# Trend Micro
# Control Manager™

安心を、ひとつ上のステージへ。

TREND MICRO™

インストールガイド

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

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、GateLock、VSAPI、eDoctor、eManager、Trend Micro Policy Server、トレンドマイクロ・プレミアム・サポート・プログラム、Certified Rescue Partner、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、RBL+、Phish Checker、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPS、LEAKPROOFは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 1998-2008 Trend Micro Incorporated. All rights reserved.

P/N: TMCMFF-AE0104 (2008/6)

# 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。


- 10 ページの「レポート機能およびログ機能の向上」
- 10 ページの「ユーザアクセス管理の向上」
- 11 ページの「製品ディレクトリの管理および監視の向上」
- 11 ページの「インテリジェントなコンポーネント監視」
- 12 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<br>• 1.5+SP1 |
| InterScan Messaging Security Suite | • 7.0<br>• 7.0+SP1 |
| InterScan Web Security Appliance | 3.0 |
| InterScan Web Security Suite | 3.0 |
| InterScan WebProtect for ISA | • 5.0<br>• 5.01 |
| Network VirusWall Enforcer 2500 | 2.0 |
| Network VirusWall Enforcer 1200 | 2.0 |
| InterScan Messaging Security Appliance 5000 | • 1.0<br>• 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<br>• 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。<br>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。<br><br>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。<br>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。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。 |
| **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。<br>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。 |
| **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。<br>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。 |
| 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。 |

# 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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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、27 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。<br>• 管理下の製品の設定やログを保存する SQL データベース<br>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。<br>• Control Manager 管理コンソールのホストとなる Web サーバ<br>• 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<br>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。<br>• 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)<br>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。<br>MCP は、Control Manager システムの新しいバックボーンとなります。<br>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。<br>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。<br>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。<br>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。

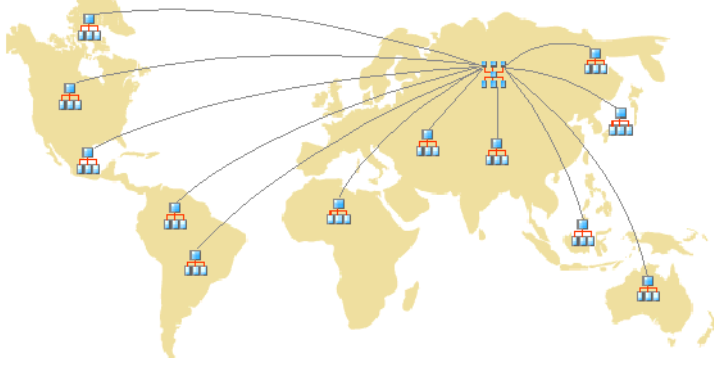


**図 2-1.　Control Manager アドバンス版の上位サーバおよび複数の下位サーバ**

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。

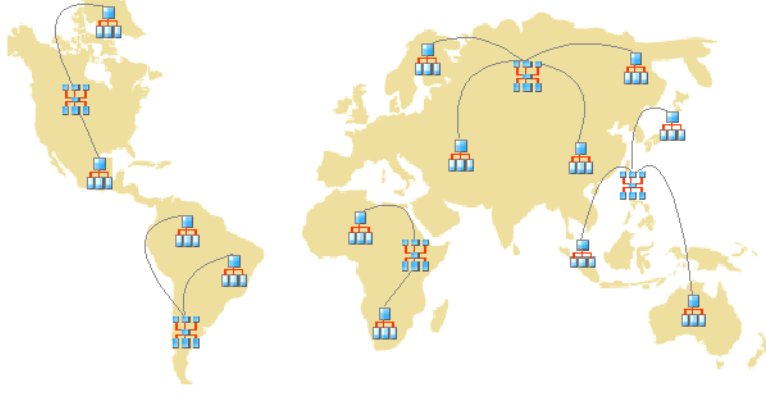
各ネットワークの構成に応じて、上記以外に処置すべきことが発生する場合もあります。

# 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<br>・Windows 2000 Server<br>・Windows 2000 Advanced Server<br>・Windows NT 4.0 + Service Pack 3<br>・Windows NT Server 4.0<br>(Service Pack 6a 以上)<br>・Microsoft Windows Server 2003<br>Standard Edition/Enterprise Edition | ・Novell Desktop 9<br>・AIX<br>・Red Hat Linux 6.2、7.1、7.2<br>・RedHat Enterprise Linux 4.3<br>・Turbolinux 6.5、7.0<br>・SuSE Linux 6.3、7.2、7.3<br>・SuSE Enterprise 9.2<br>・AS/400<br>・OS390<br>・その他 GateLock、Linux 6.x kernel、<br>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、44 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<br>・シングル CPU<br>・デュアル CPU<br>・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<br>・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)<br>・300MB 以上 (SQL 2005 Express 用、任意) |

| ソフトウェア | 最小要件 |
|---|---|
| OS | ・Microsoft Windows 2000 Server (Service Pack 3 または Service Pack 4)<br>・Windows 2000 Advanced Server (Service Pack 3 または Service Pack 4)<br>・Windows 2003 Server Standard Edition (Service Pack 1 または Service Pack 2)<br>・Windows 2003 Server Standard Edition R2 パッチなしまたは Service Pack 2<br>・Windows 2003 Server Enterprise Edition (Service Pack 1 または Service Pack 2)<br>・Windows 2003 Server Enterprise Edition R2 パッチなしまたは Service Pack 2<br>・WOW (Windows 2003 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)<br>・Microsoft IIS サーバ 6.0 (2003 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)<br>・Microsoft SQL Server 2000 (Service Pack 3 以上を推奨)<br>・Microsoft SQL Server 2005 |
| その他 | ・Microsoft .NET Framework 2.0 (Control Manager のパッケージに同梱)<br>・Windows Installer 3.1 (Control Manager のパッケージに同梱)<br>・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)<br>・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) |

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

| | |
|---|---|
| **管理コンソール** | • ブラウザ — Windows Internet Explorer 6 以上<br>• Java VM — Microsoft 版 5.0.0.3805 以上 |

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

| | 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 |

**表 3-3. 連携する運用管理ツール**

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、96 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。

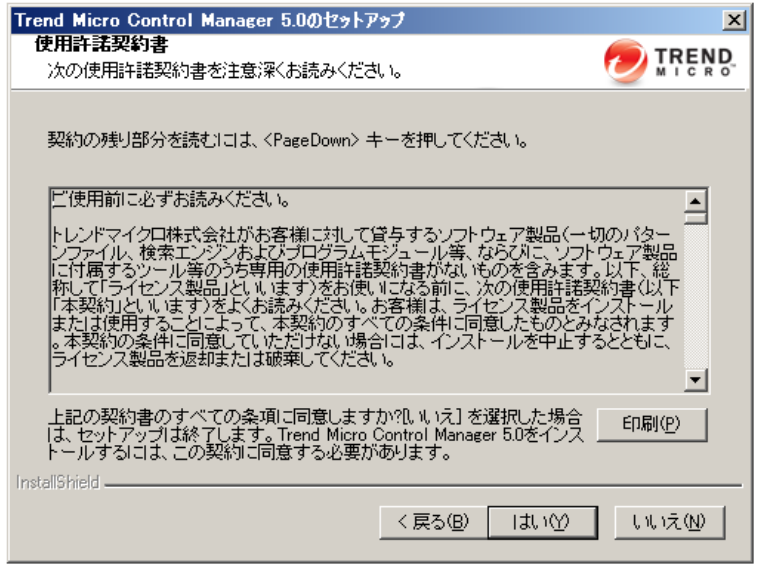



**図 3-1. 契約事項に同意する場合は [ はい ] をクリックします。**

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。

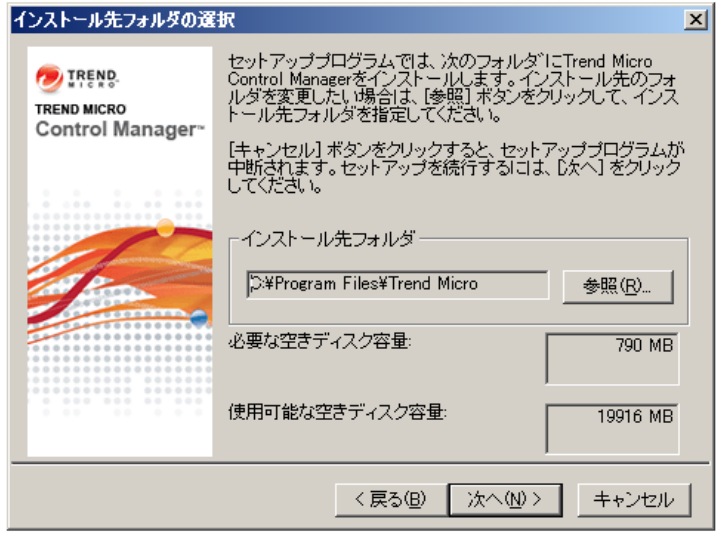



**図 3-3. インストール先フォルダの選択**

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。

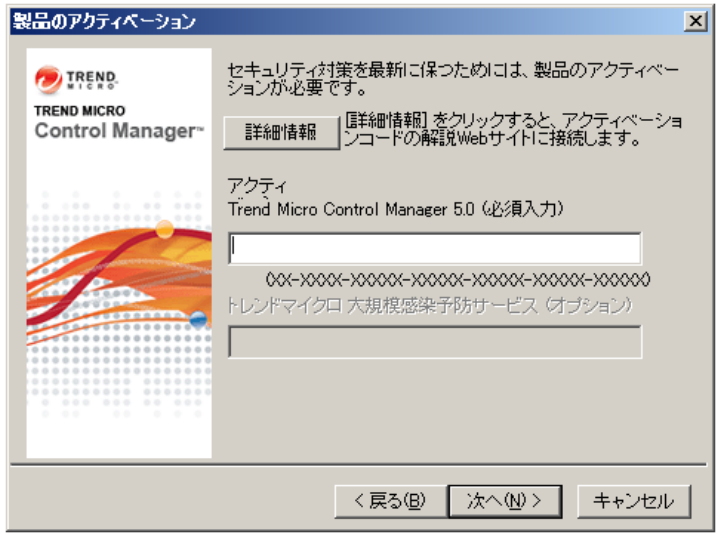



**図 3-4. Control Manager およびサービスを有効にするアクティベーションコードの入力**

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。

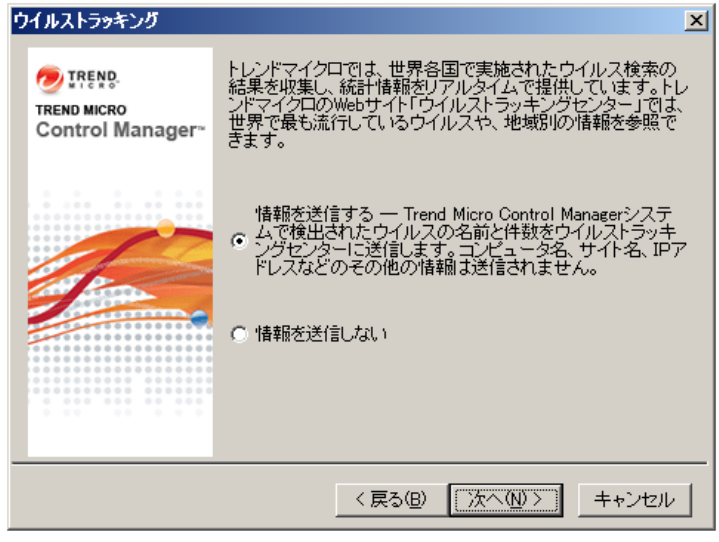



**図 3-5. ウイルストラッキングセンターへのウイルス情報送信**

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。

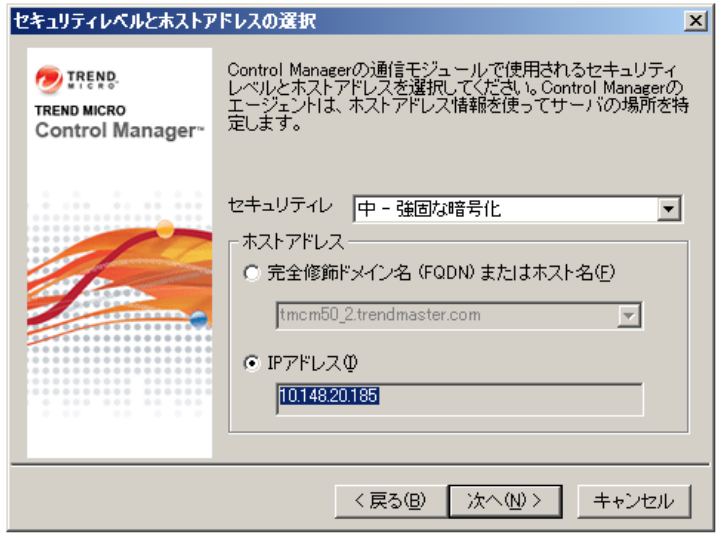



**図 3-6. セキュリティレベルの選択**

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。

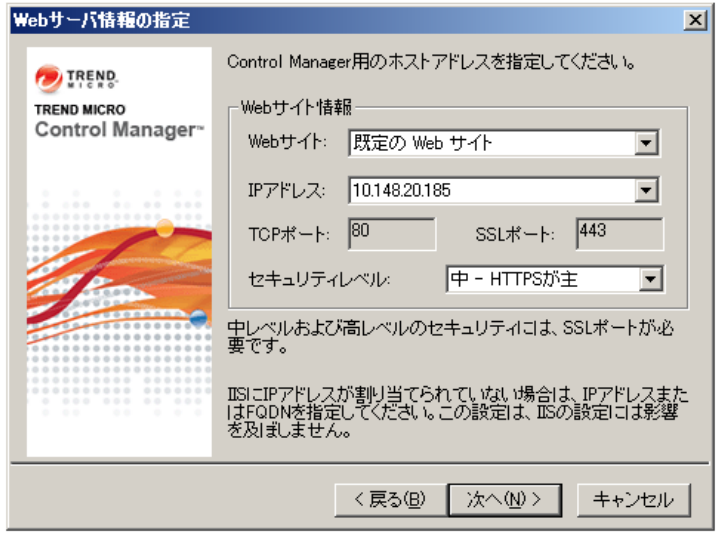



**図 3-7. Web サーバ情報の指定**

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。

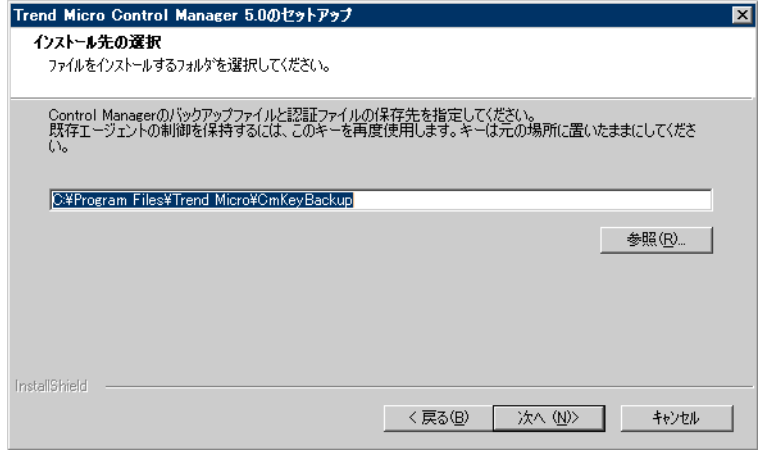



**図 3-8. バックアップファイルと認証ファイルの保存場所の選択**

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、92 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。

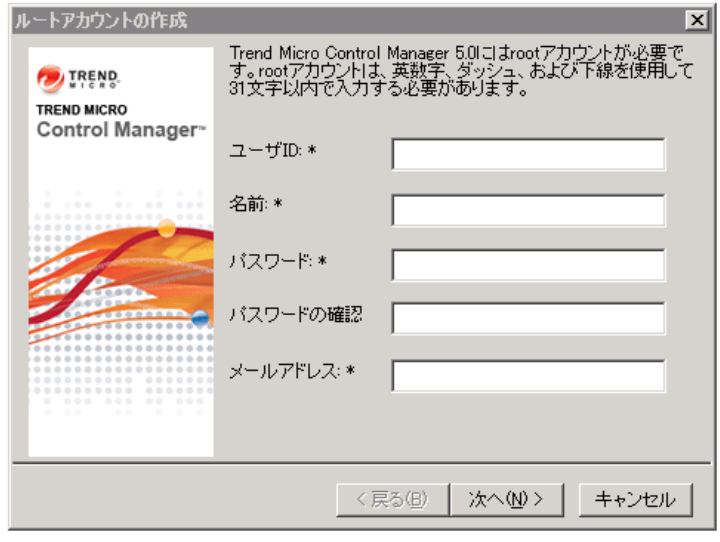



**図 3-10.　root アカウントのセットアップとプロキシサーバの設定**

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。

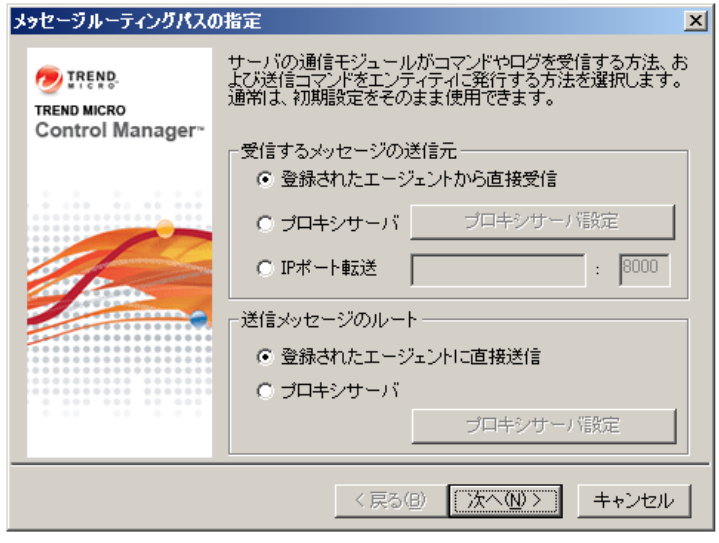



図 3-11. メッセージまたは要求のルートの定義

**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。プロキシの使用と設定の詳細については、182 ページの「プロキシの設定」を参照してください。
- 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。プロキシの使用と設定の詳細については、182 ページの「プロキシの設定」を参照してください。

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、80 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<br><br>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 92 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、96 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<br><br>(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¥*.*<br><br>¥Program Files¥Trend Micro¥Control Manager¥DataSource.xml<br><br>¥Program Files¥Trend Micro¥Control Manager¥CascadingLogConfiguration.xml<br><br>¥Program Files¥Trend Micro¥Control Manager¥Settings¥DMregisterinfo.xml<br><br>¥Program Files¥Trend Micro¥Control Manager¥EntityEmulator.xml<br><br>¥Program Files¥Trend Micro¥Control Manager¥ProductUIHandler.xml<br><br>¥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<br><br>¥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<br><br>HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥TMI<br><br>HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥CommonCGI<br><br>HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥TMCM<br><br>HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥TMI<br><br>HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥MSDE<br><br>HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥MSDE<br><br>HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥MSSQLServer<br><br>HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TMCM<br><br>HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendMicro_NTP<br><br>HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendMicro Infrastructure<br><br>HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TrendCCGI<br><br>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、96 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<br>**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<br>**エージェント** : **エージェントの混在** | Control Manager エージェント :<br>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。<br>MCP<br>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。40 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

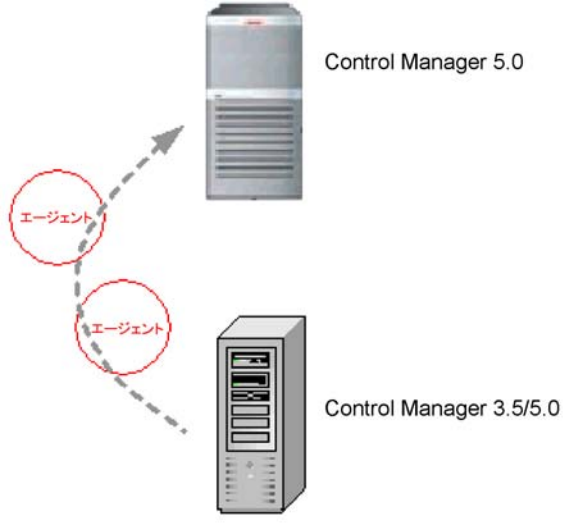



**図 4-1. 単一サーバに属するエージェントの移行**

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。86 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

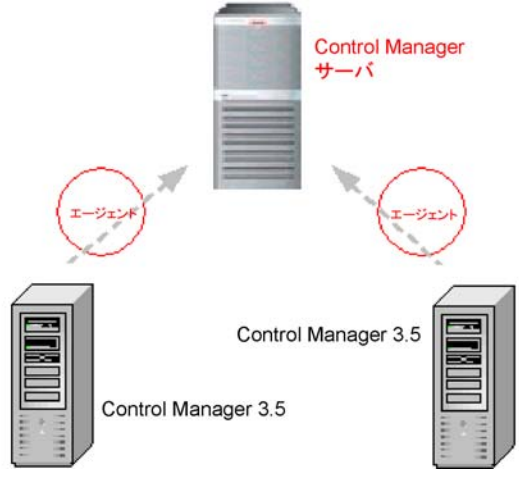



**図 4-2.　複数のサーバに属するエージェントの移行**

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、-99 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 CFG_DM_DB_PWD の値を暗号化します。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. テキストエディタを使用して、C:¥Program Files¥Trend Micro¥COMMON¥TMI¥TMI.cfg を開きます。

   **注意：** 元の設定に戻すことができるように TMI.cfg のバックアップを作成します。

4. CFG_DM_DB_DSN=Server= パラメータを移行先の SQL Server の名前に置き換えます。

5. 現在の ID とパスワードをそのまま使用します。ID とパスワードは、次のパラメータで指定されています。

   CFG_DM_DB_ID
   CFG_DM_DB_PWD

6. TMI.cfg を保存し閉じます。

7. [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。

8. [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。

9. [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。

10. 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。

11. TMI.cfg 内のものと同じ「ID」と「パスワード」を入力し、[次へ] をクリックします。表示される画面で [次へ] をクリックします。

12. [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。

13. [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。

14. 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

# 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 (101 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 6 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 6-1. 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 6-2. 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。

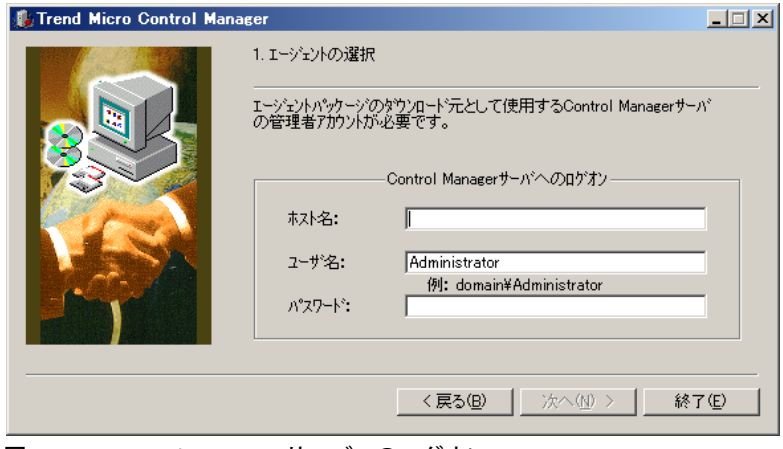



図 6-3. Control Manager サーバへのログオン

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。

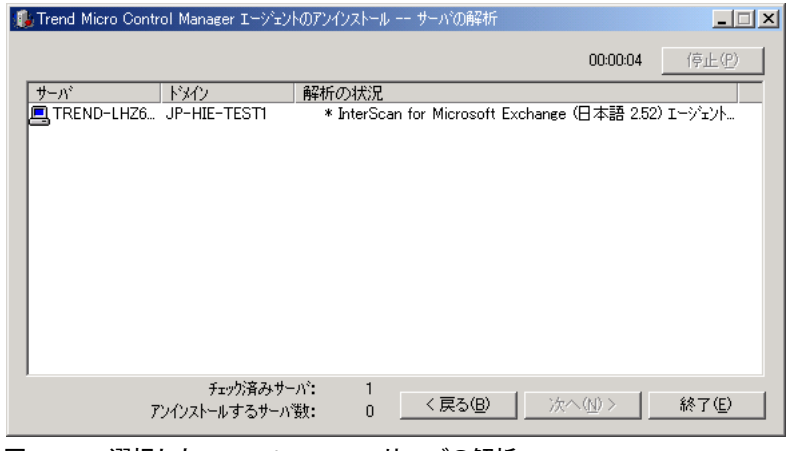



**図 6-4. 選択した Control Manager サーバの解析**

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 7 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。

# 索引

## 英数字

## あ

## か



## さ



## た

## な



## は



## や



## ら