カスタム条件オプションが表示されます。

   b. [キーワード] でデータカテゴリ用の条件フィルタルールを指定します。

      - すべての条件 — これを選択すると、論理積 (AND) として機能します。レポートに表示されるデータは、すべてのフィルタ条件に適合する必要があります。
      - いずれかの条件 — これを選択すると、論理和 (OR) として機能します。レポートに表示されるデータは、いずれかのフィルタ条件に適合する必要があります。

   c. データ用のフィルタ条件を指定します。Control Manager では、データのフィルタ用に最大 20 個の条件がサポートされています。

注意： フィルタ条件を指定しないと、アドホッククエリでは該当する列の結果がすべて返されます。フィルタ条件を指定して、クエリから返された情報のデータ分析を簡単にすることをお勧めします。

---

      i. 左側のドロップダウンリストから、フィルタ対象となる列を選択します。

      ii. 中央のドロップダウンリストから、フィルタに適用する一致条件を選択します。

      iii. 右側のフィールドに、フィルタ条件を入力します。ここには、フィルタ対象として選択した列に応じて、リストボックスまたはテキストボックスが表示されています。

      iv. データビューのフィルタ条件をさらに追加するには、[+] アイコンをクリックします。

手順 5: クエリの保存と実行

1. [クエリ設定の保存] の [保存されたアドホッククエリリストにこのクエリを保存します。] をクリックして、作成したアドホッククエリを保存します。
2. [クエリ名] に、保存するアドホッククエリの名前を入力します。

   注意： Control Manager では、保存したアドホッククエリをユーザ間で共有できます。保存したクエリは、[ログ / レポート]→[ユーザのレポート] 画面に表示されます。

3. [クエリ] をクリックします。クエリの結果を表示する [結果] 画面が表示されます。

手順 6: クエリ結果の CSV 形式または XML 形式へのエクスポート

1. 次のオプションをクリックすると、[ファイルのダウンロード] ダイアログボックスが表示されます。
   - CSV 形式で出力 — クエリ結果を CSV ファイル形式でエクスポートできます。
   - XML 形式で出力 — クエリ結果を XML ファイル形式でエクスポートできます。
2. 次のいずれかを実行します。
   - [開く] をクリックし、クエリ結果を CSV 形式または XML 形式でただちに表示します。
   - [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。ファイルを保存する場所を指定します。

保存したアドホッククエリの共有

Control Manager では、[保存されたアドホッククエリ] 画面の [ユーザのクエリ] タブを使用して、保存したアドホッククエリを共有化できます。

保存したアドホッククエリを共有するには

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [保存されたアドホッククエリ] をクリックします。[保存されたアドホッククエリ] 画面が表示されます。
3. 共有対象のアドホッククエリに対応するチェックボックスをオンにします。
4. [共有] をクリックします。保存したアドホッククエリの [共有] 列にアイコンが表示されます。

共有アドホッククエリの使用

作成したアドホッククエリは、他のユーザと共有できます。任意のユーザにより共有化されているすべてのアドホッククエリが、[保存されたアドホッククエリ] 画面の [使用可能なクエリ] タブに表示されます。ユーザは共有クエリを表示およびエクスポートできます。

[使用可能なクエリ] タブにアクセスするには

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [保存されたアドホッククエリ] をクリックします。[保存されたアドホッククエリ] 画面が表示されます。
3. [使用可能なクエリ] をクリックします。[使用可能なクエリ] タブが表示されます。

ログの削除

[ログ管理] 画面を使用すると、次の種類のログに対してログをすぐに削除したり、自動削除を設定したりできます。

- ウイルス / スパイウェアログ
- 製品イベントログ
- セキュリティログ
- Web セキュリティログ
- ネットワークウイルスログ
- エンドポイントログ
- セキュリティ違反ログ
- セキュリティ遵守ログ
- セキュリティ統計ログ
- ウイルスの兆候ログ
- ネットワークレピュテーションログ
- デスクトップスパイウェアログ
- ファイアウォール違反ログ
- アクセスログ
- サーバイベントログ

ログをただちに削除するには

1. 上部のメニューで [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューから [ログ管理] をクリックします。[ログ管理] 画面が表示されます。

4. 削除対象のログに対応するチェックボックスをオンにします。

5. 削除対象のログに対応する行で [すべて削除] をクリックします。

ログの自動削除の設定

[ログ管理] 画面では、ログに対して次の 2 通りの自動削除方法を設定できます。

- 数基準 (最小 : 30,000、最大 : 1,000,000、初期設定 : 1,000,000)
- 保存日数基準 (最小 : 1 日、最大 : 90 日、初期設定 : 45 から 90 日)

削除数には、特定のログの種類のログ数が最大数に達したときに削除するログの数を指定します。削除数の初期設定は、すべてのログの種類で 1,000 です。

ログの削除設定を指定するには

1. 上部のメニューで [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. [設定] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューから [ログ管理] をクリックします。[ログ管理] 画面が表示されます。
4. 設定しようとするログに対応するチェックボックスをオンにします。
5. [ログエントリの最大数] 列に、保存するログエントリの最大数を指定します。
6. [削除数] 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。
7. [ログの最大保存期間] に、自動削除を適用する保存日数を指定します。
8. [保存] をクリックします。

レポートの使用

Control Manager のレポートは、レポートテンプレートとレポートプロファイルの 2 つの要素で構成されます。レポートテンプレートはレポートの外観と機能を定義し、レポートプロファイルはレポートデータの発生元、スケジュール / 期間、およびレポートの受信者を定義します。

Control Manager 5.0 では、Control Manager 管理者によるレポートのカスタマイズ機能が導入され、レポートがこれまでのバージョンに比べて大きく変更されています。Control Manager 5.0 では旧バージョンのレポートテンプレートも引き続きサポートされますが、Control Manager 5.0 では管理者が独自のカスタムレポートテンプレートを設計できます。

Control Manager レポートテンプレートについて

レポートテンプレートを使用することによって、Control Manager レポートの外観と機能を定義できます。Control Manager 5.0 では、次の種類に従ってレポートテンプレートを分類します。

- Control Manager 5.0 テンプレート : データベースに対する直接検索 (データベースビュー) とレポートテンプレート要素 (図 / グラフ / 表) を使用するユーザ定義のカスタマイズされたレポートテンプレート。旧バージョンのレポートテンプレートに比べて、レポートに表示するデータを指定する際の柔軟性が大幅に向上しています。Control Manager 5.0 テンプレートの詳細については、235 ページの「Control Manager 5.0 のテンプレートについて」を参照してください。
- Control Manager 3.0 テンプレート : Control Manager 3.0 および Control Manager 3.5 で提供されていたすべてのテンプレートが含まれます。Control Manager 3.0 テンプレートの詳細については、234 ページの「Control Manager レポートテンプレートについて」を参照してください。

Control Manager 5.0 のテンプレートについて

Control Manager 5.0 のレポートテンプレートでは、レポートの情報基盤としてデータベースビューが使用されます。データビューの詳細については、214 ページの「データビューについて」を参照してください。生成されるレポートの外観と機能は、レポートの各要素により実現されます。レポートの要素には次のものがあります。

表 6-17. Control Manager 5.0 レポートテンプレートの要素

テンプレート要素	説明
改ページ	レポートに改ページを挿入します。各レポートページには、最大 3 つまでのレポートテンプレート要素を使用できます。
静的テキスト	レポートにユーザ定義の説明を記載します。静的テキストには、4,096 文字まで使用できます。
棒グラフ	レポートテンプレートに棒グラフを挿入します。
折れ線グラフ	レポートテンプレートに折れ線グラフを挿入します。
円グラフ	レポートテンプレートに円グラフを挿入します。
動的テーブル	レポートテンプレートに動的テーブル / ピボットテーブルを挿入します。
グリッドテーブル	レポートテンプレートに表を挿入します。グリッドテーブルの情報は、アドホッククエリにより表示される情報と同じです。

1 つの Control Manager 5.0 テンプレートには、最大 100 までのレポートテンプレート要素を含めることができます。レポートテンプレートの各ページには、最大 3 つまでのレポートテンプレート要素を含めることができます。レポートテンプレートにページを作成するには、改ページを使用します。

Control Manager 5.0 レポートテンプレートの理解を支援する目的で、トレンドマイクロでは、次の事前定義済みレポートテンプレートを用意しています。

注意： トレンドマイクロの事前定義済みテンプレートを表示するには、[レポートテンプレート] 画面にアクセスします。

表 6-18. Control Manager 5.0 の事前定義済みテンプレート

テンプレート	説明
TM- コンテンツ違反検出の概要	次の情報が報告されます。 ・日付別のコンテンツ違反検出 (折れ線グラフ) ・日付別の違反ポリシー数 (折れ線グラフ) ・日付別の送信者数 (折れ線グラフ) ・日付別の受信者数 (折れ線グラフ) ・違反ポリシートップ 25 (棒グラフ) ・コンテンツ違反ポリシーの概要 (グリッドテーブル) ・送信者トップ 25 (棒グラフ) ・コンテンツ違反送信者の概要 (グリッドテーブル) ・処理結果の概要 (円グラフ)
TM- 管理下の製品の接続 / コンポーネントステータス	次の情報が報告されます。 ・サーバ / アプライアンス接続ステータス (円グラフ) ・クライアントの接続ステータス (円グラフ) ・サーバ / アプライアンスのパターンファイル / ルールアップデートステータス (円グラフ) ・クライアントのパターンファイル / ルールアップデートステータス (円グラフ) ・サーバ / アプライアンスの検索エンジンアップデートステータス (円グラフ) ・クライアントの検索エンジンアップデートステータス (円グラフ) ・サーバ / アプライアンスのパターンファイル / ルール概要 (グリッドテーブル) ・クライアントのパターンファイル / ルール概要 (グリッドテーブル) ・サーバ / アプライアンスの検索エンジン概要 (グリッドテーブル) ・クライアントの検索エンジン概要 (グリッドテーブル)

表 6-18. Control Manager 5.0 の事前定義済みテンプレート

テンプレート	説明
TM- 脅威の概要 (全体)	次の情報が報告されます。 ・完全なネットワークセキュリティリスク分析の概要 (グリッドテーブル) ・ネットワーク保護境界の概要 (グリッドテーブル) ・セキュリティリスク侵入ポイント分析情報 (グリッドテーブル) ・セキュリティリスク宛先分析情報 (グリッドテーブル) ・セキュリティリスク発生元分析情報 (グリッドテーブル)
TM- スパムメール検出の概要	次の情報が報告されます。 ・日付別のスパムメール検出 (折れ線グラフ) ・日付別の受信ドメイン数 (折れ線グラフ) ・日付別の受信者数 (折れ線グラフ) ・受信ドメイントップ 25 (棒グラフ) ・スパムメール違反の概要 (全体) (グリッドテーブル) ・スパムメール受信者トップ 25 (棒グラフ) ・スパムメール受信者の概要 (グリッドテーブル)
TM- スパイウェア検出の概要	次の情報が報告されます。 ・日付別のスパイウェア検出 (折れ線グラフ) ・日付別の一意のスパイウェア数 (折れ線グラフ) ・日付別のスパイウェア発生元数 (折れ線グラフ) ・日付別のスパイウェア宛先数 (折れ線グラフ) ・スパイウェアトップ 25 (棒グラフ) ・スパイウェアの概要 (全体) (グリッドテーブル) ・スパイウェア発生元トップ 25 (棒グラフ) ・スパイウェア発生元の概要 (グリッドテーブル) ・スパイウェア宛先トップ 25 (棒グラフ) ・スパイウェア宛先の概要 (グリッドテーブル) ・処理結果の概要 (円グラフ) ・スパイウェアの処理 / 結果の概要 (グリッドテーブル)

表 6-18. Control Manager 5.0 の事前定義済みテンプレート

テンプレート	説明
TM- 脅威の兆候検出の概要	次の情報が報告されます。 ・日付別の脅威の兆候検出 (折れ線グラフ) ・日付別の違反ルール数 (折れ線グラフ) ・日付別の送信者数 (折れ線グラフ) ・日付別の受信者数 (折れ線グラフ) ・日付別の送信元 IP アドレス数 (折れ線グラフ) ・日付別の送信先 IP アドレス数 (折れ線グラフ) ・送信者トップ 25 (棒グラフ) ・受信者トップ 25 (棒グラフ) ・脅威の兆候送信者の概要 (グリッドテーブル) ・最も脅威の兆候の多い受信者の概要 (グリッドテーブル) ・送信元 IP アドレストップ 25 (棒グラフ) ・送信先 IP アドレストップ 25 (棒グラフ) ・脅威の兆候送信元の概要 (グリッドテーブル) ・最も脅威の兆候の多い送信先の概要 (グリッドテーブル) ・プロトコル名トップ 25 (棒グラフ) ・脅威の兆候を検出したプロトコルの概要 (グリッドテーブル) ・脅威の兆候の概要 (全体) (グリッドテーブル)
TM- ウイルス / 不正コード検出の概要	次の情報が報告されます。 ・日付別のウイルス / 不正コード検出 (折れ線グラフ) ・日付別の一意のウイルス / 不正コード数 (折れ線グラフ) ・日付別の感染先数 (折れ線グラフ) ・ウイルス / 不正コードトップ 25 (棒グラフ) ・ウイルス / 不正プログラムの概要 (全体) (グリッドテーブル) ・ウイルス / 不正コード感染先の概要 (グリッドテーブル) ・感染元トップ 25 (棒グラフ) ・ウイルス / 不正コード感染元の概要 (グリッドテーブル) ・感染先トップ 25 (棒グラフ) ・ウイルス / 不正プログラムの感染先概要 (グリッドテーブル) ・処理結果の概要 (円グラフ) ・ウイルス / 不正コードの処理 / 結果の概要 (グリッドテーブル)

表 6-18. Control Manager 5.0 の事前定義済みテンプレート

テンプレート	説明
TM-Web 違反検出の概要	次の情報が報告されます。 ・日付別の Web 違反検出 (折れ線グラフ) ・日付別の違反ポリシー数 (折れ線グラフ) ・日付別の違反クライアント数 (折れ線グラフ) ・日付別の違反 URL 数 (折れ線グラフ) ・違反ポリシートップ 25 (棒グラフ) ・Web 違反の概要 (全体) (グリッドテーブル) ・違反クライアントトップ 25 (棒グラフ) ・Web 違反クライアント IP アドレスの概要 (グリッドテーブル) ・違反 URL トップ 25 (棒グラフ) ・Web 違反 URL の概要 (グリッドテーブル) ・フィルタ / ブロックタイプの概要 (円グラフ)

Control Manager 3.0 レポートテンプレートについて

Control Manager 3.0 および 3.5 では、事前作成したレポートテンプレートが 65 個追加されました。これらのテンプレートは、デスクトップ製品、ファイルサーバ製品、ゲートウェイ製品、メールサーバ製品、管理下の全製品、およびネットワーク製品の 6 つのカテゴリに分類されます。

注意： Control Manager 3.5 では、スパイウェアはウイルスと区別されるようになりました。この変更は、ウイルスに関連する元のすべてのレポートのウイルス数に影響します。

レポートの 6 つのカテゴリ (次の表を参照) を表示するには、Control Manager 3.0 レポートテンプレートの画面の [レポートのカテゴリ] リストを使用します。

表 6-19. デスクトップ製品のレポートとレポートの種類

デスクトップ製品のレポート	レポートの種類
スパイウェア検出レポート	・スパイウェア検出 ・スパイウェア検出数上位 (10、25、50、100)
ウイルス検出レポート	・ウイルス検出 ・ウイルス検出数上位 (10、25、50、100)
ウイルスバスター Corp. クライアント情報レポート	・コンポーネント配信詳細 ・コンポーネント配信基本概要
ウイルスバスター Corp. 製品登録レポート	ウイルスバスター Corp. 製品登録
比較レポート	・スパイウェア検出数 (日、週、月) ・ウイルス検出数 (日、週、月)
ウイルスバスター Corp. サーバ配信レポート	・コンポーネント配信詳細 ・コンポーネント配信基本概要 ・コンポーネント配信失敗詳細
ウイルスバスター Corp. のダメージクリーンナップサービスレポート	・コンポーネント配信詳細 ・駆除されたウイルス感染上位 (10、25、50、100)

表 6-20. 管理下の全製品のレポートとレポートの種類

管理下の全製品のレポート	レポートの種類
スパイウェア検出レポート	・スパイウェア検出 ・スパイウェア検出数上位 (10、25、50、100) ・スパイウェア検出一覧
ウイルス検出レポート	・ウイルス検出 ・ウイルス検出数上位 (10、25、50、100) ・ウイルス検出一覧
比較レポート	・スパイウェア検出数 (日、週、月) ・ウイルス検出数 (日、週、月) ・ダメージクリーンナップ (日、週、月) ・スパムメール検出数 (日、週、月)

表 6-20. 管理下の全製品のレポートとレポートの種類

管理下の全製品のレポート	レポートの種類
脆弱性診断レポート	・リスクレベル別脆弱なコンピュータの割合 ・脆弱性診断 ・処理されたウイルス感染上位 (10、25、50、100) ・危険性の高い脆弱性上位 (10、25、50、100) ・リスクレベル別脆弱性

表 6-21. ゲートウェイ製品のレポートとレポートの種類

ゲートウェイ製品のレポート	レポートの種類
スパイウェア検出レポート	・スパイウェア検出 ・スパイウェア検出数上位 (10、25、50、100)
ウイルス検出レポート	・ウイルス検出 ・ウイルス検出数上位 (10、25、50、100)
比較レポート	・スパイウェア検出数 (日、週、月) ・スパムメール検出数 (日、週、月) ・ウイルス検出数 (日、週、月)
配信レートレポート	・コンポーネント配信詳細 ・コンポーネント配信基本概要 ・コンポーネント配信失敗詳細 ・大規模感染予防ポリシー配信概要 (InterScan MSS)

表 6-22. メールサーバ製品のレポートとレポートの種類

メールサーバ製品のレポート	レポートの種類
スパイウェア検出レポート	・スパイウェア検出 ・スパイウェア検出数上位 (10、25、50、100)
ウイルス検出レポート	・ウイルス検出 ・ウイルス検出数上位 (10、25、50、100) ・ウイルス感染メール送信者上位 (10、25、50、100)
比較レポート	・スパイウェア検出数 (日、週、月) ・ウイルス検出数 (日、週、月)
配信レートレポート	・コンポーネント配信詳細 ・コンポーネント配信基本概要 ・コンポーネント配信失敗詳細

表 6-23. ファイルサーバ製品のレポートとレポートの種類

ファイルサーバ製品のレポート	レポートの種類
スパイウェア検出レポート	・スパイウェア検出 ・スパイウェア検出数上位 (10、25、50、100)
ウイルス検出レポート	・ウイルス検出 ・ウイルス検出数上位 (10、25、50、100)
推移レポート	・期間別のスパイウェア検出数 (日、週、月) ・期間別のウイルス検出数 (日、週、月)
コンポーネント配信詳細レポート	・詳細 ・基本概要 ・コンポーネント配信失敗詳細レポート

表 6-24. ネットワーク製品のレポートとレポートの種類

ネットワーク製品のレポート	レポートの種類
Network VirusWall レポート	ポリシー違反レポート — 期間別のポリシー違反数 (日、週、月)
	サービス違反レポート — 期間別のサービス違反 (日、週、月)
	違反クライアント検出数上位 (10、25、50、100)

レポートのコンテンツによっては、作成に時間がかかることがあります。レポートの作成が終了すると、画面が更新されて、レポートの隣の [表示] リンクが使用できるようになります。

Control Manager 5.0 レポートテンプレートの追加

Control Manager 5.0 テンプレートは、旧バージョンの Control Manager テンプレートに比べて、レポート生成の柔軟性が向上しました。Control Manager 5.0 テンプレートでは、直接 Control Manager データベースにアクセスします。これによって、Control Manager データベースに格納されている情報に基づいてユーザがレポートを作成できます。

Control Manager 5.0 カスタムテンプレートを追加するには、次の手順を実行する必要があります。

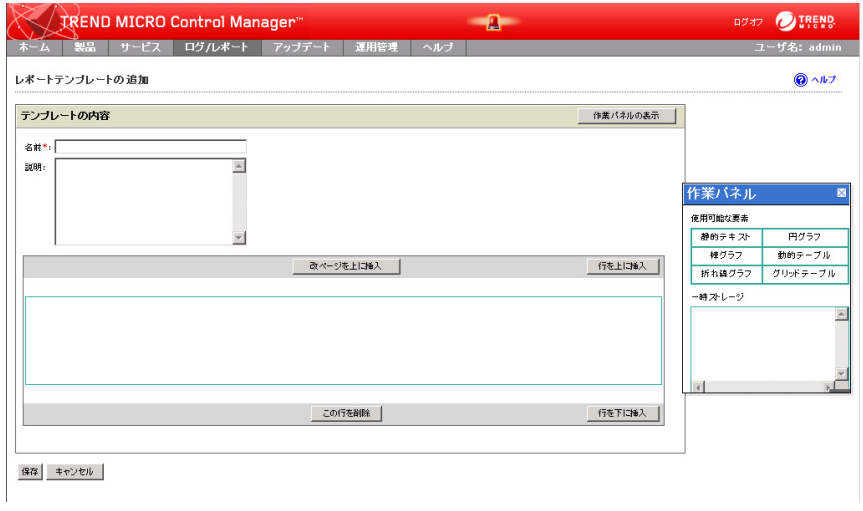
1. [レポートテンプレートの追加] 画面にアクセスしてテンプレートの名前を設定します。
2. レポートテンプレートに追加するテンプレートコンポーネントを指定します。
3. テンプレート用のデータビューを指定します。
4. テンプレート用のクエリ条件を指定します。
5. レポートに表示されるデータとデータの表示順序を指定します。
6. レポートテンプレート作成を完了します。

Control Manager 5.0 レポートテンプレートを追加するには

手順 1: [レポートテンプレートの追加] 画面にアクセスしてテンプレートの名前を設定する

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [レポートテンプレート] をクリックします。[レポートテンプレート] 画面が表示されます。

3. [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。



4. [レポートテンプレート] の [名前] にレポートテンプレートの名前を入力します。

5. [レポートテンプレート] の [説明] にレポートテンプレートの説明を入力します。

手順 2: レポートテンプレートに追加するテンプレートコンポーネントを指定する

1. レポートテンプレート要素を [作業パネル] からドラッグアンドドロップして、レポートテンプレートに追加します。

   注意： 静的テキスト以外のコンポーネントを選択すると、[手順 1: データビュー] 画面が表示されます。静的テキストを選択すると、[静的テキストの編集] 画面が表示されます。

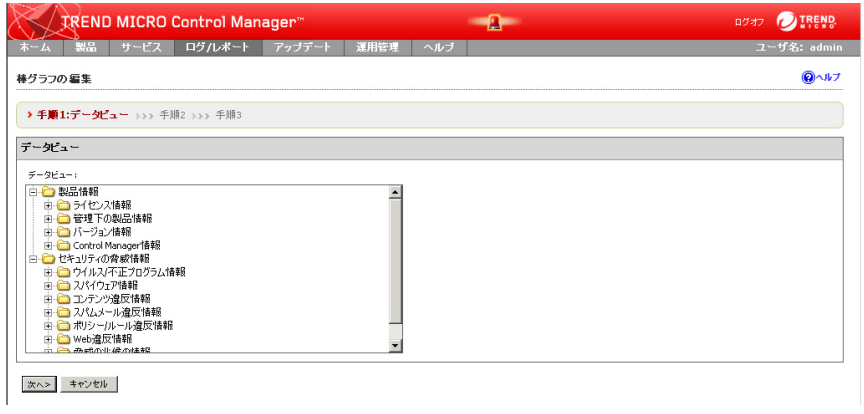
   - 棒グラフ — レポートのデータが棒グラフに表示されます。
   - 円グラフ — レポートのデータが円グラフに表示されます。
   - 動的テーブル — レポートのデータが、ピボットテーブルに似た表に表示されます。
   - グリッドテーブル — レポートのデータが、アドホッククエリテーブルに似た表に表示されます。
   - 折れ線グラフ — レポートのデータが折れ線グラフに表示されます。
   - 静的テキスト — ユーザがテンプレートに挿入するテキストです。レポートに表示される情報の簡単な説明などに使用します。

2. 複数のコンポーネントを追加して、レポートを理解しやすくします。レポートテンプレートには、最大 100 までのコンポーネントを追加できます。

3. 改ページと行をレポートテンプレートに追加して、データやレポートテンプレート要素をわかりやすく分割します。

手順 3: テンプレート用のデータビューを指定する

1. レポートテンプレート要素で [編集] をクリックします。[< レポートテンプレート要素 > の編集] 画面が表示されます。



2. [データビュー] 領域からクエリを実行するためのデータを選択します。

   データビューの詳細については、429 ページの「データビューについて」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。

手順 4: テンプレート用のクエリ条件を指定する

ヒント： フィルタ条件を指定しないと、レポートでは該当する列の結果がすべて返されます。フィルタ条件を指定して、レポートから返された情報のデータ分析を簡単にすることをお勧めします。

1. [カスタム条件] をクリックします。
2. データカテゴリの条件フィルタルールを指定します。
   - すべての条件 — これを選択すると、論理積 (AND) として機能します。レポートに表示されるデータは、すべてのフィルタ条件に適合する必要があります。
   - いずれかの条件 — これを選択すると、論理和 (OR) として機能します。レポートに表示されるデータは、いずれかのフィルタ条件に適合する必要があります。
3. フィルタに適用するデータ、演算子、および特定条件を選択します。Control Manager では、データのフィルタ用に最大 20 個の条件を指定できます。

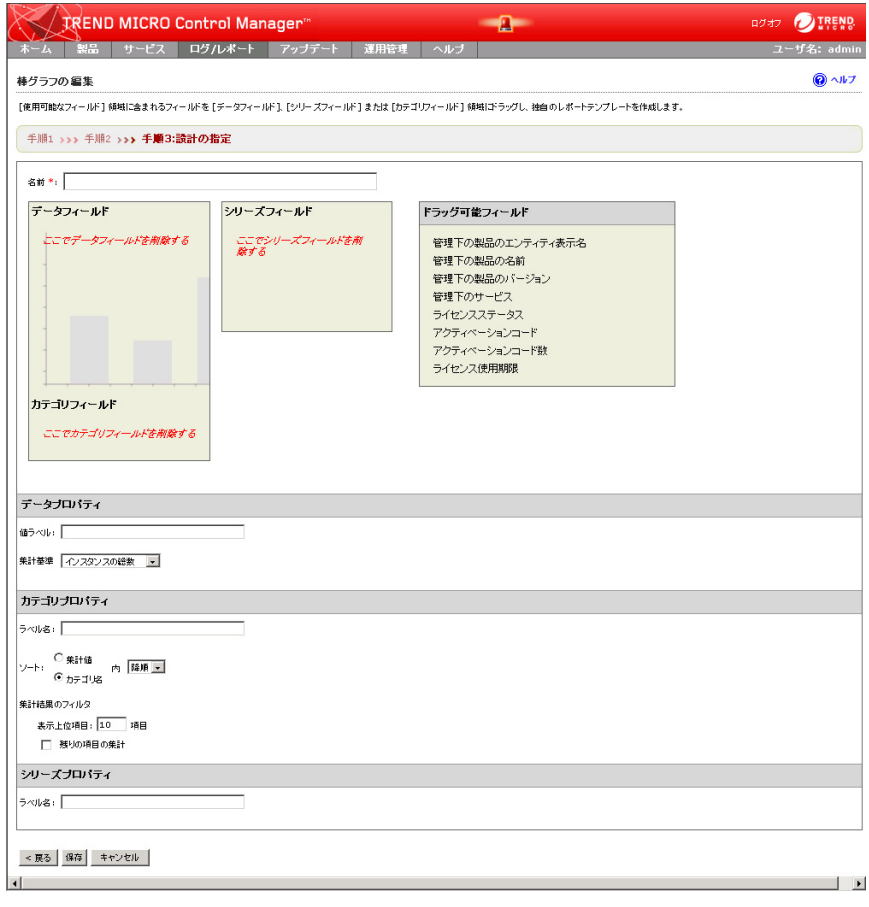
手順 5: レポートに表示されるデータとデータの表示順序を指定する

次の各レポート要素を選択した場合は、レポートに表示するデータを指定します。

- 棒グラフ
- 円グラフ
- 動的テーブル
- グリッドテーブル
- 折れ線グラフ

棒グラフを設定する場合

1. [次へ] をクリックします。[棒グラフの編集 > 手順 3: 設計の指定] 画面が表示されます。



2. [名前] に棒グラフの名前を入力します。

3. [ドラッグ可能フィールド] リストから次の領域に、必要な項目をドラッグアンドドロップします。

   - データフィールド : 棒グラフの垂直軸に沿って表示されるデータを指定します。
   - シリーズフィールド : 水平軸に沿って表示される追加データを指定します。
   - カテゴリフィールド : 棒グラフの水平軸に沿って表示されるデータを指定します。

4. [データフィールド] の表示設定を指定します。

   a. [データフィールド] のラベルに意味がわかるような説明を入力します。

   b. [集計基準] ドロップダウンリストから、[データフィールド] に対するデータの表示方法を指定します。

      - インスタンスの総数 — 合計発生件数が結果に反映されるように指定します。
      - 一意のインスタンス数 — 個別項目の件数のみ結果に反映されるように指定します。
      - 値の合計 — [データビュー] 列の「件数」にあるすべての値の合計が、結果に反映されるように指定します。

      例 : ウイルスバスター Corp. により、1 台のコンピュータで同じウイルスのインスタンスが 10 個検出されたとします。合計数の行では、10 が表示されます。個別項目の件数の行では、1 が表示されます。

5. [シリーズフィールド] の表示設定を指定します。

   a. [シリーズフィールド] のラベルに意味がわかるような説明を入力します。

6. [カテゴリフィールド] の表示設定を指定します。

   a. [カテゴリフィールド] のラベルに意味がわかるような説明を入力します。

b. [ソート] ドロップダウンリストから、グラフのデータを並べ替える方法を指定します。

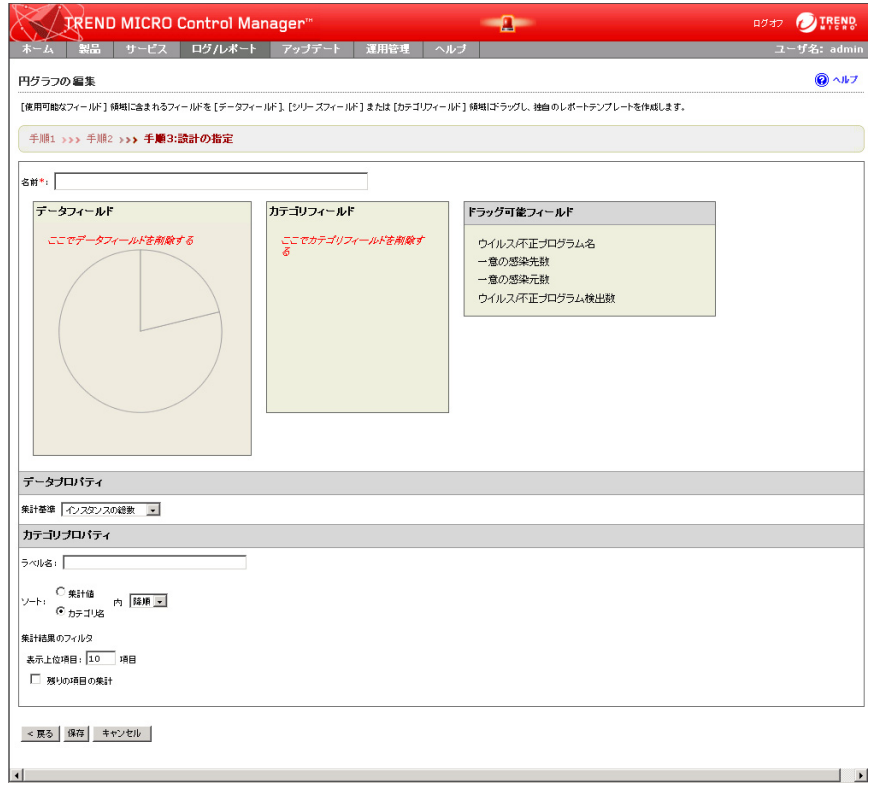
- 集計値 — [カテゴリフィールド] に表示されるデータの順序でデータを並べ替えます。
- カテゴリ名 — [カテゴリ名] のアルファベット値の順序でデータを並べ替えます。
- 昇順 — データを昇順で並べ替えます。
- 降順 — データを降順で並べ替えます。

c. [カテゴリフィールド] に表示される項目の数を指定します。指定方法は、[集計結果のフィルタ] を選択してから、[表示上位項目] テキストボックスに値を指定します。初期設定値は 10 です。

7. [保存] 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。

円グラフを設定する場合

1. [次へ] をクリックします。[円グラフの編集 > 手順 3: 設計の指定] 画面が表示されます。



2. [名前] に円グラフの名前を入力します。

3. [ドラッグ可能フィールド] リストから次の領域に、必要な項目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。

   例 : システム全体でのウイルスの検出状況を表示する円グラフを作成する場合は、[データフィールド] にシステムでのウイルスの検出総数を指定します。[カテゴリフィールド] には、ウイルスの合計数をパーセント値として分割する方法を指定します。

4. [データフィールド] の表示設定を指定します。

   a. [データフィールド] のラベルに意味がわかるような説明を入力します。

   b. [集計基準] ドロップダウンリストから、[データフィールド] に対するデータの表示方法を指定します。

      - インスタンスの総数 — 合計発生件数が結果に反映されるように指定します。
      - 一意のインスタンス数 — 個別項目の件数のみ結果に反映されるように指定します。
      - 値の合計 — [データビュー] 列の「件数」にあるすべての値の合計が、結果に反映されるように指定します。

      例 : ウイルスバスター Corp. により、1 台のコンピュータで同じウイルスのインスタンスが 10 個検出されたとします。合計数の行では、10 が表示されます。個別項目の件数の行では、1 が表示されます。

5. [カテゴリフィールド] の表示設定を指定します。

   a. [カテゴリフィールド] のラベルに意味がわかるような説明を入力します。

   b. [ソート] ドロップダウンリストから、グラフのデータを並べ替える方法を指定します。

      - 集計値 — [カテゴリフィールド] に表示されるデータの順序でデータを並べ替えます。

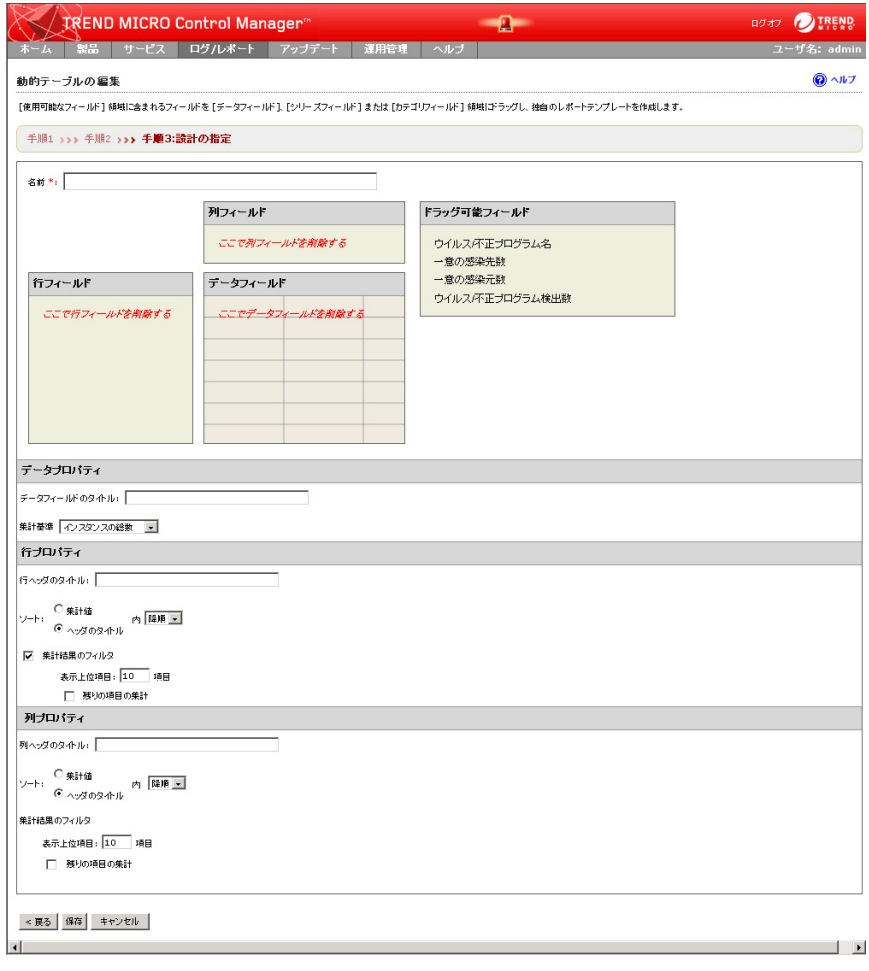
- カテゴリ名 — [カテゴリ名] のアルファベット値の順序でデータを並べ替えます。
- 昇順 — データを昇順で並べ替えます。
- 降順 — データを降順で並べ替えます。

c. [カテゴリフィールド] に表示される項目の数を指定します。指定方法は、[集計結果のフィルタ] を選択してから、[表示上位項目] テキストボックスに値を指定します。初期設定値は 10 です。

6. [保存] 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。

動的テーブルを設定する場合

1. [次へ] をクリックします。[動的テーブルの編集 > 手順 3: 設計の指定] 画面が表示されます。



2. [名前] に表の名前を入力します。

3. [ドラッグ可能フィールド] リストから次の領域に、必要な項目をドラッグアンドドロップします。

   - データフィールド — 表に表示するデータの総数を指定します。
   - 行フィールド — 表内のデータの水平方向への区切り方法を指定します。

     [ドラッグ可能フィールド] から 2 つ項目を [行フィールド] にドラッグできます。
   - 列フィールド — 表内のデータの垂直方向への区切り方法を指定します。

   例 : データビューの [ウイルス / 不正プログラムの詳細情報 (全体)] を、フィルタ条件を指定せずに使用するとします。表示しようとする項目は、感染したクライアント、感染ウイルス、および管理下の製品によって実行された処理です。その場合は、次のフィールドをそれぞれ [データフィールド]、[行フィールド]、および [列フィールド] にドラッグアンドドロップします。

   - データフィールド : ウイルス / 不正プログラム検出数
   - 行フィールド : ウイルス / 不正プログラム名 and 実行された処理
   - 列フィールド : 感染先

4. [データフィールド] の表示設定を指定します。

   a. [集計基準] ドロップダウンリストから、[データフィールド] に対するデータの表示方法を指定します。

      - インスタンスの総数 — 合計発生件数が結果に反映されるように指定します。
      - 一意のインスタンス数 — 個別項目の件数のみ結果に反映されるように指定します。
      - 値の合計 — [データビュー] 列の「件数」にあるすべての値の合計が、結果に反映されるように指定します。

      例 : ウイルスバスター Corp. により、1 台のコンピュータで同じウイルスのインスタンスが 10 個検出されたとします。合計数の行では、10 が表示されます。個別項目の件数の行では、1 が表示されます。

5. [行フィールド] の表示設定を指定します。

   a. [ソート] ドロップダウンリストから、表内のデータを並べ替える方法を指定します。

      - 集計値 — [行フィールド] に表示されるデータの順序でデータを並べ替えます。
      - ヘッダのタイトル — 行のアルファベット値順でデータを並べ替えます。
      - 昇順 — データを昇順で並べ替えます。
      - 降順 — データを降順で並べ替えます。

   b. [行フィールド] に表示される項目の数を指定します。指定方法は、[集計結果のフィルタ] を選択してから、[表示上位項目] テキストボックスに値を指定します。初期設定値は 10 です。

6. [列フィールド] の表示設定を指定します。

   a. [ソート] ドロップダウンリストから、表内のデータを並べ替える方法を指定します。

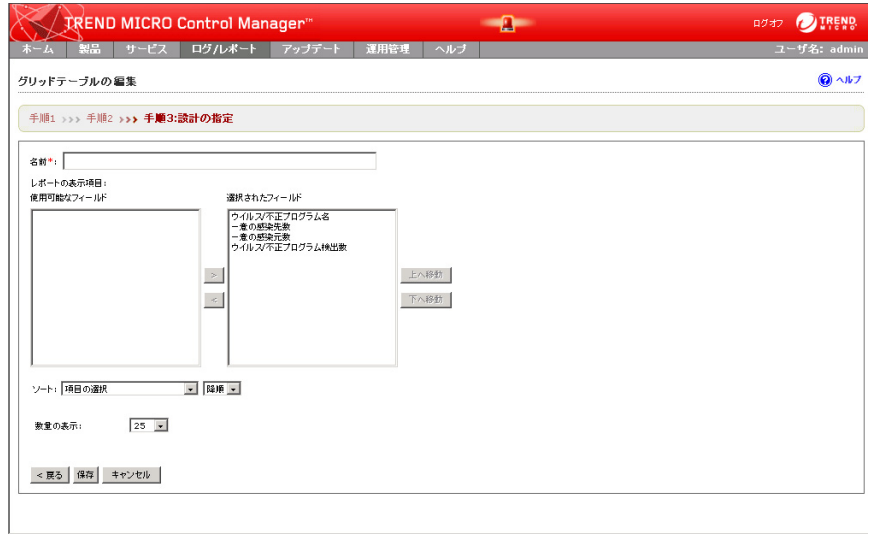
      - 集計値 — 列に表示されるデータの順序でデータを並べ替えます。
      - ヘッダのタイトル — 列のアルファベット値順でデータを並べ替えます。
      - 昇順 — データを昇順で並べ替えます。
      - 降順 — データを降順で並べ替えます。

   b. 表示される列の数を指定します。指定方法は、フィルタの列を選択してから、[表示上位項目] テキストボックスに値を指定します。初期設定値は 10 です。

7. [保存] 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。

グリッドテーブルを設定する場合

1. [次へ] をクリックします。[グリッドテーブルの編集 > 手順 3: 設計の指定] 画面が表示されます。



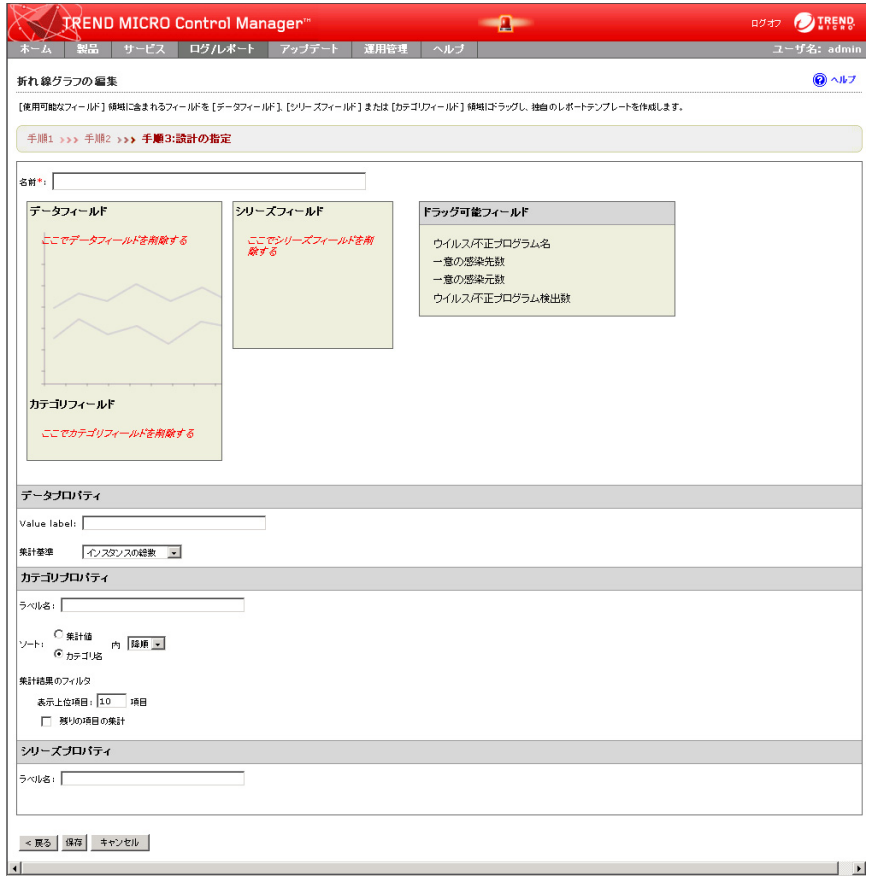
   a. [名前] にテーブルの名前を入力します。

   b. テーブルに表示する列と列の表示順序を指定します。

   c. [保存] 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。

折れ線グラフを設定する場合

1. [次へ] をクリックします。[折れ線グラフの編集 > 手順 3: 設計の指定] 画面が表示されます。



2. [名前] に折れ線グラフの名前を入力します。

3. [ドラッグ可能フィールド] リストから次の領域に、必要な項目をドラッグアンドドロップします。

   - データフィールド — テーブルに表示するデータの総数を指定します。
   - シリーズフィールド — グラフ内での垂直方向のデータの区切り方法を指定します。
   - カテゴリフィールド — グラフ内での水平方向のデータの区切り方法を指定します。

   例 : データビューの「ウイルス / 不正プログラムの詳細情報 (全体)」を、フィルタ条件を指定せずに使用するとします。グラフに表示したい項目は、一定期間におけるウイルスの感染状況です。その場合は、次のフィールドをそれぞれ [データフィールド]、[行フィールド]、および [列フィールド] にドラッグアンドドロップします。

   - データプロパティ: ウイルス / 不正プログラム検出数
   - 行プロパティ: ウイルス / 不正プログラム名
   - 列プロパティ: エンティティでの生成時間

4. [データフィールド] の表示設定を指定します。

   a. [データフィールド] のラベルに意味がわかるような説明を入力します。

   b. [集計基準] ドロップダウンリストから、[データフィールド] に対するデータの表示方法を指定します。

      - インスタンスの総数 — 合計発生件数が結果に反映されるように指定します。
      - 一意のインスタンス数 — 個別項目の件数のみ結果に反映されるように指定します。
      - 値の合計 — [データビュー] 列の「件数」にあるすべての値の合計が、結果に反映されるように指定します。

      例 : ウイルスバスター Corp. により、1 台のコンピュータで同じウイルスのインスタンスが 10 個検出されたとします。合計数の行では、10 が表示されます。個別項目の件数の行では、1 が表示されます。

5. [シリーズフィールド] の表示設定を指定します。

   a. [シリーズフィールド] のラベルに意味がわかるような説明を入力します。

6. [カテゴリフィールド] の表示設定を指定します。

   a. [カテゴリフィールド] のラベルに意味がわかるような説明を入力します。

   b. [ソート] ドロップダウンリストから、グラフのデータを並べ替える方法を指定します。

      - 集計値 — [カテゴリフィールド] に表示されるデータの順序でデータを並べ替えます。
      - カテゴリ名 — [カテゴリ名] のアルファベット値の順序でデータを並べ替えます。
      - 昇順 — データを昇順で並べ替えます。
      - 降順 — データを降順で並べ替えます。

   c. [カテゴリフィールド] に表示される項目の数を指定します。指定方法は、[集計結果のフィルタ] を選択してから、[表示上位項目] テキストボックスに値を指定します。初期設定値は 10 です。

7. [保存] 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。

手順 6: レポートテンプレート作成を完了する

1. レポートテンプレートの要素を必要に応じて追加または削除します。
2. [保存] をクリックします。

1 回限りのレポートの追加

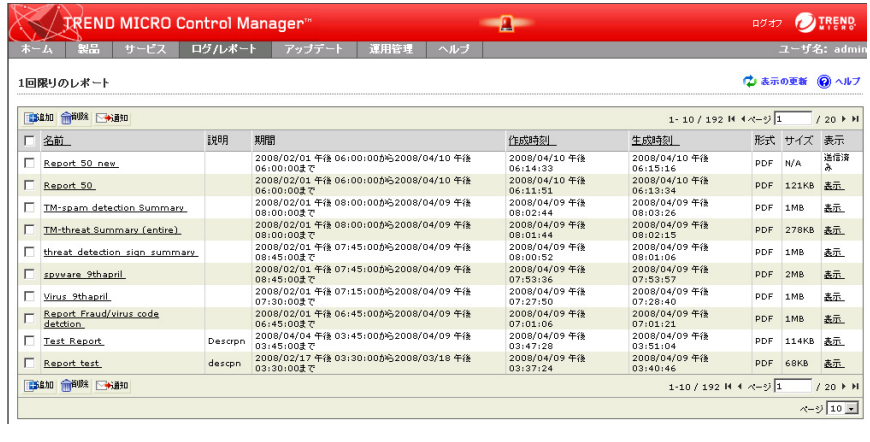
Control Manager では、Control Manager 3.0 と Control Manager 5.0 のレポートテンプレートから 1 回限りのレポートを生成する機能がサポートされています。Control Manager 5.0 のレポートテンプレートはユーザが作成する必要があります。Control Manager 3.0 のレポートテンプレートは、トレンドマイクロによって事前作成されています。1 回限りのレポートを作成するプロセスは、どの種類のレポートでも同じです。

1. [1 回限りのレポートの追加] 画面にアクセスしてレポートの種類を選択します。
2. レポートデータの生成元となる製品を指定します。
3. 製品においてデータが生成された日付を指定します。
4. レポートの受信者を指定します。

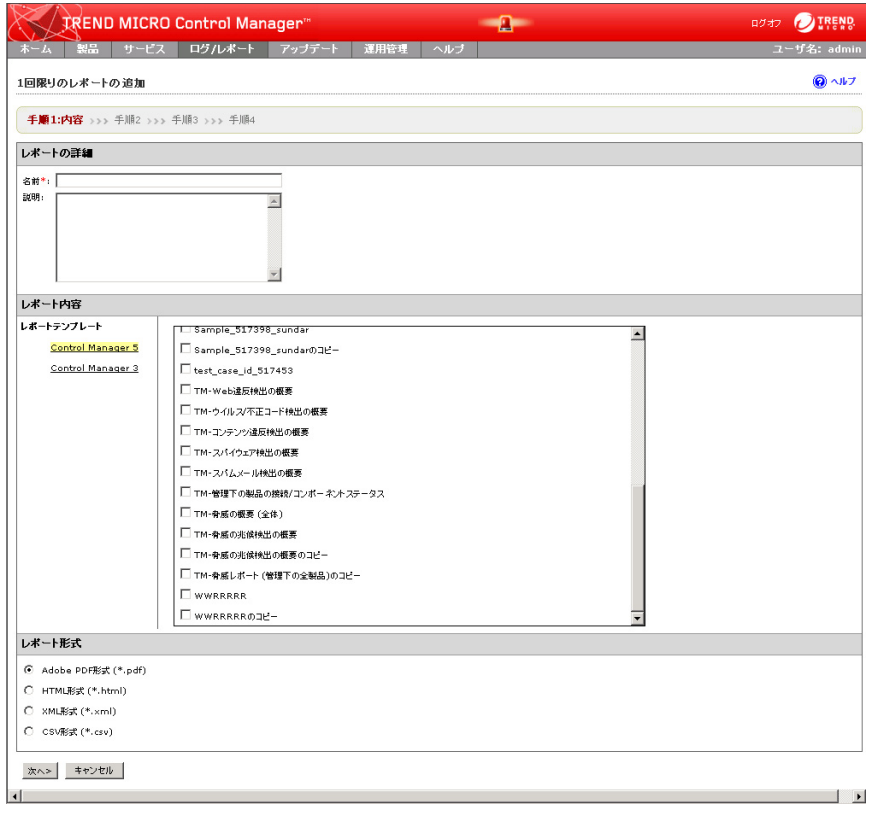
1 回限りのレポートを追加するには

手順 1: [1 回限りのレポートの追加] 画面にアクセスしてレポートの種類を選択する

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. メニューから [1 回限りのレポート] をクリックします。[1 回限りのレポート] 画面が表示されます。



3. [追加] をクリックします。[1 回限りのレポートの追加 > 手順 1: 内容] 画面が表示されます。



4. [レポートの詳細] の [名前] にレポートの名前を入力します。

5. [レポートの詳細] の [説明] にレポートの説明を入力します。

6. レポートの生成に使用する Control Manager テンプレートを選択します。

Control Manager 5.0 のレポートテンプレート

a. レポートの生成に使用する Control Manager 5.0 テンプレートを選択します。

既存のレポートが要件を完全に満たさない場合は、[レポートテンプレート] 画面から作成します。詳細については、242 ページの「Control Manager 5.0 レポートテンプレートの追加」を参照してください。

Control Manager 3 のレポートテンプレート

a. [レポート内容] で、[Control Manager 3] をクリックします。Control Manager 3 テンプレートが、右側の画面の [レポート内容] に表示されます。

b. レポートのベースとなるレポートカテゴリを選択します。

c. テンプレートのベースとなる Control Manager 3 テンプレートのデータを選択します。

7. レポートの出力形式を選択します。

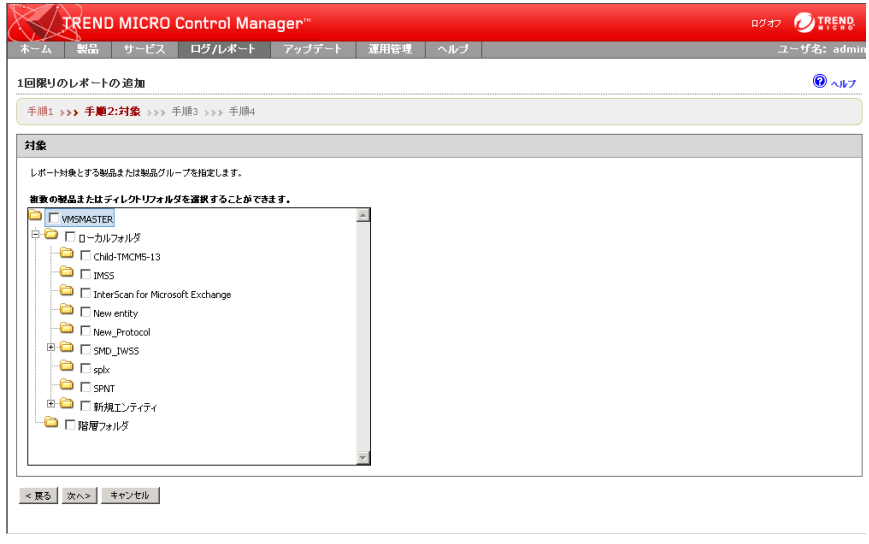
Control Manager 5.0 レポート出力形式

- Adobe PDF 形式 (*.pdf)
- HTML 形式 (*.html)
- XML 形式 (*.xml)
- CSV 形式 (*.csv)

Control Manager 3 レポート出力形式

- リッチテキスト形式 (*.rtf)
- Adobe PDF 形式 (*.pdf)
- ActiveX
- Crystal Reports 形式 (*.rpt)

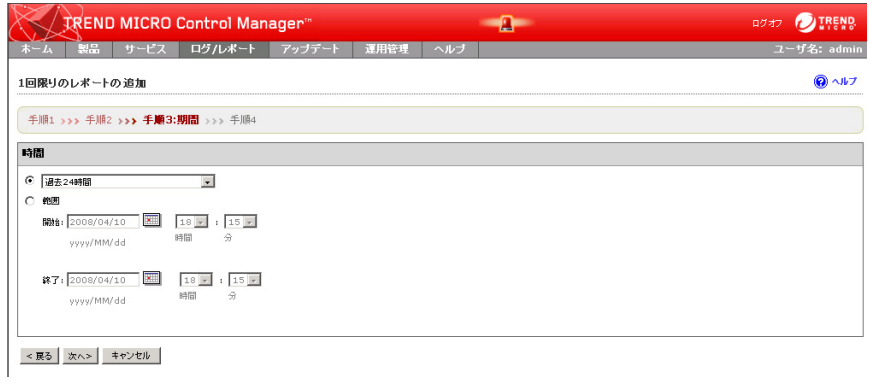
8. [次へ] をクリックします。[1 回限りのレポートの追加 > 手順 2: 対象] 画面が表示されます。



手順 2: レポートデータの生成元となる製品を指定する

1. レポート情報の収集元となる管理下の製品またはディレクトリを選択します。
2. 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。

3. [次へ] をクリックします。[1 回限りのレポートの追加 > 手順 3: 期間] 画面が表示されます。



手順 3: 製品においてデータが生成された日付を指定する

1. データの生成日時を指定します。

   ドロップダウンリストから、次のいずれかを選択します。

   - すべての日付
   - 過去 24 時間
   - 今日
   - 過去 7 日間
   - 過去 14 日間
   - 過去 30 日間

   日付の範囲を指定します。

   a. [開始] に日付を入力します。

   b. 日付の右側にある [時間] と [分] に時刻を入力します。

   c. [終了] に日付を入力します。

d. 日付の右側にある [時間] と [分] に時刻を入力します。

ヒント： [開始] と [終了] 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。

2. [次へ] をクリックします。[1 回限りのレポートの追加 > 手順 4: メッセージの内容と受信者] 画面が表示されます。

手順 4: レポートの受信者を指定する

1. レポートを添付するメールメッセージのタイトルを [件名] に入力します。
2. レポートに関する説明を [メッセージ] に入力します。
3. [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、指定した受信者へのレポート送信を有効にします。
4. [レポート受信者] リストからユーザまたはグループを選択して指定します。
5. レポートを受信するユーザまたはグループを選択し、[>>] ボタンをクリックします。
6. レポートを受信するユーザまたはグループをすべて選択したら、[完了] をクリックします。

予約レポートの追加

Control Manager では、Control Manager 3.0 と Control Manager 5.0 のレポートテンプレートから予約レポートを生成する機能がサポートされています。Control Manager 5.0 のレポートテンプレートはユーザが作成する必要があります。Control Manager 3.0 のレポートテンプレートは、トレンドマイクロによって事前作成されています。予約レポートを作成するプロセスは、どの種類のレポートでも同じです。

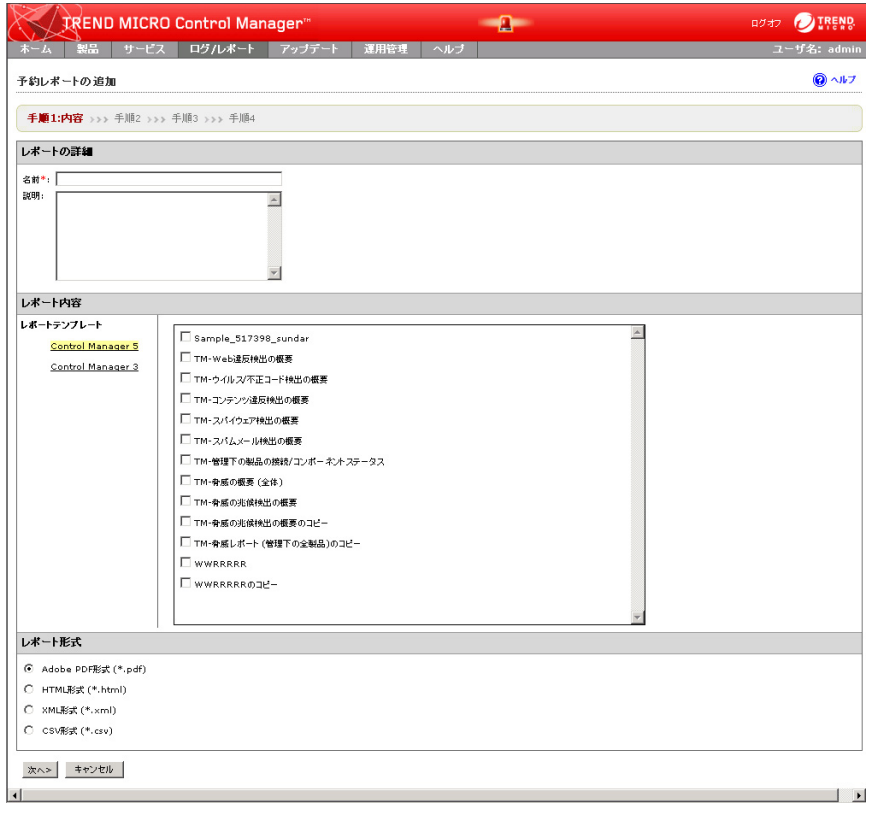
1. [予約レポートの追加] 画面にアクセスしてレポートの種類を選択します。
2. レポートデータの生成元となる製品を指定します。
3. 製品においてデータが生成された日付を指定します。
4. レポートの受信者を指定します。

予約レポートを追加するには

手順 1: [予約レポートの追加] 画面にアクセスしてレポートの種類を選択する

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [予約レポート] をクリックします。[予約レポート] 画面が表示されます。

3. [追加] をクリックします。[予約レポートの追加 > 手順 1: 内容] 画面が表示されます。



4. [レポートの詳細] の [名前] にレポートの名前を入力します。

5. レポートの生成に使用する Control Manager テンプレートを選択します。

Control Manager 5.0 のレポートテンプレート

a. レポートの生成に使用する Control Manager 5.0 テンプレートを選択します。

既存のレポートが要件を完全に満たさない場合は、[レポートテンプレート] 画面から作成します。詳細については、242 ページの「Control Manager 5.0 レポートテンプレートの追加」を参照してください。

Control Manager 3 のレポートテンプレート

a. [レポート内容] で、[Control Manager 3] をクリックします。Control Manager 3 テンプレートが、右側の画面の [レポート内容] に表示されます。

b. レポートのベースとなるレポートカテゴリを選択します。

c. テンプレートのベースとなる Control Manager 3 テンプレートデータを選択します。

6. レポートの出力形式を選択します。

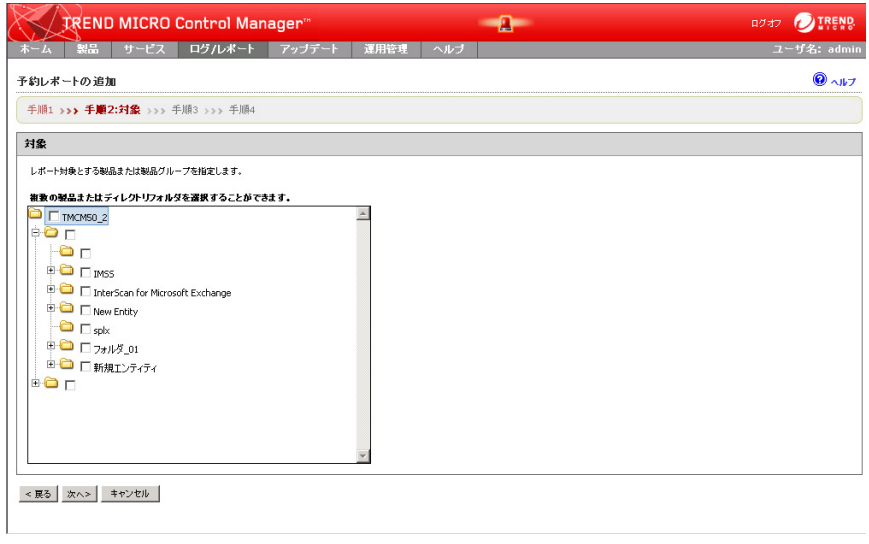
Control Manager 5.0 レポート出力形式

- Adobe PDF 形式 (*.pdf)
- HTML 形式 (*.html)
- XML 形式 (*.xml)
- CSV 形式 (*.csv)

Control Manager 3 レポート出力形式

- リッチテキスト形式 (*.rtf)
- Adobe PDF 形式 (*.pdf)
- ActiveX
- Crystal Reports 形式 (*.rpt)

7. [次へ] をクリックします。[予約レポートの追加 > 手順 2: 対象] 画面が表示されます。



手順 2: レポートデータの生成元となる製品を指定する

1. レポート情報の収集元となる管理下の製品またはディレクトリを選択します。
2. 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。

3. [次へ] をクリックします。[予約レポートの追加 > 手順 3: 実行間隔] 画面が表示されます。

手順 3: 製品においてデータが生成された日付を指定する

1. レポートの生成頻度を指定します。

   - 毎日 — 毎日生成されます。
   - 毎週 — 毎週、指定された日に生成されます。
   - 隔週 — 隔週で、指定された日に生成されます。
   - 毎月 — 毎月の最初の日、15 日、または最後の日に生成されます。

2. 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。

3. スケジュールを開始する日時を指定します。

- ただちに開始 — レポートのスケジュール実行は、レポートが有効にされた直後に開始されます。
- 開始日時 — レポートのスケジュール実行は、ここで指定された日時に開始されます。

a. [yyyy/MM/dd] に日付を入力します。

b. 日付の右側にある [時間] と [分] に時刻を入力します。

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。

4. [次へ] をクリックします。[予約レポートの追加 > 手順 4: メッセージの内容と受信者] 画面が表示されます。

手順 4: レポートの受信者を指定する

1. レポートを添付するメールメッセージのタイトルを [件名] に入力します。
2. レポートに関する説明を [メッセージ] に入力します。
3. [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、指定した受信者へのレポート送信を有効にします。
4. [レポート受信者] リストからユーザまたはグループを選択して指定します。
5. レポートを受信するユーザまたはグループを選択し、[>>] ボタンをクリックします。
6. レポートを受信するユーザまたはグループをすべて選択したら、[完了] をクリックします。

予約レポートの有効化 / 無効化

初期設定では、予約プロファイルは Control Manager によって作成時に有効にされます。プロファイルを無効にした場合 (たとえば、データベースやエージェントの移行中)、[予約レポート] 画面を使用して再度有効にできます。

予約レポートを有効 / 無効にするには

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューから [予約レポート] を選択します。[予約レポート] 画面が表示されます。
3. [予約レポート] 表の [有効] 列にある有効化 / 無効化アイコンをクリックします。無効化 / 有効化アイコンが列に表示されます。

生成したレポートの表示

メールメッセージの添付ファイルとしてレポートを送信するほか、次のいずれかの領域から生成したレポートを表示できます。

- 1 回限りのレポート
- 予約レポート

レポートを表示するには

1. 上部のメニューで [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで次のいずれかを選択します。

   1 回限りのレポート

   a. ドロップダウンメニューから [1 回限りのレポート] をクリックします。[1 回限りのレポート] 画面が表示されます。

   b. [表示] 列で表示するレポートのリンクをクリックします。

   予約レポート

   a. ドロップダウンメニューから [予約レポート] をクリックします。[予約レポート] 画面が表示されます。

   b. [履歴] 列で表示するレポートのリンクをクリックします。そのレポートの [予約レポート履歴] 画面が表示されます。

   c. [予約レポート履歴] 画面から表示するレポートを選択します。

レポート管理の設定

[レポート管理] を使用して、不要になったレポートの削除を設定します。

レポート管理を設定するには

1. [ログ / レポート] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [レポート管理] を選択します。[レポート管理] 画面が表示されます。

4. 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。
5. [保存] をクリックします。

第 7 章

管理下の製品の管理

本章では、管理者が、Trend Micro Control Manager (以下、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。

本章は次の内容で構成されています。

エージェントについて

Control Manager 3.5/5.0 では MCP と Control Manager 2.x の各エージェントを使用して、Control Manager システム上の製品を管理します。

- **Control Manager エージェント (バージョン 2.51 以降)** — Control Manager 2.5/3.0 のアーキテクチャに対応して開発されたこのエージェントは、旧バージョンのトレンドマイクロ製品に必要です。
- **Trend Micro Management Communication Protocol (以下、MCP) エージェント** — トレンドマイクロの次世代エージェントで、セキュリティの強化、シングルサインオン (SSO)、一方向および双方向通信、およびクラスタノードをサポートしています。

次の表は、Control Manager 2.x エージェントと MCP エージェントでサポートされている機能についてまとめたものです。

表 7-1. エージェントの比較

機能	MCP エージェント	CONTROL MANAGER 2.X エージェント
大規模感染予防サービス	可	可
シングルサインオン (SSO)	可	不可
一方向 / 双方向通信	可	不可
NAT サポート	可	不可
クラスタノードのサポート	可	不可
Control Manager に対するアップデートおよびコマンドについてのエージェントによるポーリング	可	不可
エージェントデータベースが破損または削除された場合の、Control Manager サーバへの再登録機能	なし (この問題は MCP エージェントでは発生しません)	8 時間後に自動的に登録
通信セキュリティ	HTTPS/HTTP	暗号化および任意の認証
コミュニケータ	不可	可
コミュニケータスケジュール設定への対応	可	可

表 7-1.　エージェントの比較

機能	MCP エージェント	CONTROL MANAGER 2.X エージェント
エージェント / コミュニケータの接続ステータス	可	可
通知 : パターンファイルの期限切れ	可	可
通知 : コンポーネントのアップデート失敗	可	可
通知 : コンポーネントの配信失敗	可	可
通知 : 製品サービスの停止	可	可

管理下の製品にはそれぞれ、次の処理を実行する固有のエージェントがあります。

表 7-2.　MCP エージェントと Control Manager 2.x エージェントの比較

MCP エージェント	CONTROL MANAGER 2.X エージェント
Control Manager サーバから管理下の製品に対するコマンドをポーリング	コミュニケータを介して Control Manager サーバからコマンドを受信
管理下の製品のステータスおよびログを収集し、HTTPS を介して Control Manager サーバに収集したログを送信	管理下の製品のステータスおよびログを収集し、コミュニケータを介して Control Manager サーバに収集したログを送信

コミュニケータについて

コミュニケータは、メッセージルーティングフレームワークともいい、旧バージョンの管理下の製品と Control Manager の通信バックボーンです。コミュニケータは、Trend Micro Management Infrastructure (以下、TMI) コンポーネントの 1 つです。コミュニケータでは、Control Manager サーバと旧バージョンの管理下の製品との通信がすべて処理されます。コミュニケータは Control Manager と対話して、旧バージョンの管理下の製品と通信します。

Control Manager 2.5 エージェントは、管理下の製品サーバにインストールするアプリケーションの 1 つで、これによって Control Manager で製品の管理ができるようになります。エージェントは、管理下の製品およびコミュニケータと対話します。エージェントは、管理下の製品とコミュニケータとの間をつなぐブリッジとして機能します。そのため、管理下の製品と同じコンピュータにエージェントをインストールする必要があります。現在、エージェントがリモートに動作する必要がある場合は次の 2 つだけです。

- ウイルスバスター コーポレートエディションが、NetWare サーバにインストールされている場合
- NetScreen ファイアウォール管理の場合

Control Manager のインストール時には、コミュニケータが管理下の製品サーバですでに使用可能かどうかがチェックされます。使用可能な場合、コミュニケータのインスタンスがさらにインストールされることはありません。1 つの製品サーバの複数のエージェントで 1 つのコミュニケータが共有されます。コミュニケータの機能は次のとおりです。

- OpenSSL オープンソースライブラリにより提供される暗号化によるメッセージのセキュリティ確保と再送攻撃対策 (anti-replay) の機能、およびトレンドマイクロ開発のエンドツーエンド認証
- Control Manager サーバから管理下の製品へのコマンドの受信と中継
- 管理下の製品から Control Manager サーバへのステータス情報の受信と中継

前述の説明において、重要な点は次のとおりです。

- TMI は独立して存在することができますが、管理下の製品はコミュニケータなしでは動作できません。
- サーバには最高で管理下の製品と同じ数だけのエージェントが入っていますが、1 つのサーバで必要とされるコミュニケータの数は 1 つだけです。
- 複数の管理下の製品でコミュニケータの機能を共有することができます。

接続ステータスアイコンについて

Control Manager の管理下の製品、コミュニケータ、および下位サーバでは、次の接続ステータスアイコンが使用されます。

表 7-3.　管理下の製品で使用されるステータスアイコン

接続ステータスの説明	管理下の製品	
製品サービスが実行中		
製品サービスが停止中		
TMI サービスが停止中		接続ステータスの異常ステータスの条件の設定値内
		接続ステータスの異常ステータスの条件の設定値を超過
コミュニケータと管理下の製品間のソケットまたはネットワーク接続が切断されている		
コミュニケータと Control Manager サーバ間で DNS の名前解決ができない		接続ステータスの異常ステータスの条件の設定値内
		接続ステータスの異常ステータスの条件の設定値を超過

表 7-4.　コミュニケータで使用されるステータスアイコン

接続ステータスの説明	コミュニケータ	
TMI サービスが実行中		
TMI サービスが停止中		接続ステータスの異常ステータスの条件の設定値内
		接続ステータスの異常ステータスの条件の設定値を超過

表 7-4.　コミュニケータで使用されるステータスアイコン

接続ステータスの説明	コミュニケータ
エージェント / コミュニケータのスケジュール設定に従って停止モードになっている	
コミュニケータと管理下の製品間のソケットまたはネットワーク接続が切断されている	
コミュニケータと Control Manager サーバ間で DNS の名前解決ができない	

表 7-5.　下位サーバで使用されるステータスアイコン

接続ステータスの説明	下位サーバ	
TMI サービスが停止中	ステータス変更なし	接続ステータスの異常ステータスの条件の設定値内
		接続ステータスの異常ステータスの条件の設定値を超過
下位サーバのサービスである Casprocessor.exe が実行中		
Casprocessor.exe または下位サーバのコミュニケータが停止中。下位サーバがシャットダウンされているか、コミュニケータサービスが無効になっている。		
下位サーバが上位サーバの管理コンソールから無効にされている		

Control Manager のセキュリティレベルについて

Control Manager では、従来のエージェントと MCP エージェントの両方について、Control Manager サーバと管理下の製品および下位サーバとの通信に、3 段階のセキュリティレベルを使用できます。MCP エージェントでは、セキュリティレベルは IIS の仮想フォルダに適用され、高、中、標準の 3 段階に分かれています。

- **高** — Control Manager の通信には HTTPS のみが使用されます。
- **中** — HTTPS が使用可能な場合には Control Manager の通信に HTTPS が使用され、HTTPS が使用不可能な場合には HTTP が使用されます。
- **標準** — Control Manager の通信には HTTP が使用されます。

それぞれのセキュリティレベルに対応するセキュリティ動作は次のとおりです。

表 7-6. MCP エージェントのセキュリティレベル別動作

機能	セキュリティレベル		
	高	中	標準
HTTPS UI アクセスのみサポート	●	●	
HTTPS および HTTP UI アクセスのサポート			●
HTTPS または HTTP 製品 UI へのリダイレクトのサポート	●	●	●
HTTPS 対応製品 (MCP) とのみ統合	●		
HTTP および HTTPS 対応製品両方との統合		●	●
Control Manager からの HTTP 経由でのアップデートダウンロードの許可	●	●	●

Control Manager により、従来のエージェントのセキュリティレベルに応じて、次の暗号化と認証が適用されます。

- **SSL によるパケットレベルの暗号化** — Control Manager では、SSL (Secure Socket Layer) によるパケットレベルの暗号化は、すべてのセキュリティレベルに適用されます。SSL によるパケットレベルの暗号化は、Web 上の安全なトランザクションを実現するために、Netscape によって開発されたプロトコルです。SSL では、公開鍵暗号方式が使用されます。公開鍵暗号方式では、ブラウザによる、一般に公開された公開鍵を使用したデータの暗号化が可能です。ただし、データの復号化は、対応するプライベートキーを知っている場合にのみ可能です。

  Control Manager エージェントでは、公開鍵を使用して通信を暗号化できます。一方、Control Manager サーバでは、プライベートキーを使用してエージェントのメッセージが復号化されます。

- **トレンドマイクロ認証** — Control Manager では、トレンドマイクロ認証のセキュリティレベル 5 (高) が適用されます。

  Control Manager では、[高] レベルを使用する場合、まず SSL によるパケットレベルの暗号化が適用されます。次にトレンドマイクロ認証を適用して暗号化が強化されます。

注意： Control Manager のセキュリティレベルを TMI.cgf で変更できます。ただし、セキュリティレベルを変更するには Control Manager システムに存在するすべての TMI.cgf、つまり Control Manager サーバ、およびすべての管理下の製品と下位サーバの TMI.cfg を変更する必要があります。すべての TMI.cfg を変更しなければ、サーバとエージェント間の通信は機能しません。

表 7-7. 従来のエージェントのセキュリティレベル別動作

セキュリティレベル (TMI.CFG で設定)	セキュリティレベルの選択 (インストール時)	エンドツーエンド認証	メッセージレベルの暗号化
1	低	適用外	40 ビット (RC4)
2	中	適用外	128 ビット (RC4)
5	高	トレンドマイクロ認証	128 ビット (RC4 ＋ 3DES)

エージェントコミュニケータスケジュール設定の使用

[エージェントの通信スケジュール] 画面で、エージェントから Control Manager サーバに情報が送信される時間帯を指定できます。通信のスケジュールを設定することにより、ネットワークトラフィックを制御できます。

Control Manager エージェントをインストールすると、初期設定の通信スケジュールが指定されます。このスケジュールは、使用する Control Manager システムの必要性に応じて変更できます。エージェントコミュニケータスケジュール設定は、日単位の設定に従います。つまり、スケジュールは日単位でエージェントに適用されます。稼動時間を週単位または月単位で設定することはできません。

スケジュールを設定すると、Control Manager に登録されたすべての管理下の製品にそのスケジュールが適用されます。

注意： 大規模感染予防モードが有効になっている状態でエージェントが停止した場合でも、このエージェントの管理下の製品では大規模感染予防サービスの各コマンドを実行します。ただし、Control Manager にはその結果を報告しません。したがって、Control Manager はステータスや結果を知ることができません。コマンド追跡機能を使用すると、大規模感染予防ポリシー関連コマンドのこの実行結果が [失敗] カテゴリに表示されます。

エージェントコミュニケータスケジュール設定による停止および稼動スケジュールは、管理下の製品のエージェントにのみ適用されます。Control Manager 3.5 の下位サーバに対しては、停止スケジュールを設定できません。

注意： [エージェントの通信スケジュール] 画面には、下位サーバのエージェントも表示されます。ただし、チェックボックスは使用できません。

エージェント / コミュニケータの接続ステータスについて

接続ステータスとは、Control Manager サーバに「生存確認 (キープアライブ)」情報を通知する、MCP エージェントや Control Manager 2.x エージェントのメッセージのことです。エージェントのこの機能により、管理下の製品の接続が維持されているかどうかを判断できます。

ヒント： 接続ステータスの稼動時間および停止時間を定義するには、[エージェントの通信スケジュール] を使用します。

エージェントでは Control Manager サーバを定期的にポーリングします。これにより、Control Manager コンソールに最新の情報が表示されるようになり、管理下の製品と Control Manager サーバ間の接続が正常であることが確認されます。

コミュニケータの接続ステータスには、次の 3 種類があります。

- 稼動中 — 稼動時間内
- 停止中 — 停止時間内、または稼動時間外
- 異常 — 通信不可能

詳細については、281 ページの「接続ステータスアイコンについて」を参照してください。

注意： エージェントは Control Manager サーバに接続ステータスを定期的に送信するだけでなく、管理下の製品のステータス情報もリアルタイムでサーバに送信します。

MCP 接続ステータス

管理下の製品のステータスを監視するために、MCP エージェントはスケジュールに基づいて Control Manager に対してポーリングを実行します。ポーリングは、管理下の製品のステータスを示したり、Control Manager からの管理下の製品へのコマンドを確認したりするために実行されます。ポーリングの実行後に、Control Manager 管理コンソールに管理下の製品のステータスが表示されます。つまり、管理下の製品のステータスは、ネットワークのステータスをリアルタイムに刻一刻と反映したものではありません。Control Manager により、各管理下の製品のステータスがバックグラウンドで順番に確認されます。管理下の製品の接続ステータスが確認されないまま一定の時間が経過すると、Control Manager により、その管理下の製品のステータスがオフラインに変更されます。

Control Manager による管理下の製品のステータスを判断する基準となるのは接続ステータスのみではありません。Control Manager では、次に示すことからも管理下の製品のステータスが判断されます。

- Control Manager は管理下の製品からログを受信します。Control Manager が、管理下の製品からいずれかの種類のログを正常に受信したということは、管理下の製品が正常に動作しているということを意味します。
- 双方向の通信モードでは、管理下の製品による保留中のコマンドの取得をトリガするために、Control Manager は積極的に通知メッセージを送信します。サーバが特定の管理下の製品に正常に接続されるということは、この管理下の製品が正常に動作していることも表しており、このイベントは 1 つの接続ステータスとみなされます。
- 一方向通信モードでは、MCP エージェントから Control Manager に対して定期的にクエリコマンドが送信されます。この定期的なクエリ動作は接続ステータスのような働きをし、Control Manager でも接続ステータスと同様の扱いを受けます。

MCP 接続ステータスは、次の方法で実装されます。

- UDP — 特定の管理下の製品が UDP を使用してサーバにアクセスできる場合、これは最も単純で高速のソリューションです。ただし、この方法は NAT またはファイアウォール環境では機能しません。また、送信側のクライアントは、サーバが実際に要求を受信しているかどうかを確認できません。
- HTTP/HTTPS — NAT またはファイアウォール環境で機能できるようにするには、複雑な HTTP 接続を使用して、接続ステータスを送信します。

Control Manager は接続ステータスを報告するために、UDP メカニズムと HTTP/HTTPS メカニズムの両方をサポートしています。Control Manager サーバは、登録プロセスで管理下の製品がどのモードを適用したかを認識します。モードを判断するために、両者の間で別のプロトコルのハンドシェイクが実行されます。

管理下の製品のステータスを示すために単に接続ステータスを送信すると同時に、追加データを Control Manager にアップロードすることもできます。通常、追加データには、コンソールに表示される、管理下の製品のアクティビティ情報が含まれます。

スケジュールバーの使用

コミュニケータスケジュールを表示、設定するには、[コミュニケータスケジュールの設定] 画面のスケジュールバーを使用します。スケジュールバーは 24 個のスロットから構成され、1 つのスロットは 1 時間を表します。

青いスロットは、エージェント / コミュニケータから Control Manager サーバに情報が送信される稼動中のステータスまたは時間帯を表します。白いスロットは停止中の時間帯を表します。特定のスロットの設定を変更して、稼動中または停止中の時間帯を定義します。

コミュニケータスケジュールでは、最大で 3 つの停止期間を指定できます。下の例では、2 つの停止期間が指定されています。

図 7-1.　スケジュールバー

ここで指定されている接続時間は、午前 0:00 から午前 7:00、午前 8:00 から午後 4:00、午後 6:00 から午前 0:00 です。

適切な接続ステータス設定について

コミュニケータ接続ステータスの実行間隔を指定するときは、コミュニケータのステータス情報の更新頻度と、システムリソースの消費の抑制の両方を考慮します。初期設定では、一般的な状況を前提にして間隔が設定されていますが、接続ステータス設定をカスタマイズする場合は次の点に注意してください。

表 7-8. 推奨される接続ステータス

接続ステータスの頻度	考慮する点
長い間隔の接続ステータス (60 分以上)	接続ステータスの実行間隔を長く設定すると、Control Manager 管理コンソールにコミュニケータステータスが反映されるまでの期間が長くなり、その間に新たに発生するイベントの数が多くなります。 たとえば、コミュニケータとの接続トラブルが発生して、その後解決された場合でも、ステータスが更新されるまでに時間がかかります。ステータスが「停止中」または「異常」と表示されていたとしても、実際にはコミュニケータとの通信が可能になっている場合があります。
短い間隔の接続ステータス (60 分未満)	接続ステータスの実行間隔を短く設定すると、Control Manager サーバの管理コンソールに、より最新のステータスが表示されるようになります。ただし、コミュニケータとの頻繁な通信によって帯域幅が多く消費されます。

エージェント通信スケジュールの設定

管理下の製品が Control Manager サーバと通信する時間帯を指定できます。最大 3 セットの停止期間を定義できます。

下位 Control Manager サーバは、上位 Control Manager サーバと常に通信する必要があります。したがって、[エージェントの通信スケジュール] 画面では、下位サーバの管理下の製品と下位サーバのエージェントの通信スケジュール変更できません。

管理下の製品のエージェント通信スケジュールを設定するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューで [エージェントの通信スケジュール] をクリックします。[エージェントの通信スケジュール] 画面が表示されます。

4. 変更する管理下の製品のスケジュールを選択します。[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。

5. スケジュールを定義します。任意の時間を指定するか、または初期設定の値をそのまま使用します。

   - 新しいスケジュールを指定するには、スケジュールバーで適切な時間枠を選択し、[保存] をクリックします。
   - 初期設定を使用するには、目的の設定を選択し、[初期設定スケジュールへのリセット] をクリックします。

エージェント / コミュニケータの初期設定スケジュールの変更

エージェント / コミュニケータの初期設定スケジュールを使用すると、エージェント / コミュニケータのスケジュールを自動設定できます。

管理下の製品のコミュニケータのスケジュールを変更するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューで [エージェントの通信スケジュール] をクリックします。[エージェントの通信スケジュール] 画面が表示されます。

4. 作業領域で [初期設定のスケジュール] をクリックします。

5. [日単位のスケジュール] で、目的の時間枠を切り替えます。

6. [保存] をクリックします。

エージェント / コミュニケータの接続ステータスの設定

[接続ステータスの設定] を使用すると、Control Manager サーバと Control Manager エージェントの通信の実行間隔および分単位の異常ステータスの条件を設定できます。

注意： エージェント / コミュニケータの接続ステータス設定は、Control Manager サーバによって直接管理される製品のコミュニケータだけに適用されます。下位にある Control Manager サーバのエージェント / コミュニケータには、定義済みの次の値が使用されます。
実行間隔 : 3 分
異常ステータスの条件 : 5 分

接続ステータスの実行間隔、および異常ステータスの条件を設定するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。リストボックスが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューで [接続ステータスの設定] をクリックします。[接続ステータスの設定] 画面が表示されます。

4. 右側の画面で、初期設定値をそのまま使用するか、または次の項目に任意の値を指定します。

   - 管理対象製品のステータスをレポートする間隔 — Control Manager サーバのメッセージに対してコミュニケータが応答する間隔。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 — コミュニケータからのポーリングを Control Manager サーバが何分間待機するかを指定します。この期間を過ぎてもコミュニケータからのポーリングがなかった場合、その管理コンソールのステータスは「停止中」になります。値は 15 ～ 1440 分の範囲で指定します。

   注意： [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。

5. [保存] をクリックします。

Control Manager サービスの停止と再起動

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 Common CGI
- Control Manager

注意： これらのサービスは、Windows OS のバックグラウンドで動作するものです。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 (大規模感染予防サービスやダメージクリーンナップサービスなど) ではありません。

Control Manager サービスを再起動するには

1. [スタート] メニューから [プログラム]→[管理ツール]→[サービス] の順に選択して、[サービス] 画面を開きます。
2. 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。
3. 対象の Control Manager サービスを右クリックして、[開始] をクリックします。

Control Manager の外部通信ポートの変更

コミュニケータは、エージェントとサーバ間の通信を実行します。

初期設定では、コミュニケータは内部通信となる Control Manager プロセス間の通信にはポート 10198 を、外部通信となる Control Manager エージェントとサーバ間の通信にはポート 10319 を使用します。

外部通信ポートの変更は、2 段階の手順を必要とします。

Control Manager サーバで外部通信ポートを変更するには

1. メモ帳などのテキストエディタを使用して、「C:¥Program Files¥Trend Micro¥COMMON¥ccgi¥commoncgi¥config¥CCGI_Config.xml」ファイルを開きます。

警告： Control Manager の *.xml または *.cfg ファイルを変更する場合は、十分に注意してください。元の設定に復元できるように、CCGI_Config.xml のバックアップを作成してください。

---

2. OuterPort パラメータに新規の値を指定します。この値は、外部通信ポートの番号を表します。

   たとえば、ポート 2222 を使用するには「OuterPort="2222"」と設定します。
3. CCGI_Config.xml を保存して閉じます。

4. テキストエディタを使用して、「C:¥Program Files¥Trend Micro¥COMMON¥TMI¥TMI.cfg」ファイルを開きます。

警告： 設定ファイルの変更を誤ると、深刻なシステム問題が生じる可能性があります。元の設定を復元できるように、TMI.cfg のバックアップを作成してください。

5. CCGI_Config.xml の値と一致するように、OuterPort パラメータの値を置き換えます。
6. TMI.cfg を保存し閉じます。
7. Control Manager のすべてのサービスをいったん停止してから再起動します。

管理下の製品サーバで外部通信ポートを変更するには

1. テキストエディタを使用して TMI.cfg を開きます。通常、管理下の製品の TMI.cfg は、C:¥Program Files¥Trend Micro¥Common¥TMI ディレクトリに置かれています。
2. Control Manager サーバの CCGI_Config.xml の値と一致するように、OuterPort の値を変更します。
3. HostID の値を、新規ポートの値と一致するように変更します。たとえば、「HostID=12.1.123.123:2222」と設定します。
4. Trend Micro Management Infrastructure サービスをいったん停止してから再起動します。
5. すべての管理下の製品サーバに対し、手順 1 ～ 5 を繰り返します。

警告： Control Manager システムのサーバおよびエージェントのすべての TMI.cfg に、この OuterPort 値を設定します。すべての TMI.cfg を変更しなければ、サーバとエージェント間の通信は機能しません。

TMI エージェントのセキュリティレベルの変更

Control Manager には、Control Manager のインストール時に指定したセキュリティレベルが適用されます。TMI.cfg を使用すると、製品を再インストールせずにセキュリティレベルを変更できます。

Control Manager のセキュリティレベルを変更するには

1. メモ帳などのテキストエディタを使用して、「C:¥Program Files¥Trend Micro¥COMMON¥TMI¥TMI.cfg」ファイルを開きます。

警告： 設定ファイルの変更を誤ると、深刻なシステム問題が生じる可能性があります。

2. 元の設定を復元できるように、TMI.cfg のバックアップを作成してください。
3. MaxSecurity パラメータの値を変更します。必要なセキュリティレベルに応じて、値「1」、「2」、または「5」を設定します。
4. TMI.cfg を保存し閉じます。
5. Windows の [サービス] 画面を開き、各 Control Manager サービスをいったん停止してから再起動します。
6. 手順 1 ～ 3 を繰り返し、Control Manager システム上のすべてのエージェントについて TMI.cfg を変更します。

警告： Control Manager システムのサーバおよびエージェントのすべての TMI.cfg に対し、同一のセキュリティレベル値 (MaxSecurity) を設定します。すべての TMI.cfg を変更しなければ、サーバとエージェント間の通信は機能しません。

コミュニケータ接続ステータスのプロトコルの変更

初期設定では、管理下の製品から Control Manager サーバへのコミュニケータ接続ステータスの送信には、コネクションレス型の UDP (User Datagram Protocol) が使用されます。

コミュニケータ接続ステータスのプロトコルを TCP に変更するには

1. メモ帳などのテキストエディタを使用して、「C:¥Program Files¥Trend Micro¥COMMON¥TMI¥TMI.cfg」ファイルを開きます。

警告： 設定ファイルの変更を誤ると、深刻なシステム問題が生じる可能性があります。元の設定を復元できるように、TMI.cfg のバックアップを作成してください。

2. AllowUDP パラメータの値を「0」に変更します。
3. TMI.cfg を保存し閉じます。
4. Windows の [サービス] 画面を開き、各 Control Manager サービスをいったん停止してから再起動します。
5. 手順 1 ～ 3 を繰り返し、Control Manager システム上のすべてのエージェントについて TMI.cfg を変更します。

警告： Control Manager システムのサーバおよびエージェントのすべての TMI.cfg に対し、同一のセキュリティレベル値 (AllowUDP) を設定します。すべての TMI.cfg を変更しなければ、サーバとエージェント間の通信は機能しません。

MCP と Control Manager の間の通信方法の確認

Control Manager は、MCP エージェントが Control Manager との通信に使用する接続方法を自動検出します。双方向通信の場合、Control Manager は CGI 通知を使用して MCP エージェントと通信します。

Control Manager が双方向通信を使用していることを確認するには

注意： この手順では、Control Manager の初期インストール設定を使用します。

1. [スタート]→[プログラム]→[Microsoft SQL Server] の順にクリックします。[SQL Server Enterprise Manager] ダイアログボックスが表示されます。
2. [Microsoft SQL Servers]→[SQL Server グループ]→[<Control Manager サーバのホスト名 >]→[データベース]→[DB_ ControlManager]→[Tables] の順にクリックします。
3. 「CDSM_Entity」を検索します。
4. CDSM_Entity から以下の項目を検索して確認します。
   - Token 列を見つけます。この列には、「URLTOKEN:**2**; http;10.1.2.3;80; cgiCmdNotify;;!CRYPT!10…」という形式で情報が表示されます。
     - 「URLTOKEN:**1**」は、エージェントで Control Manager との通信に一方向通信が使用されることを表します。
     - 「URLTOKEN:**2**」は、エージェントで Control Manager との通信に双方向通信が使用されることを表します。

Control Manager が双方向通信を使用していることを管理コンソールから確認するには

1. [製品] を選択します。[製品ディレクトリ] 画面が表示されます。
2. 製品ディレクトリで製品またはディレクトリをクリックします。その項目が製品ディレクトリで強調表示されます。
3. [フォルダ] をクリックします。右側の画面の情報が変更されます。
4. [フォルダ] リストボックスで [接続情報表示] を選択します。[モード] 列には、管理下の製品で使用される通信モード (MCP エージェントがオン) が表示されます。

製品ディレクトリについて

管理下の製品とは、Control Manager から管理されるウイルス対策製品、コンテンツセキュリティ製品、または Web セキュリティ対策製品のことです。Control Manager 管理コンソールの製品ディレクトリでは、管理下の製品はアイコン (たとえば、  や ) で表示されます。これらのアイコンは、トレンドマイクロのウイルス対策製品、コンテンツセキュリティ製品、および Web セキュリティ対策製品を表します。Control Manager では、管理下の製品のステータスによって変化する、動的なアイコンがサポートされるようになりました。管理下の製品のアイコンおよび関連付けられているステータスに関する詳細については、管理下の製品に付属するドキュメントを参照してください。

管理下の製品は、製品ディレクトリを通して、製品単位またはグループ単位で管理します。次の表は、[製品ディレクトリ] 画面のメニュー項目とボタンをまとめたものです。

表 7-9. 製品ディレクトリのオプション

メニュー項目	説明
詳細検索	1 つ以上の管理下の製品を検索するときは、このボタンをクリックして検索条件を指定します。
設定	Web ベースのコンソールにログオンし管理下の製品を設定するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。
タスク	特定の管理下の製品または管理下の製品グループ、あるいは特定の下位サーバまたは下位サーバグループに対して、最新コンポーネントの配信などの特定の機能が実行するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。 ディレクトリおよび Control Manager からタスクを開始すると、そのディレクトリに属するすべての管理下の製品に対して要求が送信されます。
ログ	製品ログをクエリして表示するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。 特定の管理下の製品を選択した場合、その製品のログのみをクエリできます。それ以外の場合は、ディレクトリ内で使用可能な製品すべてのログをクエリできます。

表 7-9.　製品ディレクトリのオプション

メニュー項目	説明
ディレクトリ管理	[ディレクトリ管理] 画面を開くときは、このボタンをクリックします。この画面から、ドラッグアンドドロップによるエンティティ / ディレクトリの移動や、新しいディレクトリの作成を実行できます。
ボタン	**説明**
検索	管理下の製品を検索するときは、目的の管理下の製品名を入力してから、このボタンをクリックします。
ステータス	ディレクトリ内の 1 つ以上の管理下の製品に関するステータス概要を取得するときは、目的の管理下の製品 / ディレクトリを選択してから、このボタンをクリックします。
フォルダ	ディレクトリ内の管理下の製品および管理下の製品のクライアントに関するステータス概要を取得するときは、目的のディレクトリを選択してから、このボタンをクリックします。

注意： 下位の Control Manager サーバに属する管理下の製品に対して、上位の Control Manager サーバによるタスクは適用できません。

製品ディレクトリにおける管理下の製品のグループ化

[ディレクトリ管理] 画面を使用して、管理モデルのニーズに合うように、製品ディレクトリ構成をカスタマイズします。たとえば、製品の場所で分類したり、メッセージングセキュリティ対策製品、Web セキュリティ対策製品、ファイルサーバ対策製品などの種類別に分類したりできます。

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 7-10. 管理下の製品をグループ化する際の利点と欠点

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造に関する推奨事項

管理下の製品および下位サーバの製品ディレクトリ構造を計画するときは、次の設定を適用することをお勧めします。

表 7-11. 管理下の製品または下位サーバのグループ化の注意点

構造	説明
社内のネットワークポリシーおよびセキュリティポリシー	社内のネットワークにアクセス権や共有権を適用する場合、社内のネットワークポリシーとセキュリティポリシーに従って管理下の製品および下位サーバをグループ化します。
組織と機能	会社の組織上および機能上の分割に従って、管理下の製品および下位サーバをグループ化します。たとえば、2 台の Control Manager サーバで製品グループとテスト担当グループを管理します。
所在地	管理下の製品 / 下位サーバの位置が Control Manager サーバと管理下の製品 / 下位サーバ間の通信に影響する場合には、グループ化の判断基準として地理的な位置を考慮します。
管理責務	管理下の製品および下位サーバを、それぞれのシステムまたはセキュリティの担当者に合わせてグループ化します。これにより、グループ設定が可能になります。

製品ディレクトリを使用することで、管理下の製品のグループ化をユーザが指定できるようになり、それらのグループに対して次の管理タスクを実行できます。

- 管理下の製品の設定
- 製品への ScanNow の実行要求 (管理下の製品でサポートされている場合のみ)
- 製品情報および製品のインストール環境の詳細情報 (製品バージョン、パターンファイルのバージョン、検索エンジンのバージョン、OS など) の表示
- 製品レベルのログの表示
- 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、製品プログラムの配信

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。

- **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。また、管理下の特定製品を別のセグメントから選択できます。

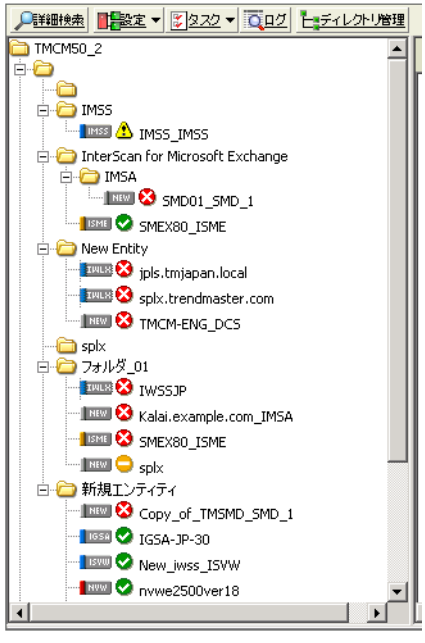
- **配信計画**

  配信計画に基づいて、最新のパターンファイル、検索エンジン、スパムメール判定ルール、製品プログラム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。

- **大規模感染予防ポリシーとダメージクリーンナップテンプレートの配信**

  大規模感染予防ポリシーとダメージクリーンナップテンプレートを効率的に配信できるかどうかは、配信計画に依存します。

次に製品ディレクトリの例を示します。



管理下の製品は、登録済みウイルス対策製品またはコンテンツセキュリティ製品として識別され、接続ステータスも表示されます。

製品ディレクトリのアイコンのリストについては、Control Manager のオンラインヘルプの「製品ディレクトリについて」を参照してください。

ディレクトリ管理機能を使用して、製品ディレクトリを配置します。製品の種類を表すフォルダ名を使用して、保護の種類や Control Manager システムの管理モデルに従って、管理下の製品をグループ化します。たとえば、Server protection フォルダを設定するために、ファイルサーバ管理者へのアクセス権を付与します。

製品ディレクトリの初期設定フォルダ

Control Manager の新規インストール直後の製品ディレクトリは、次のディレクトリで構成されます。

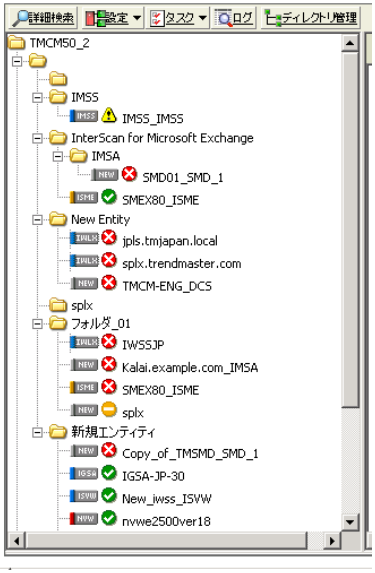
表 7-12. 製品ディレクトリの初期設定フォルダ

構造	説明
root	すべての管理下の製品と下位の Control Manager サーバは、root ディレクトリに配置されます。
階層フォルダ	階層管理環境では、上位サーバのすべての下位サーバが [階層フォルダ] に格納されます。
ローカルフォルダ	Control Manager エージェントによって処理され新規に登録された管理下の製品は、[新規エンティティ] フォルダに格納されます。
検索結果	基本検索または詳細検索を実行すると、その検索条件に合致するすべての管理下の製品が検索結果フォルダに格納されます。

次の製品ディレクトリの例で示すように、管理下の製品では、登録済みのウイルス対策製品とコンテンツセキュリティ製品が識別され、接続ステータスが提供されます。

製品ディレクトリで使用されるアイコン

表 7-13.　管理下の製品を表すアイコン

製品ディレクトリのツリー	アイコン	説明
	または	[新規エンティティ] フォルダまたはユーザ定義のフォルダの名前
	EMAN	InterScan eManager
	OSCE	ウイルスバスター コーポレートエディション
	SPNT	ServerProtect インフォメーションサーバ
		ServerProtect ドメイン
	NT	ServerProtect for Windows (一般サーバ)
	NW	ServerProtect for NetWare (一般サーバ)
	IMSS	InterScan Messaging Security Suite
	IWSS	InterScan Web Security Suite
	ISNT	InterScan VirusWall for Windows
	ISUX	InterScan VirusWall for UNIX
	ISME	InterScan for Microsoft Exchange
	ISLN	InterScan for Lotus Notes
	NVW	Network VirusWall
	FW	NetScreen Global PRO ファイアウォール
		管理下の製品接続ステータスのアイコン

注意： 本トピックには 2008 年 5 月現在、日本ではリリース / サポートされていない製品も記載されています。

管理下の新規登録製品はすべて、エージェントの種類に関係なく、通常 [新規エンティティ] フォルダに表示されます。

製品ディレクトリへのアクセス

製品ディレクトリを使用して、Control Manager サーバに登録されている管理下の製品を管理できます。

注意： 製品ディレクトリのフォルダの表示やフォルダへのアクセスは、アカウントの種類とユーザアカウントのアクセス権によって異なります。

製品ディレクトリにアクセスするには

- 上部のメニューで [製品] を選択します。[製品ディレクトリ] 画面が表示されます。

製品ディレクトリによる新規コンポーネントの手動配信

手動配信を使用すると、管理下の製品のパターンファイル、スパムメール判定ルール、および検索エンジンを必要なときに即座にアップデートできます。この方法を使用して、ウイルスの大規模感染時にコンポーネントをアップデートできます。

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、新規コンポーネントをダウンロードします。

製品ディレクトリを使用して新規コンポーネントを手動配信するには

1. 上部のメニューで [製品] を選択します。[製品ディレクトリ] 画面が表示されます。

2. 製品ディレクトリで管理下の製品またはディレクトリを選択します。管理下の製品またはディレクトリが強調表示されます。
3. 製品ディレクトリメニューで [タスク] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
4. ドロップダウンメニューから [< コンポーネント > の配信] を選択します。
5. [次へ >>] をクリックします。
6. [配信開始] をクリックして、新規コンポーネントの手動配信を開始します。
7. [コマンド追跡]画面 を使用して、進行状況を確認してください。
8. [配信開始] タスクの詳細を表示するには、[コマンド追跡] 画面の [コマンド詳細] リンクをクリックします。

管理下の製品のステータス概要の表示

[ステータス概要] 画面には、製品ディレクトリツリーにあるすべての管理下の製品について、ウイルス対策概要、コンテンツ対策概要、および Web セキュリティ概要が表示されます。

管理下の製品のステータス概要を表示するには、次の 2 とおりの方法があります。

- ホームページから
- 製品ディレクトリから

ホームページからアクセスするには

- Control Manager 管理コンソールを起動した際の初期画面では、[ホーム] 画面に Control Manager システム全体の概要情報が表示されます。この内容は、製品ディレクトリの root フォルダからアクセスする [製品ステータス] タブの内容と同じです。

製品ディレクトリからアクセスするには

1. 上部のメニューで [製品] を選択します。
2. 左側のメニューで、表示するフォルダまたは管理下の製品を選択します。
   - 管理下の製品をクリックすると、その管理下の製品の概要が [製品ステータス] タブに表示されます。
   - [root] フォルダ、[新規エンティティ] フォルダ、またはその他のユーザ定義フォルダをクリックすると、[製品ステータス] タブにウイルス対策、コンテンツ対策、および Web セキュリティの概要が表示されます。

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 1 週間分の情報がステータス概要に表示されます。この範囲を変更するには、[レポート期間] で [今日]、[過去 7 日間]、[過去 14 日間]、[過去 30 日間] のいずれかを選択します。

管理下の製品の設定

管理下の製品とエージェントのバージョンによって、管理下の製品の設定方法が異なります。管理下の製品の管理コンソールで設定する方法と、Control Manager によって生成されるコンソールで設定する方法があります。

管理下の製品を設定するには

1. 製品ディレクトリにアクセスします。
2. 製品ツリーから目的の管理下の製品またはフォルダを選択します。製品のステータスが画面の右側に表示されます。
3. 製品ツリーメニューで [設定] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
4. 次のいずれかを選択します。

   設定の複製 — [設定] 画面が表示されます。

   a. 製品ディレクトリ構造から、選択した管理下の製品の設定を複製する複製先フォルダを選択します。

   b. [複製] をクリックします。選択した管理下の製品の設定が、対象の管理下の製品に複製されます。

   < 管理下の製品の名前 > の設定 — 管理下の製品の Web ベースコンソールまたは Control Manager によって生成されるコンソールが表示されます。

   a. 管理下の製品を管理コンソールで設定します。

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。

管理下の製品に対するタスクの実行

[タスク] メニュー項目を使用すると、特定の管理下の製品に対し有効なタスクを実行できます。管理下の製品に応じて、次のすべて、または一部のタスクを実行できます。

- エンジンの配信
- パターンファイル / テンプレートの配信
- プログラムファイル配信
- リアルタイム検索開始
- ScanNow

最新ではないコンポーネントを使用している管理下の製品には、最新のスパムメール判定ルール、パターンファイル、または検索エンジンを配信します。これを適切に実行するには、Control Manager サーバに、トレンドマイクロのアップデートサーバからの最新のコンポーネントが実装されている必要があります。Control Manager サーバに最新のコンポーネントが確実に実装されるようにするには、手動ダウンロードを実行します。

管理下の製品に対してタスクを実行するには

1. 製品ディレクトリにアクセスします。
2. タスクを実行する対象の管理下の製品またはディレクトリを選択します。
3. [タスク] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
4. リストからタスクを選択します。[コマンド追跡] を使用して、進行状況を確認してください。応答画面で [コマンド詳細] リンクをクリックすると、コマンド情報が表示されます。

管理下の製品ログのクエリと表示

[ログ] タブを使用すると、グループ単位または特定の管理下の製品のログにクエリを実行してログを表示できます。

管理下の製品ログにクエリを実行してログを表示するには

1. 製品ディレクトリにアクセスします。
2. 製品ディレクトリで目的の管理下の製品またはフォルダを選択します。
3. 製品ディレクトリメニューで [ログ] の上にカーソルを置きます。リストボックスが表示されます。
4. ドロップダウンメニューから [ログ] を選択します。[アドホッククエリ 手順 2: データビュー] 画面が表示されます。

5. ログのデータビューを指定します。
   a. [使用可能なデータビュー] 領域からクエリを実行するデータを選択します。

b. [次へ] をクリックします。[手順 3: クエリ条件] 画面が表示されます。

6. ログに表示するデータとデータの表示順序を指定します。

[選択されたフィールド] リストの上部に表示される項目は、表の左端の列として表示されます。フィールドを [選択されたフィールド] リストから削除すると、対応する列が [アドホッククエリ] の表から削除されます。

a. [列の表示を変更する] をクリックします。[表示順序の選択] 画面が表示されます。

b. [使用可能なフィールド] リストからクエリ列を選択します。選択された項目が強調表示されます。

<Shift> キーまたは <Ctrl> キーを使用して、複数項目を選択できます。

c. [>] をクリックして、項目を [選択されたフィールド] リストに追加します。

d. 項目を選択し、[上へ移動] または [下へ移動] をクリックして、データの表示順序を指定します。

e. 表示順序が要件を満たしたら、[戻る] をクリックします。

7. データのフィルタ条件を指定します。

注意： 概要データのクエリを実行する際、[必要な条件] で項目を指定する必要があります。

必要な条件 —

- データの [集計日時] を指定するか、COOKIE をレポートに表示するかどうかを指定します。

カスタム条件 —

a. データカテゴリの条件フィルタルールを指定します。

- すべての条件 — これを選択すると、論理積 (AND) として機能します。レポートに表示されるデータは、すべてのフィルタ条件に適合する必要があります。
- いずれかの条件 — これを選択すると、論理和 (OR) として機能します。レポートに表示されるデータは、いずれかのフィルタ条件に適合する必要があります。

b. データのフィルタ条件を指定します。Control Manager では、データのフィルタ用に最大 20 個の条件を指定できます。

ヒント： フィルタ条件を指定しないと、アドホッククエリでは該当する列の結果がすべて返されます。フィルタ条件を指定して、クエリから返された情報のデータ分析を簡単にすることをお勧めします。

8. クエリを保存するには

a. [保存されたアドホッククエリリストにこのクエリを保存します。] をクリックします。

b. 保存したクエリの名前を [クエリ名] に入力します。

9. [クエリ] をクリックします。[アドホッククエリの結果] 画面が表示されます。

10. レポートを CSV 形式で保存するには

a. [CSV 形式で出力] をクリックします。ダイアログボックスが表示されます。

b. [保存] をクリックします。[名前を付けて保存] ダイアログボックスが表示されます。

c. ファイルを保存する場所を指定します。

d. [保存] をクリックします。

11. レポートを XML 形式で保存するには

a. [XML 形式で出力] をクリックします。ダイアログボックスが表示されます。

b. [保存] をクリックします。[名前を付けて保存] ダイアログボックスが表示されます。

c. ファイルを保存する場所を指定します。

d. [保存] をクリックします。

ヒント： 1 つの画面でより多くの結果を表示するには、[1 ページの表示件数] で別の値を選択します。1 つの画面では、1 ページに 10 件、15 件、30 件、または 50 件のクエリ結果を表示できます。

12. クエリの設定を保存するには

a. [クエリ設定の保存] 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. 保存したクエリの名前を [クエリ名] に入力します。

c. [OK] をクリックします。保存したクエリが [保存されたアドホッククエリ] 画面に表示されます。

製品ディレクトリから削除された管理下の製品の再登録

Control Manager では、次のような場合に、管理下の製品が製品ディレクトリから削除される可能性があります。

- 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

  このオプションを選択すると、既存のデータベース名を使用して新規のデータベースが作成されます。

- 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
- ディレクトリ管理を使用して、管理下の製品を誤って削除した場合

管理下の製品に関するレコードが Control Manager サーバ側で失われても、登録先サーバの情報はその製品の TMI エージェント側で保持されています。Control Manager エージェントは、8 時間後またはサービスの再起動時に、自動的にエージェント自身を再登録します。

MCP エージェントは自動的には再登録しません。管理者は MCP エージェントを使用して手動で管理下の製品を再登録する必要があります。

製品ディレクトリから削除された管理下の製品を再登録するには

- 管理下の製品のサーバで Trend Micro Control Manager サービスを再起動します。詳細については、294 ページの「Control Manager サービスの停止と再起動」を参照してください。
- **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。**初期設定では、旧バージョンの Control Manager エージェントは 8 時間おきにサーバとの接続を確認します。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。

  エージェントの接続確認時間を変更する方法については、317 ページの「Control Manager 2.x エージェント接続の再確認頻度の変更」を参照してください。
- **手動で Control Manager に再登録します。**MCP エージェントは自動的には再登録しません。したがって、手動で Control Manager サーバに再登録する必要があります。

Control Manager 2.x エージェント接続の再確認頻度の変更

初期設定では、Control Manager 2.x エージェントは Control Manager サーバとの接続を 8 時間おきに確認します。確認頻度を変更するには、エージェントコンピュータにある設定ファイルを編集します。

注意： 接続が失われると、MCP エージェントは Control Manager に接続できません。ユーザは手動で管理下の製品を再登録する必要があります。

エージェントの接続確認頻度を変更するには

1. 管理下の製品のサーバから、Control Manager エージェントのインストールディレクトリ (例 : C:¥Program Files¥Trend Micro¥IMSS¥Agent) に移動します。
2. Entity.cfg をのバックアップを作成します。
3. メモ帳などのテキストエディタを使用して、Entity.cfg を開きます。

4. パラメータ ENTITY_retry_hour を検索し、整数の値を指定して、初期設定の確認時間を変更します。

   ENTITY_retry_hour の値の単位は「時間」です。1 から 24 時間の範囲内で指定してください。

5. 変更を保存して Entity.cfg を閉じ、新しい確認時間を適用します。

管理下の製品、製品ディレクトリフォルダ、またはコンピュータの検索

[検索] ボタンを使用して、製品ディレクトリ内にある特定の管理下の製品を検索できます。

フォルダまたは管理下の製品を検索するには

1. 製品ディレクトリにアクセスします。
2. [エンティティの検索] に管理下の製品のエンティティ表示名を入力します。
3. [検索] をクリックします。

詳細検索を実行するには

1. 製品ディレクトリにアクセスします。
2. [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。

3. 製品のフィルタ条件を指定します。Control Manager では、検索用に最大 20 個の条件を指定できます。

4. [検索] をクリックして検索を開始します。検索結果が、製品ディレクトリの検索結果フォルダに表示されます。

製品ディレクトリの表示の更新

製品ディレクトリの表示を更新するには

- 製品ディレクトリで、左側のメニューの右上隅にある [表示の更新] アイコンをクリックします。

[ディレクトリ管理] 画面について

管理下の製品を Control Manager に登録すると、その製品が製品ディレクトリの初期設定フォルダの下に表示されます。

[ディレクトリ管理] 画面を使用して、管理モデルのニーズに合うように、製品ディレクトリ構成をカスタマイズします。たとえば、製品の場所で分類したり、メッセージングセキュリティ対策製品、Web セキュリティ対策製品、ファイルサーバ対策製品などの種類別に分類したりできます。

ディレクトリ管理を使用すると、フォルダを作成、変更、削除したり、フォルダ間で管理下の製品を移動したりできます。ただし、新規エンティティフォルダの削除と名前変更はできません。

各フォルダに属する管理下の製品を慎重に構成します。フォルダと管理下の製品の構造を計画して実装する際には、次の点を考慮してください。

- 製品ディレクトリ
- ユーザアカウント
- 配信計画
- アドホッククエリ
- Control Manager レポート

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 7-14. 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

表 7-14. 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
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

[ディレクトリ管理] 画面のオプションの使用

ディレクトリ管理には、次のオプションが用意されています。

- 製品ディレクトリにディレクトリを追加するオプション
- 製品ディレクトリ内にあるディレクトリの名前を変更するオプション
- 製品ディレクトリ内の管理下の製品やディレクトリを移動するオプション

注意： 権限の維持を指定するチェックボックスをオンにすると、フォルダを移動しても移動元の権限を維持できます。

- 製品ディレクトリから管理下の製品やディレクトリを削除するオプション

これらのオプションを使用して、Control Manager システム内の管理下の製品を処理して構成します。

[ディレクトリ管理] 画面を使用して変更を適用するには

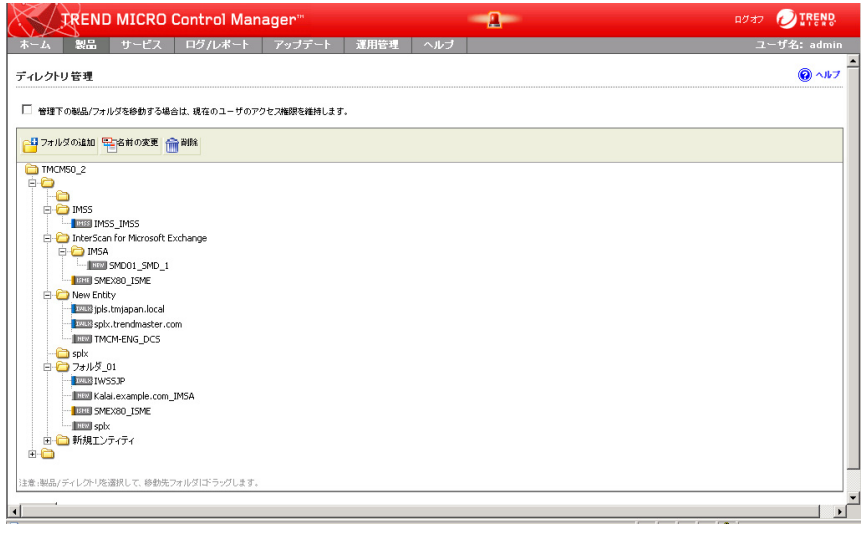
- 管理下の製品 / ディレクトリを選択してから [名前の変更] をクリックして、管理下の製品 / ディレクトリの名前を変更します。
- フォルダに属する管理下の製品を表示するには、[+] またはそのフォルダをクリックします。
- 管理下の製品 / ディレクトリを、製品ディレクトリ内の移動先にドラッグアンドドロップします。
- [フォルダの追加] をクリックして、製品ディレクトリにディレクトリを追加します。

[ディレクトリ管理] へのアクセス

[ディレクトリ管理] を使用すると、管理下の製品をグループ化できます。

[ディレクトリ管理] にアクセスするには

1. 上部のメニューで [製品] を選択します。[製品ディレクトリ] 画面が表示されます。
2. 製品ディレクトリメニューで [ディレクトリ管理] 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。



フォルダの作成

Control Manager システムの管理モデルに応じて、管理下の製品を異なるフォルダにグループ分けします。

フォルダを作成するには

1. [ディレクトリ管理] 画面にアクセスします。
2. [ローカルフォルダ] を選択します。[ローカルフォルダ] が強調表示されます。
3. [フォルダの追加] をクリックします。[ディレクトリの追加] ダイアログボックスが表示されます。
4. [ディレクトリ名] に新しいディレクトリの名前を入力します。
5. [保存] をクリックします。

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 (!、#、$、%、(、)、*、+、-、カンマ (,) 、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。

フォルダまたは管理下の製品の名前変更

ディレクトリおよび管理下の製品の名前をディレクトリ管理から変更します。

フォルダまたは管理下の製品の名前を変更するには

1. [ディレクトリ管理] 画面にアクセスします。
2. 名前を変更する管理下の製品 / ディレクトリを選択します。その項目が製品ディレクトリで強調表示されます。
3. [名前の変更] を選択します。[ディレクトリ名の変更] ダイアログボックスが表示されます。
4. [ディレクトリ名] に管理下の製品 / ディレクトリの名前を入力します。

5. [保存] 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。
6. [OK] をクリックします。管理下の製品 / ディレクトリの新しい名前が製品ディレクトリに表示されます。

注意： 管理下の製品の名前を変更すると、Control Manager データベース内に保存されている名前だけが変更されます。管理下の製品自体に影響はありません。

フォルダまたは管理下の製品の移動

フォルダを移動する際、[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。] チェックボックスの設定に注意してください。このチェックボックスをオンにして管理下の製品 / フォルダを移動すると、その管理下の製品 / フォルダでは、移動元のフォルダの権限が維持されます。このチェックボックスをオフにして管理下の製品 / フォルダを移動すると、その管理下の製品 / フォルダでは、新しい上位フォルダのアクセス権限が付与されます。

フォルダまたは管理下の製品を別の場所に移動するには

1. [ディレクトリ管理] 画面にアクセスします。
2. 右側の画面で、移動するフォルダまたは管理下の製品を選択します。
3. フォルダまたは管理下の製品を、移動先にドラッグアンドドロップします。
4. [保存] をクリックします。

ユーザ定義フォルダの削除

ディレクトリ管理内のユーザ定義フォルダを削除するときは注意が必要です。管理下の製品を誤って削除し、Control Manager サーバからその製品を登録解除してしまう可能性があります。

ユーザ定義フォルダを削除するには

ディレクトリ管理内のユーザ定義フォルダを削除するときは注意が必要です。管理下の製品を誤って削除し、Control Manager サーバからその製品を登録解除してしまう可能性があります。

注意： 新規エンティティフォルダを削除することはできません。

ユーザ定義フォルダを削除するには

1. [ディレクトリ管理] 画面にアクセスします。
2. 削除する管理下の製品 / ディレクトリを選択します。項目が強調表示されます。
3. [削除] 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。
4. [OK] をクリックします。
5. [保存] をクリックします。

警告： ユーザ定義フォルダを削除するときは注意が必要です。削除対象ではない管理下の製品を誤って削除してしまう可能性があります。

管理下の製品のアクティベーションと登録

Control Manager 5.0、管理下の製品 (ウイルスバスター コーポレートエディション、InterScan for Microsoft Exchange)、およびその他のサービス (大規模感染予防サービス、ダメージクリーンナップサービス、脆弱性診断サービス) の全機能を利用するには、ソフトウェアやサービスのアクティベーションコードを取得して、アクティベーションを実行する必要があります。

管理下の製品のアクティベーションを実行すると、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。

アクティベーションコードの特性

- 有効期限があります。
- 製品バージョンに依存しません。

注意： 旧バージョンの Control Manager では、シリアル番号が製品に添付されていました。ソフトウェアの全機能を使用するには、ユーザはオンラインで登録する必要がありました。

管理下の製品のアクティベーション

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を含む全機能を使用できるようにします。

管理下の製品を登録するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [ライセンス管理] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューで [管理下の製品] をクリックします。[ライセンス管理] 画面が表示されます。

4. [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。

5. アクティベーション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] に入力します。

6. [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。

7. 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。
8. [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、製品ディレクトリまたは [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。

管理下の製品のライセンスを [ライセンス管理] 画面で更新するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [ライセンス管理] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューで [管理下の製品] をクリックします。[ライセンス管理] 画面が表示されます。
4. リストからアクティベーションコードを選択します。

5. [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。

6. [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。

製品ディレクトリから管理下の製品のライセンスを更新するには

1. 製品ディレクトリにアクセスします。
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. 製品ディレクトリメニューで [タスク] をクリックします。ドロップダウンメニューが表示されます。
4. タスクのリストから [ライセンスプロファイルの配信] を選択します。
5. [サポート対象製品] リストから製品を選択し、[次へ >>] ボタンをクリックすると、[ライセンスプロファイル] 画面が開きます。

6. [ライセンスプロファイル] 画面で [配信開始] リンクをクリックして、アップデートされたライセンス情報をトレンドマイクロのライセンスサーバからロードします。Control Manager はライセンスプロファイルを自動的に配信します。

7. [コマンド詳細] リンクをクリックすると、[コマンド詳細] 画面が開きます。この画面では、Control Manager がライセンスプロファイルを配信した日時、前回のレポート送信時間、配信を認証したユーザ、配信に関する詳細 (処理中、成功、失敗) を確認できます。また、サーバによる配信のリストも表示できます。

Control Manager のアクティベーション

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。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、Control Manager 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を含む全機能を使用できるようにします。

ヒント： Control Manager のアクティベーション実行後、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。

Control Manager の登録およびアクティベーションを行うには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。

2. [ライセンス管理] の上にカーソルを置きます。サブメニューが表示されます。

3. [Control Manager] をクリックします。[ライセンス情報] 画面が表示されます。

4. 作業領域の [Control Manager ライセンス情報] で、[製品のアクティベーション] リンクをクリックします。

5. [新しいアクティベーションコード] ボックスに、アクティベーションコードを入力します。

6. [アクティベート] をクリックします。

7. [OK] をクリックします。

Control Manager または管理下のサービスのサポート契約の更新

Control Manager と、それに統合されている関連製品およびサービス (大規模感染予防サービス、脆弱性診断サービス、ダメージクリーンナップサービス) のサポート契約の更新は、次のいずれかの方法で行います。

お使いの製品またはサービスのサポート契約を更新するには、新しいアクティベーションコードが必要です。アクティベーションコードについては、トレンドマイクロの営業部または販売代理店にお問い合わせください。

[ステータスの確認] を使用してサポート契約を更新するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [ライセンス管理] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューで [Control Manager] をクリックします。[ライセンス情報] 画面が表示されます。
4. 作業領域で、更新する製品またはサービスの [ステータスの確認] をクリックします。
5. [OK] をクリックします。

注意： 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。

更新済みのアクティベーションコードを手動で入力してサポート契約を更新するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [ライセンス管理] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューで [Control Manager] をクリックします。[ライセンス情報] 画面が表示されます。
4. 右側の画面で、更新する製品またはサービスの [新しいアクティベーションコードを入力してください] をクリックします。
5. [新しいアクティベーションコード] ボックスに、アクティベーションコードを入力します。
6. [アクティベート] をクリックします。
7. [OK] をクリックします。

注意： 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。

下位サーバの管理

Control Manager アドバンス版には階層管理構造が用意されています。これによって、下位サーバと呼ばれる複数の Control Manager サーバを 1 台の上位サーバから制御できます。

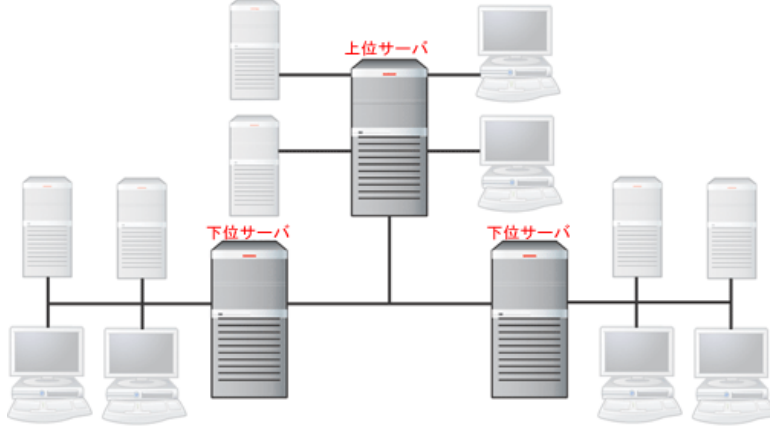


図 7-2. 階層管理構造では上位－下位の 2 層アーキテクチャを採用

上位サーバは、下位サーバと呼ばれる Control Manager スタンダード版またはアドバンス版サーバを管理する Control Manager サーバです。下位サーバは、上位サーバの管理下にある Control Manager サーバです。

上位サーバは実際に管理する管理下の製品の他に、下位サーバが直接扱う多数の管理下の製品を間接的に管理します。

次の表は、上位サーバと下位サーバの相違点をまとめています。

表 7-15. 上位サーバと下位サーバの機能の比較

機能	上位サーバで提供	下位サーバで提供
階層構造のサポート	可	不可
下位サーバの管理	可	不可
管理下の製品の管理	可	可
複数の下位サーバの操作	可	適用外
広域タスクの発行	可	不可
広域レポートの作成	可	不可

注意： 上位サーバを別の上位サーバに登録することはできません。また、1 つのサーバが同時に上位サーバと下位サーバになることはできません。

Control Manager 管理コンソールを使用する階層管理構造では、システム管理者は 1 台の上位サーバに属するすべての下位サーバに対して次の処理を管理、監視、および実行できます。

- ウイルス対策、コンテンツセキュリティ対策、および Web セキュリティ対策の概要の監視
- イベントログやセキュリティログの検索
- タスクの開始
- レポートの表示
- 下位サーバの管理コンソールへのアクセス

階層構造を使用すると、企業のウイルス対策およびコンテンツセキュリティ対策製品を広範囲にわたって効果的に管理することが可能です。

ヒント： 1 台の Control Manager 上位サーバで管理する下位サーバは 200 台以下、管理下の製品は 9,600 個以下にとどめることをお勧めします。

上位サーバと下位サーバの通信について

製品ディレクトリには、Control Manager システムにある上位サーバとすべての下位サーバが列挙されます。

次の表に、Control Manager 階層構造ツリーにおける接続ステータスを示します。

表 7-16. 上位サーバと下位サーバの関係

処理	上位 下位	上位 下位	上位 下位	上位 下位	スタンドアロンサーバ
登録解除の直接送信	●				
登録					●
Control Manager のアンインストール (データベースを保持)	●	●	●	●	●
Control Manager のアンインストール (データベースを削除)	●	●	●	●	●

この表に基づいて、次の点を考慮してください。

- 無効な下位サーバの登録解除を直接送信することはできません。
- 有効な下位サーバの登録解除の直接送信または強制では、上位サーバデータベースにある対象下位サーバのレコードは保持されますが、下位サーバデータベースにある対象下位サーバのレコードは削除されます。

- 無効な下位サーバにある Control Manager アプリケーションをアンインストールして、Control Manager のデータベースを保存し、Control Manager を再インストールした後、再インストールした Control Manager を同じ上位サーバに再登録した場合、下位サーバのステータスは無効なまま、変わりません。
- 無効な下位サーバにある Control Manager アプリケーションをアンインストールして、Control Manager のデータベースを削除し、Control Manager を再インストールした後、再インストールした Control Manager を同じ上位サーバに再登録すると、下位サーバのステータスは有効になります。

さらに、階層構造関係が有効に設定されている場合に、上位および下位サーバの重要な関係は、次のとおりです。

- 上位サーバ
  - [ステータス概要] 画面をリアルタイムにアップデートするよう、下位サーバをポーリングします。
  - 下位サーバの接続ステータスを 3 分おきにアップデートします。
- 下位サーバ
  - 上位サーバにログを送信します。
  - 新しいまたはアップデートされたレポートプロファイルを送信します。

下位サーバを無効にすることによって、2 つの Control Manager サーバ間の接続が完全に切断されるということはありません。上位サーバと下位サーバとの接続はまだ存在します。上位サーバは、下位サーバに対して単一のコマンド (有効化コマンド) を発行します。下位サーバがこのコマンドを受信して受け入れると、上位サーバはこの下位サーバの管理を再開します。

下位サーバの登録または登録解除

下位サーバの登録または登録解除を行った結果は、下位サーバの有効化または無効化を行った場合と同じ結果にはなりません。登録または登録解除を行うと、上位サーバと下位サーバ間の接続は永久に切断されますが、有効化または無効化を行うと、接続は一時的に停止されるだけで、両サーバ間の接続ステータスは維持されます。

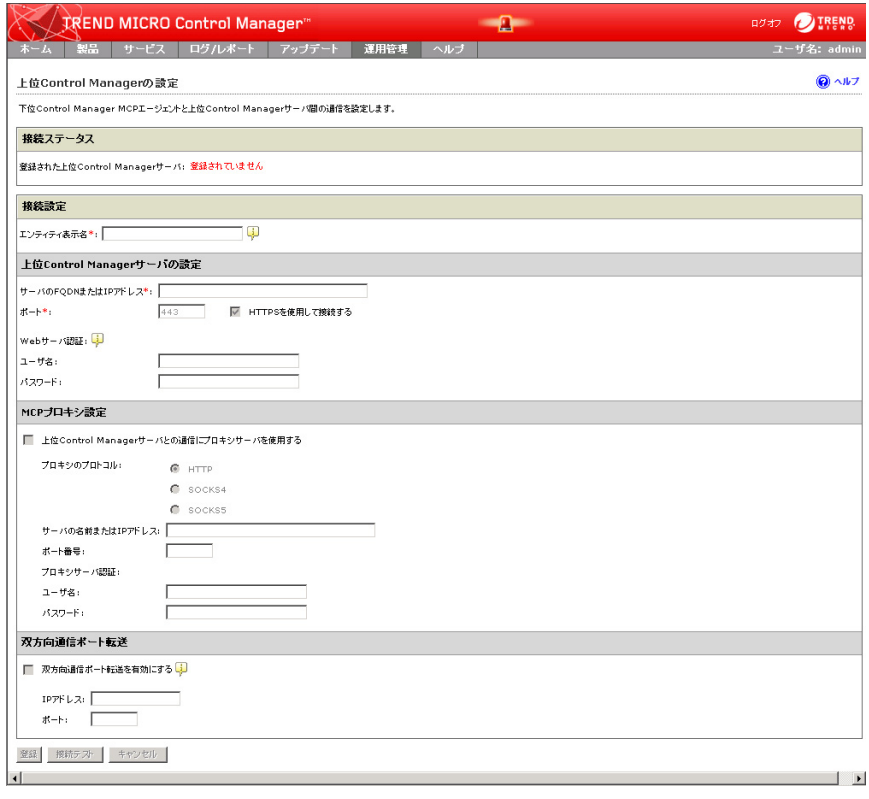
たとえば、下位サーバ「xyz」が上位サーバ「a」に登録されていた場合に、「xyz」を「a」から登録解除して、別の上位サーバ「b」に再登録したとします。これにより、「xyz」は上位サーバ「b」によって管理されるようになります。「a」の階層構造ツリーでは、リストから「xyz」が削除されます。

[上位 Control Manager の設定] 画面を使用して、Control Manager 5.0 上位サーバから登録や登録解除を実行できます。

Control Manager 下位サーバを Control Manager 上位サーバに登録するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。

3. サブメニューで [上位 Control Manager の設定] をクリックします。[上位 Control Manager の設定] 画面が表示されます。



4. 接続を設定します。

   - [エンティティ表示名] に、上位の Control Manager に表示される下位サーバ名を入力します。初期設定では、エンティティ表示名はサーバコンピュータの DNS 名になります。

5. Control Manager サーバを設定します。

   a. [サーバの FQDN または IP アドレス] に、上位の Control Manager サーバの FQDN または IP アドレスを入力します。

b. [ポート] に、上位の Control Manager が MCP エージェントとの通信に使用するポート番号を入力します。

ヒント： さらにセキュリティを向上させるには、[HTTPS を使用して接続する] を選択します。

c. Control Manager の IIS Web 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。

6. MCP プロキシを設定します。

a. Control Manager サーバへの接続にプロキシサーバを使用する場合、[上位 Control Manager サーバとの通信にプロキシサーバを使用する] を選択します。

b. プロキシで使用するプロトコルを選択します。

- HTTP
- Socks 4
- Socks 5

c. [サーバの名前または IP アドレス] にプロキシサーバの FQDN または IP アドレスを入力します。

d. [ポート番号] にプロキシサーバのポート番号を入力します。

e. プロキシサーバでユーザ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. [双方向通信ポート転送] を設定します。

a. MCP エージェントでポート転送を使用する場合は、[双方向通信ポート転送を有効にする] を選択します。

b. [IP アドレス] に転送 IP アドレスを入力します。

c. [ポート] にポート番号を入力します。

8. 下位サーバが上位の Control Manager サーバに接続できていることを確認するには、[接続テスト] をクリックします。

9. [登録] をクリックして上位の Control Manager サーバに接続します。

ヒント： 登録後にこの画面の設定を変更する場合は、[アップデート設定] をクリックして Control Manager サーバに変更を通知します。Control Manager サーバでそのサーバを管理しない場合は、[登録解除] をクリックします。

Control Manager 管理コンソールでステータスを確認するには

1. 上部のメニューで [製品] を選択します。[製品ディレクトリ概要] 画面が表示されます。
2. 新規に登録した Control Manager 下位サーバについて、[階層フォルダ] を確認します。

下位サーバの登録解除

下位サーバの登録または登録解除を行った結果は、下位サーバの有効化または無効化を行った場合と同じ結果にはなりません。登録または登録解除を行うと、上位サーバと下位サーバ間の接続は永久に切断されますが、有効化または無効化を行うと、接続は一時的に停止されるだけで、両サーバ間の接続ステータスは維持されます。

上位サーバである「a」と「b」との間で負荷を分散させるには、一般的に次の場合に負荷分散を実行します。

- 上位サーバ「a」が、上位サーバ「b」より多数の下位サーバを管理している場合。
- 上位サーバ「a」が過負荷となったため、この負荷を軽減し、一部の下位サーバを上位サーバ「b」に転送する必要がある場合

[上位 Control Manager サーバの設定] 画面を使用して、下位サーバを上位サーバから登録解除します。

注意： Control Manger 3.0/3.5 サーバでは、Control Manager 5.0 サーバから登録解除するには castool.exe が必要です。

下位の Control Manager サーバを登録解除するには

1. 下位サーバから、上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューで [上位 Control Manager サーバの設定] をクリックします。[上位 Control Manager サーバの設定] 画面が表示されます。
4. 画面の下部にある [登録解除] をクリックします。

階層フォルダへのアクセス

下位サーバの機能を表示したり、これらの機能にアクセスするには、製品ディレクトリを使用します。

注意： 上位サーバの管理コンソール経由でのみ製品ディレクトリにアクセスできます。

階層フォルダにアクセスするには

1. 上部のメニューで [製品] を選択します。[製品ディレクトリ] 画面が表示されます。

製品ディレクトリのステータス概要の表示

[製品ディレクトリ] 画面には、すべての管理下の製品について、ウイルス対策概要、スパイウェア / グレーウェア概要、コンテンツセキュリティ概要、Web セキュリティ概要、およびネットワークウイルス概要が表示されます。初期設定では、1 週間分の概要が表示されます。この範囲を変更するには、[レポート期間] で [今日]、[過去 7 日間]、[過去 14 日間]、[過去 30 日間] のいずれかを選択します。

製品ディレクトリのステータス概要を表示するには

1. [製品ディレクトリ] 画面にアクセスします。
2. 下位サーバを選択します。

   すべての下位サーバは、上位サーバにステータス概要を送信します。この間隔は、SystemConfiguration.xml ファイルで設定した時間間隔に基づきます。初期設定の時間間隔は 3 分で、開始時刻は「午前 12:00」です。管理ニーズに合わせて、これらの値を設定します。すべての下位サーバは、上位サーバにステータス概要を送信します。この間隔は、SystemConfiguration.xml ファイルで設定した時間間隔に基づきます。

注意： 下位サーバは、レコード件数が 2,500 件に達するかまたは 3 分経過すると、ステータス概要を上位サーバにアップロードします。下位サーバが新しいログを上位サーバにアップロードしていない間は、下位サーバの [製品ステータス] 画面の[コンポーネントのステータス] 表に表示される、[期限切れ]、[最新]、および [合計] の管理下の製品情報は最新ではない場合があります。

ログのアップロードの設定

下位サーバの [設定] タブを使用して、下位サーバが上位サーバにログを送信するスケジュールを設定します。

ログのアップロードを設定するには

1. 製品ディレクトリにアクセスします。
2. 製品ディレクトリで下位サーバを選択します。項目が強調表示されます。
3. 製品ディレクトリメニューで [設定] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
4. [下位サーバログの予約アップロード] リンクをクリックします。
5. [ログのアップロード] で、[下位サーバのログを上位サーバにアップロードする] チェックボックスをオンにします。

6. アップロードのスケジュールを設定します。

   - ログをただちに上位サーバに送信するように指示するには、[ただちにアップロード] を選択します。

注意： [ただちにアップロード] を選択すると、下位サーバにログを継続的に上位サーバに送信するように求めるため、ネットワークトラフィックの増加の原因となります。

   - 特定のスケジュールでログをアップロードするには、[自動アップロード] を選択します。

   a. [間隔] を [毎日] または [毎週] に設定します。

   b. リストから時間および分を選択して、[開始時刻] を設定します。初期設定では、開始時刻は 20:00 に設定されています。

7. [アップロード時間の上限を設定する] の [時間] を選択し、下位サーバが上位サーバにログをアップロードする時間の長さを決定する最大アップロード時間を設定します。初期設定の最大アップロード時間は 8 時間です。

8. [保存] をクリックします。

ヒント： 業務時間中のネットワークトラフィックの増加を抑制するため、ログのアップロードのスケジュールでは [間隔] に [毎日]、[開始時刻] には業務時間外を設定することをお勧めします。ただし、下位サーバが新しいログを上位サーバにアップロードしていない間は、下位サーバの [製品ステータス] 画面の [コンポーネントのステータス] 表に表示される管理下の製品に関する [期限切れ]、[最新]、および [合計] の情報は最新ではない場合があります。

下位サーバ接続の有効化または無効化

[設定] メニュー項目を使用して、下位サーバから上位サーバへの接続を有効または無効にします。

下位サーバ接続を有効または無効にするには

1. 製品ディレクトリにアクセスします。
2. 製品ディレクトリで下位サーバを選択します。項目が強調表示されます。
3. 製品ディレクトリメニューで [設定] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
4. [下位サーバ接続の有効化 / 無効化] リンクをクリックします。
5. [下位サーバ接続の有効化 / 無効化] で、次のいずれかの操作を実行します。
   - 無効にされた下位サーバ接続を有効にするには、[この下位サーバへの接続を有効にする] チェックボックスをオンにします。
   - 有効にされた下位サーバ接続を無効にするには、[この下位サーバへの接続を無効にする] チェックボックスをオンにします。

警告： 下位サーバへの接続を無効にする場合は注意が必要です。接続が無効にされた下位サーバの管理下の製品情報は、後で再度接続を有効にしても、自動的に上位サーバにアップロードされません。管理下の製品の情報を新たにアップロードするには、Control Manager のサービスを再起動してください。

6. [適用] をクリックします。

注意： 無効にされた下位サーバが上位サーバにログを送信することはありません。ただし、無効にされた下位サーバはローカルサーバ (つまり、無効にされた下位サーバ自体) 上でログをキューに入れることはあります。

下位サーバへのタスクの実行

[タスク] メニュー項目を使用すると、特定の下位サーバまたはすべての下位サーバに対して次の処理を実行できます。

- パターンファイル / テンプレートの配信
- エンジンの配信
- プログラムファイル配信
- 下位サーバの管理コンソールの起動

タスクを実行するには

1. 製品ディレクトリにアクセスします。
2. 製品ディレクトリで下位サーバを選択します。項目が強調表示されます。
3. 次のいずれかを実行します。

   下位サーバへのタスクの実行

   a. 製品ディレクトリメニューで [タスク] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
   b. 有効ないずれかの処理をクリックします。
   c. [コマンド追跡] を使用して、進行状況を確認してください。応答画面で [コマンド詳細] リンクをクリックすると、コマンド情報が表示されます。

   下位サーバの管理コンソールへのアクセス

   a. 製品ディレクトリメニューで [設定] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
   b. [下位 Control Manager シングルサインオン] をクリックします。下位サーバの管理コンソールが新しい画面に表示されます。
   c. 下位サーバにログオンして必要なタスクを実行します。

下位サーバレポートの表示

下位サーバの既存のレポートプロファイル (Control Manager 3 レポートテンプレート用) を表示するには、[タスク]→[レポート] メニュー項目を使用します。

Control Manager 5 レポートテンプレートを使用して生成されたレポートを表示するには、シングルサインオンを使用して下位 Control Manager 管理コンソールにログオンします。

下位サーバレポートを表示するには

1. 製品ディレクトリにアクセスします。
2. 製品ディレクトリで下位サーバを選択します。項目が強調表示されます。
3. 製品ディレクトリメニューで [タスク] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
4. ドロップダウンメニューから [レポート] を選択します。右側の画面に [レポート] 画面が表示されます。

注意 : [レポート] 画面に複数のレポートが表示されている場合、[レポートプロファイル] または [前回の作成日時] の日付に従って、レポートを並べ替えます。

5. [レポート] で、表示するレポートプロファイルの [表示] リンクをクリックします。
6. [レポート : { プロファイル名 }] 画面で、[作成要求日時] または [生成完了日時] に従って、レポートを並べ替えます。
7. [下位サーバのレポート表示] 列で、[下位サーバのレポート表示] をクリックします。新たにブラウザ画面が開き、レポートの内容が表示されます。

製品ディレクトリの表示の更新

製品ディレクトリの表示を更新するには

製品ディレクトリで、製品ディレクトリの概要画面の右上隅にある [表示の更新] アイコンをクリックします。

下位サーバの名前の変更

下位サーバのエンティティ表示名を変更するには、[名前の変更] オプションを使用します。

下位サーバの名前を変更するには

1. [ディレクトリ管理] 画面にアクセスします。
2. 名前を変更する下位サーバを選択します。その項目が製品ディレクトリで強調表示されます。
3. [名前の変更] をクリックします。[ディレクトリ名の変更] ダイアログボックスが表示されます。
4. [ディレクトリ名] に下位サーバの名前を入力します。
5. [保存] 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。
6. [OK] をクリックします。下位サーバの新しい名前が製品ディレクトリに表示されます。

階層管理から誤って削除された下位サーバの再登録

下位サーバを誤って登録解除してしまった場合、その下位サーバをいったん登録解除してから再度上位サーバに登録する必要があります。

ディレクトリ管理から誤って削除された Control Manager 3.0/3.5 下位サーバを再登録するには

1. 下位サーバの Windows 2000 コマンドプロンプトで、次の強制登録解除コマンドを実行します。

   castool /e

2. 上位サーバに再度下位サーバを登録します。

Control Manager 上位サーバへの Control Manager 下位サーバの登録

[上位 Control Manager サーバの設定] 画面を使用して、Control Manager 上位サーバから登録や登録解除を実行できます。

Control Manager 下位サーバを Control Manager 上位サーバに登録するには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. サブメニューで [上位 Control Manager サーバの設定] をクリックします。[上位 Control Manager サーバの設定] 画面が表示されます。
4. [エンティティ表示名] に、上位の Control Manager に表示される下位サーバ名を入力します。初期設定では、エンティティ表示名はサーバコンピュータの DNS 名になります。
5. Control Manager サーバを設定します。

a. [サーバの FQDN または IP アドレス] に、上位の Control Manager サーバの FQDN または IP アドレスを入力します。

b. [ポート] に、上位の Control Manager が MCP エージェントとの通信に使用するポート番号を入力します。

ヒント： さらにセキュリティを向上させるには、[HTTPS を使用して接続する] を選択します。

c. Control Manager の IIS Web 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。

6. MCP プロキシを設定します。

a. Control Manager サーバへの接続にプロキシサーバを使用する場合、[上位 Control Manager サーバとの通信にプロキシサーバを使用する] を選択し、次の設定を実行します。

b. プロキシで使用するプロトコルを選択します。

- HTTP
- Socks 4
- Socks 5

c. [サーバの名前または IP アドレス] にプロキシサーバの FQDN または IP アドレスを入力します。

d. [ポート番号] にプロキシサーバのポート番号を入力します。

e. プロキシサーバでユーザ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. [双方向通信ポート転送] を設定します。

a. MCP エージェントでポート転送を使用する場合は、[双方向通信ポート転送を有効にする] を選択し、次の設定を実行します。

b. [IP アドレス] に転送 IP アドレスを入力します。

c. [ポート] にポート番号を入力します。

8. 下位サーバが上位の Control Manager サーバに接続できていることを確認するには、[接続テスト] をクリックします。

9. [登録] をクリックして上位の Control Manager サーバに接続します。

ヒント： 登録後にこの画面の設定を変更する場合は、[アップデート設定] をクリックして Control Manager サーバに変更を通知します。Control Manager サーバでそのサーバを管理しない場合は、[登録解除] をクリックします。

Control Manager 管理コンソールでステータスを確認するには

1. 上部のメニューで [製品] を選択します。[製品ディレクトリ概要] 画面が表示されます。

2. 新規に登録した Control Manager 下位サーバについて、[階層フォルダ] を確認します。

Control Manager の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 のインストール時には、システム DSN ODBC 接続と、db_ControlManager.mdf へのアクセスに使用される ID およびパスワードが作成されます。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

管理下の製品である eManager は、データベースの拡張を検討する際の主要な要因となります。1 つの eManager ログの平均的なサイズは、約 3,000 バイトです。次に例を示します。

1 日 10 時間あたりのトラフィックが 100 メッセージであるような、メールトラフィックの量が少ない環境では、eManager が毎日 1,250 件のメッセージをブロックすると、1 日あたり 1,250 × 3,000、つまり 3,750,000 バイトがコンテンツセキュリティ違反ログに記録されます。

この場合、必要なデータベースの拡張は、1 日あたり 5MB、すなわち 1ヵ月あたり 150MB になります。

Control Manager によって管理されるその他のすべてのトレンドマイクロ製品では、データベースのサイズは各システムで 1 日あたり数キロバイト程度、増加します。

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。

db_ControlManager テーブルについて

Control Manager のデータベースのテーブルにアクセスするには、Microsoft Access プロジェクト (*.adp /*.ade) を使用します。

注意： レコードの追加、削除、または変更に SQL ツールを使用する場合は、必ずテクニカルサポートの指示に従ってください。

Control Manager のデータベースは、次のテーブルで構成されています。

表 7-17. ディレクトリ管理のテーブル

ディレクトリ管理のテーブル	説明
CDSM_Entity	管理下の製品に関する情報が保存されます。
CDSM_Agent	コミュニケータに関する情報が保存されます。
CDSM_Registry	レジストリに関する情報が保存されます。
CDSM_UserLog	管理コンソールにアクセスしたユーザ、使用されたオプション、および何時にアクセスしたかという情報が保存されます。この情報は、管理コンソールへのアクセスの監査に役立ちます。
CDSM_SystemEventlog	内部処理で生成されたシステムログが保存されます。

表 7-18. サーバコマンドコントローラのテーブル

サーバコマンドコントローラのテーブル	説明
tb_TVCSCommandList	TVCS エージェントのコマンドが保存されます。
tb_TVCSCommandTaskQueue	TVCS エージェントに対して発行されたコマンドが保存されます。
tb_CommandTracking	コマンドのステータスが保存されます。
tb_CommandItemTracking	詳細なコマンド追跡の情報が保存されます。
tb_ProcessInfo	MsgReceiver.exe、CmdProcessor.exe、LogReceiver.exe、LogRetriever.exe、および UIProcessor.exe に関する情報が保存されます。
tb_LoginUserSessionData	ユーザのログオンセッション情報が保存されます。
tb_ManualDownload	手動ダウンロードに関する情報が保存されます。
tb_ScheduleDownload	予約ダウンロードに関する情報が保存されます。

表 7-19. 管理下の製品のテーブル

管理下の製品のテーブル	説明
tb_EntityInfo	管理下の製品に関する情報が保存されます。
tb_VirtualEntity	TVCS1.8x エージェント登録に関する情報が保存されます。

表 7-20. ログのテーブル

ログのテーブル	説明
tb_TempLog	製品ログのデータが一時的に保存されます。
tb_AV*Log	各製品のログが保存されます。 * は、Virus、Event、Status、PEInfo、WebSecurity に相当します。
tb_InValidLog	不正なログの情報が保存されます。
・tb_TotalWebSecurityCount ・tb_TotalVirusCount ・tb_TotalSecurityCount ・tb_TopTenSource ・tb_TopTenDestination ・tb_TopTenVirus	ステータス概要およびレポートに使用するウイルスの概要情報が保存されます。
tb_LogPurgePolicy	ログの削除の設定が保存されます。
tb_LogPurgeCounter	ログの削除のカウントが保存されます。
・tb_InstanceForVirusOutbreak ・tb_InstanceForSpecialVirus ・tb_InstanceForVirusOutbreak	アラート通知で使用するログインスタンスが保存されます。

表 7-21. 通知のテーブル

通知のテーブル	説明
・tb_Alert_NTF_JobList ・tb_Event_NTF_JobList	通知のキューリストが保存されます。
tb_EventNotificationFilter	イベントセンターの設定が保存されます。
・tb_SendEMailNotification ・tb_SendPagerNotification ・tb_SendSNMPTrapNotification ・tb_SendWindowsNTEventLogNotification	通知方法の設定が保存されます。
tb_VirusOutBreakPolicy	ウイルスの大規模感染時に使用されるルールが保存されます。

表 7-21. 通知のテーブル

通知のテーブル	説明
tb_SpecialVirusPolicy	ユーザが「特定ウイルス用アラート」に指定したウイルス名が保存されます。
• tb_VirusOutbreakAccumulate • tb_SpecialVirusAccumulate	「ウイルスアウトブレークアラート」および「特定ウイルス用アラート」のウイルスカウンタに関する情報が保存されます。
• tb_UGNtfRelation • tb_NtfUserGROUP • tb_GroupAndUserRelation	ユーザおよびグループの通知設定が保存されます。

表 7-22. レポートのテーブル

レポートのテーブル	説明
• tb_ReportScheduleTask • tb_ReportTaskQueue	レポート作成タスクが保存および処理されます。
tb_ReportItemTracking	レポートのテンプレートファイルカタログが保存されます。

表 7-23. パターンおよびエンジン配信のテーブル

パターンおよびエンジン配信のテーブル	説明
• tb_DeploymentPlans • tb_DeploymentPlansTF	配信計画に関する情報が保存されます。
tb_DeploymentPlanTasks	配信タスクのキューが保存されます。
tb_DeployNowJobList	進行中の配信計画のステータスが保存されます。
tb_DeployCommandTracking	配信コマンドの追跡情報が保存されます。
tb_DeploymentPlanTargets	配信コマンドを適用した管理下の製品に関する情報が保存されます。

osql による db_ControlManager のバックアップ

Control Manager データベースが破損または機能しない場合、バックアップコピーを使用して設定を復元します。MSDE を使用している場合、MSDE コマンドラインインタフェースの osql を使用してデータベースのバックアップを生成します。

osql を使用してデータベースのバックアップを生成するには

1. Control Manager サーバで、Windows の [スタート]→[ファイル名を指定して実行] の順に選択します。
2. 「cmd」と入力し、[OK] をクリックします。
3. Windows 2000 のコマンドプロンプトで、次のコマンドを実行します。

```
osql -U {ID} -P { パスワード } -n -Q "BACKUP DATABASE {Control Manager データベース } TO DISK = '{ パスおよびバックアップ名 }'"
```

ここでは次を意味します。

{ID} — Control Manager データベースへのアクセスに使用される管理者のユーザ名アカウントです。これは Control Manager セットアップ時に定義されます。

{ パスワード } — Control Manager データベースへのアクセスに使用されるパスワードです。これは Control Manager セットアップ時に定義されます。

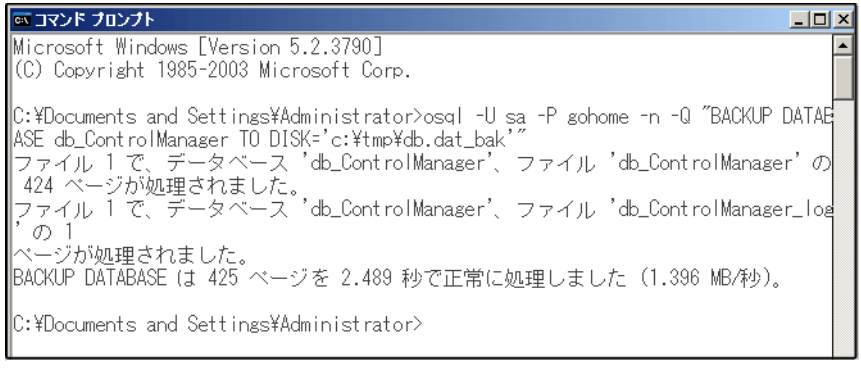
{Control Manager データベース } — Control Manager データベースの名前です。

{ パスおよびバックアップ名 } — バックアップを生成する場所とバックアップファイル名です。

次に例を示します。

```
osql -U sa -P -n -Q "BACKUP DATABASE db_ControlManager TO
DISK = 'f:¥db.dat_bak'"
```

データベースのバックアップに成功すると、次のような結果が生成されます。



バックアップファイル db.dat_bak がすでに存在する場合、コマンド osql は新しい情報をバックアップするために、新しいレコードを既存のファイルに挿入します。

ヒント： 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するなど、Control Manager データベースを変更する際は、必ずバックアップを作成してください。

osql によるバックアップ db_ControlManager の復元

ご使用の MSDE のバージョンに付属するコマンドラインインタフェース「C:¥Program Files¥Trend Micro¥MSDE¥osql」を使用して、バックアップしたデータベースを復元します。

バックアップしたデータベースを復元するには

1. Control Manager を停止します。
2. [スタート] メニューから [プログラム]→[管理ツール]→[サービス] の順に選択して、[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. [スタート] メニューから [ファイル名を指定して実行] をクリックします。
5. 「cmd」と入力し、[OK] をクリックします。
6. Windows 2000 のコマンドプロンプトで、次のコマンドを実行します。

```
osql -U {ID} -P { パスワード } -n -Q "RESTORE DATABASE
{Control Manager データベース } FROM DISK = '{ パスおよびバックアップ名 }'"
```

次に例を示します。

```
osql -U sa -P -n -Q "RESTORE DATABASE db_ControlManager
FROM DISK = 'f:¥db.dat_bak'"
```

データベースの復元に成功すると、次のような結果が生成されます。

7. [スタート] メニューから [プログラム]→[管理ツール]→[サービス] の順に選択して、[サービス] 画面を開きます。

8. 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。
9. Control Manager を起動します。

   osql の使用方法の詳細については、「MSDN ライブラリ」を参照してください。

SQL Server Enterprise Manager 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 Enterprise Manager を使用して Control Manager データベースをバックアップします。

SQL Server Enterprise Manager を使用して db_ControlManager をバックアップするには

1. Control Manager のデータベース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]→[プログラム]→[Microsoft SQL Server]→[Enterprise Manager] の順にクリックし、SQL Server Enterprise Manager にアクセスします。
2. コンソールで、[Microsoft SQL Servers]→[SQL Server グループ]→[{SQLServer} (Windows NT)]→[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。
3. db_controlmanager を右クリックし、[すべてのタスク]→[データベースのバックアップ…] をクリックします。
4. [SQL Server バックアップ - db_ControlManager] で、データベースの名前と説明を指定します。
5. [バックアップ] で、[データベース - 全体] を選択します。
6. [出力先] で、[追加] をクリックしてバックアップファイルの作成先を指定します。
7. [バックアップ先の選択] で、データベースのバックアップファイル名と保存場所のパスを入力し、[OK] をクリックします。
8. [SQL Server バックアップ - db_ControlManager] で、[OK] をクリックして、db_ControlManager のバックアップを開始します。

9. 完了メッセージが表示されたら、[OK] をクリックします。

ヒント： 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するなど、Control Manager データベースを変更する際は、必ずバックアップを作成してください。

SQL Server Enterprise Manager による db_ControlManager の復元

SQL Server Enterprise Manager 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。

バックアップした db_ControlManager を復元するには

1. Control Manager を停止します。
2. [スタート] メニューから [プログラム]→[管理ツール]→[サービス] の順に選択して、[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. [スタート] メニューから [プログラム]→[Microsoft SQL Server]→[Enterprise Manager] の順にクリックして、SQL Server Enterprise Manager にアクセスします。
5. コンソールで、[Microsoft SQL Servers]→[SQL Server グループ]→[{SQLServer} (Windows NT)]→[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] 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] メニューから [プログラム]→[管理ツール]→[サービス] の順に選択して、[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 を起動します。

SQL Server Enterprise Manager によるデータベースファイルの縮小

Control Manager データベースのトランザクションのログファイルは、「…¥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。

db_controlmanager_log.ldf ファイルのサイズを縮小するには

1. SQL Server Enterprise Manager 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、[スタート] メニューから [プログラム]→[MS SQL Server] の順にクリックして、クエリアナライザを起動します。
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. リストから db_ControlManager データベースを選択します。
6. 次の SQL スクリプトをコピーして貼り付けます。

```
DBCC shrinkDatabase(db_controlManager)
BACKUP LOG db_controlmanager WITH TRUNCATE_ONLY DBCC
SHRINKFILE(db_controlmanager_Log, 10)
```

注意： SHRINKFILE(db_controlmanager_Log, 10) 関数のパラメータ「10」は結果として得られる db_controlmanager_log.ldf ファイルのサイズをメガバイト (MB) 単位で表したものです。

7. [実行] をクリックして、SQL スクリプトを実行します。
8. 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。

SQL コマンドによるデータベースファイルの縮小

MSDE を使用している場合、または SQL コマンドを使用できる環境にある場合は、次の SQL コマンドを実行して、db_ControlManager.mdf および db_ControlManager_log.ldf ファイルがディスク容量を過剰に占有してしまうことを防止できます。

db_ControlManager.mdf および db_ControlManager_log.ldf ファイルのサイズを縮小するには、SQL クエリツールを使用して、次の SQL コマンドを実行します。

```
Alter Database db_controlManager set recovery FULL
Backup log db_controlManager with truncate_only
DBCC shrinkDatabase(db_controlManager)
```

注意： 3 番目のコマンドは、データベースのサイズによっては処理に時間がかかる場合があります。

```
EXEC sp_dboption 'db_ControlManager', 'trunc. log on chkpt.', 'TRUE'
Alter Database db_controlManager set recovery simple
Alter Database db_controlManager set auto_shrink on
```

第 8 章

トレンドマイクロのサービスの使用

本章では、Trend Micro Control Manager (以下、Control Manager) の使用時に利用できるさまざまなサービスについて説明します。

本章は次の内容で構成されています。

トレンドマイクロのサービスについて

トレンドマイクロでは、ウイルスからの攻撃の脅威とそれにかかるコストの大幅な削減には、ウイルス対策の管理に新しいアプローチが必要であると考えました。多くの調査とテストを重ねた結果、トレンドマイクロはウイルス対策の定義を革新しました。ウイルスから攻撃を受けた場合に随時対応するのではなく、予防措置を積極的に講じる集中管理型ウイルス対策システムを導入することにより、インターネットゲートウェイから、クライアントコンピュータ、ファイルサーバ、およびメールサーバに至るまで、あらゆるシステムへの攻撃に対して迅速で組織的な対応が可能になりました。

新しいアプローチには、次の機能が含まれます。

- **トレンドラボからのメッセージ** — 最新のコンポーネント情報を迅速に提供し、新しいウイルスを特定してただちに駆除できるようにウイルスの特徴を通知するリアルタイムのメッセージです。
- **大規模感染予防サービス** — 大規模感染を回避し、感染を食い止めるための大規模感染予防ポリシーを提供するトレンドマイクロ固有のサービスです。
- **ダメージクリーンナップサービス** — トロイの木馬またはワームに感染したシステムにおけるウイルスの一掃とシステムの修復を助ける包括的なサービスです。
- **脆弱性診断サービス** — システム管理者または他のネットワークセキュリティ担当者が、ネットワークのセキュリティ面でのリスクを診断できます。

ウイルス対策に対するトレンドマイクロの統合されたアプローチは、ウイルスのサンプルが管理者からトレンドラボに送信されたときに始まります。トレンドラボでは、パターンファイルが公開される前に提供される推奨設定ファイルである大規模感染予防ポリシーが作成されます。ウイルス発生の初期情報が Control Manager で取得されると、他のシステム管理者はポートをシャットダウンして業務の生産性を危険にさらすことのないように、大規模感染予防サービスを使用して攻撃の範囲をただちに確認し、攻撃に対して暫定的な処置を施すことができます。また、システム管理者は、同じ攻撃を受ける可能性のある企業内の他のシステム管理者に、推奨される大規模感染予防ポリシーを配信できます。

このような、ネットワーク全体にウイルス対策の情報を組み込み、ウイルスに関連するイベントが生じるたびにそれらのイベントをリアルタイムで確認するという、先手を打った対応は、集中管理によってのみ実現することができます。ウイルスを迅速に特定するサービスと送信システムによって、ウイルスを封じ込めるために必要な時間が短縮されるため、ウイルスの拡散を制限することができます。このような処理によって、ウイルスが企業の生産性に及ぼす影響を最小限に抑え、ウイルス駆除に要するコストを大幅に削減できます。

トレンドマイクロ エンタープライズ プロテクション ストラテジーについて

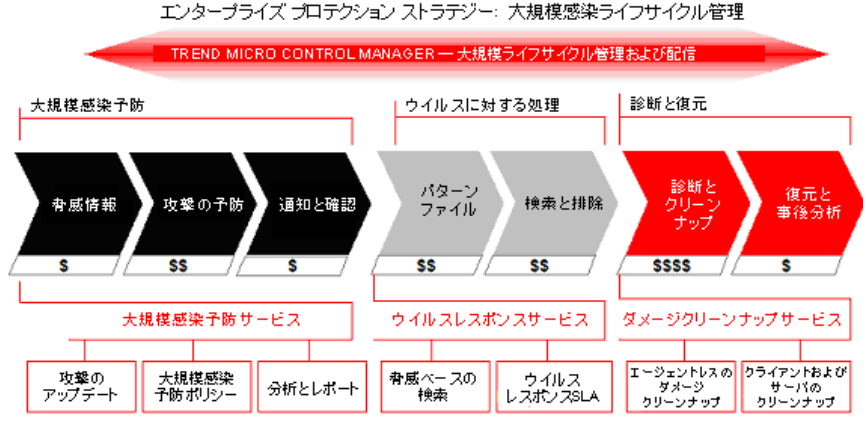


図 8-1.　エンタープライズ プロテクション ストラテジー

トレンドマイクロ エンタープライズ プロテクション ストラテジー (以下、Trend Micro EPS) では、トレンドマイクロ独自のサービスとサポートを提供し、さまざまな脅威に対して信頼性の高い対策を講じてシステムを保護します。

- 先制的な対策により、ウイルスの侵入を封じ込め、システムに残存するウイルスを一掃します。

- 業界で唯一のウイルスレスポンスサービスレベルアグリーメント (SLA) によって、ウイルス検出が保証されます。
- トレンドマイクロのウイルス対策の知識と技術が集約された Trend Micro EPS のアーキテクチャにより、ネットワーク上の攻撃されやすい箇所を保護します。

Trend Micro EPS によって「集中管理センター」が確立され、企業のネットワーク全体にわたってウイルスを識別し、除去します。

- 企業全体にわたるポリシーの実施とレポートの作成
- 異機種のプラットフォームのサポート

Trend Micro EPS では、ウイルスからの攻撃時に対処方法が考えられ、被害が最小限に抑えられるように考慮されます。

- ウイルスアウトブレークライフサイクル — 業界固有の、実際のウイルス対策の経験に基づいた手法を採用しています。
- 企業全体の監視によってネットワーク上の攻撃されやすい箇所が識別され、大規模感染に対して早期に対処することができます。
- パターンファイルの公開前後の重要な段階に焦点を合わせることによって、必要になるコストとシステムの被害を最小限に抑えます。

Trend Micro EPS の主要な価値

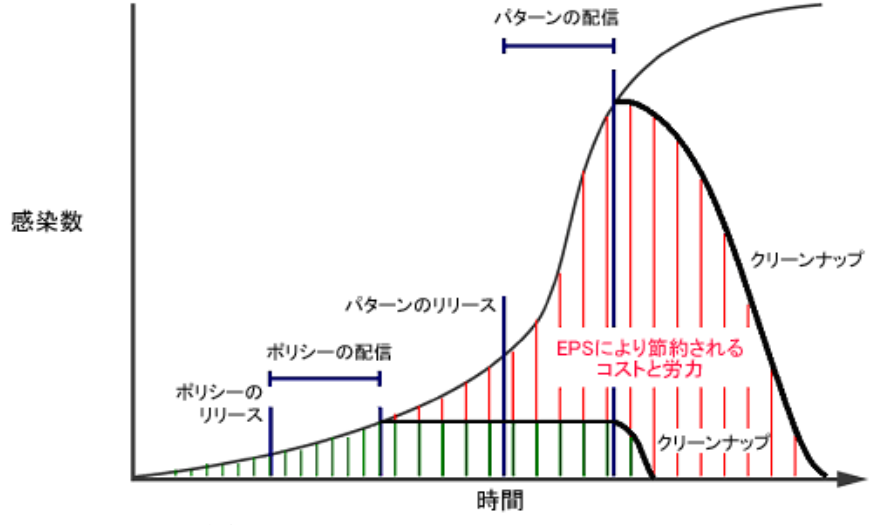


図 8-2.　コストと労力

グラフに示されているとおり、大規模感染の壊滅的な影響は、攻撃後に脆弱性をネットワークから排除することに加えて、できる限り早く対策を実施することにより、最小限に抑えることが可能です。

Trend Micro EPS と大規模感染予防サービスを使用することにより、企業はリスクを軽減し、ウイルス対策に要するコストを大幅に削減できます。ライフサイクルの早い時期およびパターンファイルの公開前にポリシーを配信することで、ウイルス対策の全体的なレベルを向上させるだけでなく、対応のためのコストおよび労力を劇的に削減することができます (図の斜線の領域)。

つまり、トレンドマイクロの専門技術、アーキテクチャ、およびサービスは、企業のネットワークにおける投資利益、全体的な保護、および生産性の向上に役立ちます。

トレンドラボからのメッセージの概要

Control Manager およびトレンドマイクロのウイルス対策製品を使用すると、システムに影響が及ぶ前に、ウイルスの大規模感染についてトレンドラボから警告を受けることができます。

[トレンドラボからのメッセージ] フィールドには、トレンドラボからリリースされる、パターンファイル、検索エンジン、クリーンナップテンプレート、大規模感染予防ポリシーなどのコンポーネントのバージョン番号とリリース時刻が表示されます。これに基づいて、管理下のシステムを早期にアップデートできます。

ウイルストラッキングセンターへのウイルス情報送信

トレンドマイクロでは、世界各国で実施されたウイルス検索の結果を収集し、統計情報をリアルタイムで提供しています。この情報は、トレンドマイクロ ウイルストラッキングセンター (WTC) で参照することができます。ウイルストラッキングセンターでは、世界で最も流行しているウイルスの上位 10 種類を表示したり、選択した地域別の情報を表示することができます。

Control Manager では、管理下の製品で検出されたウイルスの情報をウイルストラッキングセンターに送信できます。ウイルストラッキングセンターに送信されるのは、Control Manager システムで検出されたウイルスの名前と件数のみです。その他の情報 (コンピュータ名、サイト名、IP アドレスなど) は一切送信されません。これらの情報は、HTTPS のポート 443 を介して送信されます。ウイルス情報の送信はインストール時に設定しますが、インストール後も管理コンソールを使用していつでも設定を変更することができます。

ウイルストラッキングセンターへのウイルス情報の送信を設定するには

1. 上部のメニューで [運用管理] をクリックします。
2. サブメニューで [ウイルストラッキングセンター] をクリックします。
3. 作業領域で、ウイルス情報を送信する場合は [情報を送信する]、ウイルス情報を送信しない場合は [情報を送信しない] をクリックします。
4. [保存] をクリックします。

大規模感染予防サービスの概要

図 8-3. 大規模感染予防サービス

大規模感染予防サービスについて

大規模感染予防サービスは、管理下の製品でウイルスの大規模感染が識別され、パターンファイルがまだ公開されていない重要な局面で使用されます。このような局面では、システム管理者は複雑で時間のかかる連絡業務を遂行しなければなりません。また、このような業務は、組織内の、世界中に分散されているグループ間で発生する場合が多くあります。

大規模感染予防サービスから、新しい脅威に関する通知が送信されます。また、攻撃が進行するにつれて、システムステータスに関する包括的なアップデート情報が連続して送信されます。新しい脅威が識別されると、ウイルスの詳細なデータと共に、事前定義された脅威に対するポリシーがタイムリーに配布されます。これにより、企業はウイルスを食いとめ、感染の拡大を防ぐことができます。

また、大規模感染予防サービスでは、中央で推奨ポリシーが配信および管理されるため、通信不良の可能性をなくし、ポリシーを適用し、攻撃が起こったときに重要な攻撃情報を配信します。

大規模感染予防サービスでは、トレンドマイクロの Control Manager を経由して自動または手動でポリシーをダウンロードおよび配信できるため、トレンドマイクロの世界的なセキュリティリサーチおよびサポートネットワークであるトレンドラボの専門家から、ネットワーク上の重要なアクセスポイントに情報が直接インポートされます。

この契約ベースのサービスには、最小限の先行投資が必要です。またこのサービスでは、インターネットゲートウェイ、メールサーバ、ファイルサーバ、キャッシュサーバ、クライアント、リモートユーザ、ブロードバンドユーザなどのネットワーク上の重要な箇所に常駐するトレンドマイクロのウイルス対策製品を使用した企業全体の調整と大規模感染時の管理が提供されます。

大規模感染予防サービスの利点

大規模感染予防サービスを使用すると、大規模感染時の対応時間を短縮するだけでなく、実際のウイルス対策およびコスト面において大きな利益を得ることができます。

表 8-1. 大規模感染予防サービスの利点

利点	理由
複合ウイルスの攻撃に対する積極的な措置	• 業務の生産性を損なう (ポートをシャットダウンする) ことなく大規模感染を阻止 • ウイルスとその動作の定義に伴う混乱の軽減 • ポリシーの予約ダウンロードによる、途切れることのない、自動化可能なウイルス対策
専門技術と知識	• 新種ウイルスに対する予防ポリシー (推奨設定) の提供 • 既知のウイルスに対するポリシーの提供
一貫性の維持、調整作業の軽減、コスト削減	• 一貫したポリシーの適用 • 関係者への通知の効率化
ポリシーと攻撃の相互関係	• ネットワーク全体にわたる監視と管理

大規模感染予防サービスのアクティベーション

大規模感染予防サービスのアクティベーションを実行すると、管理者は、ウイルスの大規模感染時にネットワークを保護できるようになります。

大規模感染予防サービスのアクティベーションを実行するには

1. 上部のメニューで [運用管理] をクリックします。
2. サブメニューで [ライセンス管理]→[Control Manager] を選択します。
3. 右側の画面の [大規模感染予防サービスライセンス情報] で、[製品のアクティベーション] リンクをクリックします。
4. 次の作業を実行してください。
   - アクティベーションを実行するには、[製品のアクティベーション] リンクをクリックします。
   - [新しいアクティベーションコード] フィールドにアクティベーションコードを入力します。
5. [アクティベート] をクリックします。

大規模感染予防サービスのステータスの表示

大規模感染予防サービスのステータスを参照すると、次のサービスステータスの項目の状態を容易に把握できます。

表 8-2. 大規模感染予防サービスのステータス

項目	説明	設定
ポリシーの予約ダウンロード	指定したスケジュールに従って、大規模感染予防ポリシーを自動的にダウンロードするかどうかについての情報を示します。	オンまたはオフ
大規模感染予防モードの自動開始 (レッドアラート)	レッドアラート対象ウイルスに対して、自動的に大規模感染予防モードを有効にするかどうかについての情報を示します。	オンまたはオフ

表 8-2.　大規模感染予防サービスのステータス

項目	説明	設定
大規模感染予防モードの自動開始 (イエローアラート)	イエローアラート対象ウイルスに対して、自動的に大規模感染予防モードを有効にするかどうかについての情報を示します。	オンまたはオフ

また、現在使用中の Control Manager のコンポーネントとバージョンもこのページで簡単に参照できます。

大規模感染予防サービスのステータスを表示するには

1. 上部のメニューで [サービス] をクリックします。
2. サブメニューで [サービス]→[大規模感染予防] を選択します。このページは自動的に更新され、最新の脅威およびステータス情報が表示されます。

ウイルス大規模感染の予防と大規模感染予防モード

パターンファイルの公開前に、トレンドマイクロの大規模感染予防サービスから、ウイルスの各攻撃に関する情報と大規模感染予防ポリシーをダウンロードします。大規模感染予防サービスを使用すると、推奨されるポリシーが Control Manager に配信され、調整時間を最小限に抑えて、ネットワーク全体でポリシーを一貫して適用することができます。大規模感染予防サービスから送信される推奨ポリシーを使用すると、システム管理者は新しいウイルスへの対応時間を短縮して、大規模感染を封じ込め、システムへの被害を最小限に抑えて、停止時間が長くならないようにすることができます。

配信計画を使用すると、大規模感染予防の設定の適用をネットワーク上の特定の拠点に制限することができます。ただし、ユーザはネットワークの拠点を異なる配信計画に分割する必要があります。これは、複数の拠点で構成される大規模なネットワークの場合に便利です。管理者は、設定の適用を実際に大規模感染の影響を受けた範囲のみに制限することができます。

大規模感染予防モードでは、次の処理が実行されます。

- 大規模感染予防ポリシーをダウンロードします。大規模感染予防ポリシーは、ウイルスの大規模感染の発生時に推奨される、ウイルス対策製品の設定リストです。
- ウイルス対策製品の設定内容が表示されます。この内容を参照しながら、必要に応じて設定を変更することができます。

  推奨設定は、設定する必要がある管理下の製品に対してのみ表示されます。
- ネットワークへの有害なコードの侵入または拡散をブロックします。
- 感染の状況に応じて通知をカスタマイズするための設定機能を提供します。
- ポリシーの配信とステータスに関するレポートがリアルタイムに送信されます。
- ポリシーの配信を手動または自動で実行できる機能が提供されます。
- ポリシーの適用期間中にのみ有効な、特別に定義された予約アップデートと予約ダウンロードを設定できる機能が提供されます。

  この機能を利用して、新しいパターンファイルの公開後、ただちにそのパターンファイルを自動的にアップデートすることができます。
- ウイルスの特徴の識別後、ただちにその詳細情報が提供されます。

大規模感染予防ポリシーについて

大規模感染予防ポリシーは、大規模感染予防サービスによって管理下の製品に適用できるウイルス対策製品の設定ファイルです。これらの設定ファイルはウイルスの大規模感染に対応してトレンドマイクロで作成され、大規模感染予防サービスの一環として Control Manager に提供されます。

これらのポリシーは、ウイルスの大規模感染時のネットワーク保護の鍵となります。ポリシーは、インターネットゲートウェイ、メールサーバ、ファイルサーバ、キャッシュサーバ、クライアント、リモートユーザ、ブロードバンドユーザなど、ネットワーク上の重要な箇所を保護します。たとえば、メールを通じて広がるウイルスに対しては、メッセージングセキュリティ製品に対する設定を含むポリシーが提供されます。

次の図に、Control Manager からすべての層にポリシーを配信し、ウイルスの大規模感染時に重要な箇所を保護する様子を示します。

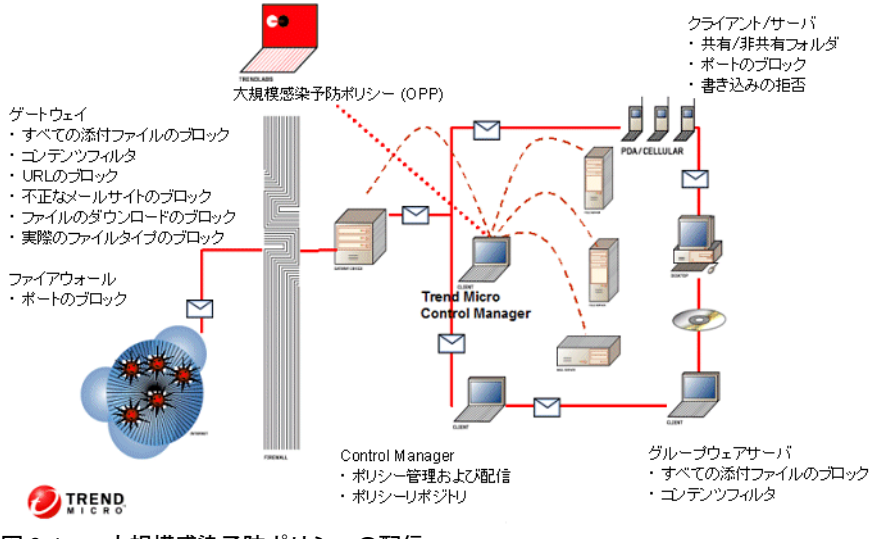


図 8-4.　大規模感染予防ポリシーの配信

大規模感染予防サービスの設定画面へのアクセス

[大規模感染予防サービスの設定] 画面にアクセスするには

1. 上部のメニューで [サービス] をクリックします。
2. サブメニューで [サービス]→[大規模感染予防]→[設定] を選択します。

大規模感染予防ポリシーのアップデート

ウイルスの大規模感染時にネットワークを保護するには、最新版の大規模感染予防ポリシーを使用することが重要です。大規模感染予防ポリシーは、手動または予約アップデートの設定を使用してアップデートします。

大規模感染予防ポリシーを手動でアップデートするには

1. 上部のメニューで [サービス] をクリックします。
2. サブメニューで [サービス]→[大規模感染予防] を選択します。このページは自動的に更新され、最新の脅威およびステータス情報が表示されます。
3. [サービスのステータス] 画面で [アップデート] をクリックし、最新の大規模感染予防ポリシーをダウンロードします。
4. 大規模感染予防ポリシーのダウンロードが完了したら、[OK] を 2 回クリックします。

余計なメンテナンスタスクをなくすため、最新の大規模感染予防ポリシーを自動的にチェックおよびダウンロードするように Control Manager のスケジュールを設定してください。

ヒント： Control Manager のインストールが完了したら、アップデートを実行してすぐにポリシーを更新することを強くお勧めします。アップデートを実行した後は、予約アップデート機能を使用して定期的に自動更新してください。

大規模感染予防ポリシーのアップデートのスケジュールを設定するには

1. 上部のメニューで [サービス] をクリックします。
2. サブメニューで [サービス]→[大規模感染予防]→[設定] を選択します。
3. 右側の画面で [ポリシーのダウンロード] タブをクリックします。
4. [ポリシーの予約ダウンロード] 設定で、[ポリシーの予約アップデートを有効にする] チェックボックスをオンにします。
5. [ダウンロード間隔] リストボックスで、更新された大規模感染予防ポリシーをチェックする間隔 (分単位) を選択します。
6. [ダウンロード元] で、最新の大規模感染予防ポリシーを提供するダウンロード元をクリックします。初期設定では、トレンドマイクロのアップデートサーバに設定されています。別のアップデートサーバを選択する場合は、そのサーバの場所を [その他のアップデートサーバ] に入力します。
7. [保存] をクリックします。
8. [OK] をクリックします。

大規模感染予防モードの開始

ウイルスの大規模感染の発生時に大規模感染予防モードを開始して、ウイルスの各攻撃に応じて大規模感染予防ポリシーを配信し、ネットワークが感染する可能性を最小限に抑えます。大規模感染予防モードは、1 つの特定のウイルス攻撃に対して開始します。

大規模感染予防モードを開始するには

1. 上部のメニューで [サービス] をクリックします。

2. サブメニューで [サービス]→[大規模感染予防] を選択します。このページは自動的に更新され、最新の脅威およびステータス情報が表示されます。

3. [サービスのステータス] 画面で [アップデート] をクリックし、最新の大規模感染予防ポリシーをダウンロードします。予約アップデートをすでに有効化し、最新の大規模感染予防ポリシーを使用している場合は、この作業を省略できます。

4. 大規模感染予防ポリシーのダウンロードが完了したら、[OK] を 2 回クリックします。

5. 現在、ネットワークに対する脅威となっているウイルスのラジオボタンを [大規模感染予防ポリシー一覧] でクリックします。Control Manager の初期設定では、最新の脅威が先頭に、そして残りの脅威がその下にアルファベット順に一覧表示されます。個々の大規模感染予防ポリシーは、それぞれ特定のウイルスを予防するように設計されています。

6. [大規模感染予防モードの開始] をクリックします。

7. [大規模感染予防ポリシー] の [有効期間] リストボックスで、Control Manager で大規模感染予防モードを継続する日数を選択します。

8. [配信計画] リストで、大規模感染予防ポリシーを管理下の製品に配信するための計画を選択します。

9. [大規模感染予防ポリシーの詳細] で、[大規模感染予防の設定で除外されているポート番号をブロックしない (N/A)] チェックボックスをオンにして、例外として定義したポートがブロックされないようにします。
10. 管理下の製品を設定するか、[< 推奨する設定] をクリックします。
11. [アクティベート] をクリックします。
12. [OK] をクリックします。大規模感染予防モードが開始され、  アイコンが管理コンソールの上部に表示されます。

大規模感染予防ポリシーの編集

大規模感染予防モードの開始後、必要に応じて大規模感染予防ポリシーを編集できます。次に例を示します。

- 大規模感染予防モードの期間の変更
- 別の配信計画の選択
- 指定したポート番号の除外
- 登録された管理下の製品の設定

大規模感染予防ポリシーを編集するには

1. 上部のメニューで [サービス] をクリックします。
2. サブメニューで [サービス]→[大規模感染予防] を選択します。このページは自動的に更新され、最新の脅威およびステータス情報が表示されます。
3. 右側の画面で [ポリシーの編集] ボタンをクリックします。
4. [大規模感染予防ポリシー] の [有効期間] リストボックスで、Control Manager で大規模感染予防モードを継続する日数を選択します。
5. [配信計画] リストで、大規模感染予防ポリシーを管理下の製品に配信する計画を選択します。配信計画を表示、編集、または追加するには、[アップデート] の上にカーソルを置き、[配信計画] をクリックします。

6. [大規模感染予防ポリシーの詳細] で、[大規模感染予防の設定で除外されているポート番号をブロックしない (N/A)] チェックボックスをオンにして、例外として定義したポートがブロックされないようにします。

7. 管理下の製品を設定するか、[< 推奨する設定] をクリックします。

ヒント： [< 推奨する設定] をクリックすると、トレンドラボの推奨する設定が適用され、ユーザ定義設定は削除されます。必要な場合、これらの推奨設定は、最新情報に基づいて大規模感染予防ポリシーがリリースされるたびにアップデートされます。推奨設定を適用することをお勧めします。

8. [アクティベート] をクリックします。

大規模感染予防モードの自動開始

大規模感染の発生は予測できません。自動大規模感染予防では、レッドまたはイエローアラートのウイルスに対する大規模感染予防ポリシーを自動的に管理下の製品に配信し、通知を送信することができます。

表 8-3. ウイルスアラートの条件

ウイルスアラート	説明
レッドアラートウイルスの条件	レッドアラートは、世界的に大規模感染が見込まれるウイルスが出現した場合に発令されます。具体的には、世界の複数の地域 (北米、アジア、西ヨーロッパなど) で 3 サイト以上の感染報告を受けたような場合がレッドアラートに相当します。 業界初の 45 分のレッドアラートソリューションプロセスが開始されます。オフィシャルパターンファイルが利用可能を知らせる通知とともに配信され、その他の関連通知が送信されます。さらに、修正ツールと脆弱性の関連情報がダウンロードページに表示されます。

表 8-3.　ウイルスアラートの条件

ウイルスアラート	説明
イエローアラートウイルスの条件	イエローアラートは、地域的に感染の流行が見込まれるウイルスが出現した場合に発令されます。具体的には、ある地域で 3 サイト以上の感染報告を受けたような場合がイエローアラートに相当します。オフィシャルパターンファイルは配信サーバへ自動的に転送され、ダウンロードできるようになります。メールを介して感染が広がる不正プログラムでは、大規模感染予防ポリシーと呼ばれるコンテンツフィルタルールが発令され、Control Manager の機能を備えたサーバで関連添付ファイルを自動的にブロックします。

大規模感染予防モードの自動開始を設定するには

1. 上部のメニューで [サービス] をクリックします。
2. [設定] をクリックします。
3. [大規模感染予防モード] タブをクリックします。
4. 次の作業を実行してください。
   - 大規模感染予防モードの自動開始 (レッドアラートウイルス) を設定するには、[レッドアラートウイルス] で [大規模感染予防モードを自動的に開始する] チェックボックスをオンにします。
   - 大規模感染予防モードの自動開始 (イエローアラートウイルス) を設定するには、[イエローアラートウイルス] で [大規模感染予防モードを自動的に開始する] チェックボックスをオンにします。
5. [ポリシーの有効期間] リストボックスから、大規模感染予防モードの有効期間の日数を選択します。
6. [配信計画] リストで、大規模感染予防ポリシーを管理下の製品に配信するための計画を選択します。

7. 次の作業を実行してください。

   - [除外する製品] から、大規模感染予防ポリシー配信の対象外とする管理下の製品を選択します。重要 : 除外された製品には大規模感染予防サービスが適用されないので、大規模感染発生中に感染する危険性が高くなります。
   - [除外するポート] で、大規模感染発生中にブロックしないポートを指定します。
   - ダメージクリーンナップサービスを自動的に開始するには、[ウイルス感染復旧] で [有効にする] チェックボックスをオンにします。[クリーンナップ] をクリックし、ダメージクリーンナップサービスを設定します。
   - 脆弱性診断サービスを自動的に開始するには、[脆弱性診断] で [有効にする] チェックボックスをオンにします。
   - [大規模感染予防ポリシーは、ポリシーの有効期間が切れると、自動的に停止します] チェックボックスをオンにすると、自動的に大規模感染予防ポリシーが停止します。

8. [保存] をクリックします。

大規模感染予防モードのダウンロード設定

大規模感染予防モード時に、更新された大規模感染予防ポリシーの有無を Control Manager でチェックする頻度を設定します。さらに、更新された大規模感染予防ポリシーの配信に使用する配信計画を選択することもできます。

大規模感染予防モードのダウンロードを設定するには

1. 上部のメニューで [サービス] をクリックします。
2. [設定] をクリックします。

3. 大規模感染予防モードのダウンロード設定で、次の作業を実行してください。
   - [ダウンロード間隔] リストボックスで、Control Manager で更新された大規模感染予防ポリシーをチェックする頻度を選択します。
   - [配信方法] リストボックスで、ダウンロードしたコンポーネントの配信に使用する配信計画を選択します。配信計画の詳細については、179 ページの「配信計画について」を参照してください。
   - パターンファイルのみを配信するには、[検索エンジンは配信しない] チェックボックスをオンにします。
4. [保存] をクリックします。

大規模感染予防モードの停止

ポリシーの有効期限が切れる前に、大規模感染予防モードを手動で停止します。

Control Manager が大規模感染予防モードの状態では、管理コンソールに  アイコンが表示されます。

大規模感染予防モードを停止するには

1. 上部のメニューで [サービス] をクリックします。
2. サブメニューで [サービス]→[大規模感染予防] を選択します。
3. [大規模感染予防モードの停止] をクリックします。
4. [OK] をクリックします。

大規模感染予防モードの履歴の参照

この大規模感染予防サービスの機能を使用すると、適用した大規模感染予防ポリシーを参照できます。[履歴] 画面には次の情報が表示されます。

表 8-4. [履歴] 画面の情報

見出し	説明
No.	タスクが実行された順序。数字が小さいほど新しいタスクになります。
ウイルス	大規模感染の原因となったウイルスまたは不正コードの名前。
発行元	大規模感染予防モードタスクを作成した Control Manager ユーザのユーザ ID。
大規模感染予防モードの実行期間	大規模感染予防モードが実行されていた期間が示されます。左側に開始時刻、右側に完了時刻または中止時刻が表示されます。
ステータス	タスクの結果。 タスクの結果やステータスを表示するには、該当する項目に対応する [表示] リンクをクリックします。
レポート	OPS 中に大規模感染予防ポリシーによって検出されたウイルスの数が表示されます。ウイルスが検出されなかった場合は、レポートにデータは表示されません。

大規模感染予防モードの履歴を参照するには

1. 上部のメニューで [サービス] をクリックします。
2. サブメニューで [サービス]→[大規模感染予防]→[履歴] を選択します。特定の大規模感染予防ポリシーのステータスを表示するには、同じ行の [表示] をクリックします。ステータス画面に、ウイルス対策製品によって検出されたウイルスの数が表示されます。

大規模感染予防モードの使用

大規模感染予防モードの概要

このチュートリアルでは、大規模感染予防モードの開始に必要な手順について説明します。このチュートリアルは、次のトピックで構成されます。

- ステップ 1: 発生源の特定
- ステップ 2: 既存のポリシーの評価
- ステップ 3: 大規模感染予防モードの開始
- ステップ 4: ステータスの監視

ステップ 1: 発生源の特定

トレンドマイクロでは、契約されたお客さまに対してウイルスの危険性をお知らせするサービスを提供しています。次のサービスを利用することにより、発生する可能性のある、または発生しつつあるウイルスや不正コードについての情報を取得することができます。

表 8-5. 発生源の特定

警告方法	説明
大規模感染予防ポリシーの予約ダウンロード	大規模感染するウイルスに対応する大規模感染予防ポリシーをダウンロードする場合、通知が送信されます。このイベントに関する通知を受け取るには、イベントセンターで、[アクティブ大規模感染予防ポリシー受信] を有効にします。 この通知を受信したら、すぐに大規模感染予防モードを開始してください。

表 8-5.　発生源の特定

警告方法	説明
トレンドラボからのメッセージ	トレンドマイクロのトレンドラボからのメッセージには、リリースされたウイルス対策 / コンテンツセキュリティコンポーネントのバージョン番号とリリース時刻が表示されます。これにより、不正コードを特定し、システムのアップデート情報を確認できます。
テクニカルアカウントマネージャ (TAM)	トレンドマイクロと特定の有償サポートを契約している場合、担当のテクニカルアカウントマネージャ (TAM) がアウトブレークアラートに関する警告情報をお知らせします。 大規模感染の警告を受け取ったとき、予約アップデートによる大規模感染予防ポリシーの更新が完了していない場合は、手動でポリシーを更新してシステムに適用してください。
トレンドマイクロウイルス警告メールサービス	このサービスは、トレンドマイクロの Web サイトで申し込むことができます。
特定ウイルス用アラート	[イベントセンター] で設定する Control Manager のこの機能によって、システムに侵入しようとする既知のウイルスの存在が警告されます。 この機能により、企業内のユーザに特定の種類のメールに注意を払うなどの警告を促し、事前に対応策を講じることができます。

ステップ 2: 既存のポリシーの評価

ウイルスの大規模感染の危険性を知らせる通知を受信したら、ただちに管理下のシステムがその脅威に対処できるかどうかを評価します。大規模感染予防サービスのステータス画面には、ご使用の Control Manager サーバにおける現在の大規模感染予防ポリシーが表示されます。この画面で、大規模感染するウイルスに対応するポリシーがあるかどうかを確認します。

ヒント： 最新のポリシーを維持するため、次の Control Manager の機能を有効にすることをお勧めします。

大規模感染予防サービスのアラートの詳細については、193 ページの「イベントセンターの使用」を参照してください。

ポリシーの予約ダウンロードの詳細については、375 ページの「大規模感染予防ポリシーのアップデート」を参照してください。

対応するポリシーが含まれているかどうかに応じて、次のいずれかの手順に進みます。

- 対応するポリシーが存在する場合
- 対応するポリシーが存在しない場合

対応するポリシーが存在する場合

Control Manager は、対象のウイルスの大規模感染に対応することができます。大規模感染予防モードを開始し、該当するウイルス用に作成されたポリシーをシステムに適用します。

対応するポリシーが存在しない場合

ウイルスに対応する大規模感染予防ポリシーが存在しない場合は、トレンドマイクロからポリシーを入手する必要があります。

期限切れの大規模感染予防ポリシーは、手動でアップデートすることをお勧めします。

ステップ 3: 大規模感染予防モードの開始

大規模感染予防モードを開始して、ウイルスに対応するポリシーを適用します。大規模感染予防モードを開始することにより、トレンドマイクロが推奨する製品設定を確認しながら、必要に応じて設定を変更することができます。ポリシーによって、既知のウイルス侵入ポイントをブロックする製品設定が適用されます。

トレンドラボが大規模感染予防ポリシーを配信する時点では、多くの場合、対応するパターンファイルが未検証です。トレントラボが新しいパターンファイルを公開する前でも、大規模感染予防ポリシー設定を適用することにより、システムを保護することができます。

大規模感染予防モードを開始する前に、イベントセンターで大規模感染通知の受信者および通知方法を設定してください。

[大規模感染予防モード] 画面では、次の項目を設定してください。

- **ポリシーの有効期間**

  [ポリシーの有効期間] リストで、ポリシーの適用期間を指定します。ポリシーの有効期間は、大規模感染予防モードを開始した時点から始まります。初期設定の有効期間は、2 日間です。

注意 : 適用中のポリシーを変更すると有効期間がリセットされ、変更した日から期間が開始されます。

- **ポリシーの配信方法**

  このステージに対する適切な配信計画を選択します。配信計画によって、製品ディレクトリのどのフォルダに対してポリシーの設定を配信するかを指定します。

注意 : 既存の配信計画で必要条件を満たさない場合は、新規に配信計画を作成します。179 ページの「配信計画について」を参照してください。

- **ブロックするウイルス侵入ポイント**

次の製品の推奨値があらかじめ設定されています。

- InterScan eManager
- InterScan WebProtect for ICAP
- InterScan Messaging Security Suite Windows 版
- InterScan Messaging Security Suite UNIX 版 /IMSA 版 /Solaris 版
- InterScan Web Security Suite Windows 版 /Solaris 版 /Linux 版 /Appliance 版
- InterScan Gateway Security Appliance
- InterScan VirusWall スタンダードエデシション Windows/Linux 版
- Network VirusWall
- Portalprotect
- InterScan for Microsoft Exchange
- InterScan for Lotus Notes/Domino
- IM Security for Microsoft Live Communications Server
- ServerProtect for Windows
- ServerProtect for Linux
- ウイルスバスター コーポレートエディション
- ファイアウォール管理 — NetScreen (サードパーティ製品)

特定の製品の設定がポリシーに含まれている場合は、画面上の該当する製品のチェックボックスが自動的にオンになります。

注意： 上記の製品が Control Manager システムに属していない場合、その製品の設定は無視されます。

製品設定を確認または変更するには

1. 製品のリンクか [+] アイコンをクリックして、設定を表示します。
2. すべての製品の設定を表示するには、[設定の表示] をクリックします。推奨設定は、現在の設定値の右側に閲覧専用のフィールドとして表示されます。
3. ニーズに合わせて、これらの値を変更します。

ステップ 4: ステータスの監視

大規模感染予防のチュートリアルが終了したら、大規模感染予防モードの履歴を使用してポリシーの進捗状況を監視します。

ヒント： ポリシーの適用期間が過ぎたら、大規模感染予防モードを手動で停止してください。大規模感染予防モードを停止しないと、予約アップデートにより新しいポリシーがダウンロードされた場合に、ポリシーの自動適用が機能しません。

第 9 章

ツールの使用

Trend Micro Control Manager (以下、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。

<root>:¥Control Manager¥WebUI¥download¥tools¥

本章は次の内容で構成されています。

エージェント移行ツール (AgentMigrateTool.exe) の使用

Control Manager 5.0 スタンダード版またはアドバンス版で提供されているエージェント移行ツールを使用して、Control Manager 3.5/5.0 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 (109 ページの「Control Manager 2.5x および MCP エージェントの移行」を参照)。

移行先のサーバの次の場所から直接、AgentMigrateTool.exe を実行します。

C:¥Program Files¥Trend Micro¥Control Manager¥

注意： MCP エージェントでは、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。

Control Manager 2.x エージェントでは、エージェント移行ツールで Windows ベースのエージェントのみを移行できます。Windows ベースではないエージェントの移行については、トレンドマイクロのサポートにお問い合わせください。

Control Manager の MIB ファイルの使用

Control Manager MIB ファイルをダウンロードして、SNMP プロトコルをサポートするアプリケーション (HP OpenView など) と共に使用します。

Control Manager の MIB ファイルを使用するには

1. Control Manager の管理コンソールにアクセスします。
2. 上部のメニューで [運用管理] を選択します。ドロップダウンメニューが表示されます。
3. [ツール] をクリックします。
4. 作業領域で [Control Manager の MIB ファイル] をクリックします。

5. [ファイルのダウンロード] 画面で [保存] を選択してサーバ上の場所を指定し、[OK] をクリックします。
6. サーバ上で、管理情報ベース (MIB) ファイルである、Control Manager MIB ファイルの cm2.mib を抽出します。
7. SNMP プロトコルをサポートするアプリケーション (HP OpenView など) を使用して cm2.mib をインポートします。

NVW 1.x SNMPv2 MIB ファイルの使用

NVW 1.x SNMPv2 MIB ファイルをダウンロードして、SNMP プロトコルをサポートするアプリケーション (HP OpenView など) と共に使用します。

NVW 1.x SNMPv2 MIB ファイルを使用するには

1. Control Manager の管理コンソールにアクセスします。
2. 上部のメニューで [運用管理] を選択します。ドロップダウンメニューが表示されます。
3. [ツール] をクリックします。
4. 作業領域で、[NVW 1.x SNMPv2 MIB ファイル] をクリックします。
5. [ファイルのダウンロード] 画面で [保存] を選択してサーバ上の場所を指定し、[OK] をクリックします。
6. サーバで、NVW 1.x SNMPv2 MIB ファイル nvw.mib2、管理情報ベース (MIB) ファイルを解凍します。
7. SNMP プロトコルをサポートするアプリケーション (HP OpenView など) を使用して nvw.mib2 をインポートします。

NVW Enforcer SNMPv2 MIB ファイルの使用

NVW Enforcer SNMPv2 MIB ファイルをダウンロードして、SNMP プロトコルをサポートするアプリケーション (HP OpenView など) と共に使用します。

NVW Enforcer SNMPv2 MIB ファイルを使用するには

1. Control Manager の管理コンソールにアクセスします。
2. 上部のメニューで [運用管理] を選択します。ドロップダウンメニューが表示されます。
3. [ツール] をクリックします。
4. 作業領域で、[NVW Enforcer SNMPv2 MIB ファイル] をクリックします。
5. [ファイルのダウンロード] 画面で [保存] を選択してサーバ上の場所を指定し、[OK] をクリックします。
6. サーバ上で、管理情報ベース (MIB) ファイルである、NVW Enforcer SNMPv2 MIB ファイルの nvw.mib2 を抽出します。
7. SNMP プロトコルをサポートするアプリケーション (HP OpenView など) を使用して nvw.mib2 をインポートします。

NVW システムログ表示ツールの使用法

NVW システムログ表示ツールを使用して、Network VirusWall 製品の Network VirusWall ログを開きます。

ログ表示ツールを使用するには

1. Control Manager の管理コンソールにアクセスします。
2. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
3. [ツール] をクリックします。
4. 右側の画面で、[NVW システムログ表示ツール] をクリックします。
5. ログ表示ツールを使用して、Network VirusWall デバイスからログをインポートします。

NVW 2.x 緊急用ツールの使用

Network VirusWall プログラムファイルを NVW 2.x 緊急用ツールを使用してアップロードすると、コマンドラインインタフェースを使用してプログラムファイルをアップロードした場合と同様に機能します。ただし、このツールは、グラフィカルユーザインタフェースの使用に慣れたユーザにとっては、ユーザフレンドリな Windows ベースのオプションです。

NVW 2.x 緊急用ツールにアクセスするには

1. Windows エクスプローラを使用して、Control Manager 3.5 のインストールフォルダを開きます。次に例を示します。

   C:¥Program Files¥Trend Micro¥Control Manager¥WebUI¥download¥tools

2. [NVW1.x_Rescue_Utility.exe] アプリケーションをダブルクリックします。

NVW Enforcer ユーティリティの使用

NVW Enforcer ユーティリティを使用して、デバイスの BMC ファームウェア、BIOS、およびプログラムファイルをアップデートします。このユーティリティはグラフィカルユーザインタフェースの使いやすいツールです。これを使用して、Network VirusWall Enforcer 2500 機器の最新のプログラムファイルやブートローダをアップロードできます。

NVW Enforcer ユーティリティにアクセスするには

1. Control Manager の管理コンソールにアクセスします。
2. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
3. [ツール] をクリックします。
4. 作業領域で、[NVW Enforcer ユーティリティ] をクリックします。
5. [ファイルのダウンロード] 画面で [保存] を選択してサーバ上の場所を指定し、[OK] をクリックします。
6. AFFU ファイルをサーバ上に解凍します。

DBConfig ツールの使用

DBConfig 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: データベースの認証モード (SQL または WA)

注意： 初期設定のモードは SQL 認証モードです。ただし、Windows 認証を設定する場合は、Windows 認証モードが必要になります。

Control Manager 3.5 では SQL 認証のみサポートしています。

DBConfig ツールを使用するには

1. Control Manager サーバで、Windows の [スタート]→[ファイル名を指定して実行] の順に選択します。
2. cmd」と入力し、[OK] をクリックします。コマンドプロンプトダイアログボックスが表示されます。
3. Control Manager のインストールディレクトリ (初期設定では、C:¥Program Files¥Trend Micro¥Control Manager¥DBConfig) に移動します。
4. 次のように入力します。

   dbconfig
   DBConfig ツールインタフェースが表示されます。
5. 変更する設定を指定します。

   例 1: DBConfig -DBName="db" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"
   例 2: DBConfig -DBName="db" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"

第 10 章

アンインストール

本章では、Trend Micro Control Manager (以下、Control Manager) サーバ、Control Manager エージェント、およびその他の関連ファイルを含む Control Manager コンポーネントをアンインストールする方法について説明します。

本章は次の内容で構成されています。

Control Manager サーバのアンインストール

Control Manager の自動アンインストールには、次の 2 つの方法があります (ここでの手順は Windows 2000 環境に適用され、使用している Microsoft Windows プラットフォームによっては詳細が多少異なる場合があります)。

- 方法 1: Control Manager のアンインストーラを使用
  Windows の [スタート] メニューから、[プログラム]→[Trend Micro Control Manager]→[Trend Micro Control Manager のアンインストール] の順に選択します。
- 方法 2: Windows の [プログラムの追加と削除] を使用

  a. Windows の [スタート] メニューから、[コントロールパネル]→[プログラムの追加と削除] の順に選択します。

  b. [Trend Micro Control Manager] を選択し、[削除] をクリックします。

     この操作によって、Trend Micro Management Infrastructure や Trend Micro Common CGI などの関連するサービスも自動的にアンインストールされます。

  c. データベースを保持する場合は [はい]、保持しない場合は [いいえ] をクリックします。

注意： データベースを保持しておくと、サーバに Control Manager を再インストールする際にエージェントの登録やユーザアカウントのデータなどのシステム情報を再使用することができます。

Control Manager サーバを再インストールするときに元のデータベースが削除されていた場合でも、次の条件を満たすとき、エージェントがサーバに再登録されます。

- エージェントのサービスを再起動したとき
- エージェントから Control Manager サーバへの定期通信時 (Control Manager エージェントの場合は 8 時間ごと、Trend Virus Control System (以下、TVCS) エージェントの場合は 12 時間ごと)

Control Manager の手動アンインストール

ここでは、Control Manager を手動でアンインストールする方法について説明します。ここで説明する手順は、Windows の「プログラムの追加と削除」、または Control Manager のアンインストールプログラムを使用して正常にアンインストールできなかった場合にのみ使用してください。

注意： Windows での手順は、使用している OS のバージョンによって異なる場合があります。ここでは Windows 2000 を使用していることを前提に説明しています。

Control Manager のアンインストールでは、次のコンポーネントを削除する必要があります。これらのコンポーネントは任意の順序でアンインストールできます。また、一括でアンインストールすることもできます。ただし、ここでは、説明の便宜上、節ごとに各モジュールのアンインストール手順を個別に説明します。各コンポーネントは以下のとおりです。

- Control Manager アプリケーション
- Trend Micro Management Infrastructure
- Trend Micro Common CGI モジュール
- データベースコンポーネント (任意)

Trend Micro Management Infrastructure と Trend Micro Common CGI モジュールは、他のトレンドマイクロの製品でも使用されています。したがって、同じコンピュータに他のトレンドマイクロ製品がインストールされている場合は、これらの 2 つのコンポーネントをアンインストールしないことを推奨します。

注意： すべてのコンポーネントをアンインストールしたら、サーバを再起動してください。各コンポーネントをアンインストールするたびに再起動する必要はありません。

Control Manager アプリケーションの削除

Control Manager アプリケーションを手動でアンインストールするには、次の手順に従ってください。

1. Control Manager サービスの停止
2. Control Manager の IIS 設定の削除
3. Crystal Reports ランタイムファイル、TMI、および CCGI のアンインストール
4. Control Manager のファイル / ディレクトリおよびレジストリキーの削除
5. データベースコンポーネントの削除
6. Control Manager サービスと NTP サービスのアンインストール

Control Manager サービスの停止

次の Control Manager サービスのすべてを停止する場合は、Windows の [サービス] 画面を使用します。

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Control Manager
- トレンドマイクロの NTP

注意： これらのサービスは、Windows OS のバックグラウンドで動作するものです。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サービス (大規模感染予防サービスなど) ではありません。

Control Manager のサービスを停止するには

1. Windows の [スタート] メニューから、[プログラム]→[管理ツール]→[サービス] の順に選択して、[サービス] 画面を開きます。

2. 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。

コマンドプロンプトからサービスを停止するには

コマンドプロンプトからサービスを停止するには、コマンドプロンプトで次のコマンドを実行します。

- net stop w3svc
- net stop tmcm

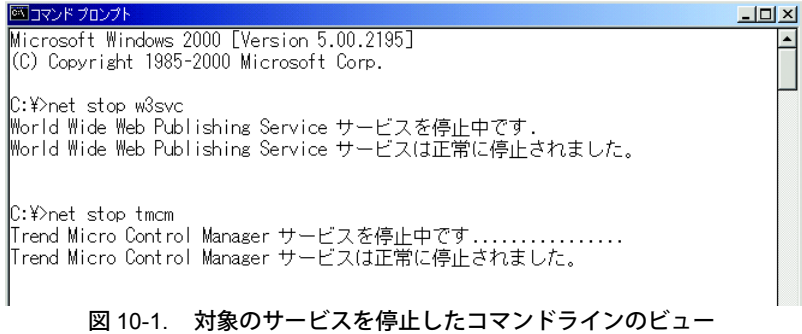


図 10-1. 対象のサービスを停止したコマンドラインのビュー

Control Manager の IIS 設定の削除

IIS (Internet Information Service) 設定の削除は、Control Manager サービスを停止した後に実行します。

Control Manager の IIS 設定を削除するには

1. Control Manager サーバで、Windows の [スタート]→[ファイル名を指定して実行] の順に選択します。[ファイル名を指定して実行] ダイアログボックスが表示されます。
2. [名前] ボックスに次のように入力します。

   %SystemRoot%¥System32¥Inetsrv¥iis.msc
3. 左側のメニューでサーバ名をダブルクリックしてコンソールツリーを展開します。

4. [既定の Web サイト] をダブルクリックします。
5. 次の仮想ディレクトリを削除します。
   - ControlManager
   - TVCSDownload
   - viewer9
   - TVCS
   - jakarta
   - WebApp
6. インストール時に設定した IIS Web サイトを右クリックします。
7. [プロパティ] をクリックします。
8. [ISAPI フィルタ] タブをクリックします。
9. 次の ISAPI フィルタを削除します。
   - TmcmRedirect
   - CCGIRedirect
   - ReverseProxy
10. IIS 6 の場合のみ、次の Web サービス拡張機能を削除します。
    - Trend Micro Common CGI Redirect Filter (CCGI を削除する場合)
    - Trend Micro Control Manager CGI 拡張機能
11. [OK] をクリックします。

Crystal Reports ランタイムファイル、TMI、および CCGI のアンインストール

TMI と CCGI のアンインストールは任意です。[プログラムの追加と削除] を使用して Crystal Reports ランタイムファイルをアンインストールします。

Crystal Reports ランタイムファイルをアンインストールするには

1. Control Manager サーバで、Windows の [スタート] メニューから [コントロールパネル]→[プログラムの追加と削除] の順に選択します。
2. 画面をスクロールして [Crystal Reports Runtime Files] を選択し、[削除] をクリックします。これで、Crystal Reports 関連の各ファイルが自動的に削除されます。

TMI と CCGI をアンインストールするには

- Microsoft のサービスツールである Sc.exe を使用して TMI と CCGI をアンインストールします。サービスツールについては、http://support.microsoft.com/kb/251192/ を参照してください。

Control Manager のファイル / ディレクトリおよびレジストリキーの削除

Control Manager サーバを手動でアンインストールするには

1. 次のディレクトリを削除します。
   - ...¥Trend Micro¥Control Manager
   - ...¥Trend Micro¥COMMON¥ccgi
   - ...¥Trend Micro¥COMMON¥TMI

2. レジストリエディタを起動し、次の Control Manager レジストリキーを削除します。

   - HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥CommonCGI
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥DamageCleanupService
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥MCPAgent
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥OPPTrustPort
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥TMI
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥TVCS
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥VulnerabilityAssessmentServices
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥TMCM
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥TMI
   - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TMCM
   - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendCCGI
   - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendMicro Infrastructure
   - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendMicro_NTP

データベースコンポーネントの削除

Control Manager の ODBC 設定を削除するには

1. Control Manager サーバで、Windows の [スタート]→[ファイル名を指定して実行] の順に選択します。[ファイル名を指定して実行] ダイアログボックスが表示されます。

2. [名前] ボックスに次のように入力します。

   odbcad32.exe

3. [ODBC データ ソース アドミニストレータ] ウィンドウで、[システム DSN] タブをクリックします。

4. [名前] から [ControlManager_Database] を選択します。

5. [削除] をクリックし、[はい] をクリックして削除を確定します。

Control Manager の SQL Server 2005 Express データベースを削除するには

1. Control Manager サーバで、Windows の [スタート] メニューから [コントロール パネル]→[プログラムの追加と削除] の順に選択します。

2. 画面をスクロールして [Microsoft SQL Server 2005] を選択し、[削除] をクリックします。これで、Crystal Reports 関連の各ファイルが自動的に削除されます。

ヒント： アンインストールに関する問題が発生した場合は、SQL Server 2005 Express をアンインストールする方法について、Microsoft の Web サイト (http://support.microsoft.com/kb/909967) を参照することをお勧めします。

Control Manager サービスと NTP サービスのアンインストール

Control Manager サービスと NTP サービスをアンインストールするには

- Microsoft のサービスツールである Sc.exe を使用して Control Manager サービスと NTP サービスをアンインストールします。サービスツールについては、http://support.microsoft.com/kb/251192/ を参照してください。

Windows ベースの Control Manager 2.x エージェントのアンインストール

エージェントをアンインストールするには、Control Manager サーバから、Control Manager エージェントセットアッププログラムを実行します。

製品側でローカルにアンインストールすることも可能です。製品側でのアンインストールの方法については、各製品のドキュメントを参照してください。

Windows ベースの Control Manager 2.x エージェントをアンインストールするには

1. 上部のメニューで [運用管理] の上にカーソルを置きます。ドロップダウンメニューが表示されます。
2. ドロップダウンメニューで [設定] の上にカーソルを置きます。サブメニューが表示されます。
3. [製品エージェントの追加 / 削除] をクリックします。[製品エージェントの追加 / 削除] 画面が表示されます。
4. [RemoteInstall.exe] をクリックし、アプリケーションをインストールします。
5. Windows エクスプローラを使用して、エージェントセットアッププログラムを保存した場所に移動します。

6. RemoteInstall.exe ファイルをダブルクリックします。Trend Micro Control Manager エージェントセットアップ画面が表示されます。

図 10-2. エージェントセットアッププログラム

7. [アンインストール] をクリックします。[ようこそ] 画面が表示されます。

8. [次へ] をクリックします。Control Manager サーバへのログオン画面が表示されます。

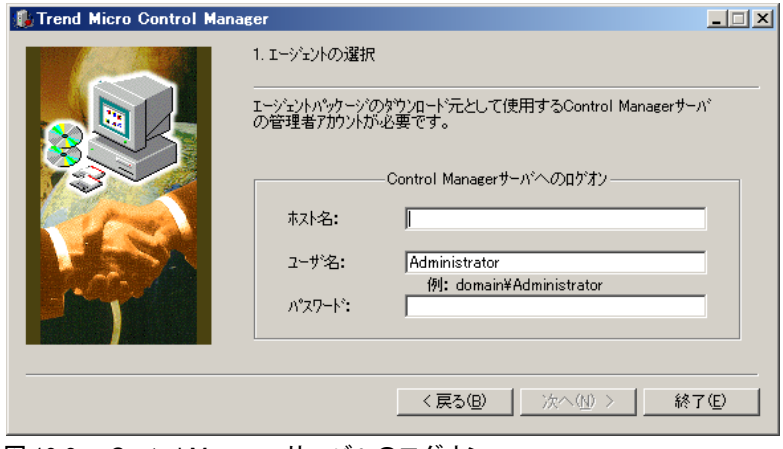


図 10-3. Control Manager サーバへのログオン

9. Control Manager サーバの管理者レベルのログオン認証情報を入力します。次の項目を入力してください。

   - ホスト名
   - ユーザ名
   - パスワード

10. [次へ] をクリックします。エージェントをアンインストールする製品を選択します。

11. [次へ] をクリックします。エージェントをアンインストールするサーバを選択します。サーバの選択方法には、次の 2 つの方法があります。

方法 1: リストから選択する

a. 左側のリストで、ウイルス対策製品サーバが存在するドメインをダブルクリックします。それにより、ドメインのツリーが展開され、ドメイン内のすべてのサーバが表示されます。

b. 左側のリストから対象サーバを選択して [追加] をクリックします。右側のリストに選択したサーバが表示されます。[すべて追加] をクリックすると、選択したドメイン内のすべてのサーバに対するエージェントが選択されます。

[追加ボタン] をクリックする代わりに、サーバをダブルクリックして右側のリストに追加することもできます。

方法 2: サーバを直接指定する

a. [サーバ名] にサーバの FQDN または IP アドレスを入力します。

b. [追加] をクリックします。右側のリストに選択したサーバが表示されます。

追加したサーバをリストから削除するには、右側のリストでサーバを選択して、[削除] をクリックします。サーバをすべて削除するには、[すべて削除] をクリックします。

12. 前の画面に戻るには [戻る]、処理を中止するには [終了]、続行するには [次へ] をクリックします。

13. 選択したサーバに対するログオン認証情報を入力します。必要なユーザ名とパスワードをそれぞれ該当フィールドに入力します。

14. [OK] をクリックします。サーバ名、OS のバージョン、IP アドレス、ドメイン、アンインストールされるエージェントの製品情報などの対象サーバの情報が表示されます。

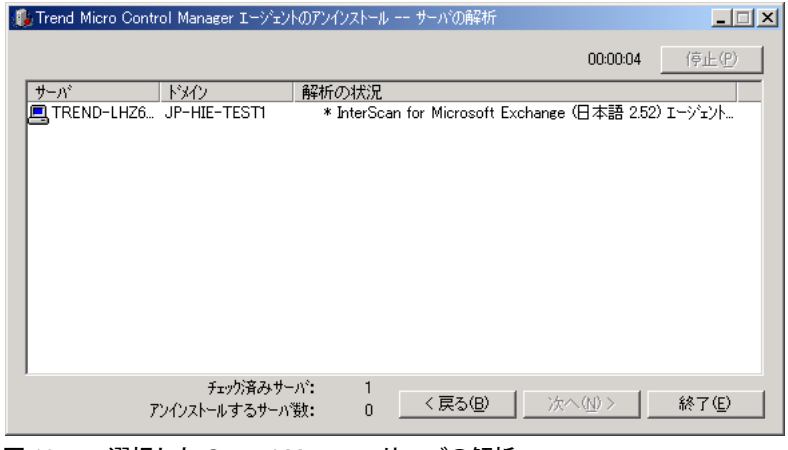


図 10-4. 選択した Control Manager サーバの解析

15. [次へ] をクリックします。画面上の表に、対象サーバのサーバ名、OS のバージョン、IP アドレス、ドメイン名、および削除するエージェントのバージョンに関する情報が表示されます。

    前の画面に戻るには [戻る]、処理を中止するには [終了]、エージェントをアンインストールするには [アンインストール] をクリックします。アンインストールが開始されます。

16. 「エージェントの削除が完了しました。」というメッセージが表示されたら、[OK] をクリックします。[終了] をクリックしてアンインストールを終了します。

第 11 章

製品サポート情報

Trend Micro Control Manager (以下、Control Manager) 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「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、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「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、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。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

中小 / 中堅企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/smb/search.do

大企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/enterprise/search.do

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

セキュリティ情報の入手先

トレンドマイクロでは、最新のセキュリティ情報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情報 Web サイトでは、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。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

http://www.trendmicro.co.jp/vinfo/

管理コンソールからセキュリティ情報サイトにアクセスすることもできます。セキュリティ情報サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから[セキュリティ情報] リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- 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

セキュリティ情報 Web サイト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ウイルスデータベース検索サイトにアクセスして、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。

http://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp

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。

http://inet.trendmicro.co.jp/esolution/attach_agreement.asp

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国の各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアのスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

「TrendLabs」では、品質保証の ISO9001:2000 認定 (フィリピン)、国際規格 COPC-2000 規格 (フィリピン)、英国の国家規格 ITIL: BS15000 (ドイツ)、情報セキュリティマネージメントの英国規格 BS7799 (フィリピン) を取得しています。

システムチェックリスト

本付録では、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。

本付録は次の内容で構成されています。

サーバアドレスチェックリスト

インストール時、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が必要になります。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。

必要な情報	例	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.company.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.company.com	
NetBIOS (ホスト) 名	yourserver	
Control Manager の SQL データベース情報		
IP アドレス	10.1.114.225	
FQDN (完全修飾ドメイン名)	server.company.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.company.com	
NetBIOS (ホスト) 名	proxyserver	
SMTP サーバ情報 (任意 : メールメッセージ通知用)		
IP アドレス	10.1.123.225	
FQDN (完全修飾ドメイン名)	mail.company.com	

必要な情報	例	設定する値
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	

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	
コンポーネントダウンロード用のプロキシ	8088	
ポケットベル COM	COM1	
TVCS エージェント用のプロキシ (任意)	223	
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 Manger のエージェントのインストール時に使用)	224	
Trend Micro Management Infrastructure (TMI) 内部プロセス通信 (リモート製品用)	10198	
TMI 外部プロセス通信	10319	
エンティティエミュレータ	10329	

注意 : Control Manager では、ポート 10319 および 10198 を排他的に使用する必要があります。

Control Manager 2.x エージェントのインストールチェックリスト

次の情報は、エージェントのインストール時に使用されます。

必要な情報	例	設定する値
Control Manager の Administrator 権限以上のアカウント	root	
公開鍵ファイルの保存先	C:¥MyDocuments¥E2EPulic.dat	

注意： エージェントのインストールでは root アカウント以外にも任意の Control Manager アカウントを使用できますが、root アカウントを使用することを推奨します。エージェントのインストール時に指定した Control Manager アカウントを削除すると、エージェントの管理が非常に難しくなります。

製品名	管理者レベルのアカウント	IP アドレス	コンピュータのホスト名
例	Admin	10.225.225.225	PH-antivirus

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。

Control Managerサーバで使用される設定ファイルは次のとおりです。

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。
ssleay32.dll	Control Manager のセキュリティレベルを処理します。
TMUpdate.dll	コンポーネントのアップデートを実行します。
ProcessManager.xml	ProcessManager.exe で使用されます。
CmdProcessorEventHandler.xml	CmdProcessor.exe で使用されます。
UIProcessorEventHandler.xml	UIProcessor.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。
CastoolConfiguration.xml	CasTool.exe で使用されます。
SystemConfiguration.xml	Control Manager のシステム設定ファイルです。
CascadingLogConfiguration.xml	下位サーバ用のログアップロード設定ファイルです。
TMI.cfg	Trend Micro Management Infrastructure の設定ファイルです。
Entity.cfg	管理下の製品の設定ファイルです。

プロセス	説明
CasTool.exe	階層構造の Control Manager 環境の確立に使用されるコマンドラインプログラムです。
ProcessManager.exe	「Trend Micro Control Manager」サービスです。 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。

プロセス	説明
UIProcessor.exe	Control Manager 管理コンソールで実行されたユーザの入力を処理し、実際のコマンドに変換します。
LogReceiver.exe	管理下の製品のログおよびメッセージを受信します。
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。
MsgReceiver.exe	Control Manager サーバ、管理下の製品、および下位サーバからメッセージを受信します。
EntityEmulator.exe	Control Manager が TVCS エージェントを使用できるようにします。
CasProcessor.exe	Control Manager サーバ (上位サーバ) が他の Control Manager サーバ (下位サーバ) を管理できるようにします。
DCSProcessor.exe	ダメージクリーンナップサービスの機能を実行します。
Ntpd.exe	Network Time Protocol (NTP) サービスです。
inetinfo.exe	Microsoft Internet Information Service プロセスです。
jk_nt_service.exe java.exe	多数のスタンドアロン CGI プログラムを使用する代わりに、インタフェースを定義することによって Web ベースのユーザインタフェースを構築するのに使用される Java サーバ側拡張です。
cm.exe	dmserver.exe および mrf.exe を管理します。
mrf.exe	コミュニケータプロセスです。
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 サーバ側) を管理します。
LWDMServer.exe	製品ディレクトリ (クライアント側 — 管理下の製品) を管理します。

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。

種類	通信ポート
内部通信	10198
外部通信	10319
ダメージクリーンナップサービスおよび脆弱性診断サービス用通信	20901, 20902

サービス	サービスポート
ProcessManager.exe	20501
CmdProcessor.exe	20101
UIProcessor.exe	20701
LogReceiver.exe	20201
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
EntityEmulator.exe	20401
CasProcessor.exe	20801
DcsProcessor.exe	20903

Control Manager のバージョン別機能比較

機能	Control Manager			
	3.X エンタープライズ版	**3.X スタンダード版**	**5.0 アドバンス版**	**5.0 スタンダード版**
バージョン 2.x および MCP エージェントを介した製品管理	●	●	●	●
アドホッククエリ			●	●
コンポーネントの自動アップデート	●	●	●	●
階層管理構造	●		●	
ウイルスログおよびシステムイベントの集中管理 (単一のデータベース)	●	●	●	●
企業全体にわたる Web ベースの集中管理	●	●	●	●
下位サーバの監視	●		●	
下位サーバのタスク発行	●		●	
コマンド追跡	●	●	●	●
コミュニケータ接続ステータス	●	●	●	●
コミュニケータスケジュール設定	●	●	●	●
コンポーネントのダウンロードの細分化	●	●	●	●
製品のグループ単位での設定	●	●	●	●
複数のダウンロード元の設定	●	●	●	●
管理下の製品および Control Manager 間の一貫したユーザインタフェース	●	●	●	●

機能	Control Manager			
	3.X エンタープライズ版	**3.X スタンダード版**	**5.0 アドバンス版**	**5.0 スタンダード版**
カスタマイズされたユーザタイプ			●	●
配信計画	●	●	●	●
ディレクトリ管理	●	●	●	●
イベントセンター	●	●	●	●
ダメージクリーンナップサービス / 脆弱性診断サービスの統合	●	●	●	●
ログ機能の向上			●	●
ウイルス対策 / コンテンツ対策製品の管理	●	●	●	●
管理下の製品のライセンス管理			●	
管理下の製品のレポート機能	●		●	
Microsoft SQL Express または Microsoft SQL 2005 のサポート			●	●
MSDE または Microsoft SQL Server 7/2000 のサポート	●	●	●	●
MSN Messenger による通知	●	●	●	●
通知およびアウトブレークアラート	●	●	●	●
アウトブレークコマンダー/大規模感染予防サービス - アウトブレークプリベンションポリシー/ 大規模感染予防ポリシーの自動ダウンロードおよび配信	●	●	●	●

機能	Control Manager			
	3.X エンタープライズ版	**3.X スタンダード版**	**5.0 アドバンス版**	**5.0 スタンダード版**
アウトブレークコマンダー/大規模感染予防サービス - アウトブレークプリベンションポリシー/ 大規模感染予防ポリシーの手動ダウンロードおよび配信	●	●	●	●
アウトブレークコマンダー/大規模感染予防サービス	●	●	●	●
サードパーティ製品のサポート	●		●	
リモート管理	●	●	●	●
レポート機能	●		●	
サーバ / エージェント間の安全な通信	●	●	●	●
シングルサインオン (SSO) をサポートする管理化の製品に対する SSO	●	●	●	●
SNMP トラップ通知			●	
管理コンソールの SSL 対応	●	●	●	●
Control Manager 2.x エージェントのサポート	●	●	●	●
サーバ､エージェント､および管理下の製品間での HTTPS 通信のサポート	●	●	●	●
MCP エージェントのサポート	●	●	●	●
TVCS エージェントのサポート	●	●		
Syslog 通知			●	
Trend Micro InterScan for Cisco Content Security および Control Security Services Module (ISC CSC SSM) の統合	●	●	●	●

機能	Control Manager			
	3.X エンタープライズ版	**3.X スタンダード版**	**5.0 アドバンス版**	**5.0 スタンダード版**
Trend Micro Network VirusWall 1200 の統合	●	●	●	●
Trend Micro Network VirusWall 2500 の統合	●	●	●	●
トレンドマイクロの新しい製品登録システムへの対応	●	●	●	●
トレンドラボからのメッセージ	●	●	●	●
ユーザアカウント管理	●	●	●	●
脆弱性診断サービス	●	●	●	●
Windows 認証			●	●

データビューについて

データビューは、Trend Micro Control Manager (以下、Control Manager) 5.0 のレポートテンプレートおよびアドホッククエリ要求で使用できます。

本付録は次の内容で構成されています。

製品情報

製品情報データビューには、Control Manager、管理下の製品、コンポーネント、および製品ライセンスに関する情報が表示されます。

表 B-1. 製品情報のデータビュー

データビュー	説明
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。
管理下の製品情報	管理下の製品または管理下の製品のクライア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。
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。
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。

セキュリティの脅威情報

ウイルス、スパイウェア、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。

表 B-2. セキュリティの脅威データビュー

データビュー	説明
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。
スパイウェア情報	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に関する概要と詳細データが表示されます。

表 B-2.　セキュリティの脅威データビュー

データビュー	説明
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。
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。
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。
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。
脅威の兆候の情報	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な動作に関する概要と詳細データが表示されます。
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。

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

管理下の製品のライセンスステータス

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-3.　管理下の製品のライセンスステータスデータビュー

データ	説明
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5
管理下のサービス	管理下の製品サービスの名前が表示されます。例 : 脆弱性診断サービス、大規模感染予防サービス
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
アクティベーションコード	管理下の製品のアクティベーションコードが表示されます。
アクティベーションコード数	管理下の製品が使用するアクティベーションコードの件数が表示されます。
ライセンス使用期限	管理下の製品の有効期限が表示されます。

管理下の製品のライセンス情報概要

アクティベーションコードに関する詳細詳細、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-4.　管理下の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。
管理下の製品 / サービス数	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
管理下の製品の種類	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
ライセンス使用期限	管理下の製品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。

管理下の製品の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-5. 管理下の製品のライセンス詳細情報データビュー

データ	説明
管理下の製品のエンティティ表示名	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。
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5
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 : 脆弱性診断サービス、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
管理下の製品の種類	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。
ライセンス使用期限	管理下の製品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

管理下の製品の配置概要

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-6.　管理下の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。
管理下の製品のカテゴリ	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、デスクトップ製品
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5
管理下の製品の役割	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
管理下の製品数	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。

管理下の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-7.　管理下の製品のステータス情報データビュー

データ	説明
管理下の製品の エンティティ表示名	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。
管理下の製品のホスト名	管理下の製品がインストールされるサーバの名前が表示されます。
管理下の製品の IP アドレス	管理下の製品がインストールされるサーバの IP アドレスが表示されます。
管理下の製品の MAC アドレス	管理下の製品がインストールされるサーバの MAC アドレスが表示されます。
管理 Control Manager のエンティティ表示名	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 エンティティ表示名	クライア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。
ドメイン名	管理下の製品が属するドメインが表示されます。
管理下の製品の接続ステータス	管理下の製品の Control Manager への接続ステータスが表示されます。例 : 標準、異常、オフライン
パターンファイルのステータス	管理下の製品が使用する各種パターンファイ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
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5

表 B-7.　管理下の製品のステータス情報データビュー

データ	説明
管理下の製品のビルド番号	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)
管理下の製品の役割	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
OS 名	管理下の製品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。

ServerProtect およびウイルスバスター Corp. サーバ / ドメインのステータス概要

管理下のクライアント / サーバ製品に関する概要情報が表示されます。例 : パターンファイル期限切れ、検索エンジン期限切れ

表 B-8.　ServerProtect およびウイルスバスター Corp. サーバ / ドメインのステータス概要データビュー

データ	説明
管理下の製品のエンティティ表示名	管理下の製品のエンティティ表示名が表示されます。
ドメイン名	管理下の製品が属するドメインが表示されます。
管理下のサーバ / クライアント数	管理下の製品サーバまたは製品クライアント数が表示されます。
パターンファイル期限切れサーバ / クライアント	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サーバ / クライアントの数が表示されます。
最新パターンファイル保有率 (%)	最新のパターンファイルを使用している管理下の製品サーバ / クライアントの割合が表示されます。

表 B-8. ServerProtect およびウイルスバスター Corp. サーバ / ドメインのステータス概要データビュー

データ	説明
検索エンジン期限切れサーバ / クライアント	期限切れの検索エンジンを使用している管理下の製品サーバ / クライアントの数が表示されます。
最新検索エンジン保有率 (%)	最新の検索エンジンを使用している管理下の製品サーバ / クライアントの割合が表示されます。

管理下の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-9. 管理下の製品のイベント情報データビュー

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。
エンティティでの生成時間	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。
管理下の製品のエンティティ表示名	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。
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5
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

表 B-9.　管理下の製品のイベント情報データビュー

データ	説明
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。

コンポーネント情報

管理下の製品の検索エンジンステータス

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-10.　管理下の製品の検索エンジンステータスデータビュー

データ	説明
管理下の製品の エンティティ表示名	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。
管理下の製品のホスト名	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。
管理下の製品の IP アドレス	管理下の製品がインストールされるサーバの IP アドレスが表示されます。
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クライアント間の接続ステータスが表示されます。
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5

表 B-10. 管理下の製品の検索エンジンステータスデータビュー

データ	説明
管理下の製品の役割	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
検索エンジン名	検索エンジンの名前が表示されます。例 : スパムメール検索エンジン (Windows)、ウイルス検索エンジン IA64 ビット検索エンジン
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 : スパムメール検索エンジン (Windows): 3.000.1153、ウイルス検索エンジン IA64 ビット検索エンジン : 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
検索エンジン最終アップデート時刻	検索エンジンを管理下の製品またはクライアントに最後に配信した時間が表示されます。

管理下の製品のパターンファイル / ルールステータス

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-11. 管理下の製品のパターンファイル / ルールステータスデータビュー

データ	説明
管理下の製品のエンティティ表示名	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。
管理下の製品のホスト名	管理下の製品がインストールされるサーバの名前が表示されます。
管理下の製品の IP アドレス	管理下の製品がインストールされるサーバの IP アドレスが表示されます。

表 B-11. 管理下の製品のパターンファイル / ルールステータスデータビュー

データ	説明
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クライアント間の接続ステータスが表示されます。
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5
管理下の製品の役割	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
パターンファイル / ルールの名前	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 / ルールの最終アップデート時刻	各種パターンファイルを管理下の製品またはクライアントに最後に配信した時間が表示されます。

管理下の製品の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-12. 管理下の製品のコンポーネントの配信データビュー

データ	説明
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
管理下の製品のバージョン	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 8.0、Control Manager 3.5
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クライア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 最終配信時刻	各種パターンファイルを管理下の製品またはクライア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
検索エンジン最終配信時刻	検索エンジンを管理下の製品またはクライア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-13. 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
検索エンジン名	検索エンジンの名前が表示されます。例 : スパムメール検索エンジン (Windows)、ウイルス検索エンジン IA64 ビット検索エンジン
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 : スパムメール検索エンジン (Windows): 3.000.1153、ウイルス検索エンジン IA64 ビット検索エンジン : 8.000.1008
最新検索エンジン保有数	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。
検索エンジン期限切れ数	期限切れの検索エンジンを使用している管理下の製品の数が表示されます。
最新検索エンジン保有率 (%)	最新の検索エンジンを使用している管理下の製品の割合が表示されます。これには、値として「N/A」を返す検索エンジンも含まれます。

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-14. 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 / ルールの名前	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
最新パターンファイル / ルール保有数	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。
パターンファイル / ルール期限切れ数	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。
最新パターンファイル / ルール保有率 (%)	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。

Control Manager 情報

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。

表 B-15. ユーザアクセス情報データビュー

データ	説明
アクティビティの時刻	アクティビティの開始時間が表示されます。
ログオンユーザ名	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。
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
アクティビティの結果	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-16. Control Manager のイベント情報データビュー

データ	説明
イベントの時刻	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
イベント結果	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-17. コマンド追跡情報データビュー

データ	説明
コマンドの時刻	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
コマンドの発行者	コマンドを発行したユーザが表示されます。

表 B-17. コマンド追跡情報データビュー

データ	説明
ステータスの最終アップデート時刻	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-18. コマンド追跡詳細情報データビュー

データ	説明
コマンドの時刻	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
管理下の製品のエンティティ表示名	コマンドの発行先である管理下の製品が表示されます。
コマンドの発行者	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。
ステータスの最終アップデート時刻	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。

データビュー: セキュリティの脅威情報

ウイルス、スパイウェア、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

概要情報

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クライアント数、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-19. 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 / 不正プログラム名	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
一意の感染先数	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、[一意の感染先数] は「3」になります。
一意の感染元数	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、[一意の感染元数] は「2」になります。

表 B-19. 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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

ウイルス / 不正プログラムの種類の概要 (全体)

検出されたウイルスのさまざまな概要が表示されます。例 : ウイルスの種類 (トロイの木馬、ハッキング用ツール)、ネットワーク上のウイルスの絶対数、ネットワーク上のウイルスの総インスタンス数

表 B-20. ウイルス / 不正プログラムの種類の概要 (全体) データビュー

データ	説明
一意のウイルス / 不正プログラム数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。
一意の感染先数	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、[一意の感染先数] は「3」になります。
一意の感染元数	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、[一意の感染元数] は「2」になります。

表 B-20. ウイルス / 不正プログラムの種類の概要 (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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」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 : 感染元のコンピュータの名前、感染元コンピュータ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-21. ウイルス / 不正プログラム感染元の概要データビュー

データ	説明
感染元	ウイルスの感染元のコンピュータの IP アドレス / ホスト名が表示されます。
一意の感染先数	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、[一意の感染先数] は「3」になります。
一意のウイルス / 不正プログラム数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

表 B-21. 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
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

ウイルス / 不正プログラム感染先の概要

特定のクライアントからのウイルス検出の概要が表示されます。例 : クライアントの名前、クライア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-22. ウイルス / 不正プログラム感染先の概要データビュー

データ	説明
感染先	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。
一意の感染元数	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、[一意の感染元数] は「2」になります。
一意のウイルス / 不正プログラム数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

表 B-22. ウイルス / 不正プログラム感染先の概要データビュー

データ	説明
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」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)

一定の期間内 (毎日、毎週、毎月) のウイルス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、ウイルスに感染したクライアント数、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-23. ウイルス / 不正プログラム検出の概要 (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。
一意のウイルス / 不正プログラム数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。
一意の感染先数	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、[一意の感染先数] は「3」になります。
一意の感染元数	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、[一意の感染元数] は「2」になります。

表 B-23. ウイルス / 不正プログラム検出の概要 (時間別推移) データビュー

データ	説明
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」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-24. 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
処理結果	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
実行された処理	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
一意の感染先数	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、[一意の感染先数] は「3」になります。
一意の感染元数	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、[一意の感染元数] は「2」になります。

表 B-24. 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
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

詳細情報

ウイルス / 不正プログラムの詳細情報 (全体)

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クライアントの名前

表 B-25. ウイルス / 不正プログラムの詳細情報 (全体) 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。
管理下の製品のエンティティ表示名	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。
管理下の製品の名前	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 / 不正プログラム名	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
感染先	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。

表 B-25. ウイルス / 不正プログラムの詳細情報 (全体) データビュー

データ	説明
感染元	ウイルスの感染元のコンピュータの IP アドレス / ホスト名が表示されます。
ログオンユーザ名	管理下の製品によってウイルスが検出されたとき、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。
処理結果	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
実行された処理	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
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。
検出ポイントの種類	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	アドホック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。アドホッククエリ内で、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 / 不正プログラム検出情報 (ホスト)

クライア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クライアント上のファイルパス

表 B-26. ウイルス / 不正プログラム検出情報 (ホスト) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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 / 不正プログラム名	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
感染先	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。
ログオンユーザ名	管理下の製品によってウイルスが検出されたとき、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。
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
検出ファイル名	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感染先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。

表 B-26. ウイルス / 不正プログラム検出情報 (ホスト) データビュー

データ	説明
処理結果	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
実行された処理	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
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

ウイルス / 不正プログラム検出情報 (HTTP/FTP)

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 クライアント

表 B-27. ウイルス / 不正プログラム検出情報 (HTTP/FTP) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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

表 B-27. ウイルス / 不正プログラム検出情報 (HTTP/FTP) データビュー

データ	説明
ウイルス / 不正プログラム名	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
感染先	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 / 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。
ログオンユーザ名	ウイルスインスタンスを実行しているユーザのログオン名が表示されます。
送受信トラフィック / 接続	ウイルスの侵入方向が表示されます。
インターネットブラウザ / 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 クライアントが表示されます。
処理結果	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
実行された処理	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
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

ウイルス / 不正プログラム検出情報 (メール)

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-28. ウイルス / 不正プログラム検出情報 (メール) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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 / 不正プログラム名	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。
ログオンユーザ名	ウイルスインスタンスを実行しているユーザのログオン名が表示されます。
メールの件名	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。
検出ファイル名	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。
処理結果	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

表 B-28. ウイルス / 不正プログラム検出情報 (メール) データビュー

データ	説明
実行された処理	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
ウイルス / 不正プログラム検出数	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。[ウイルス / 不正プログラム検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

ウイルス / 不正プログラム検出情報 (ネットワークトラフィック)

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-29. ウイルス / 不正プログラム検出情報 (ネットワークトラフィック) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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 / 不正プログラム名	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

表 B-29. ウイルス / 不正プログラム検出情報 (ネットワークトラフィック) データビュー

データ	説明
感染先	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	ウイルスの感染元のコンピュータの IP アドレス / ホスト名が表示されます。
ログオンユーザ名	管理下の製品によってウイルスが検出されたとき、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。
送受信トラフィック / 接続	ウイルス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
感染先ホスト名	ウイルスに感染したコンピュータのホスト名が表示されます。
感染先ポート	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。
感染先 MAC アドレス	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。
感染元ホスト名	ウイルスの感染元のコンピュータのホスト名が表示されます。
感染元ポート	ウイルスの感染元のコンピュータのポート番号が表示されます。
感染元 MAC アドレス	ウイルスの感染元のコンピュータの MAC アドレスが表示されます。
検出ファイル名	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。
処理結果	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
実行された処理	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

表 B-29. ウイルス / 不正プログラム検出情報 (ネットワークトラフィック) データビュー

データ	説明
ウイルス / 不正プログラム検出数	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、[セキュリティリスク検出数] は「10」、[一意のウイルス / 不正プログラム数] は「1」になります。

スパイウェア情報

概要情報

スパイウェアの概要 (全体)

スパイ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 : スパイウェアの名前、スパイウェアに感染したクライアント数、ネットワーク上に存在するスパイウェアのインスタンスの総数

表 B-30. スパイウェアの概要 (全体) データビュー

データ	説明
スパイウェア名	管理下の製品が検出したスパイウェアの名前が表示されます。
一意のスパイウェア送信先数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信先数] は「3」になります。
一意のスパイウェア送信元数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信元数] は「2」になります。

表 B-30. スパイウェアの概要 (全体) データビュー

データ	説明
スパイウェア検出数	管理下の製品が検出したスパイウェアの総数が表示されます。

スパイ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検出の概要が表示されます。例 : 感染元のコンピュータの名前、感染元コンピュータからの特定のスパイ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インスタンスの総数

表 B-31. スパイウェア送信元の概要データビュー

データ	説明
スパイウェア送信元	スパイウェアの感染元のコンピュータの名前が表示されます。
一意のスパイウェア送信先数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信先数] は「3」になります。
一意のスパイウェア数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。

スパイウェア送信先の概要

特定のクライアントからのスパイウェア検出の概要が表示されます。例 : クライアントの名前、クライアント上の特定のスパイ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のインスタンスの総数

表 B-32. スパイウェア送信先の概要データビュー

データ	説明
スパイウェア送信先	スパイ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。
一意のスパイウェア送信元数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信元数] は「2」になります。
一意のスパイウェア数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。

スパイウェア検出の概要 (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、スパイウェアに感染したクライアント数、ネットワーク上に存在するスパイウェアのインスタンスの総数

表 B-33. スパイウェア検出の概要 (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。
一意のスパイウェア数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。
一意のスパイウェア送信先数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信先数] は「3」になります。
一意のスパイウェア送信元数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信元数] は「2」になります。
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。

スパイウェアの処理 / 結果の概要

スパイ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のインスタンスの総数

表 B-34. スパイウェアの処理 / 結果の概要データビュー

データ	説明
処理結果	スパイ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
実行された処理	スパイ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
一意のスパイウェア送信先数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信先数] は「3」になります。
一意のスパイウェア送信元数	スパイ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のインスタンスが 10 件検出されました。この場合、[一意のスパイウェア送信元数] は「2」になります。
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。

詳細情報

スパイウェア詳細情報 (全体)

ネットワーク上に存在するスパイ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 : スパイウェアを検出した管理下の製品、スパイウェアの名前、スパイウェアに感染したクライアントの名前

表 B-35. スパイウェア詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
スパイウェア名	管理下の製品が検出したスパイウェアの名前が表示されます。
スパイウェア送信先	スパイウェアに感染したコンピュータの名前が表示されます。
スパイウェア送信元	スパイウェアの感染元のコンピュータの名前が表示されます。
ログオンユーザ名	管理下の製品によってスパイウェアが検出されたとき、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。
処理結果	スパイ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

表 B-35. スパイウェア詳細情報 (全体) データビュー

データ	説明
実行された処理	スパイ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
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。
検出ポイントの種類	管理下の製品によって検出されたスパイ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	アドホック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。アドホッククエリ内で、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

ホストからのスパイウェア検出

クライアントで検出されたスパイ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 : スパイウェアを検出した管理下の製品、スパイウェアを検出した検索の種類、検出されたスパイウェアへのクライアント上のファイルパス

表 B-36. ホストからのスパイウェア検出データビュー

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。

表 B-36. ホストからのスパイウェア検出データビュー

データ	説明
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
スパイウェア名	管理下の製品が検出したスパイウェアの名前が表示されます。
スパイウェア送信先	スパイウェアに感染したコンピュータが表示されます。
スパイウェア送信元	スパイウェアの感染元のコンピュータの名前が表示されます。
ログオンユーザ名	管理下の製品によってスパイウェアが検出されたとき、スパイウェアの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。
検索の種類	スパイ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
影響を受けたリソース	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
影響を受けたリソースの種類	スパイ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
スパイウェアのリスクの種類	管理下の製品が検出したスパイ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
スパイウェアのリスクレベル	スパイ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
処理結果	スパイ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

表 B-36. ホストからのスパイウェア検出データビュー

データ	説明
実行された処理	スパイ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

HTTP/FTP からのスパイウェア検出

HTTP または FTP トラフィックで検出されたスパイ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 : スパイウェアを検出した管理下の製品、スパイウェアが発生したトラフィックの方向、スパイ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 クライアント

表 B-37. HTTP/FTP からのスパイウェア検出データビュー

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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
スパイウェア名	管理下の製品が検出したスパイウェアの名前が表示されます。
スパイウェア送信先	管理下の製品がスパイウェアを検出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。
送信元 URL	スパイウェアの感染元である Web/FTP サイトの URL が表示されます。
送受信トラフィック / 接続	スパイウェアの侵入方向が表示されます。

表 B-37. HTTP/FTP からのスパイウェア検出データビュー

データ	説明
インターネットブラウザ / 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 クライアントが表示されます。
ログオンユーザ名	管理下の製品によってスパイウェアが検出されたとき、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。
処理結果	スパイ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
実行された処理	スパイ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
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。

メールからのスパイウェア検出

メールメッセージで検出されたスパイ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、スパイウェアを含んでいるメールメッセージの送信者

表 B-38. メールからのスパイウェア検出データビュー

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。

表 B-38. メールからのスパイウェア検出データビュー

データ	説明
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
スパイウェア名	管理下の製品が検出したスパイウェアの名前が表示されます。
受信者	スパイ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。
ログオンユーザ名	管理下の製品によってスパイウェアが検出されたとき、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。
メールの件名	スパイ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。
検出ファイル名	管理下の製品が検出した、スパイ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のファイル名が表示されます。
処理結果	スパイ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
実行された処理	スパイ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

表 B-38. メールからのスパイウェア検出データビュー

データ	説明
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。

ネットワークトラフィックからのスパイウェア検出

ネットワークトラフィックで検出されたスパイ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が使用したプロトコル、スパイ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-39. ネットワークトラフィックからのスパイウェア検出データビュー

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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
スパイウェア名	管理下の製品が検出したスパイウェアの名前が表示されます。
送受信トラフィック / 接続	スパイ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が使用したプロトコルが表示されます。例 : HTTP、SMTP、FTP

表 B-39. ネットワークトラフィックからのスパイウェア検出データビュー

データ	説明
スパイウェア送信先	スパイウェア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。
スパイウェア送信先ホスト名	スパイウェアに感染したコンピュータのホスト名が表示されます。
スパイウェア送信先ポート	スパイ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。
スパイウェア送信先 MAC アドレス	スパイ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。
スパイウェア送信元	スパイウェアの感染元のコンピュータの IP アドレス / ホスト名が表示されます。
スパイウェア送信元ホスト名	スパイウェアの感染元のコンピュータのホスト名が表示されます。
スパイウェア送信元ポート	スパイウェアの感染元のコンピュータのポート番号が表示されます。
スパイウェア送信元 MAC アドレス	スパイウェアの感染元のコンピュータの MAC アドレスが表示されます。
ログオンユーザ名	管理下の製品によってスパイウェアが検出されたとき、スパイウェアの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。
検出ファイル名	管理下の製品が検出した、スパイウェアに感染したファイルの名前が表示されます。
処理結果	スパイ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
実行された処理	スパイ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

表 B-39. ネットワークトラフィックからのスパイウェア検出データビュー

データ	説明
スパイウェア検出数	管理下の製品が検出したスパイ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のインスタンスが 10 件検出されました。この場合、[スパイウェア検出数] は「10」、[一意のスパイウェア数] は「1」になります。

コンテンツ違反情報

概要情報

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-40. 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
違反ポリシー	クライア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
一意のポリシー違反送信者数	管理下の製品のポリシーに違反するコンテンツを送信したメールアドレス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、[一意のポリシー違反送信者数] は「3」になります。

表 B-40. 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
一意のポリシー違反受信者数	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、[一意のポリシー違反受信者数] は「2」になります。
ポリシー違反検出数	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、[ポリシー違反検出数] は「10」、[一意の違反ポリシー数] は「1」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-41. コンテンツ違反送信者の概要データビュー

データ	説明
ポリシー違反送信者	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。
ポリシー違反検出数	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、[ポリシー違反検出数] は「10」、[一意の違反ポリシー数] は「1」になります。
一意のポリシー違反受信者数	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、[一意のポリシー違反受信者数] は「2」になります。

表 B-41. コンテンツ違反送信者の概要データビュー

データ	説明
一意の違反ポリシー数	管理下の製品が検出したポリシー違反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、[ポリシー違反検出数] は「10」、[一意の違反ポリシー数] 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クライアント数、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-42. 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
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。
一意の違反ポリシー数	管理下の製品が検出したポリシー違反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、[ポリシー違反検出数] は「10」、[一意の違反ポリシー数] は「1」になります。
一意のポリシー違反送信者数	管理下の製品のポリシーに違反するコンテンツを送信したメールアドレス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、[一意のポリシー違反送信者数] は「3」になります。
一意のポリシー違反受信者数	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、[一意のポリシー違反受信者数] は「2」になります。

表 B-42. 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
ポリシー違反検出数	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、[ポリシー違反検出数] は「10」、[一意の違反ポリシー数] は「1」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アクション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アクション、アクションの実行で影響を受けるメールメッセージの数

表 B-43. 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
実行された処理	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アクションの種類が表示されます。例 : 通知、添付ファイル削除、削除
メール数	管理下の製品が指定のアクションを実行したメールメッセージの数が表示されます。

詳細情報

コンテンツ違反の詳細情報 (全体)

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-44. コンテンツ違反の詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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	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。
メールの件名	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。
違反ポリシー	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。
検出ファイル名	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。
検出フィルタの種類	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
検出フィルタの処理	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アクションが表示されます。例 : 駆除、隔離、削除

表 B-44. コンテンツ違反の詳細情報 (全体) データビュー

データ	説明
実行された処理	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アクションの種類が表示されます。例 : 配信、削除、通知
ポリシー違反検出数	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。

スパムメール違反情報

概要情報

スパムメール違反の概要 (全体)

特定のドメインでのスパムメール検出の概要が表示されます。例 : スパムメールを受信したドメイン名、スパムメールを受信したクライアント数、ネットワーク上のスパムメール違反の総数

表 B-45. スパムメール違反の概要 (全体) データビュー

データ	説明
受信者ドメイン	スパムメールを受信したドメインが表示されます。
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。
スパムメール違反検出数	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、[スパムメール違反検出数] は「10」になります。

スパムメール受信者の概要

特定のクライアントでのスパムメール違反の概要が表示されます。例 : クライアントの名前、そのクライアント上のウイルスのインスタンスの総数

表 B-46. スパムメール受信者の概要データビュー

データ	説明
受信者名	スパムメールの受信者の名前が表示されます。
スパムメール違反検出数	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、[スパムメール違反検出数] 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クライアント数、ネットワーク上のスパムメール違反の総数

表 B-47. 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。

表 B-47. 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
スパムメール違反検出数	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、[スパムメール違反検出数] は「10」になります。

詳細情報

スパムメール詳細情報 (全体)

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-48. スパムメール詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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。
メールの件名	スパムメールの件名のコンテンツが表示されます。
違反ポリシー	メールが違反しているポリシーの名前が表示されます。

表 B-48. スパムメール詳細情報 (全体) データビュー

データ	説明
実行された処理	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
スパムメール違反検出数	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、[スパムメール違反検出数] 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、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-49. スパムメール接続情報データビュー

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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
スパムメール送信元 IP アドレス	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。
検出フィルタの種類	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)

表 B-49. スパムメール接続情報データビュー

データ	説明
実行された処理	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
スパムメール違反検出数	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、[スパムメール違反検出数] は「10」になります。

ポリシー/ ルール違反情報

詳細情報

ファイアウォールルール違反の詳細情報 (全体)

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-50. ファイアウォールルール違反の詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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

表 B-50. ファイアウォールルール違反の詳細情報 (全体) データビュー

データ	説明
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
セキュリティリスクレベル	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
送受信トラフィック / 接続	違反の侵入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 アドレス	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。
送信先ポート	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 アドレス	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。
実行された処理	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 : 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
ポリシー/ ルール違反検出数	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、[ポリシー/ ルール違反検出数] は「10」になります。

エンドポイントセキュリティ違反の詳細情報 (全体)

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。例 : 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

表 B-51. エンドポイントセキュリティ違反の詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
違反クライアントのホスト名	ポリシー/ ルールに違反するコンピュータのホスト名が表示されます。
違反クライアントの IP アドレス	ポリシー/ ルールに違反するコンピュータの IP アドレスが表示されます。
違反クライアントの MAC アドレス	ポリシー/ ルールに違反するコンピュータの MAC アドレスが表示されます。
違反ポリシー/ ルール	違反ポリシー/ ルールの名前が表示されます。
違反サービス	ポリシー/ ルールに違反するサービス / プログラムの名前が表示されます。
ログオンユーザ名	管理下の製品によってポリシー/ ルール違反が検出されたとき、クライア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	ネットワークを保護するために管理下の製品が実行するアクションが表示されます。例 : ブロック、リダイレクト、放置

表 B-51. エンドポイントセキュリティ違反の詳細情報 (全体) データビュー

データ	説明
修復処理	ポリシー違反を解決するために管理下の製品が実行するアクションが表示されます。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
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。
ポリシー/ ルール違反検出数	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、[ポリシー/ ルール違反検出数] は「10」になります。

エンドポイントセキュリティ遵守の詳細情報 (全体)

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-52. エンドポイントセキュリティ遵守の詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
遵守クライアントのホスト名	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。

表 B-52. エンドポイントセキュリティ遵守の詳細情報 (全体) データビュー

データ	説明
遵守クライアントの 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。
遵守クライアントの MAC 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 MAC アドレスが表示されます。
遵守ポリシー/ ルール	遵守ポリシー/ ルールの名前が表示されます。
遵守サービス	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。
ログオンユーザ名	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、クライア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。
ポリシー/ ルール遵守検出数	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、[ポリシー/ ルール遵守検出数] は「10」になります。

Web 違反情報

概要情報

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-53. Web 違反の概要 (全体) データビュー

データ	説明
違反ポリシー	URL が違反しているポリシーの名前が表示されます。

表 B-53. Web 違反の概要 (全体) データビュー

データ	説明
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
一意の違反クライアント数	指定のポリシーに違反するクライア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、[一意の違反クライアント数] は「4」になります。
一意の違反 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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」になります。
Web 違反検出数	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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」になります。

Web 違反クライアントホストの概要

特定のクライアントからの Web 違反検出の概要が表示されます。例 : 違反クライアントの 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-54. Web 違反クライアントホストの概要データビュー

データ	説明
違反クライアントのホスト	Web ポリシーに違反するクライアントの IP アドレス / ホスト名が表示されます。
一意の違反ポリシー数	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、[一意の違反ポリシー数] は「1」になります。

表 B-54. Web 違反クライアントホストの概要データビュー

データ	説明
一意の違反 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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」になります。
Web 違反検出数	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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」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-55. Web 違反 URL の概要データビュー

データ	説明
違反 URL	Web ポリシーに違反する URL が表示されます。
フィルタ / ブロックの種類	違反 URL へのアクセスを阻止するフィルタ / ブロックの種類が表示されます。例 : URL ブロック、URL フィルタ、Web ブロック
一意の違反クライアント数	指定のポリシーに違反するクライア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、[一意の違反クライアント数] は「4」になります。
Web 違反検出数	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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」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-56. 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
Web 違反検出数	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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」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、違反クライアントの数、ネットワーク上の Web 違反の総数

表 B-57. Web 違反検出の概要 (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。
一意の違反ポリシー数	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、[一意の違反ポリシー数] は「1」になります。

表 B-57. Web 違反検出の概要 (時間別推移) データビュー

データ	説明
一意の違反クライアント数	指定のポリシーに違反するクライア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、[一意の違反クライアント数] は「4」になります。
一意の違反 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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」になります。
Web 違反検出数	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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」になります。

詳細情報

Web 違反の詳細情報 (全体)

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。例 : 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

表 B-58. Web 違反の詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。

表 B-58. Web 違反の詳細情報 (全体) データビュー

データ	説明
管理下の製品の名前	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
送受信トラフィック / 接続	違反の侵入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
違反 URL	Web ポリシーに違反している URL の名前が表示されます。
クライアントホスト	ポリシーに違反しているクライアントの IP アドレス / 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
違反ポリシー	URL が違反しているポリシーの名前が表示されます。
違反ファイル	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。
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)。
実行された処理	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
Web 違反検出数	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、[Web 違反検出数] は「10」、[一意の違反 URL 数] は「1」になります。

脅威の兆候の情報

概要情報

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-59. 脅威の兆候の概要 (全体) データビュー

データ	説明
違反ポリシー/ 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
一意の脅威の兆候の送信先数	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、[一意の脅威の兆候の送信先数] は「2」になります。
一意の脅威の兆候の送信元数	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、[一意の脅威の兆候の送信元数] は「3」になります。
一意の脅威の兆候の受信者数	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、[一意の脅威の兆候の受信者数] は「2」になります。

表 B-59. 脅威の兆候の概要 (全体) データビュー

データ	説明
一意の脅威の兆候の送信者数	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、[一意の脅威の兆候の送信者数] は「3」になります。
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] は「10」になります。
軽減数	Network VirusWall Enforcer デバイスまたは Total Discovery Mitigation Server がアクションを実行するクライアント数が表示されます。
クリーンナップされたクライアント数	Total Discovery Mitigation Server が駆除を実行するクライアントの総数が表示されます。
クライアントのクリーンナップ率 (%)	[脅威の兆候の違反検出数] の総数との比較で、Total Discovery Mitigation Server が駆除を実行したクライア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-60. 脅威の兆候の送信元の概要データビュー

データ	説明
脅威の兆候の送信元 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。
一意の違反ポリシー/ 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/ ルールの数です。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、[一意の違反ポリシー/ ルール数] は「1」になります。
一意の脅威の兆候の送信先数	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、[一意の脅威の兆候の送信先数] は「2」になります。
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] は「10」になります。

最も脅威の兆候の多い送信先の概要

脅威の兆候が最も頻繁に検出されるクライア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-61. 最も脅威の兆候の多い送信先の概要データビュー

データ	説明
脅威の兆候の送信先 IP アドレス	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。
一意の違反ポリシー/ 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/ ルールの数です。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、[一意の違反ポリシー/ ルール数] は「1」になります。
一意の脅威の兆候の送信元数	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、[一意の脅威の兆候の送信元数] は「3」になります。
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] 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-62. 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
脅威の兆候の受信者	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。
一意の違反ポリシー/ 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/ ルールの数です。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、[一意の違反ポリシー/ ルール数] は「1」になります。
一意の脅威の兆候の送信者数	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、[一意の脅威の兆候の送信者数] は「3」になります。
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] 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-63. 脅威の兆候の送信者の概要データビュー

データ	説明
脅威の兆候の送信者	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。
一意の違反ポリシー/ 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/ ルールの数です。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、[一意の違反ポリシー/ ルール数] は「1」になります。
一意の脅威の兆候の受信者数	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、[一意の脅威の兆候の受信者数] は「2」になります。
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] 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-64. 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
プロトコル名	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
一意の違反ポリシー/ 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/ ルールの数です。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、[一意の違反ポリシー/ ルール数] は「1」になります。
一意の脅威の兆候の送信先数	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、[一意の脅威の兆候の送信先数] は「2」になります。
一意の脅威の兆候の送信元数	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、[一意の脅威の兆候の送信元数] は「3」になります。
一意の脅威の兆候の受信者数	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、[一意の脅威の兆候の受信者数] は「2」になります。

表 B-64. 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
一意の脅威の兆候の送信者数	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、[一意の脅威の兆候の送信者数] は「3」になります。
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] 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-65. 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
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。
一意の違反ポリシー/ 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/ ルールの数です。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、[一意の違反ポリシー/ ルール数] は「1」になります。
一意の脅威の兆候の送信先数	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、[一意の脅威の兆候の送信先数] は「2」になります。

表 B-65. 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
一意の脅威の兆候の送信元数	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、[一意の脅威の兆候の送信元数] は「3」になります。
一意の脅威の兆候の受信者数	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、[一意の脅威の兆候の受信者数] は「2」になります。
一意の脅威の兆候の送信者数	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、[一意の脅威の兆候の送信者数] は「3」になります。
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] は「10」になります。

詳細情報

脅威の兆候の詳細情報 (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 : 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-66. 脅威の兆候の詳細情報 (全体) 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。
管理下の製品の エンティティ表示名	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。
管理下の製品の名前	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
Mitigation Server エンティティ表示名	Mitigation Server のエンティティ表示名を表示します。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。
送受信トラフィック / 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
脅威の兆候の送信先 IP アドレス	脅威の兆候が影響を与えるクライアントの IP アドレスが表示されます。
脅威の兆候の送信先ポート	脅威の兆候が影響を与えるクライアントのポート番号が表示されます。

表 B-66. 脅威の兆候の詳細情報 (全体) データビュー

データ	説明
脅威の兆候の送信先 MAC アドレス	脅威の兆候が影響を与えるクライアントの MAC アドレスが表示されます。
脅威の兆候の送信元 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。
脅威の兆候の送信元ホスト名	脅威の兆候の発生元のホスト名が表示されます。
脅威の兆候の送信元ポート	脅威の兆候の発生元のポート番号が表示されます。
脅威の兆候の送信元 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。
ドメイン名	脅威の兆候の発生元のドメインが表示されます。
VLAN ID	脅威の兆候の発生元の VLAN ID が表示されます。
リスクの種類	管理下の製品が検出したセキュリティリスク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、不正行為
脅威の確実性レベル	脅威の兆候がネットワークにおよぼす危険度のレベルが表示されます (トレンドマイクロによる判定)。
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。
違反ポリシー/ 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。
脅威の兆候の受信者	脅威の兆候の受信者が表示されます。
脅威の兆候の送信者	脅威の兆候の送信者が表示されます。
メールの件名	スパイ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。
違反 URL	脅威の兆候と考えられる URL が表示されます。
ログオンユーザ名	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。
インスタントメッセンジャー/ IRC ユーザ名	Total Discovery Appliance 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。

表 B-66. 脅威の兆候の詳細情報 (全体) データビュー

データ	説明
インターネットブラウザ / 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 クライアントが表示されます。
チャネル名	メッセンジャーソフトウェアまたは IRC が通信に使用するプロトコルが表示されます。
疑わしいファイル	不審なファイルの名前が表示されます。
圧縮ファイル内の疑わしいファイル	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。
ファイルサイズ	不審なファイルのサイズが表示されます。
ファイル拡張子	不審なファイルの拡張子が表示されます。例 : .wmf、.exe、.zip
実ファイルタイプ	ファイルの拡張子ではなく、ファイルのヘッダを使用して検出した「実際の」ファイルタイプが表示されます。
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。
認証	認証が使用されたかどうかが表示されます。
bot コマンド	BOT が制御チャネルに送受信するコマンドが表示されます。
bot URL	BOT がコマンドを受信する URL が表示されます。
制約の種類	ファイルを正しく検索できない理由が表示されます。
実行された軽減処理	脅威の兆候に対して Mitigation Server が実行したアクションの結果が表示されます。
軽減結果の説明	脅威の兆候に対して Mitigation Server が実行したアクション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
脅威の兆候の違反検出数	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、[脅威の兆候の違反検出数] は「10」になります。

脅威情報 (全体)

完全なネットワークセキュリティリスク分析情報

デスクトップに影響する全体的なセキュリティリスクの情報が表示されます。例 : セキュリティリスクの名前、セキュリティリスク検出の総数、影響を受けるクライアント数

表 B-67. 完全なネットワークセキュリティリスク分析情報データビュー

データ	説明
セキュリティリスクカテゴリ	管理下の製品が検出したセキュリティリスクのさまざまなカテゴリが表示されます。例 : ウイルス、スパイウェア、フィッシング対策
セキュリティリスク名	管理下の製品が検出したセキュリティリスクの名前が表示されます。
検出ポイントの種類	管理下の製品によって検出されたセキュリティリスク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)
一意のセキュリティリスク / 違反送信先数	セキュリティリスク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、[セキュリティリスク / 違反検出数] は「10」、[一意のセキュリティリスク / 違反送信先数] は「2」になります。
一意のセキュリティリスク / 違反送信元数	セキュリティリスク / 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、[セキュリティリスク / 違反検出数] は「10」、[一意のセキュリティリスク / 違反送信元数] は「3」になります。

表 B-67. 完全なネットワークセキュリティリスク分析情報データビュー

データ	説明
セキュリティリスク / 違反検出数	管理下の製品が検出したセキュリティリスク / 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、[セキュリティリスク / 違反検出数] は 10 で、[一意のウイルス / 不正プログラム数] は「1」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リスク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)、セキュリティリスクの種類、影響を受けるクライアント数

表 B-68. ネットワーク保護境界情報データビュー

データ	説明
管理下の製品のカテゴリ	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
管理下の製品の名前	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
セキュリティリスクカテゴリ	管理下の製品が検出したセキュリティリスクのさまざまなカテゴリが表示されます。例 : ウイルス、スパイウェア、フィッシング対策
一意のセキュリティリスク / 違反送信先数	セキュリティリスク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、[セキュリティリスク / 違反検出数] は「10」、[一意のセキュリティリスク / 違反送信先数] は「2」になります。

表 B-68. ネットワーク保護境界情報データビュー

データ	説明
一意のセキュリティリスク / 違反送信元数	セキュリティリスク / 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、[セキュリティリスク / 違反検出数] は「10」、[一意のセキュリティリスク / 違反送信元数] は「3」になります。
セキュリティリスク / 違反検出数	管理下の製品が検出したセキュリティリスク / 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、[セキュリティリスク / 違反検出数] は 10 で、[一意のウイルス / 不正プログラム数] は「1」になります。

セキュリティリスク検出ポイント分析情報

検出ポイントに焦点を当てたセキュリティリスク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)、セキュリティリスクの名前、最後にセキュリティリスクが検出された時間

表 B-69. セキュリティリスク検出ポイント分析情報データビュー

データ	説明
検出ポイントの種類	管理下の製品が検出したセキュリティリスク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
管理下の製品の名前	セキュリティリスク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
セキュリティリスクカテゴリ	管理下の製品が検出したセキュリティリスクのカテゴリが具体的に表示されます。例 : ウイルス、スパイウェア対策、コンテンツフィルタリング

表 B-69. セキュリティリスク検出ポイント分析情報データビュー

データ	説明
一意のセキュリティリスク / 違反送信先数	セキュリティリスク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、[セキュリティリスク / 違反検出数] は「10」、[一意のセキュリティリスク / 違反送信先数] は「2」になります。
一意のセキュリティリスク / 違反送信元数	セキュリティリスク / 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、[セキュリティリスク / 違反検出数] は「10」、[一意のセキュリティリスク / 違反送信元数] は「3」になります。
セキュリティリスク / 違反検出数	管理下の製品が検出したセキュリティリスク / 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、[セキュリティリスク / 違反検出数] は 10 で、[一意のウイルス / 不正プログラム数] は「1」になります。

セキュリティリスク送信先分析情報

感染したクライアントに焦点を当てた情報が表示されます。例 : クライアントの名前、ネットワークにセキュリティリスクが侵入したさまざまな方法、感染したクライアント数

表 B-70. セキュリティリスク送信先分析情報データビュー

データ	説明
セキュリティリスク / 違反送信先	セキュリティリスク / 違反の影響を受けるコンピュータの名前が表示されます。

表 B-70. セキュリティリスク送信先分析情報データビュー

データ	説明
セキュリティリスクカテゴリ	管理下の製品が検出したセキュリティリスクのさまざまなカテゴリが表示されます。例 : ウイルス、スパイウェア、フィッシング対策
セキュリティリスク名	管理下の製品が検出したセキュリティリスクの名前が表示されます。
セキュリティリスク / 違反検出数	管理下の製品が検出したセキュリティリスク / 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、[セキュリティリスク / 違反検出数] は「10」になります。
最終感染 / 違反日時	セキュリティリスク / 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リスク / 違反が検出された日時が表示されます。

セキュリティリスク送信元分析情報

セキュリティリスクの発生元に焦点を当てた情報が表示されます。例 : セキュリティリスクの発生元の名前、ネットワークにセキュリティリスクが侵入したさまざまな方法、感染したクライアント数

表 B-71. セキュリティリスク送信元分析情報データビュー

データ	説明
セキュリティリスク / 違反送信元	セキュリティリスク / 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。
セキュリティリスクカテゴリ	管理下の製品が検出したセキュリティリスクのさまざまなカテゴリが表示されます。例 : ウイルス、スパイウェア、フィッシング対策
セキュリティリスク名	管理下の製品が検出したセキュリティリスクの名前が表示されます。

表 B-71. セキュリティリスク送信元分析情報データビュー

データ	説明
セキュリティリスク / 違反検出数	管理下の製品が検出したセキュリティリスク / 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、[セキュリティリスク / 違反検出数] は「10」になります。
最終感染 / 違反日時	セキュリティリスク / 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リスク / 違反が検出された日時が表示されます。

索引

英数字

あ

か

さ

た

な

は

ま

や

ら