

Trend Micro InterScan™ for Microsoft Exchange



クイックスタートガイド



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、スパイバスター、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPS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 © 1998-2007 Trend Micro Incorporated. All rights reserved.

P/N: SMEXFF-AE0104 (2007/07)

目次

はじめに	11
ドキュメント	12
対象読者	13
 第 1 章 製品の概要	15
機能と利点	16
新しい機能	18
バージョンの比較	23
InterScan のテクノロジー	24
ウイルス検索エンジン	24
ウイルス検索エンジンのアップデート	25
ウイルスパターンファイル	26
パターンファイルの番号	26
ウイルス検索エンジンでのウイルスパターンファイルの使用法	27
アップデートについて	27
パターンファイルの差分アップデート	27
InterScan でのアップデートの使用法	28
トレンドマイクロの推奨設定	28
トレンドマイクロの推奨処理	29
スパムメール検索エンジンとスパムメール判定ルール	29
 第 2 章 製品のインストールと削除	31
最小要件	32
開始する前に	35
パイロットインストール	35

適切なテストサイトの作成	35
ロールバック計画の準備	36
パイロットインストールの実行と評価	37
導入計画	37
ネットワークトラフィックに関する考慮事項	38
複数のサーバへの InterScan の導入	38
複数の LAN セグメントへの InterScan の導入	41
インストールの準備	42
アップグレード時の設定の例外	42
エンドユーザメール隔離	43
Trend Micro Control Manager エージェント	44
アクティベーションコード	45
インストール前のチェックリスト	46
新規インストールの実行	47
クラスタ環境でのインストール	47
InterScan 8.0 へのアップグレード	47
クラスタ環境でのアップグレード	49
セットアッププログラムの実行	49
Exchange 2000 Server および Exchange Server 2003 環境でのインストール .	49
Exchange Server 2007 ハブトランスポート / メールボックスサーバ環境でのインストール ...	69
Exchange Server 2007 エッジトランスポートサーバ環境でのインストール	86
クラスタ環境でのインストール	103
インストール後の処理	103
正常にインストールされたことの確認	103
インストール後のテスト	105
サイレントインストール	107
サイレントインストールの制限	109
サイレントインストールの実行	109

InterScan のアンインストール	110
製品 CD-ROM を使用したアンインストール	112
Windows コントロールパネルを使用したアンインストール	120
クラスタ環境での InterScan のアンインストール	122
第 3 章 製品の登録、アクティベーション、アップデート	125
InterScan のアクティベーション	126
アクティベーションの実行	126
アクティベーションコード	126
InterScan のアップデート	129
クラスタ環境でのアップデート	131
プロキシサーバの設定	131
コンポーネントの手動アップデート	132
予約アップデートの設定	133
ダウンロード元	134
コンポーネントのロールバック	136
第 4 章 製品の管理	139
製品コンソールの使用	140
管理コンソールのメインビュー	140
製品コンソールの構成要素	141
製品コンソールの起動	144
クラスタ上の仮想サーバの表示	145
リアルタイムモニタの概要	145
サーバ管理の概要	147
サーバ管理のアクティベーション	149
サーバ管理を使用した設定の複製	149

仮想サーバの InterScan リソースの手動作成	151
第 5 章 Exchange サーバのセキュリティの確立と維持.....	155
セキュリティの確立	156
セキュリティの維持	157
InterScan のアップデート	159
大規模感染の状況の管理	160
第 6 章 サポートと問い合わせ	163
製品サポート情報	164
サポートサービスについて	164
製品 Q&A のご案内	165
セキュリティ情報	166
セキュリティ情報の入手先	166
トレンドマイクロへのウイルス解析依頼	167
ウイルス解析サポートセンター「TrendLabs」	167
第 7 章 Exchange 環境に対する脅威の概要.....	169
用語の説明	170
ウイルス / 不正プログラム	170
ワーム	172
トロイの木馬型プログラム	172
ジョークプログラム	173
マスメーリング型ウイルス	173
圧縮ファイル	174
マクロウイルス / 不正プログラムについて	175
スパイウェア / グレーウェア	176

InterScan による Exchange 環境の保護	178
付録 A Windows イベントログコード	179
付録 B 事前設定ファイル.....	183
付録 C Trend Micro Control Manager について	187
Control Manager の基本機能	188
Trend Micro Management Communication Protocol について	189
ネットワーク負荷とパッケージサイズの低減	190
NAT およびファイアウォール環境のサポート	191
HTTPS サポート	192
一方向および双方向通信のサポート	192
一方向通信	193
双方向通信	193
シングルサインオン (SSO) サポート	193
クラスタノードのサポート	194
Control Manager エージェントハートビート	194
スケジュールバーの使用	195
適切な接続ステータス設定について	196
Control Manager への InterScan の登録	197
Control Manager による InterScan の管理	198
製品ディレクトリについて	198
InterScan の初期設定フォルダへのアクセス	201
製品ディレクトリへのアクセス	201
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	202
InterScan のステータス概要の表示	203

InterScan と管理下の製品の設定	204
InterScan と管理下の製品に対するタスクの実行	205
InterScan と管理下の製品ログのクエリと表示	206
製品ディレクトリから削除された InterScan の再登録	208
InterScan、製品ディレクトリフォルダ、またはコンピュータの検索	209
製品ディレクトリの表示の更新	210
ディレクトリ管理について	210
ディレクトリ管理のオプションの使用	211
ディレクトリ管理へのアクセス	212
フォルダの作成	212
フォルダまたは InterScan の名前変更	212
フォルダまたは InterScan の移動	213
ユーザ定義フォルダの削除	213
ショートカットについて	214
ショートカットとは	214
ショートカットへのアクセス	215
ショートカットへの InterScan の追加	215
ショートカットからの InterScan の削除	217
Control Manager からの新しいコンポーネントのダウンロードと配信	218
アップデート管理について	219
手動ダウンロードについて	219
コンポーネントの手動ダウンロード	220
予約ダウンロードの除外設定	227
予約ダウンロードについて	227
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	228
レポートの使用	235
ローカルレポート	235
広域レポート	236

レポートテンプレートについて	236
レポートプロファイルについて	238
レポートプロファイルの作成	238
レポートプロファイルの設定の確認	244
予約レポートプロファイルの有効化	245
オンデマンド予約レポートの作成	245
作成されたレポートの表示	246
 付録 D 用語集.....	 249
 索引	 257

はじめに

本書では、Exchange サーバを保護する Trend Micro InterScan for Microsoft Exchange (以下、InterScan) 8.0 を導入する際に、実行する必要があるタスクに関する基本的な情報が記載されています。本書は、InterScan の計画、導入、テストを行う、InterScan の初心者ユーザおよび上級ユーザを対象としています。

ここでは、次のトピックについて説明しています。

- 12 ページの「ドキュメント」
- 12 ページの「本書について」
- 13 ページの「対象読者」
- 13 ページの「ドキュメントの表記規則」

ドキュメント

InterScan には、次のドキュメントが付属しています。

- オンラインヘルプ — InterScan の Web コンソールから参照できる、Web ベースのドキュメントです。
オンラインヘルプでは、InterScan のコンポーネントと機能について説明します。
- クイックスタートガイド — InterScan の製品 CD-ROM に収録されている PDF 形式のドキュメントです。トレンドマイクロの Web サイトからもダウンロードできます。

ヒント：ドキュメントおよびプログラムファイルの最新版については、最新版ダウンロードサイト (<http://www.trendmicro.co.jp/download>) から該当するリンクにアクセスしてチェックすることをお勧めします。

本書について

「Trend Micro InterScan for Microsoft Exchange クイックスタートガイド」では、次の項目について説明します。

- 「製品の概要」 — InterScan の機能の概要。
- 「製品のインストールと削除」 — InterScan のインストールおよび削除の手順。
- 「製品の登録、アクティベーション、アップデート」 — InterScan のアクティベーションとアップデートの手順。
- 「製品の管理」 — InterScan サーバの管理に関する情報。
- 「Exchange サーバのセキュリティの確立と維持」 — Exchange 環境の安全性を確保する方法に関する情報。
- 「サポートと問い合わせ」 — サポート情報の検索に関する情報。
- 「Exchange 環境に対する脅威の概要」 — セキュリティリスクに関する情報。

対象読者

InterScan のドキュメントは、以下を含むセキュリティシステムについて基本的な知識があることを前提としています。

- ウイルス対策およびコンテンツセキュリティ保護
- スпамメール保護
- ネットワークに関する概念 (IP アドレス、ネットマスク、トポロジ、LAN 設定など)
- さまざまなネットワークトポロジ
- Microsoft Exchange Server 管理
- Microsoft Exchange Server 2007 サーバの役割の設定
- さまざまなメッセージ形式

ドキュメントの表記規則

情報を簡単に検索し、理解できるように、ドキュメントでは、次の表記規則を使用しています。

表記	説明
注意：	設定上の注意
ヒント：	推奨事項
警告：	避けるべき操作や設定についての注意

表 1. 本書で使用している表記規則

製品の概要

この章では、Microsoft Exchange (以下、Exchange) 2000、2003、および 2007 メールサーバを保護する Trend Micro InterScan for Microsoft Exchange Server (以下、InterSan) 8.0 の機能について説明します。InterScan をインストールすることによって、ウイルス / 不正プログラム、トロイの木馬、ワーム、スパイウェア / グレーウェアからサーバを保護できます。また InterScan は、スパムメールや望ましくないコンテンツを含むメッセージを排除することにより、業務効率やネットワークの整合性を維持します。InterScan の通知は、重大なシステムイベントまたはアウトブレイクの活動が発生するたびに、管理者またはその他の指定したユーザにタイムリーに警告を送信します。

注意： 本製品には**通常版**および**アドバンス版**の 2 種類があります。コンテンツフィルタおよびスパムメール対策機能は、**アドバンス版**でのみ使用できます。

この章の内容は次のとおりです。

- 16 ページの「機能と利点」
- 18 ページの「新しい機能」
- 24 ページの「InterScan のテクノロジー」
- 27 ページの「アップデートについて」

機能と利点

InterScan の機能によって次の利点を得ることができます。

高速で簡単なインストール

- 1 つのインストールプログラムを使用して 1 台または複数の Microsoft Exchange サーバにインストールできます。
- クラスタ環境にインストールできます。

強力な独自のウイルス対策機能

- Exchange 2000、2003、および 2007 サーバに対して SMTP 検索 (トランスポート 検索) ができます。
- Microsoft Virus Scanning API を利用して、Exchange ストアの下位レベルでメッセージを検索できます。
- メモリ上での検索をマルチスレッドで実行することによって、メッセージを素早く検索できます。
- ウイルス / 不正プログラム、トロイの木馬、およびワームを検出し、処理できます。
- スパイウェア / グレーウェアを検出し、処理できます。
- 実際のファイルタイプを識別して、拡張子を偽ったファイルも適切に検出できます。
- ウイルス / 不正プログラムに対してトレンドマイクロの推奨処理を使用したり、処理をカスタマイズできます。
- すべてのマクロウイルス / 不正プログラムを検出して削除したり、ヒューリスティックルールを使用してこれらを処理できます。

添付ファイルのブロック

- 指定した添付ファイルをブロックしたり、ファイルタイプ別に添付ファイルをブロックできます。

コンテンツフィルタ (アドバンス版のみ)

- ルールベースのフィルタを使用して、嫌がらせ、攻撃、および他の好ましくないと見なされるメッセージコンテンツを排除できます。

スパムメール対策 (アドバンス版のみ)

- 検出レベルを調整できるスパムメール対策フィルタを使用して、スパムメールを排除するとともに、メッセージの誤検出を削減できます。
- サーバ側で設定するルールを使用して、クライアントによって管理される承認する送信者リストを制御できます。

隔離

- 疑わしいメールを隔離するよう InterScan を設定できます。
- 隔離イベントのログを検索し、安全であると判断した場合は隔離されたメッセージを再送信できます。

Web ベースの製品コンソール

- SSL を使用して、セキュリティで保護された製品コンソールからリモートサーバにアクセスできます。

通知

- カスタマイズ可能な通知を使用して、InterScan の処理に関する警告を管理者に送信できます。
- 大規模感染や重大なシステムイベントが発生するたびに、指定した受信者に通知できます。

タイムリーで役立つレポートとログ

- システムイベント、ウイルス / 不正プログラム、およびプログラムのアップデートイベントの詳細なログを使用して最新の状態を保持し、グラフィカルなレポートを印刷またはメール送信できます。

アップデート

- 予約または手動でコンポーネントアップデートを実行できます。アップデート元はカスタマイズ可能です。

新しい機能

本バージョンの InterScan には、次の新機能があります。

Microsoft Operations Manager (MOM) 2005 のサポート

本バージョンの InterScan では、すべてのアプリケーションの統合情報を管理できる Microsoft Operations Manager (MOM) 2005 をサポートしています。InterScan では、重要な情報に対する MOM アラート機能をサポートしています。

Trend Micro Control Manager 3.5 との統合

本バージョンの InterScan では、次のバージョンの Trend Micro Control Manager (以下、Control Manager) をサポートしています。

- Control Manager 3.5 (Build 1347) + Patch 2 (Build 1411)

InterScan 8.0 と Control Manager 間の通信には、Trend Micro Control Manager Management Communication Protocol (MCP) エージェントと呼ばれる新しいプロトコルが使用されます。旧バージョンの InterScan と Control Manager で使用されていた Trend Micro Management Infrastructure (TMI) プロトコルは、InterScan 8.0 ではサポートされていません。InterScan 8.0 では、Control Manager からのシングルサインオンをサポートしています。InterScan の製品コンソールには、Control Manager の製品コンソールから直接アクセスできます。InterScan 製品コンソール用のユーザ名とパスワードを別途入力する必要はありません。

Outlook 迷惑メール対策との統合とエンドユーザメール隔離との統合のサポート

Exchange 2000 Server および Exchange Server 2003 に対しては、InterScan 8.0 は「Outlook 迷惑メール対策との統合」ソリューションと「エンドユーザメール隔離との統合」ソリューションを提供します。インストール時にどちらかのソリューションを選択できます。

Outlook 迷惑メール対策との統合ソリューションでは、インテリジェントメッセージフィルタ (IMF) による評価が使用されます。Exchange 2000 Server の場合、インテリジェントメッセージフィルタ (IMF) はインストールできないため、「Outlook 迷惑メール対策との統合」は Exchange 2000 Server で使用する InterScan ではサポートされていません。

迷惑メールフォルダの統合

本バージョンの InterScan では、検出されたスパムメールを標準の Outlook フォルダに送信することを選択できます。独立したスパムメールフォルダを作成する必要はなくなりました。

手動レポートと予約レポートでのサーバ名

手動レポートおよび予約レポートにサーバ名を追加することによって、複数のサーバを管理している場合にレポートのソースを区別できます。

Microsoft Exchange Server 2007 のサポート

本バージョンの InterScan では、Microsoft Exchange Server 2007 の以下のサーバの役割をサポートしています。

- エッジトランスポートサーバの役割
- ハブトランスポートサーバの役割
- メールボックスサーバの役割
- サーバの役割の組み合わせ (メールボックスサーバ + ハブトランスポートサーバ)
- クラスタ化メールボックスサーバの役割

InterScan はサーバの役割ごとに異なる機能を実行します。

注意： InterScan では、クライアントアクセスサーバの役割はサポートしていません。

基本的なインストール

InterScan 8.0 では、標準の新規インストールおよびビルドアップグレードの他に、InterScan 7.0 から InterScan 8.0 へのアップグレードをサポートしています。

インストールプロセスの改善

本バージョンの InterScan では、インストールプロセスが効率よく実行されるように、インストール機能が強化されています。

- InterScan 8.0 は、サイレントインストール機能を備えているため、事前定義されたテキストファイルを使用して、プロンプトなしに InterScan 8.0 をインストールできるため、ローカル配信を簡単に実行できます。

- Control Manager エージェントとエンドユーザメール隔離のインストールは、InterScan のインストールおよびアンインストールプロセスと統合されています。

注意：InterScan 8.0 では、Exchange 2000 Server および Exchange Server 2003 に対してのみエンドユーザメール隔離をサポートしています。

- InterScan 8.0 をインストールするには、ローカル管理者以上の権限が必要です。

検索不能メッセージ部分に対応する新たなカテゴリ

InterScan 8.0 では、検索不能なメッセージ件数とウイルス件数を区別します。

検索不能ファイルには、[検索の制限条件] の設定の範囲外のファイル、暗号化されたファイル、およびパスワードで保護されたファイルが含まれます。本バージョンの InterScan では、概要、ログ、リアルタイムモニタ、レポート、および通知において検索不能ファイルを表す「検索不能なメッセージ部分」という新しいカテゴリが導入されました。

新たな [メッセージ部分の隔離] 処理オプションの追加

ウイルス検索、添付ファイルブロック、およびコンテンツフィルタに [メッセージ部分の隔離] 処理オプションが追加されました。旧バージョンの InterScan では、利用可能な処理オプションは [メッセージ全体の隔離] だけでした。

コンテンツフィルタログの改善

本バージョンの InterScan では、キーワードが一致した場合にコンテンツフィルタログ内にキーワードが表示されます。キーワードまたは正規表現が長すぎる場合、情報の一部はログに表示されません。

IntelliTrap

本バージョンの InterScan では、IntelliTrap テクノロジーが導入されています。IntelliTrap では、パッキングアルゴリズムの検索によってパックされたファイルが検出されます。

InterScan で IntelliTrap を有効にすることによって、ウイルスに感染した添付ファイルに対してユーザ定義の処理を実行し、送信者、受信者、または管理者に通信を送信できます。

信頼検索

リアルタイム検索で、ハブトランスポートレベルでメールが既に検索されている場合に、ストアレベルでのそのメールの検索をスキップすることができます。この機能は InterScan を Exchange Server 2007 に対して使用する場合に利用可能です。

InterScan は、エッジまたはハブトランスポートサーバでメールを検索すると、そのメールに検索情報を追加します。そのメールがメールボックスに配信されると、リソースを重複して使用することがないように、InterScan は検索情報をチェックします。InterScan が検索を実行するのは、そのメールが InterScan でまだ検索されていないか、あるいは古いエンジンまたはパターンファイルを使用して検索されている場合に限られます。

手動検索と予約検索の機能強化

InterScan 8.0 では、アップデートによって手動検索または予約検索が中断されることはありません。

Exchange Server 2007 の場合、手動検索画面と予約検索画面はコンボサーバの役割 (ハブトランスポート + メールボックスサーバの役割) とメールボックスサーバの役割でのみ表示されます。InterScan 8.0 では、Exchange Server 2007 に対してのみ差分検索オプションを使用できます。

次の 3 つのオプションがあります。

- 特定の期間に配信されたメッセージの検索
- 添付ファイルを含むメッセージの検索
- InterScan でまだ検索されていないメッセージの検索

クラスタのサポート

InterScan では、Exchange 2000 Server および Exchange Server 2003 での使用時には、共有ディスククラスタモデルをサポートしています。また、Server 2007 での使用時には、シングルコピークラスタ (SCC) モデルとクラスタ連続レプリケーション (CCR) モデルをサポートしています。

InterScan では、クラスタ管理に Exchange 仮想サーバ (EVS) 管理モデルを使用します。各仮想サーバで個々に InterScan の構成情報が保持され、別のノードにフェイルオーバーするときでもデータの一貫性は維持されます。

注意：CCR モデルでは、別のノードへのフェイルオーバーが実行されたときに、データの整合性が維持されません。

バージョンの比較

次の表に、InterScan の前バージョンとの機能の比較を示します。

サポート	InterScan 3.7	InterScan 6.2	InterScan 7.0	InterScan 8.0
OS のバージョン	- Windows NT Server 4.0 SP5 以上 - Windows 2000 Server SP1 以上	- Windows 2000 Server SP1 以上 - Windows Server 2003	- Windows 2000 Server SP2 以上 - Windows Server 2003	- Windows 2000 Server SP4 以上 - Windows 2003 Server SP1、SP2、または R2 (32 ビット) - Windows Server 2003 SP1、SP2、または R2 (64 ビット)
Exchange 最小バージョン要件	Exchange 5.5 SP2	- Exchange 2000 Server SP1 - Exchange Server 2003	- Exchange 2000 Server SP3 - Exchange Server 2003	- Exchange 2000 Server SP3 以上 - Exchange Server 2003 SP2 以上 - Exchange Server 2007
検索メカニズム	ESE API	- Microsoft VS API 2.0 - Microsoft VS API 2.5	- Microsoft VS API 2.0 - Microsoft VS API 2.5	- Microsoft VS API 2.0 - Microsoft VS API 2.5 - Microsoft VS API 2.6
Exchange インフォメーションストアの検索	あり	あり	あり	あり
SMTP (トランスポート) 検索	あり	あり	あり	あり
隔離ファイルの管理	あり	あり	あり	あり
メッセージフィルタ	- メールストアレベル (送信) - SMTP レベル (受信および送信メッセージ)	受信および送信メッセージ	受信および送信メッセージの削除機能として統合	受信および送信メッセージの削除機能として統合
通知	InterScan プロファイルに依存	Collaborative Data Object (CDO)	Collaborative Data Object (CDO)	Collaborative Data Object (CDO)

表 1-1. InterScan バージョンの比較

InterScan のテクノロジー

トレンドマイクロの検索エンジンとスパムメールエンジンは、ウイルス / 不正プログラムおよびその他のセキュリティ上の脅威を検出し、スパムメールを排除します。これら 2 つのエンジンは、アップデートサーバまたはユーザが設定したダウンロード元から配信されたトレンドラボ提供の最新のパターンファイルに基づいて動作します。

ウイルス検索エンジン

トレンドマイクロのすべてのウイルス対策製品には、その中核にトレンドマイクロ独自のウイルス検索エンジンが組み込まれています。このエンジンは業界でも長い歴史を持ち、また高いパフォーマンスを発揮することが証明されています。

InterScan 検索エンジンは、Microsoft Exchange で利用できる VS API (Virus Scanning Application Programming Interface) 2.0 および 2.5 と緊密に連携するように設計されています。Microsoft VS API では、次のことが可能です。

- クライアントがメッセージまたは添付ファイルにアクセスする前に検索します。下位レベルでの検索により、ファイルレベルでの検索では削除不能なウイルスの削除が可能になります。
- 検索をメッセージ受信者の人数分複数回行うのではなく、メッセージの送信前に 1 回で検索できるため、処理時間が短縮されます。送信前に 1 回検索するこの仕組みによって、ユーザがメッセージをコピーしたときに検索が繰り返されないようになります。

トレンドマイクロのウイルス検索エンジンでは以下のことを行います。

- マルチスレッドでのリアルタイム検索

InterScan ではすべての検索がメモリ内で実行され、また検索リクエストを複数処理できます。複数の検索リクエストを受信した場合は、即座に実行できないリクエストに優先順位を付けて待ち行列に格納し、リソースが使用可能となったときにそれらのリクエストを実行します。手動または予約検索の実行中に、クライアントがメールにアクセスすると、InterScan は要求されているメールを即座にリアルタイム検索します。

InterScan では SMTP リアルタイムメール検索をサポートしています。これは Exchange 2000 Server と Exchange Server 2003 の両方でサポートされています。

- 重複検索の回避

メッセージの検索が完了すると、そのメッセージは検索済みとして記録されます。そのメッセージに再びアクセスした場合、そのメッセージがすでに検索されているかどうかチェックされ、そのメッセージがもう一度検索されることはありません。

トレンドマイクロのウイルス検索エンジンは、ICSA (International Computer Security Association) などのコンピュータの国際的なセキュリティ組織から毎年認証を受けています。

ウイルス検索エンジンのアップデート

トレンドマイクロでは、新しいバージョンのウイルス検索エンジンを定期的に提供しています。新しいエンジンは、たとえば次の場合にリリースされます。

- トレンドマイクロのソフトウェアに、新しい検出テクノロジーが組み込まれた場合
- 現在のウイルス検索エンジンでは処理できない、危険度の高いウイルス / 不正プログラムが新たに発見された場合
- 検索性能が強化された場合
- 別のファイル形式、スクリプト言語、エンコード、または圧縮形式に対するサポートが追加された場合

最新のウイルス検索エンジンのバージョン番号を確認するには、次のサイトを参照してください。

<http://www.trendmicro.co.jp/download/engine.asp>

Exchange サーバ上で InterScan が現在使用しているウイルス検索エンジンのバージョンを調べるには、製品コンソールを開き、[概要]→[システム] の順に選択します。ウイルス検索エンジンは頻繁にアップデートすることをお勧めします。

ウイルスパターンファイル

トレンドマイクロのウイルス検索エンジンでは、ウイルスパターンファイルと呼ばれる外部データファイルを使用して、最新のセキュリティリスクに対応しています。

次の Web サイトで、最新バージョン、リリース日、およびファイルに記載された新しいすべてのウイルス定義を確認できます。

<http://www.trendmicro.co.jp/support/pattern.asp>

Exchange サーバ上で InterScan が現在使用しているウイルス検索エンジンのバージョンを調べるには、製品コンソールを開き、コンソールを開き、[概要]→[システム] の順に選択します。パターンファイルは頻繁にアップデートすることをお勧めします。

パターンファイルの番号

お使いのソフトウェア製品内のパターンファイルがトレンドマイクロから提供されている最新のパターンファイルであるか比較するために、パターンファイルにはバージョン番号があります。

パターンファイル番号は、xx.xxx.xx という最大 7 桁の数字で構成されています。

ファイルパターンの番号が 1.786.01 の場合を例にとります。

- 最初の桁 (1) は新規のナンバリングシステムであることを示しています(パターンファイル識別子のこのセグメント内の 2 桁の 2 番目の数字は、番号が 9 から 10 に増えるまで使用されません)。
- 次の 3 桁 (786) は従来のパターンファイル番号を示しています。
- 最後の 2 桁 (01) は、トレンドマイクロのエンジニア用のパターンファイルリリースに関するその他の情報です。

注意：スパムメール判定ルールの番号ではこの形式は使用されていません。

最新の脅威に対応するため、常に必ず最新のバージョンのパターンファイルを使用するようにしてください。

ウイルス検索エンジンでのウイルスパターンファイルの使用方法

ウイルス検索エンジンは、パターンファイルと連携し、パターンマッチングというプロセスを使用して検出の第 1 レベルを実行します。各ウイルス / 不正プログラムには、一意の「シグネチャ」、すなわちそれによって他のコードと区別可能な特性を表す文字列が含まれているので、TrendLabs の専門家は、このコードの実行機能を持たない断片をパターンファイルに取り込みます。ウイルス検索エンジンでは、各検索済みファイルの特定領域をパターンファイルのパターンと比較し、一致するものを探します。一致するものが検出された場合、システム管理者にメールで通知が送られます。

注意：ウイルス検索エンジンには、ディスク領域管理用に古いパターンファイルの自動クリーンアップルーチンが含まれています。

アップデートについて

アップデート機能を使用することにより、InterScan のすべてのコンポーネントの最新版をインターネット経由でダウンロードできます。InterScan のコンポーネントには、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアのパターンファイルが含まれます。

アップデートは、ネットワークサービスを中断せず、コンピュータの再起動も必要としません。InterScan では、あらかじめ決めておいた間隔で定期的に最新コンポーネントを受信するか、手動アップデートを実行することができます。

パターンファイルの差分アップデート

アップデートではパターンファイルの差分アップデートをサポートしています。毎回、パターンファイルをすべてダウンロードするのではなく、新しい部分のみをダウンロードし、既存のパターンファイルに追加できます。この効率的なアップデート方法により、ウイルス対策ソフトウェアのアップデートに必要な帯域幅を大幅に削減できます。

アップデートおよび差分アップデートを使用するように InterScan を設定すると、アップデートに費やす時間が短縮されます。

InterScan でのアップデートの使用方法

InterScan を設定して、アップデートサーバを手動および予約アップデートのダウンロード元として使用できます。コンポーネントアップデートの時間になると、InterScan はアップデートサーバに直接ポーリングします。アップデートプログラムは新しいコンポーネントの有無を確認し、InterScan がアップデートをダウンロードします。

ヒント：複数のサーバ環境で効率よくダウンロードするには、1 つの InterScan サーバに対して、他の InterScan サーバがこのサーバから最新版をダウンロードできるように設定します。この設定によって、その InterScan サーバは、差分アップデートを受け取る環境内の他のサーバに対して、仮想アップデートサーバとして機能します。

トレンドマイクロの推奨設定

トレンドマイクロの推奨設定では、実際のファイルタイプを識別してファイルのヘッダを調べ、不正コードが隠れている可能性があると考えられるファイルタイプのみを検索することにより、パフォーマンスを最適化します。実際のファイルタイプの認識は、無害なファイル拡張子タイプを装う可能性がある不正コードの識別に役立ちます。トレンドマイクロの推奨設定が管理者に提供する利点のいくつかを次に示します。

- **パフォーマンスの最適化** — 検索に使われるサーバシステムリソースを最小限に抑えます。トレンドマイクロの推奨設定を使用すると、サーバで実行されている他の重要なアプリケーションに影響を与えません。
- **時間の節約** —トレンドマイクロの推奨設定では、実際のファイルタイプ認識機能を使用するため、トレンドマイクロの推奨設定を実行する場合の検索時間は、**すべての添付ファイル**に必要な時間よりも大幅に短くなります。つまり、感染するリスクが高いファイルのみが検索されます。この時間の差は、手動検索でトレンドマイクロの推奨設定を使用する場合に顕著です。

トレンドマイクロの推奨処理

トレンドマイクロの推奨処理では、ウイルス / 不正プログラムの種類が識別され、ウイルスのそれぞれの種類がコンピュータシステムや環境に侵入する方法に基づいて処理が推奨されます。トレンドマイクロの推奨処理では、不正コード、複製、およびペイロードの各種類をウイルス / 不正プログラムとして分類します。InterScan によりウイルスが検出されると、そのウイルス / 不正プログラムの種類に対応した推奨処理(駆除、メッセージ部分の隔離、メッセージ全体の削除)が実行され、環境内の攻撃されやすいポイントが保護されます。

検出時の処理に詳しくない場合、またはある特定のタイプのウイルス / 不正プログラムに適した処理を確定できない場合、トレンドマイクロの推奨処理を使用することをお勧めします。

トレンドマイクロの推奨処理を使用すると、次の利点があります。

- **時間の節約と保守の容易さ** —トレンドマイクロの推奨処理では、トレンドマイクロが推奨する処理が使用されます。処理の設定に時間を割く必要はありません。
- **アップデート可能** —ウイルス / 不正プログラム作成者は、ウイルス / 不正プログラムによるコンピュータの攻撃方法を絶えず変えています。トレンドマイクロの推奨処理の設定は、新しいウイルスパターンファイルごとにアップデートされ、最新の脅威や、ウイルス / 不正プログラムによる攻撃の最新の方法からユーザを保護します。

スパムメール検索エンジンとスパムメール判定ルール

InterScan では、トレンドマイクロのスパムメール検索エンジンおよびトレンドマイクロのスパムメール判定ルールを使用してスパムメールを検出し、これらに対して処理を実行します。トレンドマイクロは頻繁にエンジンおよびパターンファイルをアップデートし、これらをダウンロードできるようにしています。InterScan では、手動アップデートまたは予約アップデートによりこれらのコンポーネントをダウンロードできます。

スパムメール検索エンジンは、スパムメールシグネチャおよびヒューリスティックルールを使用してメールを検査します。ここではメールを検索し、パターンファイルのルールおよびパターンにどれだけ一致しているかにより、それぞれのメッセージにスコアを割り当てます。InterScan はスパムメールスコアをユーザが定義したスパムメール検出レベルと比較します。スパムメールスコアが検出レベルを超えた場合、InterScan はそのスパムメールに対して処理を実行します。

例: 多くのスパムメール送信者は、そのメール内に多くの感嘆符、または複数の連続した感嘆符 (!!!!) を使用します。InterScan は、このように感嘆符を多用するメッセージを検出すると、そのメールのスパムメールスコアを上げます。

注意: ユーザは、スパムメール検索エンジンがスパムメールスコアの割り当てに使用する方法を変更できませんが、スパムメールであるかどうかを判定するために InterScan で使用される検出レベルを調整することはできます。

製品のインストールと削除

Trend Micro InterScan for Microsoft Exchange (以下、InterScan) を、インストールプログラムを利用して 1 台以上のサーバにローカルまたはリモートでインストールします。

この章では、次の項目について説明します。

- 32 ページの「最小要件」
- 35 ページの「開始する前に」
- 42 ページの「インストールの準備」
- 47 ページの「新規インストールの実行」
- 47 ページの「InterScan 8.0 へのアップグレード」
- 49 ページの「クラスタ環境でのアップグレード」
- 110 ページの「InterScan のアンインストール」
- 122 ページの「クラスタ環境での InterScan のアンインストール」

最小要件

Microsoft Exchange 2000 Server または Microsoft Exchange Server 2003 で InterScan をインストールするには、以下の最小システム要件を満たす必要があります。

プロセッサ

Intel Pentium II 266 MHz 以上のプロセッサ

(Intel Pentium または互換の 733MHz プロセッサを推奨)

メモリ

512MB RAM、1GB の RAM を推奨

ディスク空き領域

700MB のディスク空き領域、1GB のディスク空き領域を推奨

(領域のおよそ半分は一時ファイルの保管に使用)

OS

- Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows Server 2003 Service Pack 1 (32 ビット)
- Microsoft Windows Server 2003 R2 (32 ビット)
- Microsoft Windows Server 2003 Service Pack 2 (32 ビット)

メールサーバ

- Microsoft Exchange 2000 Server Service Pack 3 以上
- Microsoft Exchange Server 2003 Service Pack 2 以上

Web サーバ

- Microsoft Internet Information Services (IIS) 5.0
- Microsoft Internet Information Services (IIS) 6.0
- Apache Web サーバ 2.0

ブラウザ

フレームをサポートする Java 対応の Web ブラウザ

- Microsoft Internet Explorer 6.0 および 7.0
- Mozilla Firefox 2.0

Java ソフトウェア

Java 2 Runtime Environment バージョン 1.4.1_02 以上

注意：Java 仮想マシンは次の Web サイトから入手できます。<http://jp.sun.com>

Microsoft Exchange Server 2007 で InterScan をインストールするには、以下の最小システム要件を満たす必要があります。

プロセッサ

- Intel Extended Memory 64 Technology (Intel EM64T) をサポートする、x64 アーキテクチャベースのプロセッサ
- AMD64 プラットフォームをサポートする、AMD 64 ビットプロセッサを搭載する x64 アーキテクチャベースのコンピュータ

メモリ

1GB の RAM、2GB の RAM を推奨 (メールボックスごとに 5MB の RAM)

ディスク空き領域

1GB のディスク空き領域、1.1GB のディスク空き領域を推奨

(領域のおよそ半分は一時ファイルの保管に使用)

OS

- Microsoft Windows Server 2003 Service Pack 1 (64 ビット)
- Microsoft Windows Server 2003 R2 (64 ビット)
- Microsoft Windows Server 2003 Service Pack 2 (64 ビット)

メールサーバ

Microsoft Exchange Server 2007

Web サーバ

- Microsoft Windows Server 2003 には IIS 6.0 が必要です。
- Apache Web サーバ 2.0

ブラウザ

フレームをサポートする、Java 対応の次のような Web ブラウザ

- Microsoft Internet Explorer 6.0 および 7.0
- Mozilla Firefox 2.0

Java ソフトウェア

Java 2 Runtime Environment バージョン 1.4.1_02 以上

注意：Java 仮想マシンは次の Web サイトから入手できます。

<http://jp.sun.com>

クラスタ環境の場合

- Exchange 2000 Server および Exchange Server 2003: 共有ディスククラスタモデル
- Exchange Server 2007: シングルコピークラスタ (SCC) モデル
- Exchange Server 2007: クラスタ連続レプリケーション (CCR) モデル

注意：システム要件に記載されているオペレーティングシステムの種類やハードディスク容量などは、本ドキュメント作成時点の情報です。システム要件は、オペレーティングシステムのサポート終了や、弊社製品の改良、検索エンジンやパターンファイルのバージョンアップなどに伴い、変更、追加、または削除される場合があります。また、製品の運用環境によっては、ログファイルの保存、他のソフトウェアとの共存などにより、必要となるメモリサイズやハードディスク容量も異なりますので、ご注意ください。最新のシステム要件については、弊社 Web サイトやサポート窓口にご確認ください。

開始する前に

次のセクションでは、InterScan をインストールする場合の推奨事項を説明します。インストールを開始する前にこのセクションをお読みください。

パイロットインストール

実環境に導入する前にパイロットインストールを実行することをお勧めします。パイロットインストールにより、フィードバックを収集し、機能が動作するかどうかを調べ、実際の運用開始後に必要になるサポートのレベルを知ることができます。

パイロットインストールを実行するには

1. 適切なテストサイトを作成します。
2. ロールバック計画を作成します。
3. パイロット環境でインストールを実行し、評価します。

適切なテストサイトの作成

できるかぎり実際の環境に近いテスト環境を作成します。テストサーバと実際のサーバは、以下について同じものを使用する必要があります。

- OS および Exchange サーバのバージョン、Service Pack、およびパッチ
- Trend Micro Control Manager、ウイルスバスター コーポレートエディション、Trend Micro ServerProtect などのウイルス対策製品
- 同じタイプのネットワークポロジ。実際の環境の代理環境として十分に機能する必要があります。

注意：トレンドマイクロ製品の体験版の多くは、次のトレンドマイクロ Web サイトからダウンロードできます。

<http://www.trendmicro.co.jp/download/>

ロールバック計画の準備

インストールまたはアップグレード処理で問題が発生した場合に備えて、ロールバック回復計画を作成することをお勧めします。このプロセスでは、ローカルな企業ポリシーおよび技術的特性を考慮する必要があります。

InterScan の設定のバックアップと復元

InterScan の設定を変更する場合、事前に現在の設定のバックアップを作成しておきます。

Exchange 2000/2003 環境で InterScan および設定をバックアップするには

1. バックアップするデータベースが格納されている対象サーバ上の InterScan Master Service を停止します。
2. Conf.mdb、Log.mdb、または Report.mdb ファイルをコピーします。

Exchange 2007 環境で InterScan および設定をバックアップするには

1. バックアップするデータベースが格納されている対象サーバ上の InterScan Master Service と SQL Server (SCANMAIL) Service を停止します。
2. Conf.mdf、Log.mdf、または Report.mdf ファイルをコピーします。

Exchange 2000/2003 環境で InterScan の設定を復元するには

1. 設定の復元先の対象サーバ上の InterScan Master Service を停止します。
2. Conf.mdf、Log.mdf、または Report.mdf ファイルを置換します。
3. InterScan Master Service を開始します。

Exchange 2007 環境で InterScan の設定を復元するには

1. 設定の復元先の対象サーバ上の InterScan Master Service と SQL Server (SCANMAIL) Service を停止します。
2. Conf.ldf、Log.ldf、または Report.ldf を削除します。
3. Conf.mdf、Log.mdf、または Report.mdf ファイルを置換します。
4. SQL Server (SCANMAIL) Service と InterScan Master Service を開始します。

パイロットインストールの実行と評価

パイロットをインストールし、ウイルス対策およびコンテンツセキュリティの適用とネットワークパフォーマンスの両方の点から評価します。パイロットプロセス中に発生した成功と失敗のリストを作成します。潜在的な「落とし穴」を特定し、それによって適切なインストールの計画を作成します。

導入計画

InterScan インストールプログラムでは、1 台または複数のローカルまたはリモートサーバへのインストールがサポートされています。InterScan は、フロントエンド (ブリッジヘッド) サーバとバックエンドサーバの両方を保護するように設計されており、サーバクラスタリングを幅広くサポートしています。

LAN セグメントに InterScan を導入し、設定する場合は、次の事項を考慮してください。

- サーバ上のネットワークトラフィックの負荷
- ネットワークで複数のメールサーバを使用しているのか、1 つのブリッジヘッドサーバと複数のバックエンドサーバを使用しているのか、あるいはその両方か
- 企業ネットワークに複数の LAN (ローカルエリアネットワーク) セグメントが含まれているかどうか

ネットワークトラフィックに関する考慮事項

導入計画を作成するときは、InterScan によって発生するネットワークトラフィックと CPU の負荷を考慮します。

InterScan が次の処理を実行するときにネットワークトラフィックが発生します。

- トレンドマイクロのアップデートサーバに接続し、アップデートされたコンポーネントをチェックし、ダウンロードするとき
- 管理者または他の指定された受信者に警告および通知を送信するとき

リアルタイムで、あるいは予約または手動検索中に Exchange サーバに到着したメールを検索するときに、CPU の負荷が増加します。他のウイルス対策製品とは異なり、InterScan ではマルチスレッド検索が使用されるため、CPU の負荷は軽減されます。

複数のサーバへの InterScan の導入

Exchange サーバが 1 つしかないネットワークの場合、InterScan の導入は比較的単純です。InterScan を Exchange サーバにインストールし、メッセージングセキュリティが最適になるようにそれを設定します。

複数の Exchange サーバを使用している企業の場合は、InterScan の導入は複雑になることがあります。よく使用される方法は、1 つのサーバをゲートウェイのすぐ背後にフロントエンドサーバとして導入し、残りのメールサーバをバックエンドサーバとして導入する方法です。バックエンドサーバは、多くの場合、フェイルオーバーリカバリの利点を得られるようにクラスタにインストールされます。このモデルを使用して InterScan を導入するときは、39 ページの表 2-1 に示す点を考慮してください。

もう 1 つの戦略は、InterScan を DMZ 上の Exchange サーバに導入する方法です。これによって、サーバがさらされるリスクが増加します。Exchange サーバをインターネットに公開した場合、重大な懸念事項は SMTP トラフィックです。インターネットに公開された Exchange サーバに InterScan をインストールする場合は、SMTP 検索を有効にすることをお勧めします。SMTP 検索は初期設定で有効になっています。InterScan ではリアルタイム検索で SMTP トラフィックが検索されます。設定については注意深く考慮し、初期設定を変更するのは、その結果が理解できている場合のみにしてください。

サーバの役割	推奨設定
フロントエンドメールサーバ: - 通常、周辺機器またはファイアウォール、あるいはその両方のすぐ背後に配置されます。 - Active Directory と頻繁に通信し、メールボックスアドレスとルーティング情報を検索します。 - 主としてすべてのメールをバックエンドメールサーバに転送し、バックエンドメールサーバからクライアントのメールボックスに配信します。 - SMTP プロトコルを使用して多数のメッセージを受信します。 - インターネット上を安全に送信するために暗号化された多数のメッセージを受信し、メールの認証を解決します。 - トラフィックの負荷が高く、特にメールアドレスの解決と設定データの読み取りのために Active Directory と通信するときに高くなります。	- トレンドマイクロのアップデートサーバを、フロントエンドサーバのコンポーネントアップデート元として設定し、そのフロントエンドサーバをアップデート元として使用するようバックエンドサーバを設定します。これによって、全体的なネットワークトラフィックが減少し、インターネットへの公開も軽減されます。 - フロントエンドメールサーバ上で SMTP 検索を設定します。 注意: SMTP 検索を提供しているのは、InterScan 6.2 以上です。 - スパムメールや好ましくないコンテンツを含むメールや添付ファイルをフロントエンドメールサーバで排除するように InterScan を設定します。これにより、バックエンドサーバはこれらのメッセージを処理する必要がなくなり、その負荷が軽減されます。
バックエンドメールサーバ: - ローカルネットワーク内のネットワーク周辺機器の背後に配置され、インターネットからは隠べいされています。 - インフォメーションストア上のクライアントのメールボックスにメールを配信し、保存します。 - 特に混在環境で、x.400 プロトコルを使用してローカルメッセージを受信する場合があります。 - 多くの場合、クラスタ化されており、バックアップからの復元が必要になる可能性はあまりありません。	- 厳格なオプションを使用してウイルス検索を実行するようにバックエンドメールサーバを設定します。 - Exchange メールボックスでの定期的な予約検索によって、構成では対応できない予期しないソースからの脅威の侵入を防止します。

表 2-1. フロントエンドサーバとバックエンドサーバへの InterScan の導入

サーバの役割	推奨設定
エッジトランスポートサーバ: - Active Directory へのアクセスはできません。 - XML ベースのルーティング - ポート 25 の SMTP 中継 - 分散管理 - メッセージ検疫 - 設定、コネクタ、受信者、SMTP 設定、およびエージェント設定に関する情報は、サーバに格納されたファイルによって定義されます。エッジトランスポートサーバの役割はこのファイルによって定期的にアップデートされます。 - スタンドアロン形式で配置されます。 - エッジトランスポートサーバの役割では、次の主な配置サーバがあります。(1) 組織のネットワークの周辺部に位置し、インターネットと直接つながるもの。(2) インターネットに直接つながるサードパーティメールサーバの背後に位置するもの。	- リアルタイムウイルス検索を実行するように、エッジトランスポートサーバを設定します。 - アップデート機能によってアップデートを実行し、新たなセキュリティリスクに対して防御するため予約アップデートを定期的に実行するように、エッジトランスポートサーバを設定します。

表 2-2. エッジトランスポートサーバ、ハブトランスポートサーバ、およびメールボックスサーバへの InterScan の導入

サーバの役割	推奨設定
ハブトランスポートサーバ: - メールボックスサーバの役割やパブリックフォルダサーバの役割を持つサーバから独立したハードウェア上に、カテゴリザなどのすべてのトランスポートコンポーネントをインストールし、設定することができます。 - 組織およびインターネットでのメール転送に使用される組織内部のサーバの役割 - 集中管理 - Active Directory への直接アクセスが可能です。 - すべての認証を処理します。 - ルーティングはすべて Active Directory ベースで実行されます。 - ポート 25 の SMTP 中継およびメッセージ中継を使用します。 - 負荷分散が可能です。	- リアルタイムウイルス検索を実行するように、ハブトランスポートサーバを設定します。 - ハブトランスポートサーバのコンポーネントのアップデートのダウンロード元として、トレンドマイクロアップデートサーバを設定します。 - アップデートのダウンロード元としてハブトランスポートサーバを使用するように、メールボックスサーバを設定します。この設定により、全体的なネットワークトラフィックが減少し、インターネットとの接触が少なくなります。

表 2-2. エッジトランスポートサーバ、ハブトランスポートサーバ、およびメールボックスサーバへの InterScan の導入

複数の LAN セグメントへの InterScan の導入

大規模な企業では、インターネットで分離された異なる LAN セグメント上に複数の Exchange サーバが配置されている場合もあります。このような場合は、各 LAN セグメントに InterScan を個別にインストールすることをお勧めします。

注意：InterScan for Microsoft Exchange は、Exchange メールサーバを保護するように設計されています。InterScan では、Exchange 以外のメールサーバ、ファイルサーバ、デスクトップ、またはゲートウェイデバイスに対する保護は行いません。ファイルサーバおよびデスクトップを保護するウイルスバスター コーポレートエディションや、ネットワークの周辺を保護する Trend Micro InterScan Web Security Suite、InterScan Messaging Security Suite など、その他のトレンドマイクロ製品と共に使用すると、InterScan による保護が強化されます。

インストールの準備

スムーズなインストールの準備のために、このセクションの情報を確認し、インストール前のチェックリストを参照してください。

Microsoft Exchange サーバごとに 1 つの InterScan をインストールすることをお勧めします。InterScan では、1 つのインストールプログラムからローカルおよびリモートのコンピュータに対してインストールを実行できます。ローカルコンピュータとはインストールプログラムを実行するコンピュータであり、リモートコンピュータとは InterScan がインストールされるその他すべてのコンピュータです。InterScan は複数のサーバに同時にインストールできます。必要な操作は、これらのサーバをネットワークに統合することと、管理者権限を持つアカウントを使用してそれらにアクセスすることのみです。

次の表に、InterScan の新規インストールに最低限必要な権限を示します。

Exchange のバージョン	最低限必要な権限	ドメイン管理者の権限がない場合に制限される機能
Exchange 2000 Server および Exchange Server 2003	ローカル管理者および ドメインユーザ	エンドユーザメール隔離と サーバ管理のアクティベーションを実行できません。
Exchange Server 2007 エッジトランスポート	ローカル管理者	該当なし
Exchange Server 2007 ハブ / メールボックス / クラスター	ローカル管理者および Exchange 組織管理者	該当なし

表 2-3. 新規インストールに最低限必要な権限

アップグレード時の設定の例外

InterScan 7.0 から InterScan 8.0 にアップグレードする場合、インストールプログラムは、インストール中に以前の設定を使用します。ただし、例外が 3 つあり、動作が異なります。

エンドユーザメール隔離

インストールプロセスが終了すると、[Outlook 迷惑メール対策との統合] オプションと [エンドユーザメール隔離との統合] オプションとの切り替えができなくなります。次の表に、ドメイン管理者権限を持つアカウントを使用してアップグレードを実行したときのエンドユーザメール隔離の設定を示します。

Exchange のバージョン	インストール時に [Outlook 迷惑メール対策との統合] を選択した場合	インストール時に [エンドユーザメール隔離との統合] を選択した場合
Exchange 2000 Server	エンドユーザメール隔離の以前の設定がすべて維持されます。	エンドユーザメール隔離の以前の設定がすべて維持されます。
Exchange Server 2003	- エンドユーザメール隔離のメールボックスが削除されます。 - エンドユーザメール隔離のアカウントが削除されます。 - 以前使用していたエンドユーザメール隔離の承認する送信者リストと迷惑メール対策の差出人セーフリストが結合されます。	エンドユーザメール隔離の以前の設定がすべて維持されます。

表 2-4. ドメイン管理者権限を使用したエンドユーザメール隔離の設定

次の表に、ローカル管理者権限を持つアカウントを使用してアップグレードを実行したときのエンドユーザメール隔離の設定を示します。

Exchange のバージョン	インストール時に [Outlook 迷惑メール対策との統合] を選択した場合	インストール時に [エンドユーザメール隔離との統合] を選択した場合
Exchange 2000 Server	エンドユーザメール隔離の以前の設定がすべて維持されます。	エンドユーザメール隔離の以前の設定がすべて維持されます。

表 2-5. ローカル管理者権限を使用したエンドユーザメール隔離の設定

Exchange のバージョン	インストール時に [Outlook 迷惑メール対策との統合] を選択した場合	インストール時に [エンドユーザメール隔離との統合] を選択した場合
Exchange Server 2003	- 権限不足のため、エンドユーザメール隔離のメールボックスは削除されずに残ります。 - 権限不足のため、エンドユーザメール隔離のアカウントは削除されずに残ります。 [スパムメール管理] メニューは表示されません。 - 以前使用していたエンドユーザメール隔離の承認する送信者リストと迷惑メール対策の差出人セーフリストが結合されます。 - 製品コンソールで [スパムメール管理] メニューは表示されません。	エンドユーザメール隔離の以前の設定がすべて維持されます。

表 2-5. ローカル管理者権限を使用したエンドユーザメール隔離の設定

Trend Micro Control Manager エージェント

本バージョンの InterScan では、Trend Micro Control Manager (以下、Control Manager) 3.5 Patch 2 をサポートしています。Control Manager サーバと Control Manager エージェントとの通信には、以前のバージョンと異なる通信メカニズムが使用されます。インストールプロセスには、移行の設定も含まれます。次の表に、アップグレードを実行したときの Control Manager の設定を示します。

Exchange のバージョン	[InterScan エージェントを Control Manager サーバに登録する]を選択した場合	[InterScan エージェントを Control Manager サーバに登録する]を選択しなかった場合
Exchange 2000 Server/Exchange Server 2003	- 元の Control Manager サーバから登録を解除します。 - InterScan 7.0 Control Manager エージェントをアンインストールします。 - InterScan 8.0 Control Manager エージェントをインストールします。 - 新しい設定で登録します。 - 新しく登録された InterScan サーバが InterScan for Microsoft Exchange フォルダに表示されます。このフォルダは、Control Manager サーバへの InterScan エージェントの初回登録時に、Control Manager サーバによって自動的に作成されます。	- 元の Control Manager サーバから登録を解除します。 - InterScan 7.0 Control Manager エージェントをアンインストールします。 - Control Manager エージェントのすべての情報をデータベースから削除します。

表 2-6. Control Manager の設定

注意：InterScan 8.0 は、InterScan 7.0 Control Manager エージェントを削除して、Trend Micro Management Communication Protocol (MCP) エージェントをインストールします。MCP エージェントと以前のエージェントとは使用するプロトコルが異なるため、元の階層構造は MCP エージェントには転送されません。

アクティベーションコード

アップグレードを実行すると、常に新しいアクティベーションコードが InterScan で使用されるようになります。

インストール前のチェックリスト

項目	注意事項
最低限必要なアカウント権限	• Exchange 2000 Server および Exchange Server 2003 の場合、必要な権限はローカル管理者権限とドメインユーザ権限です。ただし、その後、ドメイン管理者権限を持つアカウントを使用して、エンドユーザメール隔離とサーバ管理のアクティベーションを実行する必要があります。 • Exchange Server 2007 ハブ / メールボックス / クラスタの場合、必要な権限はローカル管理者権限と Exchange 組織管理者権限です。ただし、その後、ドメイン管理者権限を持つアカウントを使用して、エンドユーザメール隔離のアクティベーションを実行する必要があります。 • Exchange Server 2007 エッジトランスポートの場合、必要な権限はローカル管理者権限です。
サービスの停止 / 再開	インストール前に Exchange のサービスを停止したり、正常にインストールされた後に再開したりする必要はありません。 警告: IIS 5.0 を使用する Windows 2000 サーバに通常実装されているようなロックダウンツールが、インストール先サーバで動作している場合、事前にロックダウンツールを削除してください。IIS サービスが無効な状態になり、インストールが正常に完了しなくなる場合があります。
アクティベーションコード	インストール中にセットアッププログラムからアクティベーションコードの入力が要求されます。インストール時に製品のアクティベーションを実行しないで、後で製品コンソールからアクティベーションを実行することもできます。ただし、アクティベーションを実行するまでは、使用できる InterScan のサービスが制限されます。
プロキシサーバ	インストール中に、セットアッププログラムから、プロキシ情報を入力するように求められます。プロキシサーバでネットワーク上のインターネットトラフィックを処理している場合、最新のコンポーネントを受信するには、プロキシサーバの情報、ユーザ名、およびパスワードを入力する必要があります。インストール中にプロキシ情報を空白のままにした場合は、後で製品コンソールから設定できます。

表 2-7. インストール前のチェックリスト

新規インストールの実行

Exchange サーバに前のバージョンの InterScan がインストールされていない場合は、新規インストールを実行する必要があります。インストールを開始する前に、46 ページの表 2-7、「インストール前のチェックリスト」を参照してください。

クラスタ環境でのインストール

InterScan は Windows 2000 または 2003 のクラスタにインストールできます。

- Exchange Server 2003 または Exchange Server 2007 SSC モデルを使用する Windows 2003 クラスタ (Single Quorum Device クラスタ)
- Exchange Server 2007 CCR モデルを使用する Windows 2003 クラスタ (Majority Node Set クラスタ)

クラスタへのインストールの場合、仮想サーバごとにリソースが追加され、クラスタ内のすべてのノードに同時にインストールされます。

注意：一貫性のある保護のためには、Microsoft Exchange サーバごとに 1 つの InterScan をインストールすることをお勧めします。

InterScan では、Windows NTFS ボリュームマウントポイント機能をサポートしています。26 文字のドライブ文字制限を超えることができます。マウントポイントディスクに InterScan をインストールできます。たとえば、共有ディスクが G の場合、マウントポイントディスクは G:\mountpoint disk になります。マウントディスクを選択して、データを初期設定のパスまたはカスタマイズしたファイルパスにインストールできます。

InterScan 8.0 へのアップグレード

セットアッププログラムを実行して、前バージョンの InterScan をアップグレードできます。インストールを開始する前に、46 ページの表 2-7、「インストール前のチェックリスト」を参照してください。

InterScan 8.0 では、InterScan 7.0 からのアップグレードがサポートされています。現在、バージョン 7.0 を使用している場合、セットアッププログラムによって自動的に削除され、InterScan 8.0 がインストールされます。

注意：アップグレードがサポートされていないバージョンの InterScan を使用している場合は、インストールに使用したのと同じバージョンのアンインストールプログラムを使用してそれをアンインストールします。たとえば、InterScan 6.2 を使用している場合は、InterScan 6.2 のアンインストールプログラムを使用してアンインストールします。

アップグレードの際、InterScan 8.0 に以前のバージョンと同等の設定項目がある場合、それらの設定内容は維持されます。同等の設定項目がない場合は、バージョン 7.0 の初期設定が使用されます。

アップグレード後のログおよびフォルダ

InterScan 8.0 にアップグレードすると、ログおよびフォルダは次のようになります。

- ログはアップグレード後も維持され、クエリを実行できます。

ヒント：アップグレードの前に、ログファイルのサイズを確認してください。ログファイルが非常に大きい場合は、アップグレードする前に既存のバージョンを使用して不必要なファイルを削除することをお勧めします。これにより、アップグレードに必要な時間が大幅に短縮されます。

- 隔離フォルダとバックアップフォルダは、アップグレード時に維持されます。

アップグレード後の設定および処理

InterScan 8.0 にアップグレードすると、ウイルス検出時の設定および処理は次のようになります。

- **エンドユーザメール隔離** — 承認する送信者リストはアップグレード後も維持されます。
- **メッセージ部分の隔離** — メッセージ部分を隔離する新しいオプションが追加されます。

クラスタ環境でのアップグレード

クラスタ環境でのアップグレード手順は、クラスタでない通常のサーバの場合と同じです。

警告： フェイルオーバー中のクラスタでアップグレードを実行しないでください。

クラスタでアップグレードする場合、InterScan では、バージョンまたはビルドのアップグレード時に、Exchange のシステムアテンダントサービスおよび IIS Admin サービスが停止することはありません。

セットアッププログラムの実行

次のセクションでは、通常のインストールのプロセスについて説明しています。セットアッププログラムで [キャンセル] ボタンをいつでもクリックできます。終了確認のダイアログボックスが表示され、[はい] をクリックすると、インストールが中止されます。インストールを中止すると、一時ディレクトリのファイルを除くすべてのファイルとレジストリの変更が取り消されます。

Exchange 2000 Server および Exchange Server 2003 環境でのインストール

1. セットアッププログラムの取得
 - a. トレンドマイクロの Web サイト
 - i. トレンドマイクロの Web サイトから InterScan をダウンロードします。
 - ii. ファイルを一時ディレクトリに解凍します。
 - iii. setup.exe を実行して InterScan をインストールします。

- b. InterScan の製品 CD-ROM
 - i. CD-ROM を挿入し、setup.exe を実行します。
[InterScan for Microsoft Exchange セットアップ] 画面が表示されます。
- 2. [次へ] をクリックしてインストールを続行します。[使用許諾契約書] 画面が表示されます。



図 2-1. セットアップ開始画面

3. 契約の条件に同意して、インストールを続行するには、[使用許諾契約の条項に同意します] をクリックします。[次へ] をクリックして続行します。[処理の選択] 画面が表示されます。

注意： 契約の条件に同意しない場合は、[使用許諾契約の条項に同意しません] をクリックします。これを選択すると、システムが変更されることなく、セットアッププログラムが終了します。

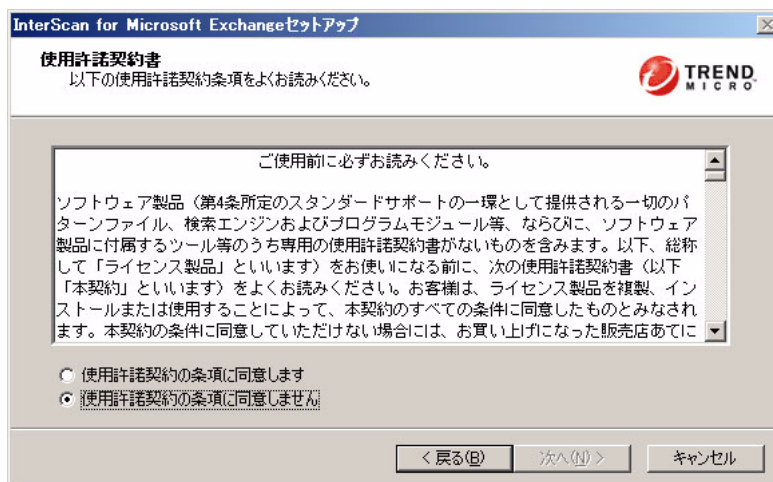


図 2-2. [使用許諾契約書] 画面

4. 次のいずれかの処理を選択します。
- 次の場合は、[インストール / アップグレード] を選択します。
 - 新規インストールを実行する場合
 - InterScan 7.0 から InterScan 8.0 にアップグレードする場合。アップグレードの詳細については、47 ページの「InterScan 8.0 へのアップグレード」を参照してください。

- InterScan 8.0 ベータ版から InterScan 8.0 リリース版にアップグレードする場合
- サーバから InterScan を削除する場合は、[アンインストール] を選択します。アンインストールの詳細については、110 ページの「InterScan のアンインストール」を参照してください。

[次へ] をクリックして続行します。[サーバの役割の選択] 画面が表示されます。

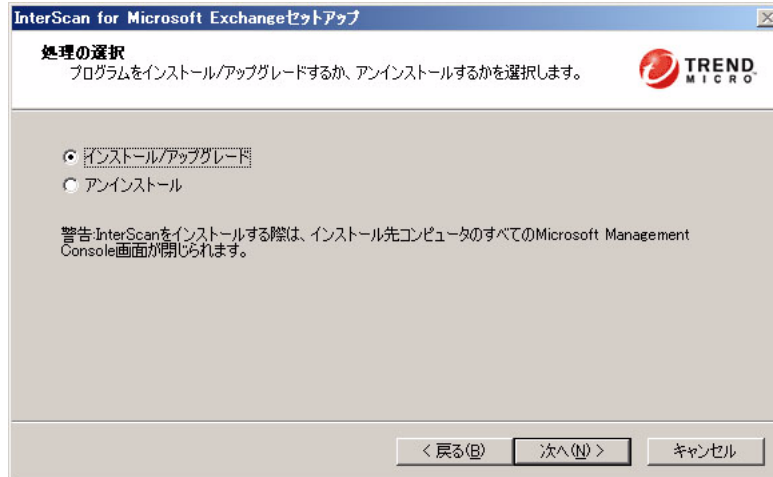


図 2-3. [処理の選択] 画面

5. Exchange 2000 Server または Exchange Server 2003 で InterScan をインストールする場合は、[Exchange Server 2000/2003] を選択します。[対象サーバの選択] 画面が開きます。

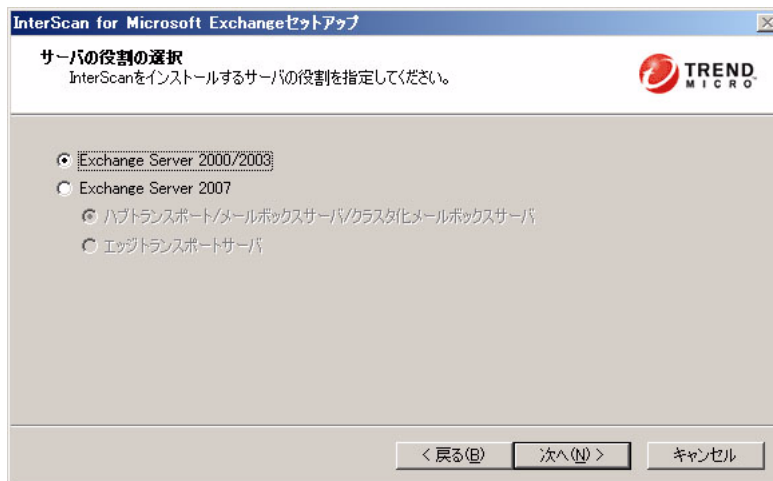


図 2-4. [Exchange Server 2000/2003] が選択された [サーバの役割の選択] 画面

6. 次のいずれかの方法で、InterScan をインストールするコンピュータを選択します。
- [コンピュータ名] に、インストールするサーバの名前を入力し、[追加] をクリックしてサーバのリストにコンピュータを追加します。
 - [参照] をクリックしてネットワーク上のコンピュータを参照し、リストに追加するドメインまたはコンピュータをダブルクリックします。
- a. リストからサーバを削除するには [削除] をクリックします。

- b. [次へ] をクリックし、対象サーバのリストを保存し、インストールを続行します。[ログオン] 画面が表示されます。

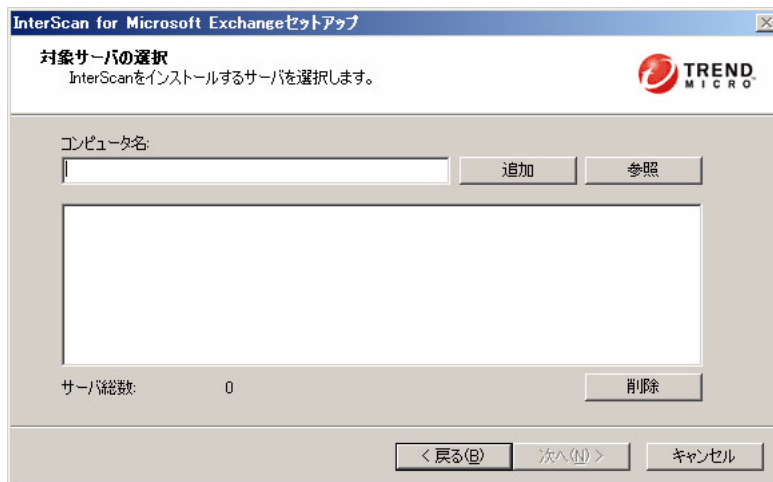


図 2-5. [対象サーバの選択] 画面

セットアッププログラムでは、InterScan をいくつかの単一サーバにインストールすることも、1 つのドメイン内のすべてのコンピュータにインストールすることもできます。すべての対象サーバにアクセスできる適切な権限を持つアカウントを使用してください。

クラスタへのインストール

InterScan では、1 つのクラスタ環境のすべての仮想サーバへのインストールもサポートされています。クラスタにインストールするときは、仮想サーバ名またはノード名を入力します。インストールプログラムによって、すべての仮想サーバおよびノードに同時にインストールされます。

7. InterScan をインストールする対象サーバにログオンします。InterScan をインストールする対象サーバにログオンするためのユーザ名とパスワードを入力します。[次へ] をクリックして続行します。[共有 / 対象ディレクトリの設定] 画面が表示されます。

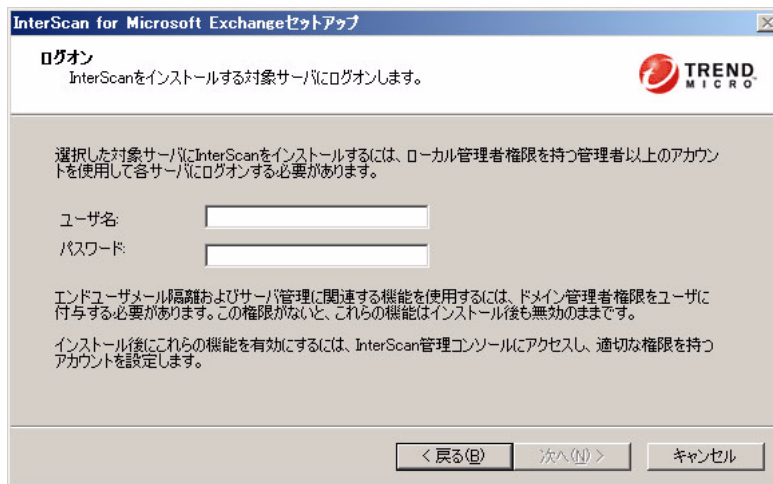


図 2-6. [ログオン] 画面

8. 指定したユーザがアクセス権を持っているディレクトリ共有名を入力するか、初期設定の管理共有ディレクトリ、C\$ をそのまま使用します。セットアッププログラムでは、インストール中は一時ファイルをコピーするために共有ディレクトリを使用します。それには管理者のみがアクセスできます。InterScan をインストールする対象サーバ上のディレクトリパスを入力してください。[次へ] をクリックして続行します。[対象サーバのシステム要件の確認] 画面が表示されます。

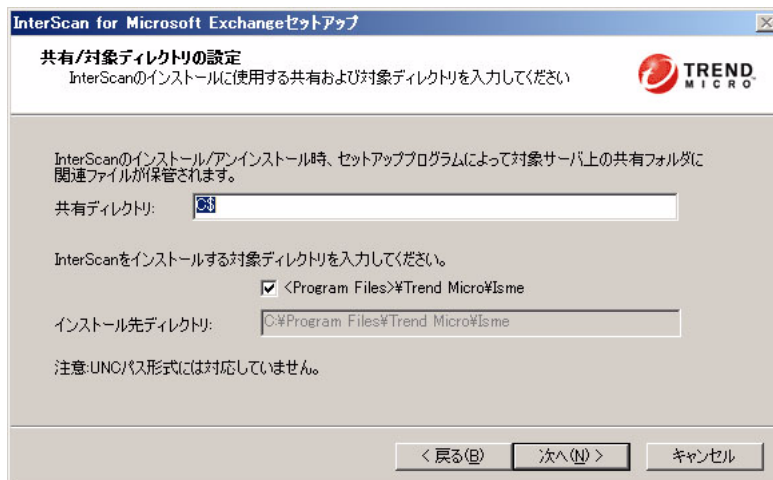


図 2-7. [共有 / 対象ディレクトリの設定] 画面

9. InterScan データファイルをインストールする仮想サーバをダブルクリックします。設定を確認した後、[次へ] をクリックして続行します。[サーバの種類の選択] 画面が表示されます。

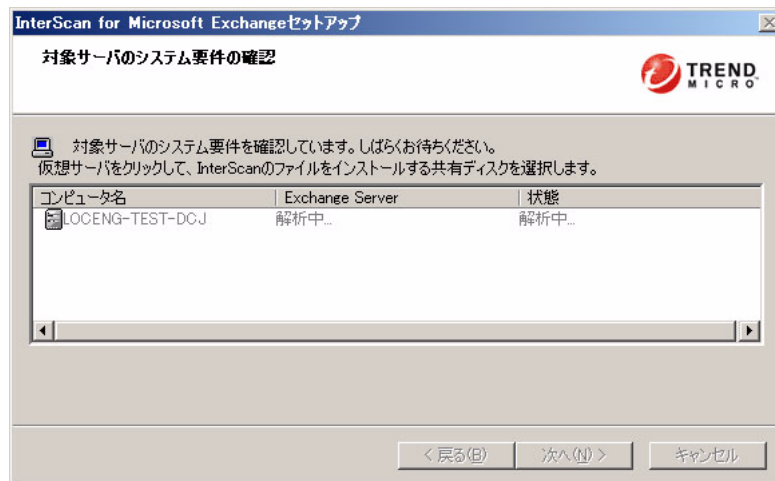


図 2-8. [対象サーバのシステム要件の確認] 画面

10. InterScan が Web サーバとして使用するものとして次のいずれかを選択します。
- Microsoft Internet Information Services (IIS) — Windows Server 2003 を使用している場合、IIS 6.0 が必要です。Windows 2000 Server を使用している場合、IIS 5.0 が必要です。[既定の Web サイト] または [仮想 Web サイト] を選択します。

- **Apache Web サーバ 2.0** — Apache Web サーバ 2.0 以上が見つからない場合、セットアッププログラムによって自動的に Apache Web サーバ 2.0 がインストールされます。IIS Web オプションはグレー表示されます。

[ポート番号] の横に、このサーバの待機ポートとして使用するポート番号を入力します。SSL セキュリティを有効化するオプションもあります。この機能を使用するには、[SSL を有効にする] チェックボックスをオンにします。[次へ] をクリックして続行します。[接続設定] 画面が表示されます。

図 2-9. [Web サーバの種類の選択] 画面

警告： クラスタ環境では SSL を使用しないことをお勧めします。クラスタ環境で SSL を使用すると、SMTP サービスが長い時間保留され、最終的に SMTP リソースで障害が発生します。クラスタで SSL を使用する必要がある場合は、各 Exchange 仮想サーバグループで SMTP リソースの保留タイムアウトを延長してください。

11. プロキシサーバでネットワーク上のインターネットトラフィックを処理する場合、[インターネットへの接続にプロキシサーバを使用する] チェックボックスをオンにし、プロキシで使用している URL アドレスとポート番号を入力します。初期設定では、プロキシサーバは無効になっています。通信に SOCKS 5 を使用する場合は、[SOCKS 5] を選択します。プロキシで認証を必要とする場合は、ユーザ名とパスワードを入力します。[次へ] をクリックして続行します。[製品のアクティベーション] 画面が表示されます。

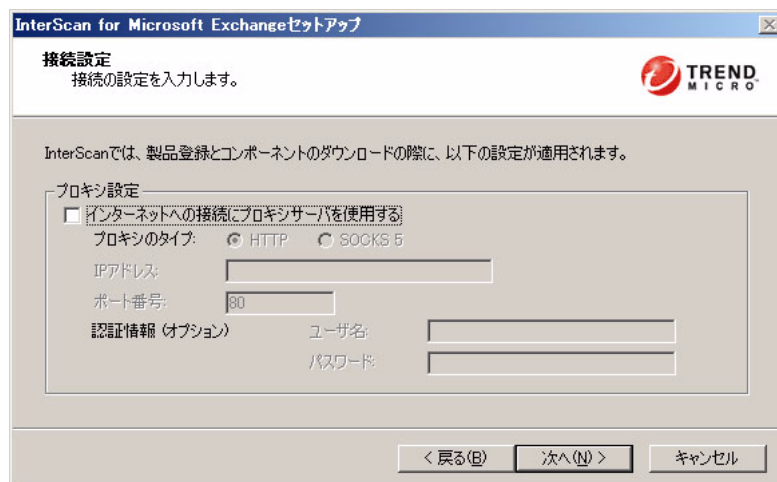


図 2-10. [接続設定] 画面

12. [製品のアクティベーション] 画面で、製品版のアクティベーションコードを入力します。[次へ] をクリックして続行します。[ウイルストラッキングセンターへのウイルス情報送信] 画面が表示されます。

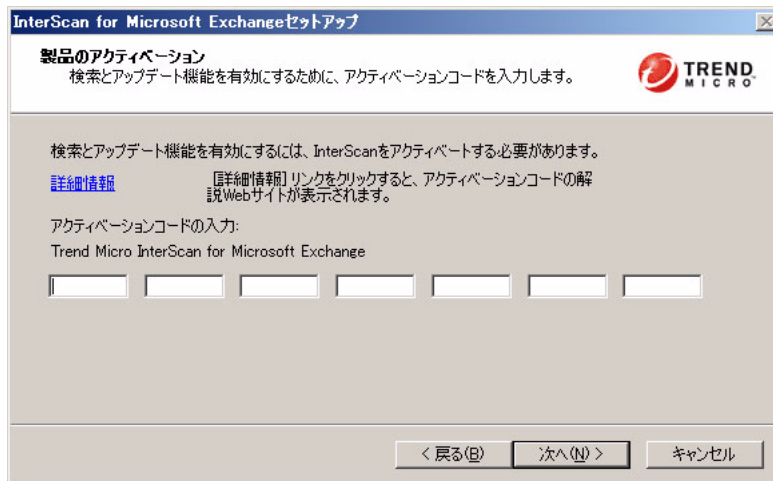


図 2-11. [製品のアクティベーション] 画面

注意： ハイフン (-) を含むアクティベーションコード全体をコピーして、この画面のアクティベーションコードの最初の入力ボックスにカーソルを置き、貼り付けることができます。セットアッププログラムによって、文字列全体が解析され、アクティベーションコードの残りのボックスに値が再入力されます。

13. 記述されている内容を読み、トレンドマイクロのウイルストラッキングプログラムに参加する場合は [情報を送信する] を選択します。参加しない場合でも、インストールを続行できます。[次へ] をクリックして続行します。[エンドユーザーメール隔離] 画面が表示されます。

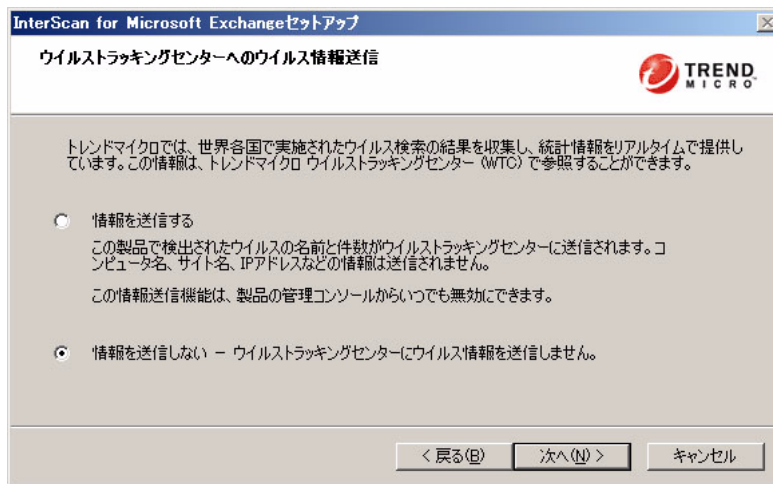


図 2-12. [ウイルストラッキングセンターへのウイルス情報送信] 画面

14. InterScan で検出されたスパムメールを保管するフォルダのオプションを次の中から 1 つ選択します。

- InterScan で検出されたすべてのスパムメールを Outlook の迷惑メールフォルダに送る場合は、[Outlook 迷惑メール対策との統合] を選択します。
- Outlook に InterScan スパムメールフォルダを作成する場合は、[初期設定のスパムメールフォルダ名を使用する] を選択します。初期設定のフォルダ名とは異なるスパムメールフォルダ名を指定することもできます。

[次へ] をクリックして続行します。[Control Manager サーバの設定] 画面が表示されます。

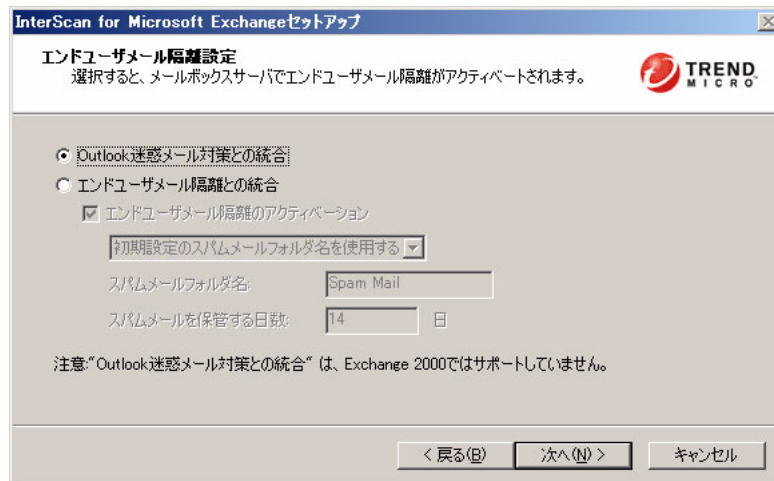


図 2-13. [エンドユーザメール隔離設定] 画面

15. Control Manager サーバの設定を指定します。また、InterScan と Control Manager サーバ間にプロキシサーバを使用する場合は、プロキシサーバを設定します。[次へ] をクリックして続行します。[InterScan 管理コンソールの管理者アカウント] 画面が表示されます。

図 2-14. [Control Manager サーバの設定] 画面

16. この画面を使用して、新しい管理者アカウントを作成するのか、Active Directoryの既存のアカウントを使用するのかを選択します。[スキップして、サーバ管理のアクティベーションを後で再実行する。]を選択することもできます。

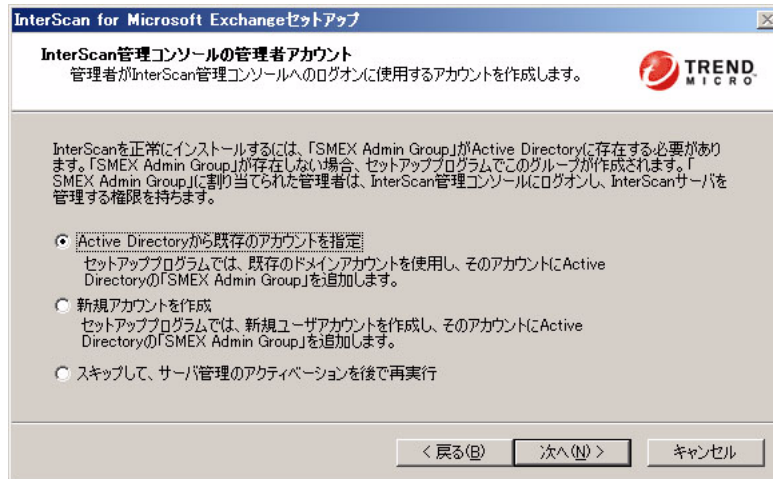


図 2-15. InterScan 管理コンソールの管理者アカウントの設定

この画面では、InterScan 管理者のログオンアカウントを作成します。管理者はここで作成したアカウントを使用して、InterScan 製品コンソールにログオンし、InterScan サーバを管理できます。これらのアカウントを持つ管理者は、サーバ管理機能を使用して、1 つの InterScan サーバから別の InterScan サーバに設定を複製できます。

製品コンソールログオンアカウントを作成するには、[ログオン] 画面でドメイン管理者権限を持つ Windows 管理者アカウントを使用する必要があります。ドメイン管理者権限を持っていない場合、後で InterScan 製品コンソールからアクティベーションを実行することができます。

- a. 製品コンソールアカウントを設定するには、次のいずれかを選択します。

- [Active Directory から既存のアカウントを指定] を選択します。
[InterScan 管理コンソールの管理者アカウント] 画面に、ユーザ名とパスワードの入力欄が表示されます。

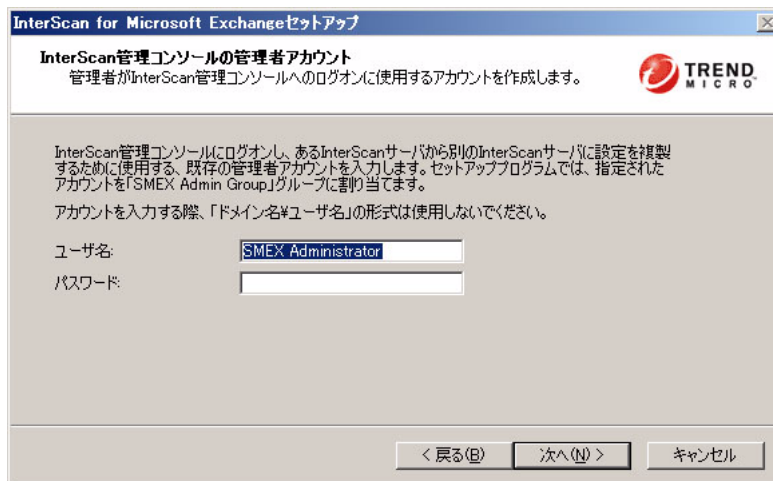


図 2-16. 既存のアカウントに関する情報の指定

セットアップによって Active Directory に「SMEX Admin Group」が作成され、アカウントがグループに追加されます。これは、インストールの初期設定です。

- [新規アカウントの作成] を選択します。[InterScan 管理コンソールの管理者アカウント] 画面に、新しいアカウントのユーザ名とパスワードの入力欄が表示されます。

セットアップによって Active Directory に「SMEX Admin Group」が作成され、次に新しいドメインユーザアカウントが作成され、それがグループに追加されます。

注意： Active Directory にすでに「SMEX Admin Group」が存在する場合は、新たに作成されることはありません。

図 2-17. [InterScan 管理コンソールの管理者アカウント] 画面

- [スキップして、サーバ管理のアクティベーションを後で再実行] を選択します。製品コンソールで [サーバ管理] をクリックして、この機能のアクティベーションを実行します。
- b. [次へ] をクリックして続行します。[設定の確認] 画面が表示されます。

17. [設定を確認して [次へ] をクリックします。[インストールの進行状況] 画面が表示されます。

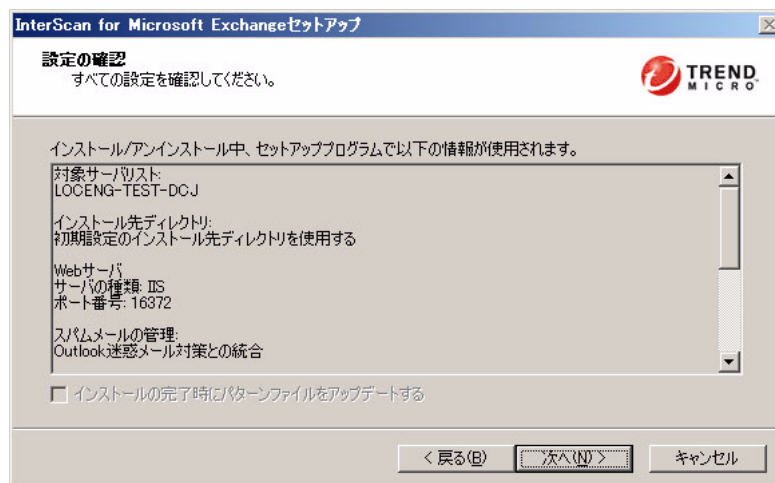


図 2-18. [設定の確認] 画面

18. [詳細の表示] をクリックすると、InterScan をインストールするコンピュータのリストと各コンピュータのステータスが表示されます。インストールが完了したら、[次へ] をクリックします。[インストールの完了] 画面が表示されます。

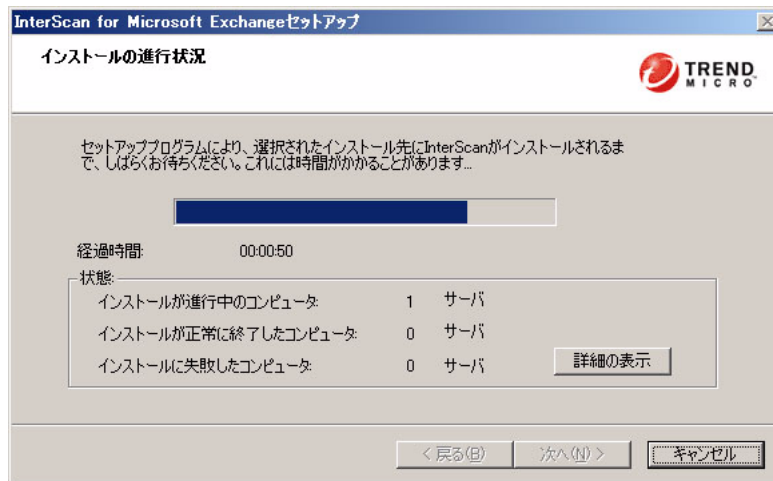


図 2-19. [インストールの進行状況] 画面

19. この画面で、インストールが正常に完了したことが通知されます。[終了] をクリックすると、セットアッププログラムが終了して、Readme ファイルが表示されます。

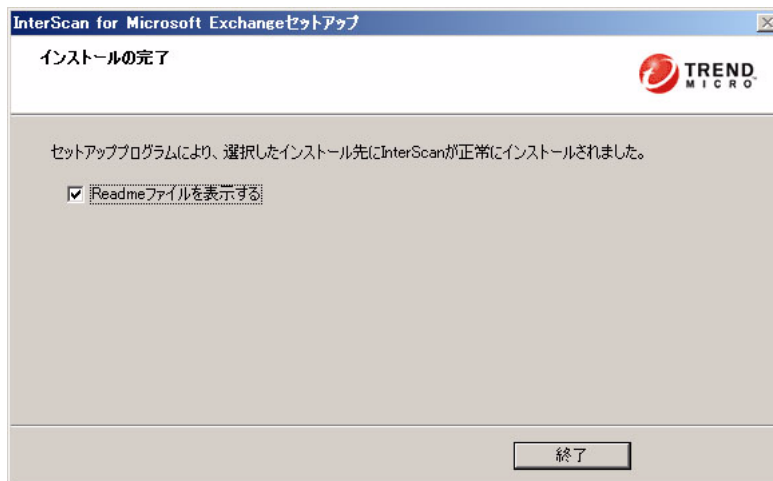


図 2-20. [インストールの完了] 画面

Exchange Server 2007 ハブトランスポート / メールボックスサーバ環境でのインストール

InterScan をインストールするには

1. セットアッププログラムのソースを選択します。
 - a. トレンドマイクロの Web サイト
 - i. トレンドマイクロの Web サイトから InterScan をダウンロードします。
 - ii. 一時ディレクトリにファイルを展開します。
 - iii. setup.exe を実行して InterScan をインストールします。

- b. InterScan の製品 CD-ROM
 - i. CD-ROM を挿入し、setup.exe を実行します。

[InterScan for Microsoft Exchange セットアップ] 画面が表示されます。

- 2. [次へ] をクリックしてインストールを続行します。[使用許諾契約書] 画面が表示されます。



図 2-21. [InterScan for Microsoft Exchange セットアップ] 画面

3. 契約の条件に同意して、インストールを続行するには、[使用許諾契約の条項に同意します] をクリックします。[次へ] をクリックして続行します。[処理の選択] 画面が表示されます。

注意： 契約の条件に同意しない場合は、[使用許諾契約の条項に同意しません] をクリックします。これを選択すると、システムが変更されることなく、セットアッププログラムが終了します。

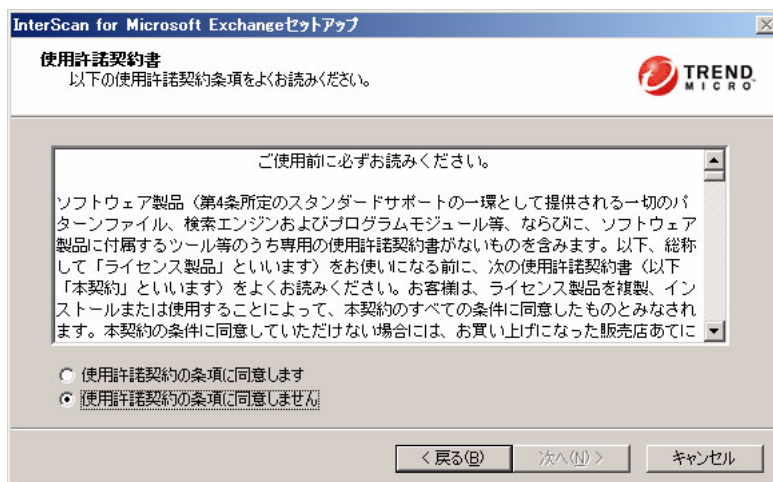


図 2-22. [使用許諾契約書] 画面

4. 次のいずれかの処理を選択します。
- 次の場合は、[インストール / アップグレード] を選択します。
 - 新規インストールを実行する場合

- InterScan 8.0 ベータ版から InterScan 8.0 リリース版にアップグレードする場合
- サーバから InterScan を削除する場合は [アンインストール] を選択します。
110 ページの「InterScan のアンインストール」を参照してください。
[次へ] をクリックして続行します。[サーバの役割の選択] 画面が表示されます。

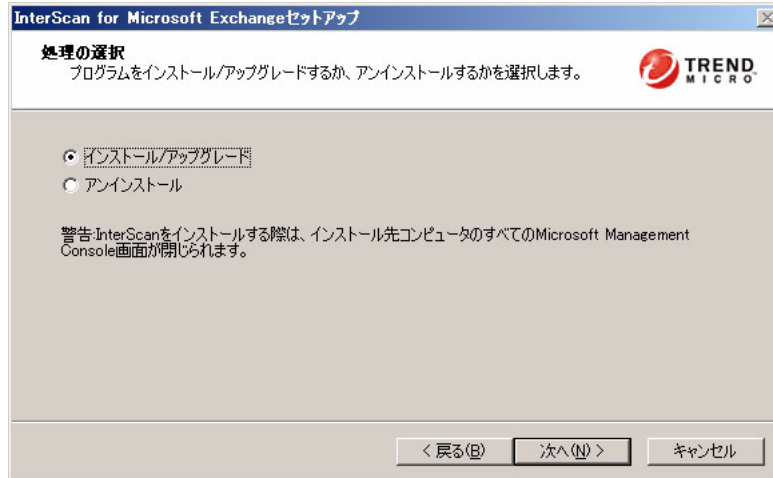


図 2-23. [処理の選択] 画面

5. ハブトランスポート、メールボックスサーバ、またはクラスタ化メールボックスサーバで InterScan をインストールする場合は、[ハブトランスポート / メールボックスサーバ / クラスタ化メールボックスサーバ] を選択します。[次へ] をクリックして続行します。[対象サーバの選択] 画面が表示されます。

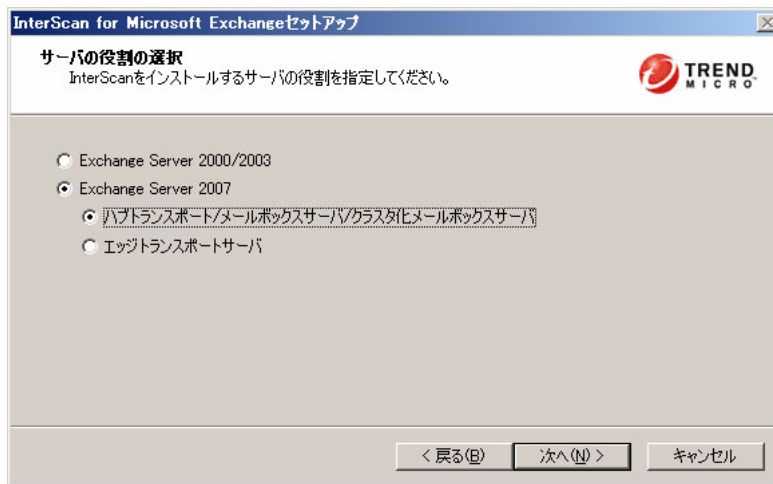


図 2-24. [サーバの役割の選択] 画面

6. 次のいずれかの方法で、InterScan をインストールするコンピュータを選択します。
- [コンピュータ名] にインストールするサーバの名前を入力し、[追加] をクリックしてサーバのリストにコンピュータを追加します。
 - [参照] をクリックしてネットワーク上のコンピュータを参照し、リストに追加するドメインまたはコンピュータをダブルクリックします。
- a. リストからサーバを削除するには [削除] をクリックします。

- b. [次へ] をクリックして、対象サーバのリストを保存し、インストールを続行します。[ログオン] 画面が表示されます。

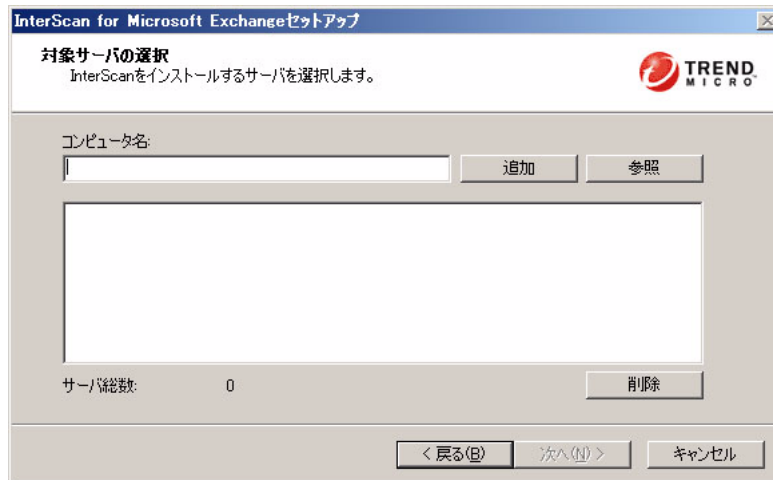


図 2-25. 対象サーバの選択

注意： セットアッププログラムでは、InterScan をいくつかの単一サーバにインストールすることも、1 つのドメイン内のすべてのコンピュータにインストールすることもできます。すべての対象サーバにアクセスできる適切な権限を持つアカウントを使用してください。

7. InterScan をインストールする対象サーバにログインします。ハブトランスポートまたはメールボックスサーバ環境では、Exchange 組織管理者権限とローカル管理者権限を持つアカウントを使用します。InterScan をインストールする対象サーバへのログインに使用するユーザ名とパスワードを入力します。[次へ] をクリックして続行します。[共有 / 対象ディレクトリの設定] 画面が表示されます。

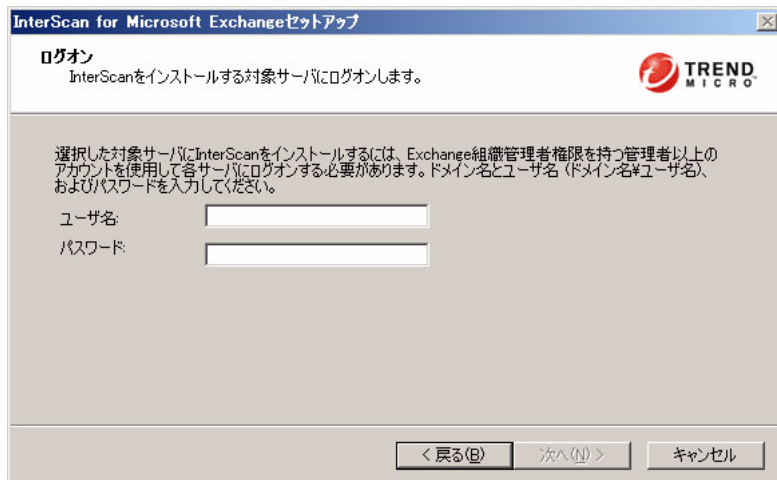


図 2-26. [ログイン] 画面

8. 指定したユーザがアクセス権を持っているディレクトリ共有名を入力するか、初期設定の一時共有ディレクトリ、C\$ をそのまま使用します。セットアッププログラムでは、インストール中は一時ファイルをコピーするために共有ディレクトリを使用します。それには管理者のみがアクセスできます。InterScan をインストールする対象サーバ上のディレクトリパスを入力してください。[次へ] をクリックして続行します。[対象サーバのシステム要件の確認] 画面が表示されます。

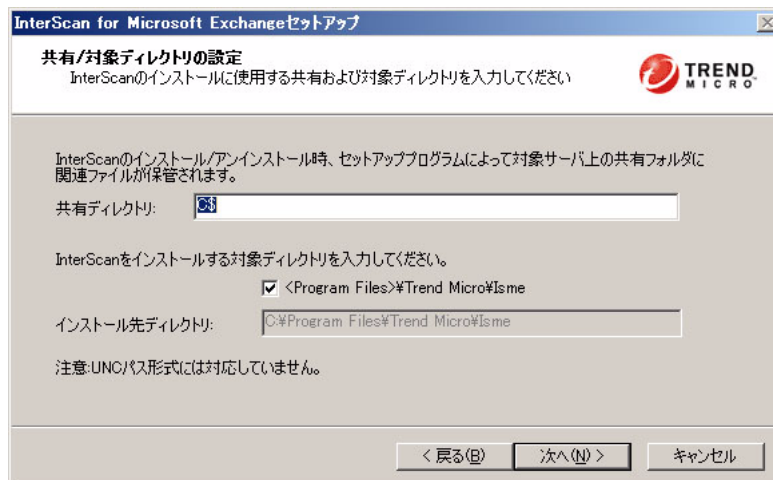


図 2-27. [共有 / 対象ディレクトリの設定]

9. InterScan データファイルをインストールする仮想サーバをダブルクリックします。設定を確認した後、[次へ] をクリックして続行します。[Web サーバの種類
の選択] 画面が表示されます。

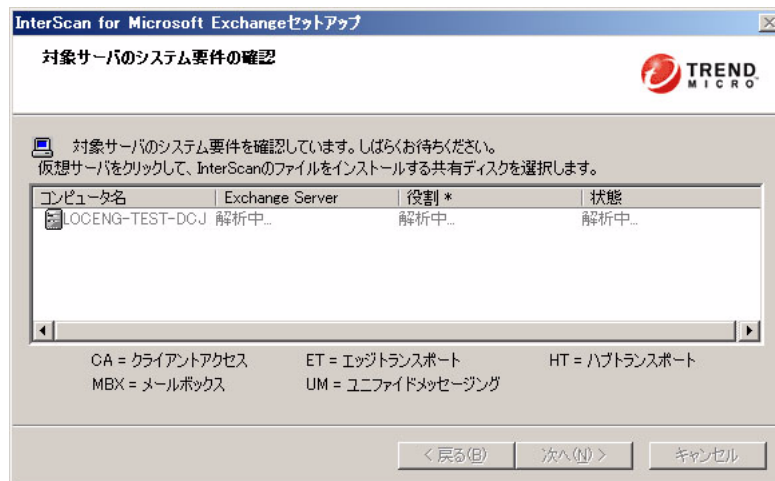


図 2-28. [対象サーバのシステム要件の確認] 画面

注意： 設定が正しくない場合は、[戻る] をクリックするとインストールの前画面に戻れます。

10. InterScan が Web サーバとして使用するものとして次のいずれかを選択します。
- Microsoft Internet Information Services (IIS) — 対象サーバに IIS 6.0 がインストールされている必要があります。[既定の Web サイト] または [仮想 Web サイト] を選択します。
 - Apache Web サーバ 2.0 — Apache Web サーバ 2.0 以上が見つからない場合、セットアッププログラムによって自動的に Apache Web サーバ 2.0 が自動的にインストールされます。IIS Web オプションはグレー表示されます。

[ポート番号] の横に、このサーバの待機ポートとして使用するポート番号を入力します。SSL セキュリティを有効化するオプションもあります。この機能を使用するには、[SSL を有効にする] チェックボックスをオンにします。[次へ] をクリックして続行します。[接続設定] 画面が表示されます。

図 2-29. [Web サーバの種類の選択] 画面

11. プロキシサーバでネットワーク上のインターネットトラフィックを処理する場合、[インターネットへの接続にプロキシサーバを使用する] チェックボックスをオンにし、プロキシで使用している URL アドレスとポート番号を入力します。初期設定では、プロキシサーバは無効になっています。通信に SOCKS 5 を使用する場合は、[SOCKS 5]を選択します。プロキシで認証を必要とする場合は、ユーザ名とパスワードを入力します。[次へ] をクリックして続行します。[製品のアクティベーション] 画面が表示されます。

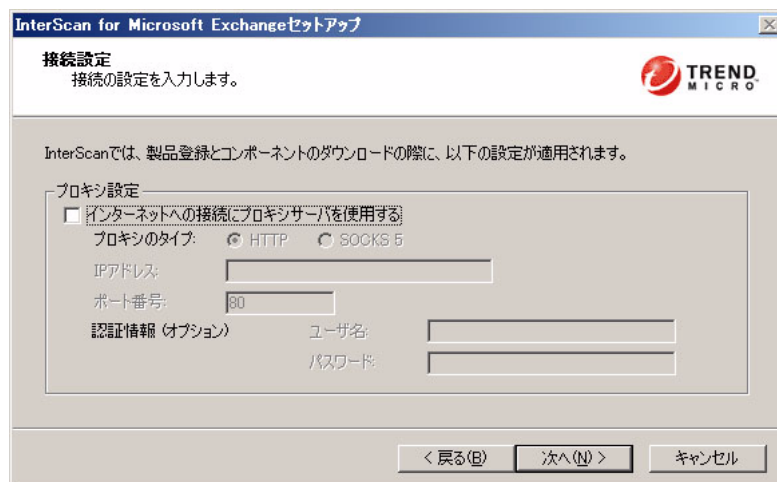


図 2-30. [接続設定] 画面

12. [製品のアクティベーション] 画面で、製品版のアクティベーションコードを入力します。[次へ] をクリックして続行します。[ウイルストラッキングセンターへのウイルス情報送信] 画面が表示されます。

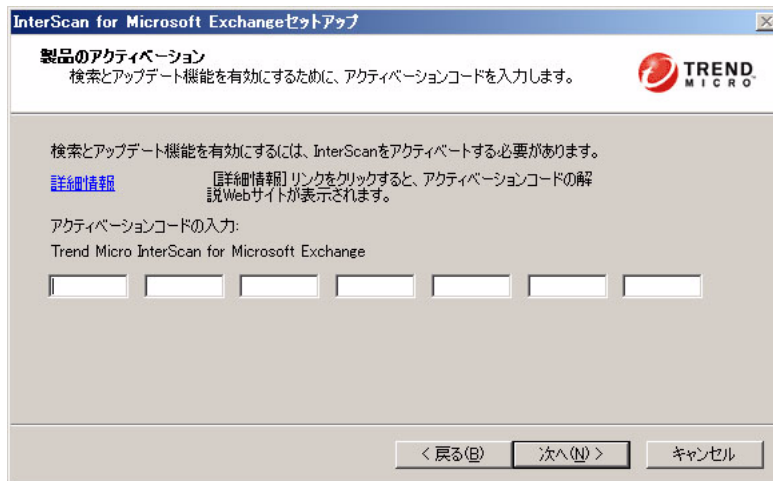


図 2-31. [製品のアクティベーション] 画面

注意： ハイフン (-) を含むアクティベーションコード全体をコピーして、この画面のアクティベーションコードの最初の入力ボックスにカーソルを置き、貼り付けることができます。セットアッププログラムによって、文字列全体が解析され、アクティベーションコードの残りのボックスに値が再入力されます。

13. 記述されている内容を読み、トレンドマイクロのウイルストラッキングプログラムに参加する場合は [情報を送信する] を選択します。参加しない場合でも、インストールを続行できます。[次へ] をクリックして続行します。[Control Manager サーバの設定] 画面が表示されます。

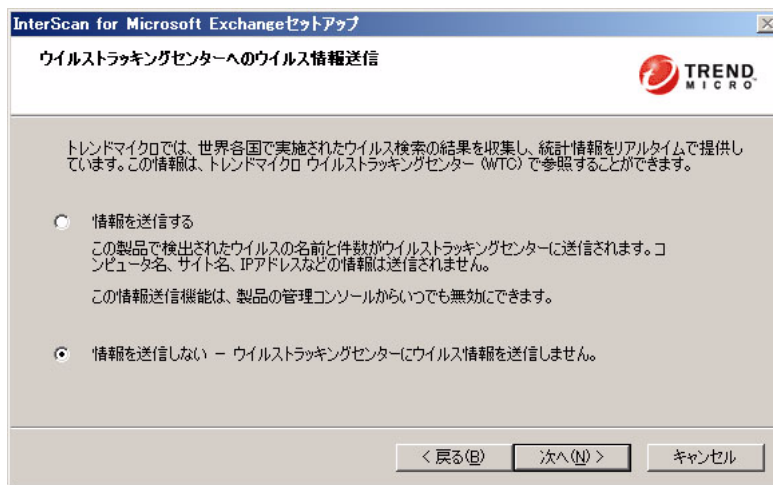


図 2-32. [ウイルストラッキングセンターへのウイルス情報送信] 画面

14. Control Manager サーバを設定します。また、InterScan と Control Manager サーバ間にプロキシサーバを使用する場合は、プロキシサーバを設定します。[次へ] をクリックして続行します。[管理グループの選択] 画面が表示されます。

InterScan for Microsoft Exchange セットアップ

Control Managerサーバの設定
Control Managerサーバへの接続設定を入力してください。

☐ InterScanエージェントをControl Managerサーバに登録する

Control Managerサーバの設定

サーバのアドレス:

ポート番号: ☒ HTTPSによる接続

☐ Control Managerサーバへの接続にプロキシサーバを使用する

Webサーバの認証

ユーザ名: パスワード:

< 戻る(B) 次へ(N) > キャンセル

図 2-33. [Control Manager サーバの設定] 画面

15. [Active Directory グループの選択] をクリックして、InterScan の管理権限を持つ Active Directory グループを設定します。または、[スキップして、後でアクティベートする。] をクリックすることによって、インストール後にこの機能を設定することもできます。[次へ] をクリックして続行します。[設定の確認] 画面が表示されます。

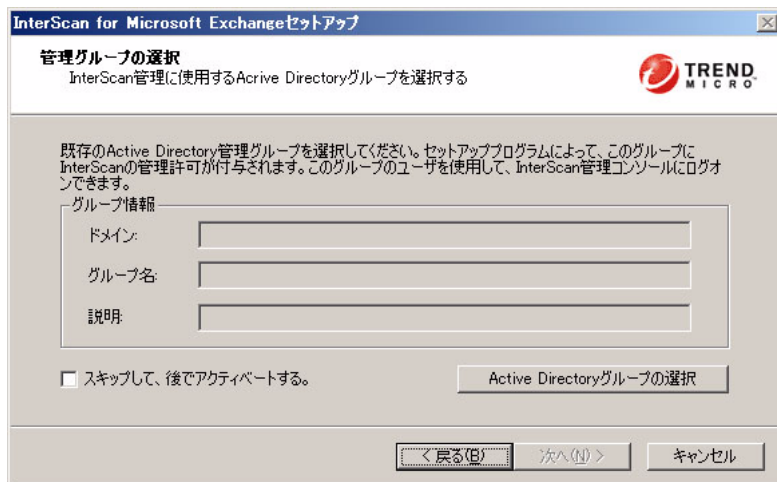


図 2-34. [管理グループの選択] 画面

16. 設定を確認した後、[次へ] をクリックして続行します。[インストールの進行状況] 画面が表示されます。

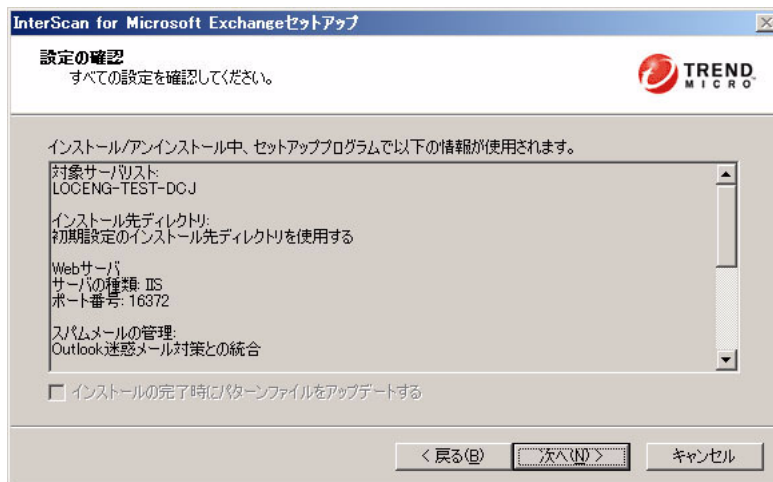


図 2-35. [設定の確認] 画面

17. [詳細の表示] をクリックすると、InterScan をインストールするコンピュータのリストと各コンピュータのステータスが表示されます。インストールが完了したら、[次へ] をクリックします。[インストールの完了] 画面が表示されます。

注意： 64 ビットコンピュータでの設定、ログ、およびレポート用に、InterScan によって Microsoft SQL Server 2005 Express がインストールされます。Microsoft SQL Server 2005 Express のセキュリティレベルは最高に設定されます。

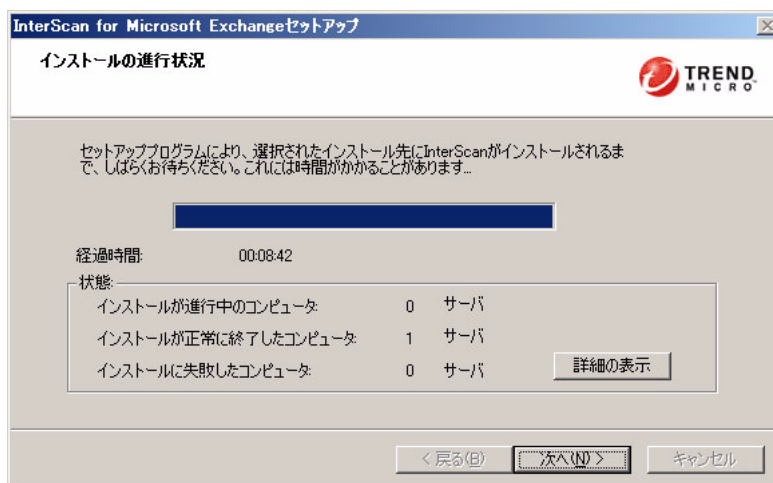


図 2-36. [インストールの進行状況] 画面

18. この画面で、インストールが正常に完了したことが通知されます。[終了] をクリックすると、セットアッププログラムが終了して、Readme ファイルが表示されます。

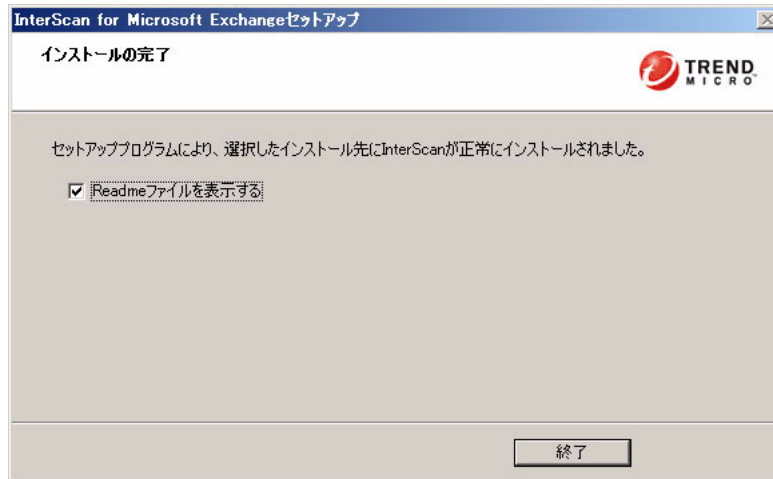


図 2-37. [インストールの完了] 画面

Exchange Server 2007 エッジトランスポートサーバ環境でのインストール

InterScan をインストールするには

1. セットアッププログラムのソースを選択します。
 - a. トレンドマイクロの Web サイト
 - i. トレンドマイクロの Web サイトから InterScan をダウンロードします。
 - ii. 一時ディレクトリにファイルを展開します。
 - iii. setup.exe を実行して InterScan をインストールします。

b. InterScan の製品 CD-ROM

i. CD-ROM を挿入し、setup.exe を実行します。

[InterScan for Microsoft Exchange セットアップ] 画面が表示されます。

2. [次へ] をクリックしてインストールを続行します。[使用許諾契約書] 画面が表示されます。

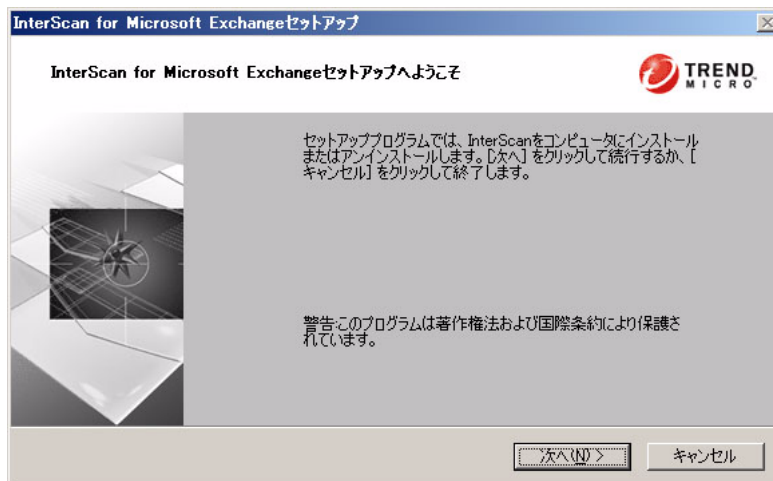


図 2-38. [InterScan for Microsoft Exchange セットアップ] 画面

3. 契約の条件に同意して、インストールを続行するには、[使用許諾契約の条項に同意します] をクリックします。[次へ] をクリックして続行します。[処理の選択] 画面が表示されます。

注意： 契約の条件に同意しない場合は、[使用許諾契約の条項に同意しません] をクリックします。これを選択すると、システムが変更されることなく、セットアップが終了します。

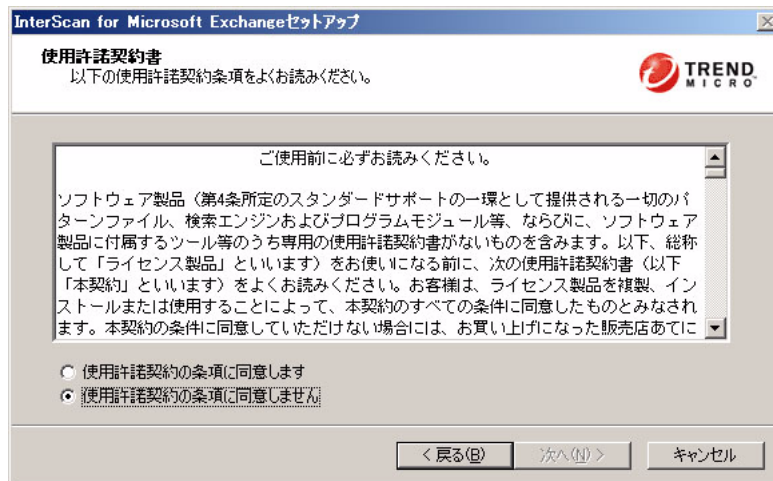


図 2-39. [使用許諾契約書] 画面

4. 次のいずれかの処理を選択します。
 - 次の場合は、[インストール / アップグレード] を選択します。
 - 新規インストールを実行する場合

- InterScan 8.0 ベータ版から InterScan 8.0 リリース版にアップグレードする場合
- サーバから InterScan を削除する場合は [アンインストール] を選択します。アンインストールの詳細については、110 ページの「InterScan のアンインストール」を参照してください。

[次へ] をクリックして続行します。[サーバの役割の選択] 画面が表示されます。

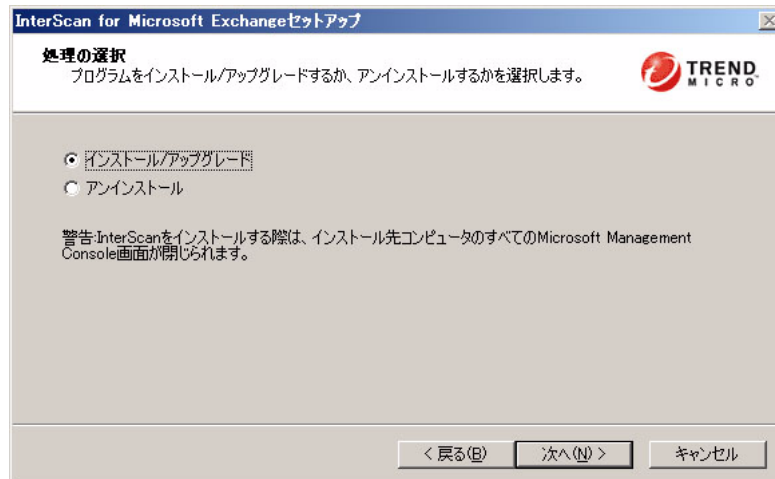


図 2-40. [処理の選択] 画面

5. エッジトランスポートサーバの役割を持つサーバで InterScan をインストールするには、[エッジトランスポートサーバ] を選択します。[次へ] をクリックして続行します。[対象サーバの選択] 画面が表示されます。

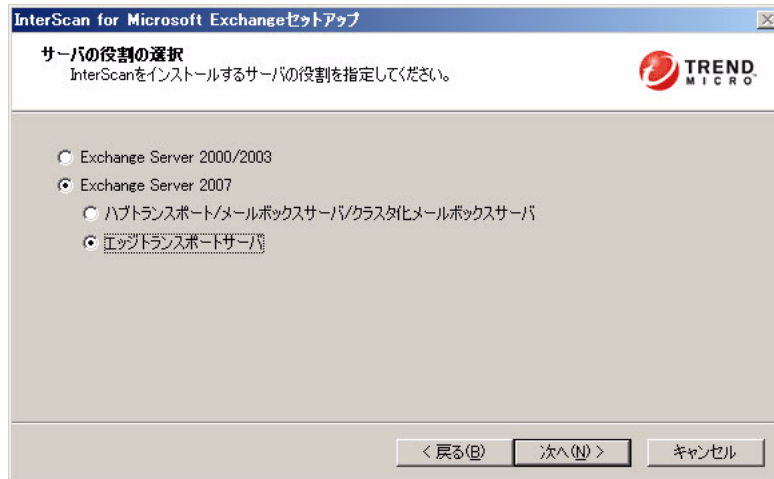


図 2-41. [サーバの役割の選択] 画面

6. 次のいずれかの方法で、InterScan をインストールするコンピュータを選択します。
- [コンピュータ名] にインストールするサーバの名前を入力し、[追加] をクリックしてサーバのリストにコンピュータを追加します。
 - [参照] をクリックしてネットワーク上のコンピュータを参照し、リストに追加するドメインまたはコンピュータをダブルクリックします。
- a. リストからサーバを削除するには [削除] をクリックします。

- b. [次へ] をクリックして、対象サーバのリストを保存し、インストールを続行します。[ログオン] 画面が表示されます。

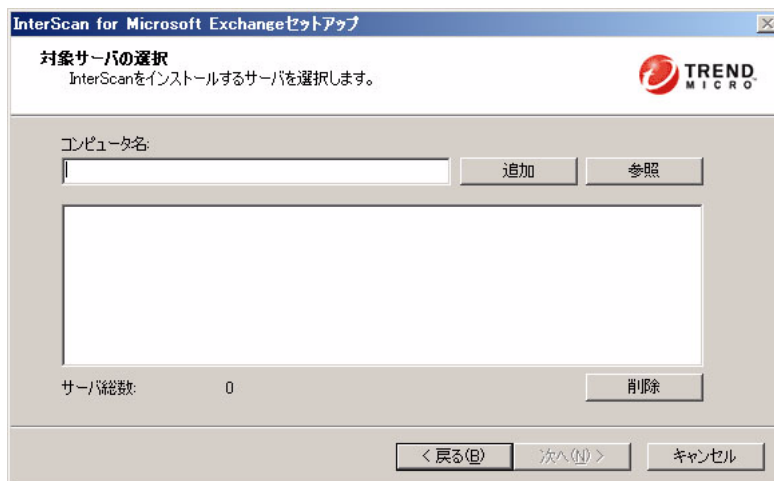


図 2-42. 対象サーバの選択

注意： セットアッププログラムでは、InterScan をいくつかの単一サーバにインストールすることも、1 つのドメイン内のすべてのコンピュータにインストールすることもできます。すべての対象サーバにアクセスできる適切な権限を持つアカウントを使用する必要があります。

7. InterScan をインストールする対象サーバにログオンします。ローカル管理者権限を持つアカウントを使用してください。InterScan をインストールする対象サーバにログオンするためのユーザ名とパスワードを入力します。[次へ] をクリックして続行します。[共有 / 対象ディレクトリの設定] 画面が表示されます。

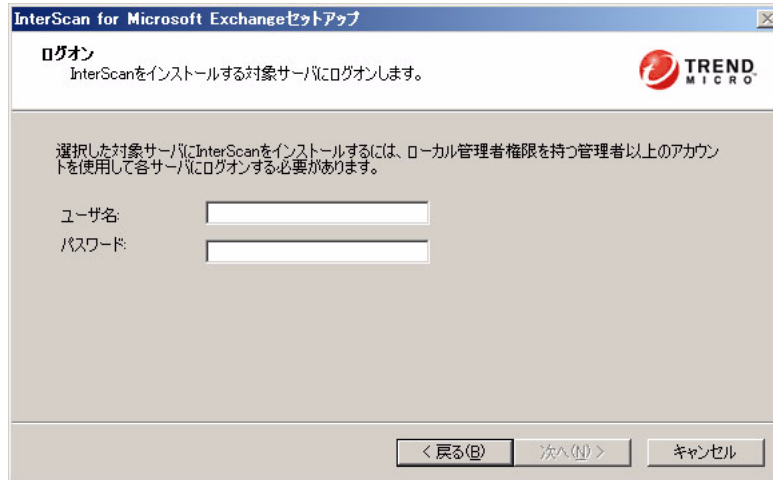


図 2-43. [ログオン] 画面

8. 指定したユーザがアクセス権を持っているディレクトリ共有名を入力するか、初期設定の一時共有ディレクトリ、C\$ をそのまま使用します。セットアッププログラムでは、インストール中は一時ファイルをコピーするために共有ディレクトリを使用します。それには管理者のみがアクセスできます。InterScan をインストールする対象サーバ上のディレクトリパスを入力してください。[次へ] をクリックして続行します。[対象サーバのシステム要件の確認] 画面が表示されます。

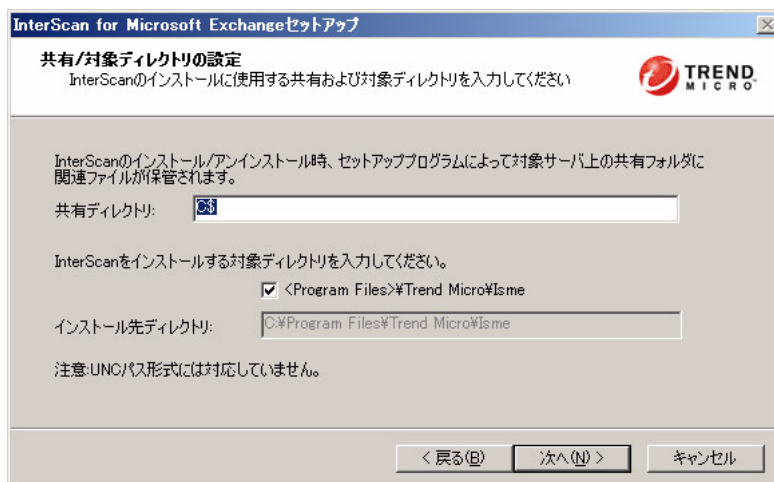


図 2-44. [共有 / 対象ディレクトリの設定]

9. InterScan データファイルをインストールする仮想サーバをダブルクリックします。設定を確認した後、[次へ] をクリックして続行します。[Web サーバの種類
の選択] 画面が表示されます。

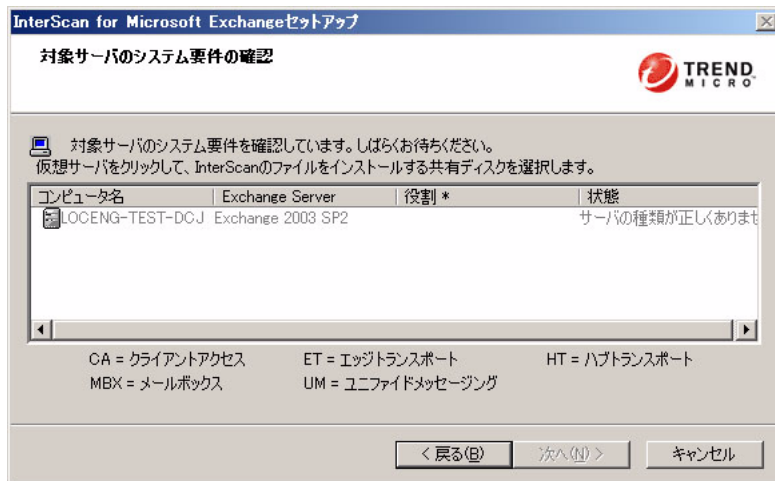


図 2-45. [対象サーバのシステム要件の確認] 画面

注意： 設定が正しくない場合は、[戻る] をクリックするとインストールの前画面に戻れます。

10. InterScan が Web サーバとして使用するものとして次のいずれかを選択します。

- Microsoft Internet Information Services (IIS) — 対象サーバに IIS 6.0 がインストールされている必要があります。[既定の Web サイト] または [仮想 Web サイト] を選択します。
- Apache Web サーバ 2.0 — Apache Web サーバ 2.0 以上が見つからない場合、セットアッププログラムによって自動的に Apache Web サーバ 2.0 が自動的にインストールされます。IIS Web オプションはグレー表示されます。

[ポート番号] の横に、このサーバの待機ポートとして使用するポート番号を入力します。SSL セキュリティを有効化するオプションもあります。この機能を使用するには、[SSL を有効にする] チェックボックスをオンにします。[次へ] をクリックして続行します。[接続設定] 画面が表示されます。

図 2-46. [Web サーバの種類の選択] 画面

11. プロキシサーバでネットワーク上のインターネットトラフィックを処理する場合、[インターネットへの接続にプロキシサーバを使用する] チェックボックスをオンにし、プロキシで使用している URL アドレスとポート番号を入力します。初期設定では、プロキシサーバは無効になっています。通信に SOCKS 5 を使用する場合は、[SOCKS 5] を選択します。プロキシで認証を必要とする場合は、認証に使用するユーザ名とパスワードを入力します。[次へ] をクリックして続行します。[製品のアクティベーション] 画面が表示されます。

図 2-47. [接続設定] 画面

12. [製品のアクティベーション] 画面で、製品版のアクティベーションコードを入力します。[次へ] をクリックして続行します。[ウイルストラッキングセンターへのウイルス情報送信] 画面が表示されます。

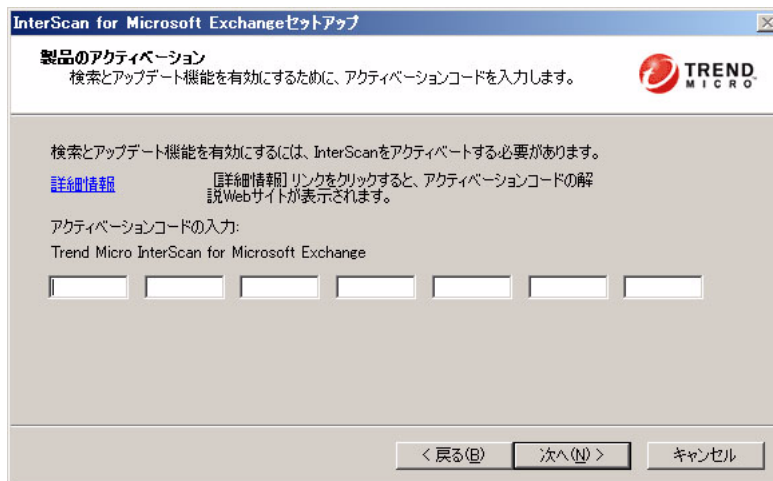


図 2-48. [製品のアクティベーション] 画面

注意： ハイフン (-) を含むアクティベーションコード全体をコピーして、この画面のアクティベーションコードの最初の入力ボックスにカーソルを置き、貼り付けることができます。セットアッププログラムによって、文字列全体が解析され、アクティベーションコードの残りのボックスに値が再入力されます。

13. 記述されている内容を読み、トレンドマイクロのウイルストラッキングプログラムに参加する場合は [情報を送信する] を選択します。参加しない場合でも、インストールを続行できます。[次へ] をクリックして続行します。[Control Manager サーバの設定] 画面が表示されます。

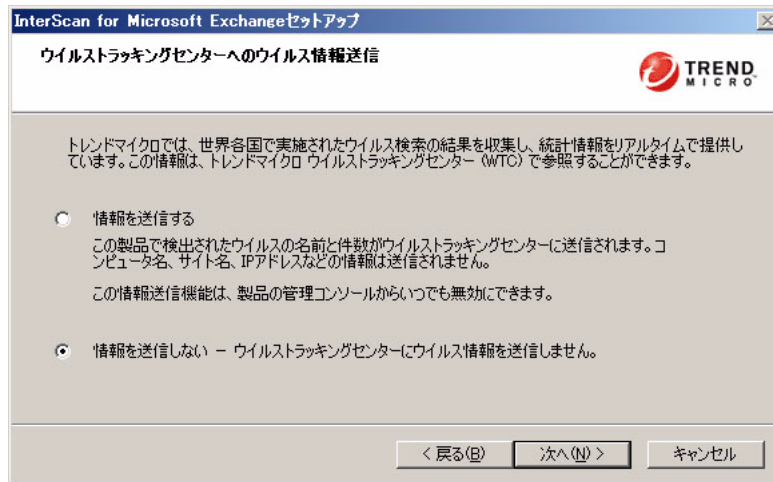


図 2-49. [ウイルストラッキングセンターへのウイルス情報送信] 画面

14. Control Manager サーバを設定します。また、InterScan と Control Manager サーバ間にプロキシサーバを使用する場合は、プロキシサーバを設定します。[次へ] をクリックして続行します。[設定の確認] 画面が表示されます。

図 2-50. [Control Manager サーバの設定] 画面

15. 設定を確認して [次へ] をクリックします。[インストールの進行状況] 画面が表示されます。

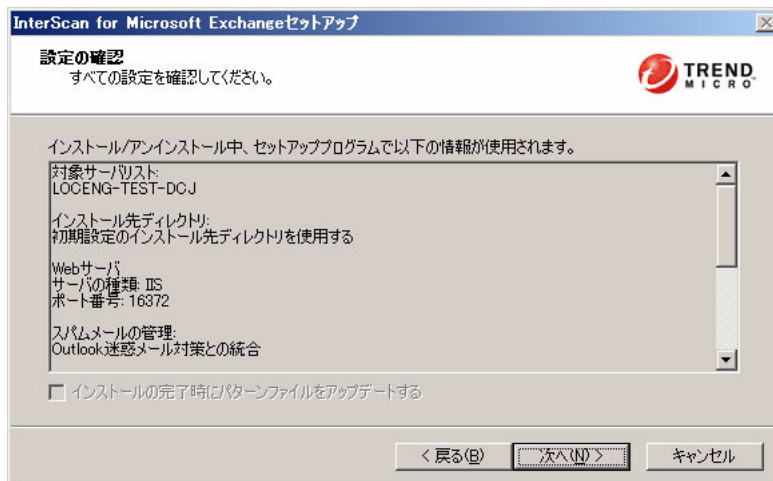


図 2-51. [設定の確認] 画面

16. [詳細の表示] をクリックすると、InterScan をインストールする各コンピュータのリストと各コンピュータのステータスが表示されます。インストールが完了したら、[次へ] をクリックします。[インストールの完了] 画面が表示されます。

注意： 64 ビットコンピュータでの設定、ログ、およびレポート用に、InterScan によって Microsoft SQL Server 2005 Express がインストールされます。Microsoft SQL Server 2005 Express のセキュリティレベルは最高に設定されます。

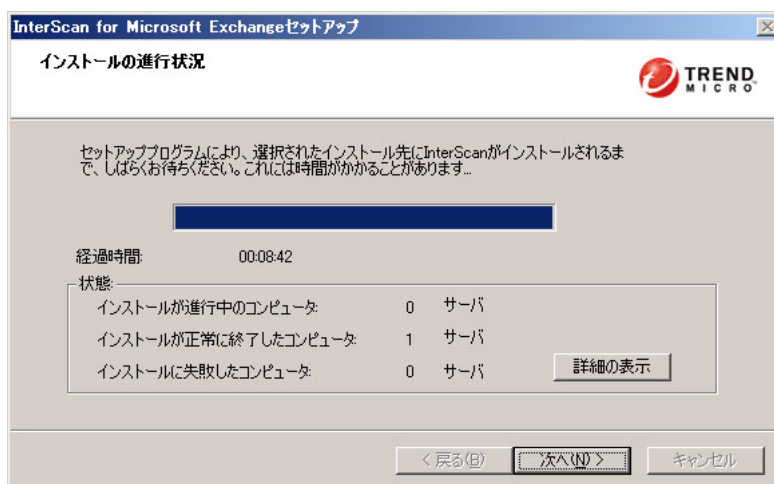


図 2-52. [インストールの進行状況] 画面

17. この画面で、インストールが正常に完了したことが通知されます。[終了] をクリックすると、セットアッププログラムが終了して、Readme ファイルが表示されます。

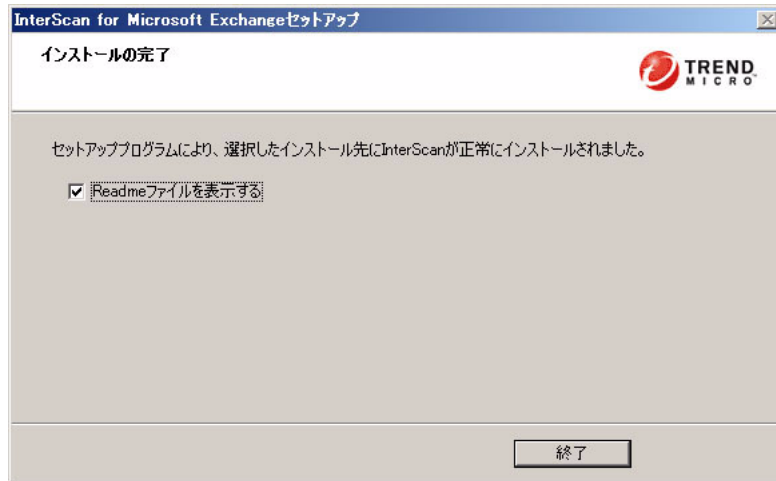


図 2-53. [インストールの完了] 画面

18. InterScan 製品コンソールにログオンするには、ローカル管理者権限を持つアカウントを使用します。

クラスタ環境でのインストール

通常の InterScan セットアッププログラムを使用して、Windows 2000 または 2003 クラスタのすべての仮想サーバに InterScan をインストールできます。クラスタへのインストールの場合、通常の対象サーバを選択するときと同じように仮想サーバを選択できます。セットアッププログラムによって、クラスタに属する各ノードに InterScan が同時にインストールされ、InterScan リソースが各仮想サーバグループに追加されます。

クラスタサーバで InterScan をインストールする手順は、クラスタでない通常のサーバでのインストール手順と同様です。詳細については、49 ページの「セットアッププログラムの実行」を参照してください。

InterScan をインストールするときに、Exchange 仮想サーバがオフラインになっていたり、インストールされていない場合は、クラスタへのインストールは正常に行われません。この場合、サーバをオンラインにした後、仮想サーバグループ上にリソースを手動で作成する必要があります。

クラスタサーバの手動インストールの詳細については、151 ページの「仮想サーバの InterScan リソースの手動作成」を参照してください。

インストール後の処理

正常にインストールされたことの確認

InterScan は、初期設定では次のディレクトリにインストールされます。

C:\Program Files\Trend Micro\Isme

InterScan をインストールすると、次のサービスが追加されます。

**InterScan for Microsoft Exchange Master Service
InterScan for Microsoft Exchange Remote Configuration Server**

注意： エッジトランスポートサーバの役割を持つ Exchange Server 2007
サーバで InterScan を使用する場合、このサービスは追加されません。

InterScan for Microsoft Exchange System Watcher

InterScan をインストールすると、次のレジストリキーが追加されます。

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Scanmail for Exchange

注意： Exchange 2000 Server、Exchange Server 2003、Exchange Server 2007 ハブト
ランスポートおよびメールボックスサーバ、Exchange Server 2007 メール
ボックスサーバで InterScan を使用する場合は、以下のキーが追加されます。
Exchange Server 2007 エッジトランスポートサーバおよび Exchange Server
2007 ハブトランスポートサーバで InterScan を使用する場合、これらのキーは
追加されません。

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSEExchangeIS\
VirusScan**

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSEExchangeIS\
<サーバ名>\Private-<MDB-GUID>\VirusScanEnabled**

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSEExchangeIS\
<サーバ名>\Private-<MDB-GUID>\VirusScanBackgroundScanning**

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSEExchangeIS\
<サーバ名>\Public-<MDB-GUID>\VirusScanEnabled**

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSEExchangeIS\
<サーバ名>\Public-<MDB-GUID>\VirusScanBackgroundScanning**

インストール後のテスト

EICAR テストスクリプトを使用して InterScan 機能をテストし、インストールが正常に完了したかどうかを確認することをお勧めします。EICAR (European Institute for Computer Antivirus Research) は、ウイルス対策ソフトウェアが適切にインストールされ、設定されたことを確認するために開発されました。

詳細については、次の EICAR の Web サイトを参照してください。

<http://www.eicar.org>

EICAR テストスクリプトは、*.com 拡張子が付いたテキストファイルです。これはウイルス / 不正プログラムではなく、複製されず、ペイロードを含みません。

警告： ウイルス対策製品のインストールをテストするために、実際のウイルス / 不正プログラムを使用しないでください。

Exchange サーバの構成によっては、EICAR テストの間、ウイルス対策製品を無効にする必要があります (無効にしないと、Exchange サーバに到達する前に EICAR が検出されてしまう場合があります)。一方で、ウイルス対策製品を無効にすると、サーバには感染の恐れがあります。このため、テスト環境で EICAR のみを使用することをお勧めします。

リアルタイム検索をテストするには

1. テスト対象の Exchange 2000、2003、または 2007 に有効なメールクライアントを接続してあることを確認してください。
2. <http://www.antivirus.com/vinfo/testfiles/index.htm> にアクセスして、業界標準の EICAR テストファイルのコピーをテスト用にダウンロードします。
3. リアルタイム検索およびリアルタイムモニタが正常に実行されていることを確認します。[リアルタイムモニタ] 画面で、「リアルタイム検索の実行開始日時」というメッセージが表示されているかどうか確認します。

4. メールクライアントを開き、「Test InterScan」という件名のテストメッセージを作成します。そのメールに EICAR テストファイルのコピーを添付し、テスト用メールボックス宛に送信します。
5. メッセージがメールボックスに送信されたら、[リアルタイムモニタ] 画面に戻ります。メッセージが検索されているのがリアルタイムモニタでわかります。また、リアルタイムモニタでテストファイルが検出されているのもわかります。リアルタイムモニタ以外でも、InterScan 管理コンソールのウイルスログでウイルスの検出結果を確認できます。

ウイルス通知をテストするには

1. ウイルス / 不正プログラムを検出して管理者に通知するようにウイルス検索を設定します。
 - a. [ウイルス検索]→[対象] の順に選択します。必要に応じて、[トレンドマイクロの推奨設定] を選択します。
 - b. 必要に応じて、[トレンドマイクロの推奨設定] を選択します。[処理] をクリックします。[トレンドマイクロの推奨処理] を選択し、ドロップダウンリストから [通知する] を選択します。
 - c. [通知] をクリックします。[管理者に通知する] チェックボックスをオンにし、ページ拡張アイコンをクリックして設定項目を表示します。[送信先] を選択し、通知の送信先メールアドレスを入力します。
 - d. [保存] をクリックします。
2. EICAR テストスクリプトを含むメールを送信し、管理者がメールを受信したことを確認します。
 - a. 「Test InterScan」という件名のテストメッセージを作成し、EICAR テストスクリプトのコピーをメールに添付します。
 - b. メールをテスト用メールボックスに送信します。
 - c. 管理者のメールボックスに移動し、通知を表示します。

サイレントインストール

本バージョンの InterScan では、サイレントインストールをサポートしています。

サイレントインストールの一般的な手順は次のとおりです。

1. Windows のコマンドプロンプトを起動します。
2. InterScan for Exchange ディレクトリを見つけます。
3. 「Setup /R」と入力して記録モードを開始します。
4. 記録が完了したら、事前設定ファイル (setup-xxx.iss) を InterScan for Exchange ディレクトリにコピーします。
5. 「Setup /S <事前設定ファイル名>」と入力して、サイレントインストールを実行します。

新しい事前設定ファイルを記録しない場合は、パラメータを使用して既存の事前設定ファイルのユーザ名とパスワードを変更することもできます。次の表に、サイレントインストールの設定に使用できるパラメータを示します。

パラメータ	説明
Setup /H [Help] ?	ヘルプ画面を表示します。
Setup /R <事前設定ファイルのパス>	記録モードを開始します。パスを空白にした場合、初期設定パスとして Windows ディレクトリが使用されます。
Setup /S <事前設定ファイルの名前>	指定したファイル名のファイルを使用して、サイレントインストールを実行します。
Setup /USER <ユーザ名>	事前設定ファイルに定義されているログオンユーザ名と異なるユーザ名を指定することによって、定義されているユーザ名 / パスワードを変更します。サイレントインストールを開始する前にパスワードを入力する必要があります。

表 2-8. サイレントインストールの設定パラメータ

パラメータ	説明
Setup /CONSOLEUSER <ユーザ名>	事前設定ファイルに定義されているコンソールユーザ名と異なるユーザ名を指定することによって、定義されているユーザ名 / パスワードを変更します。サイレントインストールを開始する前にパスワードを入力する必要があります。
Setup /PROXYUSER <ユーザ名>	事前設定ファイルに定義されている InterScan プロキシユーザ名と異なるユーザ名を指定することによって、定義されているユーザ名 / パスワードを変更します。サイレントインストールを開始する前にパスワードを入力する必要があります。
Setup /CMPROXYUSER <ユーザ名>	事前設定ファイルに定義されている Control Manager エージェントプロキシユーザ名と異なるユーザ名を指定することによって、定義されているユーザ名 / パスワードを変更します。サイレントインストールの開始前にパスワードを入力する必要があります。
Setup /CMWEBUSER <ユーザ名>	事前設定ファイルに定義されている Control Manager エージェント Web ユーザ名と異なるユーザ名を指定することによって、定義されているユーザ名 / パスワードを変更します。サイレントインストールの開始前にパスワードを入力する必要があります。
Setup /MV	「詳細モード」に切り替えて、コマンドプロンプトウィンドウに進行状況を表示します。初期設定は簡潔モードです。このモードでは、処理過程は表示されず、ログファイルへの記録のみ行われます。
Setup /L <ログファイルのパス>	ログファイルのパスを指定します。初期設定パスは InterScan ソースファイルフォルダです。

表 2-8. サイレントインストールの設定パラメータ

サイレントインストールの制限

サイレントインストールの制限は次のとおりです。

- サイレントインストールはローカルコンピュータに対してのみ実行できます。
- サイレントインストールはクラスタサーバには実行できません。
- 最初に、記録モードを使用して事前設定ファイルを生成します。その後、事前設定ファイルの設定を変更します。ただし、「Do not edit」セクションの設定は変更しないでください。
- アップグレードを実行する場合は、最新バージョンを使用して設定を記録します。アップグレードの実行時には以前の設定が維持されます。
- 各対象サーバ間で使用言語が異なる場合は、言語ごとに個別に設定を記録します。英語の OS で記録した事前設定ファイルを、ドイツ語の OS を使用している対象サーバに適用しないでください。

サイレントインストールの実行

サイレントインストールの手順は通常のインストールの手順と基本的に同じです。それぞれのサーバの役割に応じて、次のいずれかのインストールセクションを参照してください。49 ページの「Exchange 2000 Server および Exchange Server 2003 環境でのインストール」、69 ページの「Exchange Server 2007 ハブトランスポート / メールボックスサーバ環境でのインストール」、86 ページの「Exchange Server 2007 エッジトランスポートサーバ環境でのインストール」。

サイレントインストールは、次の点で通常のインストールプロセスと異なります。

- [InterScan for Microsoft Exchange セットアップ] 画面に、インストールプロセスが事前設定ファイルに記録されることを通知するメッセージが表示されます。
- 記録モードでは、ユーザ名とパスワードのみ記録されます。対象サーバへのログオンは実行されません。
- 記録が完了すると、ファイルの名前と場所の情報がセットアップ画面に表示されます。
- [対象サーバのシステム要件の確認] 画面と[処理の選択] 画面は表示されません。

InterScan のアンインストール

InterScan のアンインストールを実行すると、次のコンポーネントが削除されます。

- InterScan 製品コンソール
- すべてのプログラムファイル
- エンドユーザメール隔離 (エンドユーザの承認する送信者リストを含む)
- プログラムフォルダ
- ディレクトリ
- レジストリに追加されたエントリ

Exchange Server 2007 で InterScan 8.0 を使用している場合、InterScan 8.0 をアンインストールしても、以下のコンポーネントは削除されません。

- Microsoft Visual C++ 2005 再頒布可能パッケージ
- Microsoft Visual C++ 2005 再頒布可能パッケージ (X64)

警告： InterScan は、Windows コントロールパネルまたはセットアッププログラムを使用してアンインストールしてください。セットアッププログラムによって多数のレジストリエントリが自動的に削除されます。InterScan は手動でアンインストールしないでください。

次の表に、InterScan のアンインストールに最低限必要な権限を示します。

Exchange のバージョン	最低限必要な権限	ドメイン管理者の権限がない場合に制限される機能
Exchange 2000 Server および Exchange Server 2003	ローカル管理者および ドメインユーザ	エンドユーザメール隔離の メールボックスを削除でき ません。エンドユーザメール 隔離のメールボックスを手 動で削除する必要があります。
Exchange Server 2007 エッジトランスポート	ローカル管理者	該当なし
Exchange Server 2007 ハブ / メールボックス / クラスタ	ローカル管理者および Exchange 組織管理者	該当なし

表 2-9. InterScan のアンインストールに最低限必要な権限

製品 CD-ROM を使用したアンインストール

1. 製品 CD-ROM から setup.exe を実行します。

注意： インストール中にセットアッププログラムで [キャンセル] をクリックすると、終了確認のダイアログボックスが表示されます。このダイアログボックスで [はい] をクリックすると、アンインストールが中止されます。

2. [InterScan for Microsoft Exchange セットアップ] 画面が開きます。[次へ] をクリックし、続行します。



図 2-54. [InterScan for Microsoft Exchange セットアップ] 画面

3. [使用許諾契約書] 画面が表示されます。契約の条件に同意しない場合は、[使用許諾契約の条項に同意しません] をクリックします。これを選択すると、システムが変更されることなく、プロセスが終了します。契約の条件に同意する場合は、[使用許諾契約の条項に同意します] をクリックし、[次へ] をクリックして続行します。[処理の選択] 画面が表示されます。

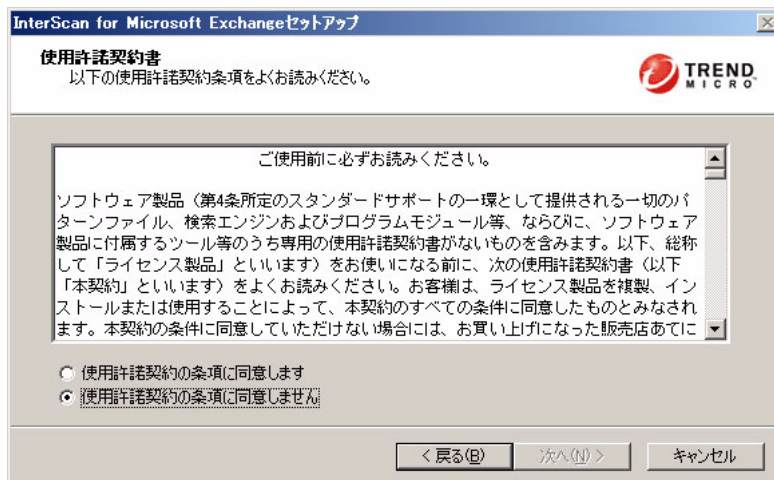


図 2-55. [使用許諾契約書] 画面

4. サーバから InterScan を削除する場合は、[アンインストール] を選択します。[対象サーバの選択] 画面が表示されます。

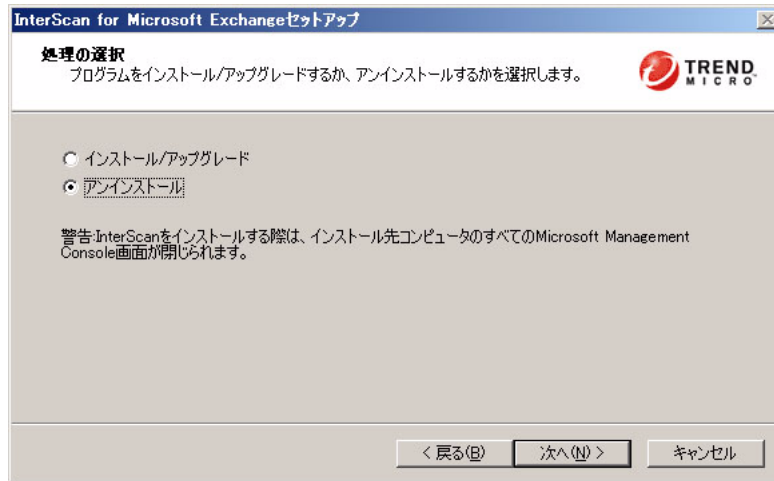


図 2-56. [処理の選択] 画面

サーバから InterScan をアンインストールするには、次の手順に従ってください。

- a. 次のいずれかの方法で、InterScan をアンインストールするコンピュータを選択します。
 - [コンピュータ名] に InterScan をアンインストールするサーバの名前を入力します。
 - [参照] をクリックして、ネットワーク上のコンピュータを参照し、リストに追加するコンピュータをダブルクリックします。
 - b. そのコンピュータを InterScan をアンインストールするサーバのリストに追加するには [追加] をクリックし、リストからサーバを削除するには [削除] をクリックします。
 - c. [次へ] をクリックして、対象サーバのリストを保存し、アンインストールを続行します。
5. サーバから InterScan をアンインストールします。

- a. 次のいずれかの方法で、InterScan をアンインストールするコンピュータを選択します。
 - [コンピュータ名] にアンインストールするサーバの名前を入力し、[追加] をクリックしてサーバのリストにコンピュータを追加します。
 - [参照] をクリックしてネットワーク上のコンピュータを参照し、リストに追加するドメインまたはコンピュータをダブルクリックします。
- b. リストからサーバを削除するには [削除] をクリックします。
- c. [次へ] をクリックして、対象サーバのリストを保存し、アンインストールを続行します。

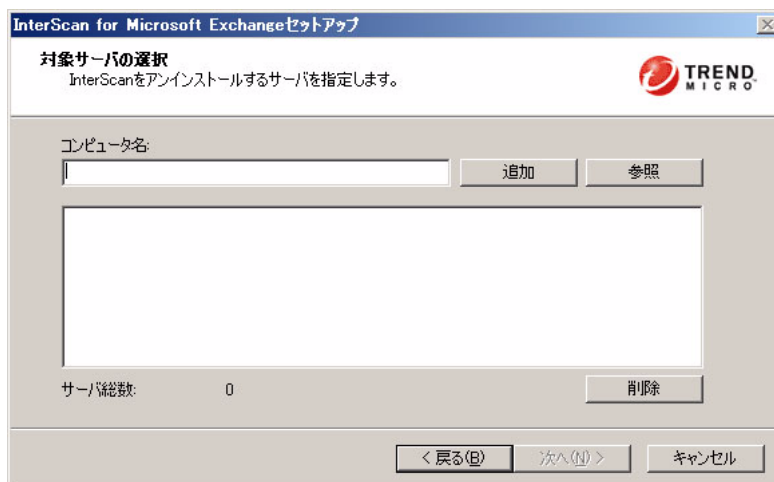


図 2-57. [対象サーバの選択] 画面

6. [ログオン] 画面が表示されます。InterScan をアンインストールする対象サーバにログオンするためのユーザ名とパスワードを入力します。[次へ] をクリックして続行します。[共有ディレクトリの設定] 画面が表示されます。

図 2-58. [ログオン] 画面

7. [共有ディレクトリの設定] 画面が表示されます。この画面で、InterScan をアンインストールする対象サーバの共有ディレクトリを指定します。

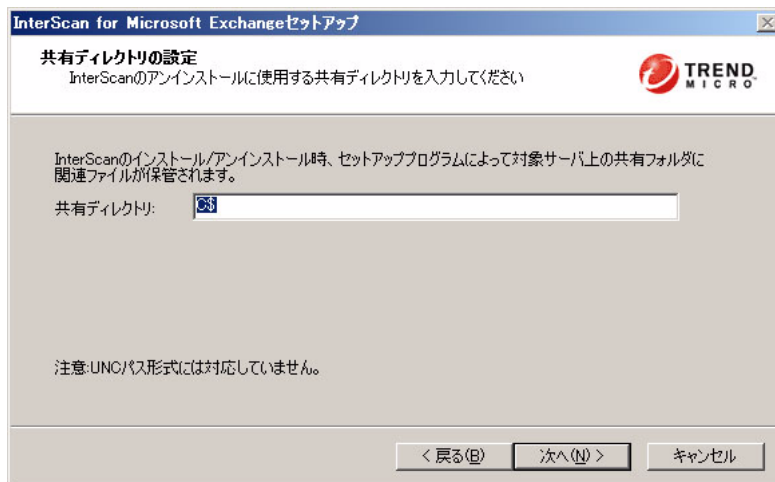


図 2-59. [共有ディレクトリの設定] 画面

- a. アンインストールプロセスのサポートファイルを格納する対象サーバ上のフォルダを指定します。
- b. [次へ] をクリックします。

8. [システム要件の確認] 画面が表示されます。画面を参照してアンインストールの設定が正しいことを確認し、[次へ] をクリックして続行します。

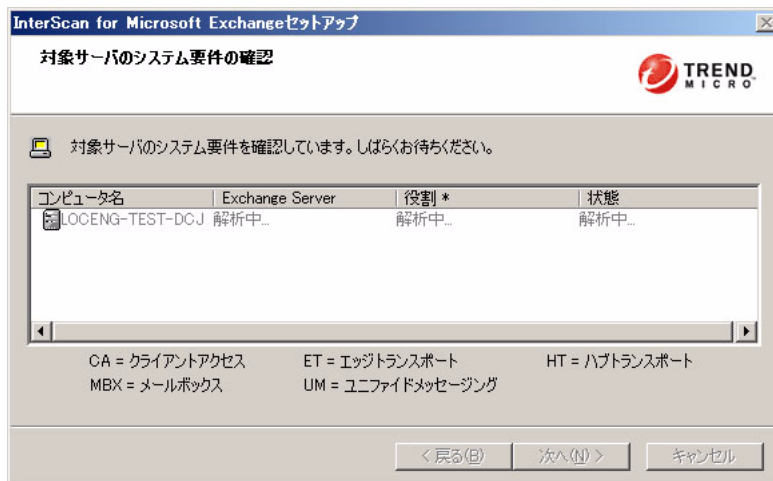


図 2-60. [対象サーバのシステム要件の確認] 画面

9. [削除オプション] 画面が表示されます。削除するコンポーネントを選択して [次へ] をクリックします。

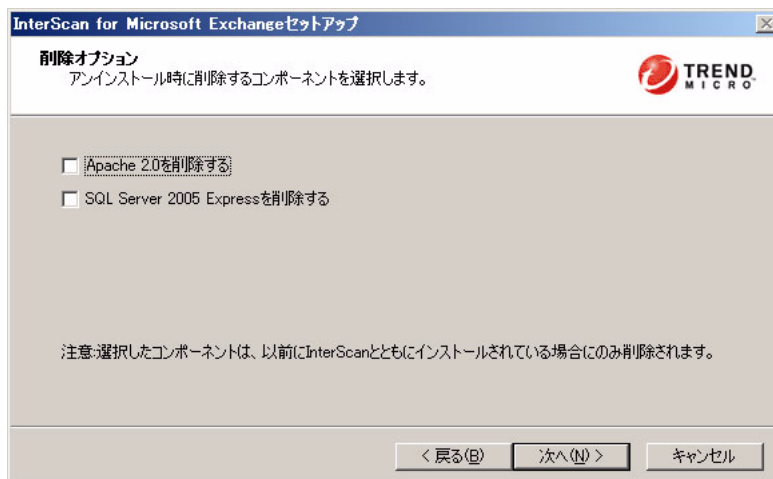


図 2-61. [削除オプション] 画面

10. [設定の確認] 画面が表示されます。設定を確認した後 [次へ] をクリックして、アンインストールプロセスを開始します。

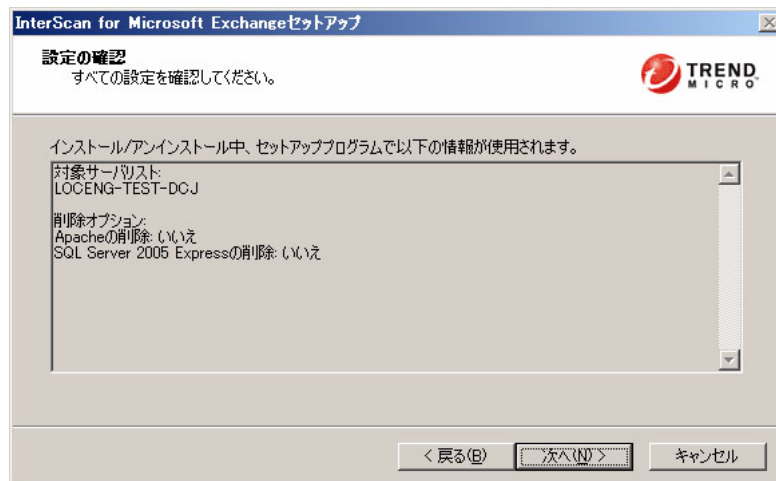


図 2-62. [設定の確認] 画面

11. [アンインストールの進行状況] 画面が開きます。アンインストールが完了したら、[次へ] をクリックし、続行します。

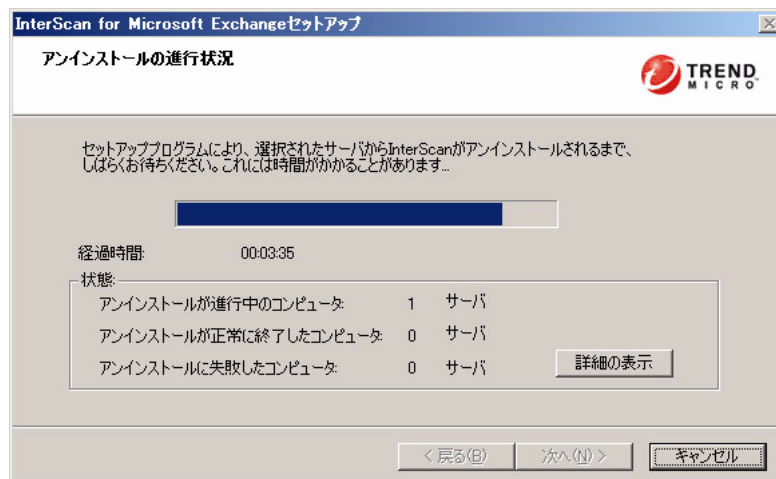


図 2-63. [アンインストールの進行状況]

12. [アンインストールの完了] 画面が開き、サーバから正常にアンインストールされたことが通知されます。[終了] をクリックし、セットアッププログラムを終了します。セットアッププログラムによって、選択したサーバから InterScan がアンインストールされます。

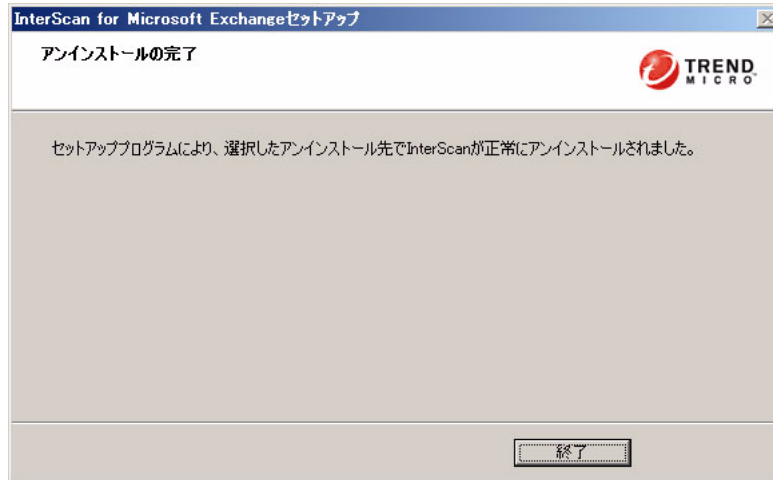


図 2-64. [アンインストールの完了] 画面

Windows コントロールパネルを使用したアンインストール

Windows のコントロールパネルを使用して InterScan をアンインストールできますが、Microsoft SQL Server 2005 Express と Apache を個別にアンインストールする必要があります。セットアッププログラムを使用して InterScan をアンインストールすると、関連するコンポーネントとプログラムがすべて削除されます。そのため、セットアッププログラムを使用して InterScan をアンインストールすることをお勧めします。

InterScan をアンインストールするには

1. Windows の [スタート] メニューから、[設定]→[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. [Trend Micro InterScan for Microsoft Exchange] を選択して、[削除] をクリックします。
3. 削除の確認メッセージが表示されたら、[はい] をクリックして InterScan を削除します。

注意： InterScan 8.0 を Exchange Server 2007 で使用する場合、Microsoft Visual C++ 2005 再頒布可能パッケージおよび Microsoft Visual C++ 2005 再頒布可能コンポーネント (X64) がインストールされます。これらは InterScan をアンインストールしてもアンインストールされません。

クラスタ環境での InterScan のアンインストール

クラスタから InterScan をアンインストールする手順は、クラスタでない通常のサーバからアンインストールする手順とよく似ています。クラスタ以外の InterScan をアンインストールする詳細については、112 ページの「製品 CD-ROM を使用したアンインストール」を参照してください。

クラスタから InterScan をアンインストールするには

再度 setup.exe を実行し、InterScan をアンインストールします。

同一のクラスタに属する各クラスタノードから InterScan を同時に削除し、各オンライン仮想サーバ上のリソースを削除します。各 Exchange 仮想サーバからすべての変更を適切に削除します。

クラスタから InterScan を手動で削除するには

1. [プログラムの追加と削除] を使用して、各ノードの InterScan をアンインストールします。
2. Windows クラスタアドミニストレータを使用して、InterScan リソースを削除します。

3. 次のいずれかのコマンドを使用して、InterScan クラスタリソースタイプの登録を解除します。
- Microsoft Exchange 2000 Server/Exchange Server 2003/Exchange Server 2007 SCC の場合 : `cluster restype clusRDLL /delete /type`
 - Microsoft Exchange 2007 CCR の場合 : `cluster restype clusRDLLCCR /delete /type`

注意： InterScan 8.0 を Exchange Server 2007 で使用する場合、Microsoft Visual C++ 2005 再頒布可能パッケージおよび Microsoft Visual C++ 2005 再頒布可能コンポーネント (X64) がインストールされます。これらは InterScan をアンインストールしてもアンインストールされません。

製品の登録、アクティベーション、アップデート

この章では、Trend Micro InterScan for Microsoft Exchange (以下、InterScan) のアクティベーションとアップデートの方法について説明します。

この章の内容は次のとおりです。

- 126 ページの「InterScan のアクティベーション」
- 126 ページの「アクティベーションコード」
- 129 ページの「InterScan のアップデート」
- 132 ページの「コンポーネントの手動アップデート」
- 133 ページの「予約アップデートの設定」

InterScan のアクティベーション

InterScan の機能を使用するには、製品の購入時 (または体験版の入手時) に取得したアクティベーションコードを使用して、製品の機能を有効にする必要があります。

アクティベーションの実行

次の場合にアクティベーションを実行する必要があります。

- InterScan をはじめてインストールする場合
たとえば、トレンドマイクロの販売代理店から通常版またはアドバンス版を購入し、アクティベーションコードを入手した場合です。
- 体験版を製品版に変更する場合、または通常版からアドバンス版に変更する場合
たとえば、トレンドマイクロの担当者から新しいアクティベーションコードを入手し、製品コンソールを使用して新しいバージョンをアクティベートする場合です。

注意：体験版では、30 日間はすべての機能を利用できます。その後、InterScan のタスクは引き続き実行されますが、ウイルス検索、メッセージフィルタ、コンポーネントのアップデートは実行されません。

アクティベーションコード

InterScan には、通常版とアドバンス版の 2 種類のアクティベーションコードがあります。また、それぞれに体験版と製品版の 2 種類があります。

ヒント：テスト環境でパイロットインストールを実行する場合は、InterScan の体験版を使用します。製品版をインストールするときは、無料の体験版での経験を参考にしてください。

通常版アクティベーションコード

通常版アクティベーションコードを使用すると、InterScan のウイルス検索と添付ファイルブロックが使用可能になります。最新のウイルス検索エンジンとウイルスパターンファイルを受信し、リアルタイム、手動、および予約で検索を実行できます。InterScan では、感染した添付ファイルを検出して、そのファイルに対する処理を実行します。

製品の種類	通常版の機能
体験版	体験版アクティベーションコードを使用することにより、限られた期間、InterScan のすべての機能を実装できます。体験期間内は、InterScan では、ウイルス検索エンジンとパターンファイルのアップデートだけでなく、ウイルス検索と添付ファイルブロックも実行されます。
製品版	製品版アクティベーションコードでは、サポートサービスを受ける権利が得られ、スパムメール対策、コンテンツフィルタ、エンドユーザメール隔離ツールを除く、InterScan のすべての機能を実装できます。InterScan は、サポート契約の有効期限が近づくと、画面にメッセージを表示します。

表 3-1. 通常版アクティベーションコードの機能

アドバンス版アクティベーションコード

アドバンス版アクティベーションコードを使用すると、InterScan 通常版のすべての機能に加えて、コンテンツフィルタ、スパムメール対策、エンドユーザメール隔離機能も使用可能になります。ウイルス検索エンジンとパターンファイルのアップデートに加えて、スパムメール検索エンジンとスパムメール判定ルール of アップデートも受信できます。コンテンツフィルタは、Exchange サーバに到着するメールから望ましくないコンテンツを排除します。スパムメール検索エンジンとスパムメール判定ルールは、Exchange クライアントのメールボックスにスパムメールが配信されないようにします。

製品の種類	アドバンス版の機能
体験版	体験版アクティベーションコードを使用することにより、限られた期間、InterScan のすべての機能を使用できます。体験期間内は、すべてのコンポーネントのアップデート、ウイルス検索、添付ファイルブロック、コンテンツフィルタ、スパムメール対策、エンドユーザメール隔離の機能を利用できます。
製品版	製品版アクティベーションコードでは、サポートサービスを受ける権利が得られ、InterScan のすべての機能を実装できます。InterScan は、サポート契約の有効期限が近づくと、画面にメッセージが表示されます。

表 3-2. アドバンス版アクティベーションコードの機能

アクティベーションコードの比較

次に表に、それぞれのタイプのアクティベーションコードで利用できる機能を示します。

機能	アドバンス版アクティベーションコード		通常版アクティベーションコード	
	製品版	体験版	製品版	体験版
管理コンソール	あり	あり	あり	あり
レポート、ログ、および隔離ファイル管理におけるスパムメール対策項目とコンテンツフィルタ項目	あり	あり	なし	なし
ウイルス検索	あり	あり	あり	あり
添付ファイルブロック	あり	あり	あり	あり
スパムメール対策	あり	あり	なし	なし
コンテンツフィルタ	あり	あり	なし	なし
手動検索 / 予約検索	あり	あり	あり	あり

表 3-3. 種類別アクティベーションコードの利用可能な機能

機能	アドバンス版アクティベーションコード		通常版アクティベーションコード	
	製品版	体験版	製品版	体験版
アップデート	あり	あり	あり	あり
エンドユーザメール隔離	あり	あり	なし	なし
Control Manager のサポート	あり	あり	あり	あり

表 3-3. 種類別アクティベーションコードの利用可能な機能

次のいずれかの方法で InterScan をアクティベーションを実行できます。

インストール時の実行

1. セットアッププログラムを起動します。
2. [製品のアクティベーション] 画面にアクティベーションコードを入力します。
3. インストールを完了し、InterScan をアクティベートします。

インストール後の実行

1. InterScan 管理コンソールで [管理]→[製品ライセンス] の順にクリックします。
2. [製品ライセンス] 画面で [新規入力] をクリックします。
3. 所定の欄にアクティベーションコードを入力します。
4. [アクティベート] をクリックします。

InterScan のアップデート

ウイルス対策ソフトウェアは、最新の技術を使用していないと効力を発揮しません。新しいウイルス / 不正プログラムやその他の不正コードは絶えずリリースされています。そのため、InterScan のコンポーネントを定期的にアップデートして、新しいセキュリティ上の脅威に対して防御することが極めて重要です。アップデートが可能な InterScan のコンポーネントは次のとおりです。

- ウイルスパターンファイル
- スパイウェアパターンファイル
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル
- ウイルス検索エンジン
- スпамメール判定ルール
- スпамメール検索エンジン

最新のコンポーネントを使用しているかどうかを調べるには、製品コンソールから [概要] 画面を表示します。この画面には、現在のバージョンと、ダウンロードできる最新バージョンのリストが表示されます。

InterScan をアップデートする前に、次の作業を行う必要があります。

- 製品のアクティベート。126 ページの「InterScan のアクティベーション」を参照してください。
- プロキシサーバでネットワーク上のインターネットトラフィックが処理されている場合、プロキシサーバ情報の設定
- アップデート方法とダウンロード元の設定。方法には手動アップデートおよび予約アップデートがあります。ダウンロード元には、アップデートサーバ、インターネット、およびイントラネット UNC パスがあります。

クラスタ環境でのアップデート

InterScan はクラスタ内のノードごとにインストールおよび設定する必要があります。単一のノード上のすべての仮想サーバは、同じコンポーネントとダウンロード元を使用します。あるノード上の仮想サーバが別のノードにフェイルオーバーされると、InterScan によってコンポーネントのバージョンが比較され、最新のものに維持されます。このため、フェイルオーバー後に [概要] 画面でコンポーネントのバージョンを確認すると、フェイルオーバー前より新しいバージョンが表示される場合があります。

注意： Microsoft Exchange Server 2007 CCR モデルでは、InterScan リソースがオンラインになると、自動的にアップデートが実行されます。

プロキシサーバの設定

大多数の企業では、セキュリティを強化し、帯域幅を効率的に利用するために、プロキシサーバを使用しています。システムでプロキシサーバを使用している場合、インターネットへ接続して、InterScan を最新の状態に維持するために必要な最新コンポーネントをダウンロードし、ライセンスステータスをオンラインでチェックするようにプロキシ設定値を設定します。

プロキシサーバは次の機能で使用されます。

- アップデート
- 製品ライセンスの確認
- ウイルストラッキング

プロキシサーバを設定するには

1. InterScan 製品コンソールにログインします。
2. サイドバーから [管理]→[プロキシ] の順にクリックします。[プロキシ] 画面が開きます。

3. [アップデートおよび製品ライセンスの確認にプロキシサーバを使用する] チェックボックスをオンにします。
4. プロキシサーバのサーバ名または IP アドレスと、ポート番号を入力します。
5. SOCKS 5 プロトコルを使用するよう、[SOCKS 5 を使用する] を選択します。
6. プロキシサーバにパスワードが必要な場合は、表示されるフィールドにユーザー名とパスワードを入力します。
7. [保存] をクリックし、設定を保存します。

コンポーネントの手動アップデート

ウイルス検索エンジン、パターンファイル、スパムメール検索エンジン、スパムメール判定ルール、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、およびスパイウェアパターンファイルを、InterScan をインストールした直後と、大規模感染が発生するたびに手動でアップデートすることをお勧めします。これにより、Exchange 環境のセキュリティベースラインが確立されます。

コンポーネントの手動アップデートには、2 つのステップがあります。最初にアップデートをダウンロードする元を選択し、次にアップデートするコンポーネントを選択します。[アップデート] をクリックすると、指定した元から最新のコンポーネントがダウンロードされます。

コンポーネントを手動でインストールするには

1. InterScan 製品コンソールにログオンします。
2. [アップデート]→[手動] の順に選択します。
3. アップデートするコンポーネントを選択します。
4. [アップデート] をクリックします。InterScan はコンポーネントのダウンロードを開始し、経過時間とダウンロードの残りの割合を示す進行状況バーが表示されます。

予約アップデートの設定

アップデートサーバを定期的にチェックし、使用可能なコンポーネントがあれば、それを自動的にダウンロードするように InterScan を設定します。予約アップデート中、InterScan では、指定したダウンロード元に最新のコンポーネントが存在するかどうかをチェックします。

ヒント：大規模感染が発生した場合、トレンドマイクロはパターンファイルのアップデートに素早く対応します (アップデートは 1 週間に複数回発行される場合があります)。また、トレンドマイクロではウイルス検索エンジンと他のコンポーネントを定期的にアップデートします。トレンドマイクロでは、コンポーネントを毎日アップデートすることをお勧めします。大規模感染時には、1 日 2 回以上のアップデートをお勧めします。これによって、InterScan に最新のコンポーネントを確実に追加できます。

予約アップデートを設定するには

1. アップデートのダウンロード元を選択します。
 - a. [アップデート]→[ダウンロード元] の順に選択します。[アップデートファイルのダウンロード元] 画面が表示されます。
 - b. ダウンロード元を選択します。
 - c. [保存] をクリックします。
2. スケジュールを設定します。
 - a. [アップデート]→[予約] の順に選択します。
 - b. [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、スケジュールに従って InterScan によるアップデートが開始されるように設定します。
 - c. アップデートスケジュールを設定します。

- i. アップデートの頻度を選択します。分ごと、時間ごと、日ごと、週ごとがあります。
 - ii. 時間および分を選択することによって、アップデートの [開始時間] を設定します。新しくアップデートが発生すると、この時間にダウンロードが開始されます。
3. ダウンロード元からダウンロードするコンポーネントを選択します。
 - a. 各予約アップデート中にダウンロードするコンポーネントを選択します。

注意： 表の最上部にあるチェックボックスをオンにすると、すべてのコンポーネントが選択されます。

- b. [保存] をクリックします。選択したコンポーネントのダウンロードは、設定したスケジュールに従って開始されます。

ダウンロード元

InterScan を最新の状態に維持するには、最新のコンポーネントをダウンロードする必要があります。この画面を使用して、InterScan が最新コンポーネントをダウンロードする元を設定します。初期設定の場所は、トレンドマイクロのアップデートサーバです。手動ダウンロードまたは予約ダウンロード中、InterScan はここで設定した場所をチェックし、その場所から最新のコンポーネントをダウンロードします。

ダウンロード元を設定するには

- トレンドマイクロのアップデートサーバ

トレンドマイクロは、新しいコンポーネントが使用可能になり次第、そのコンポーネントをアップデートサーバにアップロードします。アップデートを頻繁にタイムリーに実行する必要がある場合、ダウンロード元としてトレンドマイクロのアップデートサーバを選択します。

詳細については、27 ページの「アップデートについて」を参照してください。

- イン트라ネット上のリソース

最新のコンポーネントが格納されているイントラネット上の場所からコンポーネントをダウンロードします。

ネットワーク上の別のサーバの UNC パスを入力します。

注意： 集中管理型のイントラネット上の場所を 1 つ以上設定することによって、ネットワークトラフィックを大幅に削減し、アップデート時間を大幅に短縮できます。この方法は、メールサーバをインターネットに直接接続したくない場合にも有効です。また、フロントエンドサーバをインターネット上のトレンドマイクロのアップデートサーバに接続し、フロントエンドサーバからコンポーネントを受信するようにバックエンドサーバを設定することも可能です。

- その他のダウンロード元

インターネットまたは他のアップデート元からコンポーネントをダウンロードします。

テスト時には、特別なサーバからコンポーネントを受信するように設定する場合があります。たとえば、トレンドマイクロのベータ版テストに参加している場合、指定のテストサーバの名前を入力します。

他のサーバが InterScan サーバから最新版をダウンロードできるようにする

[他のサーバがこのサーバからアップデートをダウンロードできるようにする] をクリックして、現在のサーバにあるアップデートパッケージのコピーを作成するように InterScan を設定します。通常、InterScan では、ダウンロードするよう設定されたコンポーネントまたは InterScan が必要とするコンポーネントの差分だけをダウンロードします (27 ページの「パターンファイルの差分アップデート」を参照)。アップデートパッケージをコピーするように InterScan を設定した場合、ダウンロードできるすべてのコンポーネントがダウンロードされます。

例：2つのExchangeサーバ「a」と「b」が存在し、それぞれにInterScanがインストールされているとします。InterScanは、サーバ「a」を毎日アップデートし、すべてのコンポーネントをダウンロードするように設定されています。InterScanは、サーバ「b」を毎週アップデートし、スパムメール判定ルールコンポーネントだけをダウンロードするように設定されています。両方のサーバは、必要に応じて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受信します。このため、この2つのサーバ上のコンポーネントは必ずしも同じであるとは限らず、この2つのサーバがアップデートサーバにポーリングしたとき、異なる差分アップデートが必要になります。より効率的なサーバの構成方法は、アップデートパッケージをコピーするようにサーバ「a」を設定することです。これによって、サーバ「a」をサーバ「b」のダウンロード元に設定し、サーバ「b」は、アップデートサーバから受信するのと同じようにサーバ「a」からアップデートの差分を受信できるようになります。

注意：アップデートパッケージはクラスタに必ずコピーしてください。つまり、このオプションは有効であってもグレー表示されるため、初期設定で、1つの仮想サーバからそのノード上のすべての仮想サーバにコンポーネントをコピーする必要があります。

コンポーネントのロールバック

InterScanによって最新のコンポーネントがダウンロードされているが、誤警告の発生などの理由によりそれより前のコンポーネントを使用したい場合、手動でコンポーネントアップデートをロールバックできます。

手動で前のコンポーネントにロールバックするには

1. 次のInterScanサービスを停止します。
 - InterScan for Microsoft Exchange Remote Configuration Server
 - InterScan for Microsoft Exchange Master Service

2. 次の場所にあるファイルをすべて削除します。
 - <インストールフォルダ>%AU_Data%AU_Cache%
 - <インストールフォルダ>%AU_Data%AU_Temp%
 - <インストールフォルダ>%AU_Data%AU_Storage%
 - <インストールフォルダ>%web%activeupdate%
3. ウイルスパターンファイル、スパイウェアパターンファイル、IntelliTrap パターンファイル、および IntelliTrap 除外パターンファイルをロールバックします。
 - a. 最近ダウンロードされたパターンファイルを次の場所から削除します。

<インストールフォルダ>%engine%vsapi%latest%pattern%
 - b. 次のファイルを削除します。ロールバックするための旧バージョンのファイルが InterScan によってダウンロードされていることを確認します。
 - ウイルスパターンファイル:
lpt\$vpn.xxx
 - スパイウェアパターンファイル:
ssaptn.xx
 - IntelliTrap パターンファイル:
tmblack.xxx
 - IntelliTrap 除外パターンファイル:
tmwhite.xxx

ここで「xxx」は、最新のパターンファイルのバージョンを指しています。

例: 最近のウイルスパターンファイル lpt\$vpn.345 がダウンロードされていて、前のダウンロードパターンファイル lpt\$vpn.344 にロールバックする場合、lpt\$vpn.345 を削除すると、lpt\$vpn.344 が InterScan によって使用されるようになります。
 - c. 次の場所にあるファイルをすべて削除します。

- <インストールフォルダ>%engine%\sapi\primary\pattern%
 - <インストールフォルダ>%engine%\sapi\secondary\pattern%
4. スпамメール判定ルールをロールバックするには、次の手順に従ってください。
- a. 次の場所にある最新のルールを削除します。
- <インストールフォルダ>%engine%\TMASE\latest\rule%
 - 例: tmxxxxxx.*
「xxxxxx」は最新のバージョンを意味します。
- b. 次の場所にあるファイルをすべて削除します。
- <インストールフォルダ>%engine%\TMASE\primary
 - <インストールフォルダ>%engine%\TMASE\secondary
 - <インストールフォルダ>%engine%\TMASE\latest\rule
 - <インストールフォルダ>%engine%\TMASE\latest\cache%
5. 次の InterScan サービスを再度起動します。
- InterScan for Microsoft Exchange Remote Configuration Server
 - InterScan for Microsoft Exchange Master Service

製品の管理

この章では、Trend Micro InterScan for Microsoft Exchange (以下、InterScan) の製品コンソールの開き方、使用方法、および InterScan サーバの管理方法について説明します。

この章の内容は次のとおりです。

- 140 ページの「製品コンソールの使用」
- 145 ページの「リアルタイムモニタの概要」
- 147 ページの「サーバ管理の概要」

製品コンソールの使用

InterScan のアクセスおよび制御は、直感的に使用できる製品コンソールから行います。製品コンソールを使用すると、ネットワーク上の任意のコンピュータから複数の Exchange サーバおよびリモートサーバを管理することができます。製品コンソールは、パスワードで保護されており、許可された管理者のみが InterScan の設定を変更できます。

注意：製品コンソールにアクセスし、使用するには、フレームをサポートする Java 対応の Web ブラウザが必要です。

管理コンソールのメインビュー

InterScan の管理コンソールには直感的に使用できるユーザインタフェースが採用されているため、InterScan の構成および管理に必要なすべての機能に簡単にアクセスできます。



図 4-1. 製品コンソール

製品コンソールの構成要素

バナー領域

InterScan のバナー領域には製品名やサーバ情報、各種リンクが含まれます。



図 4-2. 製品コンソールのバナー領域

バナーには、次のものが表示されます。

- **現在のサーバ** — このコンソールの管理対象サーバです。
- **リアルタイムモニタ** — クリックすると、リアルタイムモニタにアクセスします。
詳細については、145 ページの「リアルタイムモニタの概要」を参照してください。
- **サーバ管理** — クリックすると、サーバ管理コンソールにアクセスします。
詳細については、147 ページの「サーバ管理の概要」を参照してください。
- **ログオフ** — クリックすると、セッションが終了し、製品コンソールが閉じます。製品コンソールをログオフすることで、許可されていないユーザが設定を変更するのを防ぐことができます。
- **ヘルプ** — ドロップダウンリストからオプションを選択すると、サポート情報を表示できます。

ヘルプオプションには、次のものがあります。

- **目次と索引** — オンラインヘルプの目次および索引を表示します。
- **製品 Q&A** — 製品のトラブルシューティングの最新情報を確認できる製品 Q&A ページを表示します。
- **セキュリティ情報** — 最新のセキュリティリスク情報を掲載するトレンドマイクロのセキュリティ情報ページを表示します。
- **購入情報** — 最寄の販売代理店およびサービスプロバイダを検索できるトレンドマイクロの Web ページを表示します。
- **サポート情報** — トレンドマイクロのテクニカルサポートの Web ページにアクセスできます。
- **バージョン情報** — InterScan とコンポーネントのバージョン番号、および InterScan のシステム情報を表示します。

サイドバー — InterScan のメインメニュー項目へのアクセスを提供します。

概要
ウイルス検索
添付ファイルブロック
コンテンツフィルタ
スパムメール対策
手動検索
予約検索
▶ アップデート
▶ 通知
▶ レポート
▶ ログ
▶ 隔離
▶ 管理

図 4-3. 製品コンソールのサイドバー

設定領域 — InterScan のすべての構成およびオプションを設定、変更するための作業領域です。

ウイルス 検索

ヘルプ

☐ リアルタイムウイルス検索を有効にする

対象

処理

通知

初期設定の検索

ウイルス、ワーム、トロイの木馬などの不正コードを検索する方法を選択:

☒ すべての添付ファイル

☐ トレンドマイクロの推奨設定:実際のファイルタイプを識別します

☐ ファイルの種類を指定

☐ メッセージ本文を検索する

IntelliTrap

☐ IntelliTrapを有効にする

スパイウェアの検索

☐ すべてを選択

☐ スパイウェア

☐ ダイアラー

☐ ハッキングツール

☐ パスワード解読アプリケーション

☒ アドウェア

☐ ジョークプログラム

☐ リモートアクセスツール

☐ その他

詳細オプション

検索の制限条件

保存

リセット

図 4-4. 製品コンソールの設定領域

製品コンソールの起動

InterScan 製品コンソールでは、一度に 1 台ずつサーバを管理できます。

注意： ローカル管理者権限を持つアカウントまたは InterScan 管理グループに属するアカウントを使用します。InterScan を Exchange 2000/2003 で使用する場合は、「SMEX Admin Group」に属するアカウントを使用できます。InterScan を Exchange 2007 で使用する場合は、Active Directory グループ、またはサーバ管理のアクティベーションで使したフォレストに含まれる任意の Active Directory グループに属するアカウントを使用できます。

ローカルサーバで製品コンソールを起動するには

1. [スタート]→[すべてのプログラム]→[Trend Micro InterScan for Microsoft Exchange]→[InterScan 管理コンソール] の順にクリックします。
2. [ユーザ名] および [パスワード] を入力し、[ログオン] をクリックします。

リモートサーバで製品コンソールを起動するには

フレームをサポートしている Java 対応の Web ブラウザを使用して、次のいずれかの URL にアクセスします。

<http://<サーバ名>:<ポート番号>/SMEX>

<https://<サーバ名>:<ポート番号>/SMEX>

「サーバ名」は InterScan がインストールされているサーバの名前、「ポート番号」はそのコンピュータへのアクセスに使用しているポート番号です。

注意： 初期設定では、HTTP にはポート 16372、HTTPS にはポート 16373 が使用されます。

クラスタ上の仮想サーバの表示

それぞれの Exchange 仮想サーバは独立した管理ユニットであり、1 つのクラスタノード内にいくつ配置されていると、独自の構成とログの記憶域を備えている必要があります。製品コンソールは、指定された Exchange 仮想サーバに関連付けられたネットワーク名または IP アドレスを使用して、そのサーバ上での InterScan の動作を制御します。

各ノードには InterScan のショートカットがあり、すべての仮想サーバのリンクを表示できます。[すべてのプログラム]→[Trend Micro InterScan for Microsoft Exchange]→[InterScan 管理コンソール] の順に選択すると、すべての仮想サーバが表示されます。

注意：InterScan リソースを手動で作成または削除しても、仮想サーバのリンクは更新されません。

リアルタイムモニタの概要

リアルタイムモニタには、1 台の Exchange サーバの情報がリアルタイムに表示されます。この情報には、サーバに届く受信および送信メッセージについて InterScan が行う検索が表示されます。また、サーバで検出されたウイルスおよびスパムメールの現在の数も表示されます。



図 4-5. リアルタイムモニタ画面

リアルタイムモニタを使用すると、ローカルサーバ、またはネットワークに接続されている任意のサーバを監視できます。これは集中的に InterScan サーバを管理するための有益な方法です。

リモートサーバのリアルタイムモニタを表示するには

1. 製品コンソールを使用して、リモートサーバにアクセスします。
2. [リアルタイムモニタ] をクリックします。[リアルタイムモニタ] 画面が開き、リモートサーバの情報が表示されます。

サーバ管理の概要

InterScan サーバ管理画面を使用すると、ネットワーク上のすべての InterScan サーバを表示できます。Exchange 2000 Server および Exchange Server 2003 環境では、同一ドメインフォレスト内で異なるドメインに属するサーバを表示し、設定をコピーするには特定のアクセス許可が必要です。

Exchange 2000 および Exchange 2003 環境で、同一フォレスト内で異なるドメインへのアクセス許可を付与するには

1. regedit (Windows 2000 では regedt32) を実行します。
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg で、[winreg] を右クリックしてポップアップメニューから [アクセス許可] を選択します (Windows 2000 の場合は、[セキュリティ]→[アクセス許可] を選択)。
3. 管理元のサーバ管理コンソールが属するドメインの「SMEX Admin Group」を追加して、[読み取り] の [許可] を有効にします。
4. HKLM\SOFTWARE\TRENDMICRO\ScanMail for Exchange で、[ScanMail for Exchange] を右クリックしてポップアップメニューから [アクセス許可] を選択します (Windows 2000 の場合は、[セキュリティ]→[アクセス許可] を選択)。
5. 管理元のサーバ管理コンソールが属するドメインの「SMEX Admin Group」を追加して、[フル コントロール] の [許可] を有効にします。

注意：Exchange 2007 環境では、この作業は不要です。

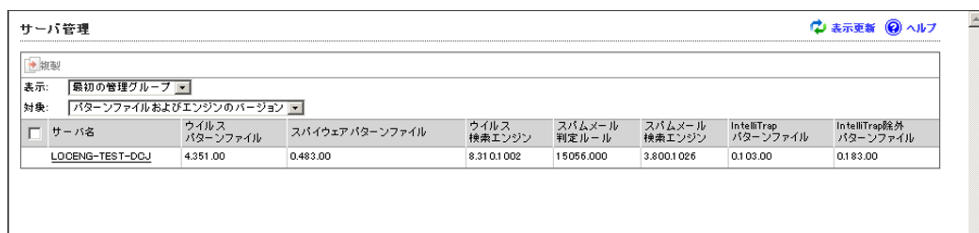


図 4-6. サーバ管理画面

サーバ管理コンソールでは、以下の機能を使用することができます。

対象	表示される内容
コンポーネントのバージョンの表示	現在のウイルス検索エンジン、ウイルスパターンファイル、スパイウェアパターンファイル、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、スパムメール検索エンジン、およびスパムメール判定ルールについての情報を表示します。
検索結果の表示	検索されたメッセージの合計数、および検索結果を表示します。検索結果には、検出されたウイルス / 不正プログラム、駆除不能なウイルス / 不正プログラム、ブロックされた添付ファイル、スパムメール、コンテンツ違反、および駆除不能なメッセージ部分の数も表示されます。
検索ステータスの表示	Exchange 2000 Server および Exchange Server 2003 の場合、ウイルス検索、添付ファイルブロック、コンテンツフィルタ、およびスパムメール対策の検索ステータスが表示されます。Exchange 2007 Server の場合、ストアウイルス検索、トランスポートウイルス検索、ストア添付ファイルブロック、トランスポート添付ファイルブロック、ストアコンテンツフィルタ、トランスポートコンテンツフィルタおよびスパムメール対策の検索ステータスが表示されます。
前回の複製の表示	前回の複製のステータス、および前回の複製の期間を表示します。
リモートサーバへの設定の複製	設定を、リスト内の単一または複数のリモートサーバに複製します。

表 4-1. サーバ管理コンソールの表示項目

サーバ管理のアクティベーション

サーバ管理コンソールにはリモートサーバの状態も表示されるため、設定をリモートサーバにコピーすることができます。InterScan のインストールプロセスでサーバ管理のアクティベーションを行っていない場合、サーバ管理コンソールを使用するには、まずサーバ管理のアクティベーションを実行する必要があります。サーバ管理のアクティベーションを実行するには、ローカル管理者権限を持つアカウントを使用してログオンします。その後、製品コンソールの上部にある [サーバ管理] リンクをクリックします。

- Exchange 2000 Server または Exchange Server 2003 で使用する InterScan のサーバ管理のアクティベーション — [Active Directory から既存のアカウントを指定] または [新規アカウントを作成] を選択します。アクティベーションウィザード画面の指示に従って、サーバ管理のアクティベーションに必要な処理を実行します。
- Exchange Server 2007 で使用する InterScan のサーバ管理のアクティベーション — Active Directory の既存のアカウントを指定し、アクティベーションウィザード画面の指示に従って、サーバ管理のアクティベーションに必要な処理を実行します。

サーバ管理を使用した設定の複製

サーバ管理を使用すると、異なる InterScan サーバ間で、任意またはすべての設定を複製できます。この方法によるサーバの複製は、個別にサーバを設定するよりも非常に速く簡単にできます。また、同様の保護を行うすべての InterScan サーバ内で、確実に同じ設定を共有できます。

サーバの設定を 1 台以上の対象サーバに複製するには

1. [サーバ管理] をクリックして、[サーバ管理 > 複製] 画面を開きます。
2. 複製先のサーバを選択します。
3. [複製] をクリックします。画面が表示されます。

4. 複製する設定を選択します。
 - 複製先のサーバにすべての構成を複製する場合は、[すべての設定] をクリックします。
 - 各構成を個別に複製する場合は、[指定した設定] をクリックします。

注意： 現在ログオンしているサーバが、複製元となります。

5. サーバに依存する設定を上書きする場合は、[サーバに依存する設定 (隔離ディレクトリやバックアップディレクトリ) を上書きする] チェックボックスをオンにします。このチェックボックスをオンにすると、InterScan で、隔離、バックアップ、およびアーカイブとして設定されているフォルダのディレクトリパスをコピーすることができます。
6. [配信] をクリックします。進行状況バー、および複製の進捗状況を示す画面が表示されます。

仮想サーバの InterScan リソースの手動作成

インストールの際は、InterScan をクラスタの仮想サーバにインストールできます。ただし、インストールが終了した後は、セットアッププログラムを再び実行して、別のサーバに InterScan をインストールすることはできません。これは、InterScan で、クラスタ環境内の同一ビルドのアップグレードがサポートされていないからです。インストールの後にクラスタに仮想サーバを追加し、InterScan でそのサーバを保護する場合は、まず、新しい仮想サーバで使用される InterScan のリソースを手動で作成する必要があります。

仮想サーバの InterScan リソースを手動で作成するには

1. InterScan リソースを手動で作成します。InterScan リソースタイプを次のように選択します。
 - Microsoft Exchange 2000 Server: InterScan for Exchange クラスタエージェント
 - Microsoft Exchange Server 2003: InterScan for Exchange クラスタエージェント
 - Microsoft Exchange Server 2007 SCC: InterScan for Exchange クラスタエージェント (シングルコピークラスタ用)
 - Microsoft Exchange Server 2007 CCR: InterScan for Exchange クラスタエージェント (MNS クラスタ用)

2. 対象の仮想サーバのサーバグループに、InterScan リソースを作成します。
新しいリソースは、リソースタイプに依存します。以下に、InterScan リソースの依存関係を示します。
 - Microsoft Exchange 2000 Server - 物理ディスク、ネットワーク名、Microsoft Exchange インフォメーションストア。
 - Microsoft Exchange Server 2003 - 物理ディスク / マウントポイントディスク、ネットワーク名、Microsoft Exchange インフォメーションストア。
 - Microsoft Exchange Server 2007 SCC - 物理ディスク / マウントポイントディスク、ネットワーク名、Microsoft Exchange インフォメーションストア。
 - Microsoft Exchange Server 2007 CCR - ネットワーク名および Microsoft Exchange インフォメーションストア。

InterScan は、ユーザの**物理ディスク**リソースに作成されたディスクにデータを配置します。ディスクのデータは移動または変更しないでください。マウントポイントディスクにインストールする場合は、マウントポイントディスクのリソースを選択します。

3. SMEX リソースプロパティの [グループに適用する] をオフにします。[SMEX のリソース] を右クリックし、[プロパティ]→[詳細設定] で、[グループに適用する] チェックボックスをオフにします。
4. 対象サーバに関するレポートを表示するための仮想ディレクトリを、仮想サーバがインストールされている各ノードに作成します。この手順を実行する前に、対象の仮想サーバが現在のノードにあることを確認します。インストールオプションに応じて、Internet Information Services (IIS) または Apache を使用して仮想ディレクトリを作成できます。
 - IIS Web サーバを使用して仮想ディレクトリを作成する場合：
 - i. IIS を開くには、次の順にクリックします。
< コンピュータ名 > → [InterScan Web サイト] → [SMEX] → < 仮想ディレクトリ >
< コンピュータ名 > は、ローカルコンピュータの名前です。

- ii. 仮想ディレクトリを作成します。ディレクトリパスを次のように入力します。

< 対象サーバ上の共有ディスク >: \Isme\data\report

例 :G: ¥Isme¥data¥report

- Apache Web サーバを使用して仮想ディレクトリを作成する場合 :

- i. Httpd.conf を開くには、[スタート] メニューから、次の順にクリックします。

[すべてのプログラム]→[Apache HTTP Server 2.0.52]→
[Configure Apache Server]→[Edit the Apache Httpd.conf
Configuration File]

- ii. 次のテキスト文字列を検索します。

SMEX Virtual Path -- Start

- iii. 次のように入力します。

Alias /Isme/< レポートディレクトリ名 >/ "< 共有ディスクのラベル >:/Isme/data/report/"

<DirectoryMatch "^< 共有ディスクのラベル >:/Isme/data/report">

Options None

AllowOverride None

Order allow,deny

Allow from all

</DirectoryMatch>

例 :

Alias /Isme/report-ZERO1/ "F:/Isme/data/report/"

<DirectoryMatch "^[F]:/Isme/data/report">

Options None

AllowOverride None

Order allow,deny

```
Allow from all
</DirectoryMatch>
```

- iv.** SSL を使用している場合は、次のテキスト文字列を検索します。

```
# SMEX SSL -- Start
```

仮想サーバ用の領域に、次のように入力します。

```
Alias /Isme/< レポートディレクトリ名 >/ "< 共有ディスクのラベル >:/Isme_1300/data/report/"
```

```
<Directory "< 共有ディスクのラベル >:/Isme/data/report">
```

```
Options None
```

```
AllowOverride None
```

```
Order allow,deny
```

```
Allow from all
```

```
</Directory>
```

- v.** [スタート] メニューから Apache サーバを再起動します。

- 5.** Exchange 2000 および Exchange 2003 で、次のように入力し、エンドユーザーメール隔離機能のアカウントおよびメールボックスを作成します。

EUQ_< 仮想サーバ名 >

例:

EUQ_VirtualServer1

Exchange サーバのセキュリティの 確立と維持

Trend Micro InterScan for Microsoft Exchange (以下、InterScan) は、Exchange 環境全体の包括的なセキュリティを実現するために設計されました。ここでは、InterScan の主要機能の概要およびセキュリティベースラインを迅速に確立し、維持する方法について説明します。

この章の内容は次のとおりです。

- 156 ページの「セキュリティの確立」
- 157 ページの「セキュリティの維持」
- 159 ページの「InterScan のアップデート」
- 160 ページの「大規模感染の状況の管理」

セキュリティの確立

InterScan をアクティベートすると、InterScan の機能を設定できます。次の手順に従って Exchange サーバのセキュリティを設定することをお勧めします。

1. InterScan をアップデートします。
InterScan によって最適に保護できるよう、インストール後すぐにコンポーネントをアップデートします。
159 ページの「InterScan のアップデート」を参照してください。
2. InterScan が正常に実行および機能していることを確認します。
製品コンソールから、[リアルタイムモニタ] をクリックします。[リアルタイムモニタ] 画面が開き、InterScan の動作がリアルタイムで表示されます。[リアルタイム検索の実行開始日時] と表示されれば、InterScan により検索が実行されていることを示します。
3. インフォメーションストア全体の手動検索を実行します。
インストールに続いて、インフォメーションストア全体の手動検索を実行することをお勧めします。InterScan では、ウイルス / 不正プログラムまたはその他の不正コードを検出すると、トレンドマイクロの初期設定に従ってこれらに対して処理を実行します。

手動検索が完了すると、Exchange 環境の基本的なセキュリティが確立されます。

注意： InterScan はトレンドマイクロの初期設定値を使用し、望ましくないコンテンツのフィルタリング、害を及ぼす可能性のある添付ファイルのブロック、およびウイルス / 不正プログラムやその他のセキュリティ上の脅威に関する検索をリアルタイムで実行します。最適な保護および効果が得られるよう、InterScan の設定をカスタマイズします。

セキュリティの維持

Exchange サーバのセキュリティを維持するには、次のことをお勧めします。

1. InterScan が常に最新であるようにするため、ウイルス検索エンジン、ウイルスパターンファイル、スパムメール検索エンジン、スパムメール判定ルール、およびスピアウェアパターンファイルを定期的にアップデートします。このアップデートを容易にするため、InterScan では予約アップデートを設定できます。予約アップデートでは、設定したスケジュールに従ってトレンドマイクロのアップデートサーバをチェックし、利用可能なコンポーネントを自動的にダウンロードします。
133 ページの「予約アップデートの設定」を参照してください。
2. ウイルス / 不正プログラムおよびその他のセキュリティリスクは、保護されていないローカルなコンピュータやサーバなどの予期しない感染元から、または非常に緩い設定をすり抜けて、Exchange サーバを攻撃します。このようなリスクを大幅に削減するには、定期的に予約検索を実行します。
3. [ウイルス検索] 画面で [マスメーリング型ウイルスに対する処理を有効にする] チェックボックスをオンにし、早期にウイルスの大規模感染を警告します。
4. 攻撃が発生した場合、その拡大を防ぐため、管理者が早期に通知を受信することは極めて重要です。ネットワークで大規模感染の危険がある場合に主要なネットワークセキュリティ担当者に警告を送信するよう、InterScan を設定することをお勧めします。アウトブレイクアラートを使用して、指定したユーザに自動的に通知するよう InterScan を設定できます。

5. 全体的なネットワークセキュリティについて検討します。InterScan は、Exchange メールサーバを保護するように設計されています。InterScan では、Exchange 以外のメールサーバ、ファイルサーバ、デスクトップ、またはゲートウェイデバイスに対する保護は行いません。ファイルサーバおよびデスクトップを保護するウイルスバスター コーポレートエディションや、ネットワークの周辺を保護する Trend Micro InterScan Web Security Suite、InterScan Messaging Security Suite など、その他のトレンドマイクロ製品と共に使用すると、InterScan による保護が強化されます。

ネットワークセキュリティのニーズすべてに対応するソリューションのより包括的なリストについては、トレンドマイクロの Web サイトを参照してください。

<http://www.trendmicro.com/jp/products/enterprise.htm>

6. ファイルベースのウイルス対策ソフトウェアでは、通常、検索対象から除外するフォルダを設定することができます。InterScan を別のウイルス対策ソフトウェアと併用する場合は、次のフォルダを検索対象から除外するよう設定することをお勧めします。
- Isme¥storage¥quarantine
 - Isme¥storage¥backup
 - Isme¥storage¥archive
 - Isme¥temp
 - Isme¥Debug

注意：これらのディレクトリ名は、インストール時に InterScan が初期設定で使用する名前です。

InterScan のアップデート

ウイルス対策ソフトウェアは、最新の技術を使用していないと効力を発揮しません。新しいウイルス / 不正プログラムやその他の不正コードは絶えずリリースされています。そのため、InterScan のコンポーネントを定期的にアップデートして、新しいセキュリティ上の脅威に対して防御することが極めて重要です。アップデート可能な InterScan のコンポーネントは、ウイルス検索エンジン、ウイルスパターンファイル、スパムメール検索エンジン、スパムメール判定ルール、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、およびスパイウェアパターンファイルです。

InterScan をアップデートする前に、次の作業を行う必要があります。

- 製品のアクティベート。126 ページの「InterScan のアクティベーション」を参照してください。
- プロキシサーバでネットワーク上のインターネットトラフィックが処理されている場合、プロキシサーバ情報の設定。131 ページの「プロキシサーバの設定」を参照してください。
- アップデート方法とアップデート元の設定。アップデートの方法には、**手動アップデート**および**予約アップデート**があります。アップデート元には、アップデートサーバ、インターネット、およびイントラネット UNC パスがあります。132 ページの「コンポーネントの手動アップデート」、また 133 ページの「予約アップデートの設定」も参照してください。

大規模感染の状況の管理

ウイルス / 不正プログラム、トロイの木馬、ワーム、またはその他のスパイウェア / グレーウェアが、突然ネットワーク上の多くの Exchange サーバやパーソナルコンピュータを攻撃すると、大規模感染が発生します。セキュリティパッチなどの最新コンポーネントが適用されていないソフトウェア、設定が不十分なウイルス対策ソフトウェア、または、新たに発生してまだパターンファイルのない不正プログラムなど、攻撃が発生する理由はいくつもあります。アウトブレイク時には、多くの場合組織内のグローバルな分散グループとの通信が混乱し、対応に時間が掛かります。

アウトブレイクが発生したときに管理者が実行する処理は、4 つの一般的な段階に分けることができます。

1. そのセキュリティイベントが確かな問題であり、誤った警告ではないことの確認
2. セキュリティイベントへの対応
3. セキュリティイベントの分析
4. Exchange サーバおよびメールボックスの回復

InterScan には、アウトブレイクの各段階で管理者を支援するいくつかの便利な機能があります。アウトブレイクの脅威が発生した場合、次の機能を検討してください。

1. セキュリティイベントが本当に不正プログラムのアウトブレイクであることを確認するには、次の手順に従ってください。
 - トレンドマイクロの Web サイトで、ウイルスの警告と最新のセキュリティ情報を確認します。

<http://www.trendmicro.co.jp/vinfo/>

- InterScan 通知を確認します。InterScan は、アウトブレイクの状況が発生すると、自動的に警告を送信するように設定することができます。さらに InterScan は、検出された脅威に対して処理を実行する際に、管理者またはその他の指定したユーザに通知するよう設定できます。

- セキュリティイベントを素早く分析するには、[概要] 画面を表示するか、手動レポートを作成します。セキュリティイベントの詳細については、ログのクエリを実行します。

2. 対応

- 手動アップデートを使用して、すぐに最新の InterScan コンポーネントをダウンロードします。
159 ページの「InterScan のアップデート」を参照してください。
- アップデートに続き、インフォメーションストア全体の手動検索を実行します。トレンドマイクロの推奨設定やトレンドマイクロの推奨処理などのトレンドマイクロが推奨する初期設定を使用するか、さらに具体的な検索フィルタを設定します。検索対象が正確に分かっている場合には、[ウイルス検索] 画面で [指定のファイル] を選択し、InterScan で検出するファイル名を入力します。

3. 分析

- ログクエリを実行し、攻撃についての情報を取得します。ログには、日時、送信者と受信者、感染した添付ファイルの名前などの有益な情報が含まれています。
- セキュリティ問題の分析に対する支援が必要な場合には、トレンドマイクロサポートにお問い合わせください。

4. 復旧

- Exchange 環境を復旧したら、設定とセキュリティポリシーの変更を検討します。次の点について考慮してください。
 - 処理を実行する前にファイルをバックアップするよう InterScan を設定します。これにより、InterScan では、回復不可能な処理を実行することなく、多くの脅威を検出し、除去することができます。
 - リアルタイムモニタを使用したり、ログやレポートを生成することにより、結果を監視します。
 - サーバ管理ツールを使用し、テスト済みの安全な InterScan サーバから別のサーバへ、迅速かつ簡単に構成を複製できます。

サポートと問い合わせ

この章では、テクニカルサポートを利用する手順、および管理者が Trend Micro InterScan for Microsoft Exchange (以下、InterScan) を運用するにあたって役に立つ情報を提供します。

この章の内容は次のとおりです。

- 164 ページの「製品サポート情報」
- 164 ページの「サポートサービスについて」
- 165 ページの「製品 Q&A のご案内」
- 166 ページの「セキュリティ情報」
- 167 ページの「ウイルス解析サポートセンター「TrendLabs」」

製品サポート情報

InterScan 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。

http://esupport.trendmicro.co.jp/supportjp/supportcentral/supportcentral_adv_ja.do

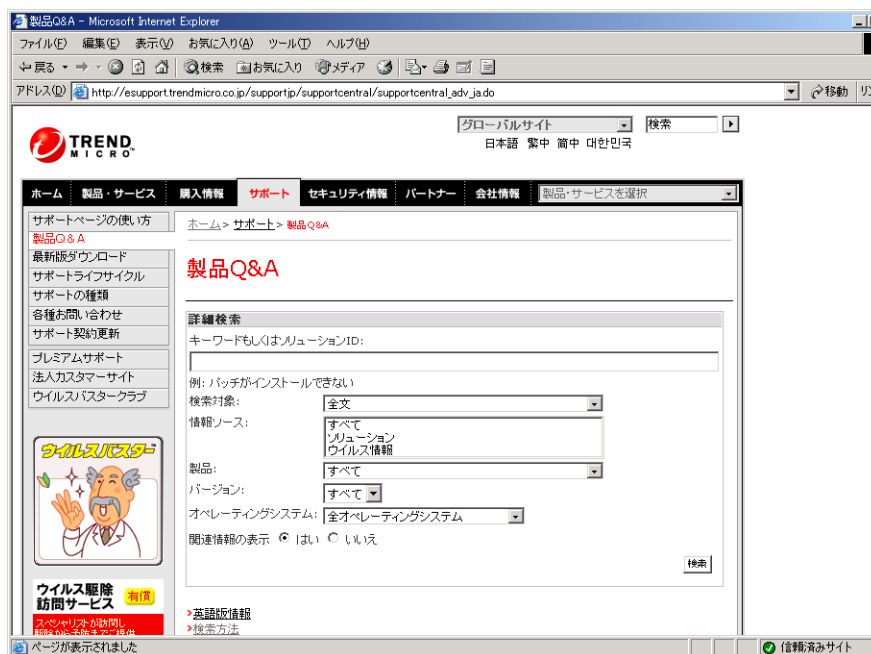


図 6-1. 製品 Q&A の Web サイト

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/supform.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を含む 800 名以上 (2006 年 1 月現在) 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ジメントの英国規格 BS7799 (フィリピン) を取得しています。

Exchange 環境に対する脅威の概要

Trend Micro InterScan for Microsoft Exchange (以下、InterScan) は、Exchange 環境におけるウイルス / 不正プログラム、トロイの木馬、ワーム、スパイウェア / グレーウェアの拡大、感染を阻止します。

この章の内容は次のとおりです。

- 170 ページの「用語の説明」
- 178 ページの「InterScan による Exchange 環境の保護」

用語の説明

コンピュータセキュリティは急速に変化しています。コンピュータおよびネットワークに対する潜在的な危険または好ましくない活動を説明するために、さまざまな用語や語句が管理者や情報セキュリティの専門家によって考案および採用されています。本ガイドで使用するそれらの用語とその意味を次で説明します。

ここで説明する用語には、実際のセキュリティリスクを表すものと、それほど有害ではなくても、迷惑な、歓迎されない活動を表すものがあります。トロイの木馬、ウイルス / 不正プログラム、ワームなどは、実際のセキュリティリスクを表す用語の一例です。ジョークプログラム、スパイウェア / グレーウェアなどの用語は、害を及ぼす可能性はあっても、単に迷惑で歓迎されないという程度の活動を表すのに使用されます。InterScan は、この章で説明するすべての事象から Exchange サーバを保護します。

ウイルス / 不正プログラム

コンピュータウイルス / 不正プログラムとは、複製する能力を持ったコードのセグメントです。ウイルス / 不正プログラムは通常、ファイルがウイルス / 不正プログラムに感染することによって複製されます。ファイルがウイルス / 不正プログラムに感染すると、ファイルが実行されるときにウイルス / 不正プログラムも実行され、ウイルス / 不正プログラムのコピーがファイルに添付されます。このことによって、感染したファイルがさらに他のファイルを感染させるようになります。生物学上のウイルスと同様に、コンピュータウイルス / 不正プログラムは急速に広がり、多くの場合、撲滅するのが困難です。

一部のコンピュータウイルス / 不正プログラムは、増殖することに加えて、別の共通点も持っています。それは、ウイルス / 不正プログラムのペイロード (発病機能を担う部分) を運ぶダメージルーチンです。ウイルス / 不正プログラムのペイロードは、メッセージや画像を表示するだけの場合もありますが、ファイルを破壊したり、ハードディスクを再フォーマットしたり、その他の被害を引き起こしたりする可能性もあります。ウイルス / 不正プログラムにダメージルーチンが含まれていない場合でも、ストレージ領域やメモリを消費し、コンピュータの全体的なパフォーマンスを低下させて、問題を引き起こすことがあります。

一般にウイルス / 不正プログラムは次の3つに大別されます。

- ファイル感染型

ファイル感染型ウイルス / 不正プログラムには、DOS ウイルス / 不正プログラム、Windows ウイルス / 不正プログラム、マクロウイルス / 不正プログラム、およびスクリプトウイルス / 不正プログラムなどさまざまな種類があります。これらすべてにはウイルス / 不正プログラムとしての共通の特徴がありますが、感染するホストファイルまたはプログラムの種類が異なります。

- システム領域感染型

システム領域感染型ウイルス / 不正プログラムはハードディスクのパーティションテーブルやハードディスクおよびフロッピーディスクのブートセクタに感染します。

- スクリプト

スクリプトウイルス / 不正プログラムはスクリプトプログラミング言語で記述されたウイルス / 不正プログラムです。Visual Basic スクリプト、JavaScript などで記述され、通常は HTML ドキュメントに埋め込まれています。

VBScript (Visual Basic Script) および Jscript (JavaScript) ウイルス / 不正プログラムは Microsoft の Windows Scripting Host を利用して動作し、他のファイルに感染します。Windows Scripting Host は Windows 98 および Windows 2000 などの Windows OS に含まれるので、単に Windows のエクスプローラから *.vbs や *.js ファイルをダブルクリックするだけでウイルス / 不正プログラム活動が実行されます。

ではスクリプトウイルス / 不正プログラムのどこが特別なのでしょう。スクリプトウイルス / 不正プログラムは、アセンブリタイプのプログラミング知識を必要とするバイナリウイルス / 不正プログラムとは異なり、テキストでプログラミングされます。スクリプトウイルスは、下位レベルのプログラミングを必要とせず、可能な限りコンパクトなコードで機能を実現します。また Windows に事前に定義されているオブジェクトを使用して、感染したシステムの多くの部分に容易にアクセスすることもでき、たとえばファイルを感染させたり、マスメーリングを実行したりします。さらに、コードがテキストで記述されるので、他者がそのコードの枠組みを簡単に解釈し模倣できます。そのため、多くのスクリプトウイルス / 不正プログラムには改変された亜種がいくつか存在します。

たとえば「I love you」ウイルスの出現直後、ウイルス対策ベンダーは、件名やメールの本文が改変されて広まった、オリジナルのコードのコピーを発見しました。

どのような種類のウイルスであっても、その基本的な仕組みは同じです。ウイルスには自己の複製を明示的に作成するコードが含まれます。ファイル感染型ウイルス / 不正プログラムの場合は通常、感染したプログラムをユーザが誤って実行したときに、制御を取得するための改変が加えられています。ウイルスコードの実行が終了すると、多くの場合、感染しているファイルには何も問題がないように見せるためにオリジナルのホストプログラムに制御が戻されます。

また、異なるプラットフォーム間で活動するウイルス / 不正プログラムもあります。この種のウイルス / 不正プログラムは、たとえば Windows と Linux などのように、異なるプラットフォームに属するファイルにも感染します。ただし、このようなウイルス / 不正プログラムは非常にまれで、その機能が 100% 実現されることはほとんどありません。

ワーム

コンピュータワームとは自己完結したプログラムまたはプログラムのセットで、それ自体またはそのセグメントの機能の複製を他のコンピュータシステムに拡大します。通常、ネットワーク接続またはメールの添付ファイルを介して感染します。ワームはウイルス / 不正プログラムとは異なり、自身をホストプログラムに添付する必要がありません。ワームは、しばしば Microsoft Outlook などのメールアプリケーションを使用して感染します。また、ユーザがダウンロードすることを想定して、自己の複製を共有フォルダに作成したり、Kazaa などのファイル共有システムを利用して感染します。場合によっては、ICQ、AIM、mIRC などのチャットアプリケーションやその他のピアツーピア (P2P) プログラムを使用して、自己の複製を感染させます。

トロイの木馬型プログラム

トロイの木馬型プログラム (以下、トロイの木馬) は、表面的には無害なソフトウェアに潜んでいるプログラムです。ウイルス / 不正プログラムと違って自己複製はせず、ユーザに複製させてそれを他のユーザに送信させます。しばしばコンピュータゲームや画像ソフトウェアなど魅力的なソフトウェアの中に潜み、初心者がそれを他のユーザに送信してしまいます。トロイの木馬には破壊的なペイロードが含まれていない場合があります。その代わりに、システムまたはネットワーク全体のセキュリティを脅かすようなルーチンを含んでいる場合があります。

ジョークプログラム

ジョークプログラムとは、一般的には悪意のない、通常の実行可能プログラムです。

ジョークプログラムはコンピュータユーザをからかう目的で作成されます。データを破壊する意図はありませんが、場合によっては、データの損失を招く可能性のある操作 (古いバックアップからのファイルの復元、ドライブのフォーマット、ファイルの削除など) をユーザが誤ってしてしまうことがあります。

ジョークプログラムは通常の実行可能プログラムであるため、他のプログラムに感染したり、コンピュータシステムやデータに損傷を加えたりすることはありません。時折、一時的にマウスやキーボードなどのデバイスの設定を変更することもあります。しかし、ジョークプログラムが終了するか、コンピュータを再起動すれば、コンピュータは元の状態に戻ります。ジョークプログラムは、一般には無害ですが、組織にとっては大きな損害となる可能性があります。

マスメーリング型ウイルス

メールを標的としたウイルス / 不正プログラム、たとえば悪名高い Melissa、Loveletter、AnnaKournikova などは、感染したコンピュータのメールクライアントを自動化することで、メールを通じてウイルスを増殖させる能力を持ちます。マスメーリング型の活動とは、Exchange 環境内でクライアントやサーバの間に感染が急速に拡大する状況を表しています。マスメーリング型ウイルスは、駆除に費用がかかり、ユーザの間でパニックを引き起こす可能性があります。トレンドマイクロでは、マスメーリング型ウイルスが一般的に示す動作を検出するウイルス検索エンジンを設計しました。その動作は、Trend Labs のアップデートサーバを使用してアップデートされる、ウイルスパターンファイルに記録されます。

InterScan では、マスメーリング型の活動を検出するたびに、マスメーリング型ウイルスに対して特別な処理を実行できます。マスメーリング型の活動に対して設定された処理は、その他すべての処理に優先されます。マスメーリング攻撃に対する初期設定の処理は、「メッセージ全体の削除」です。

例：メール内にワームまたはトロイの木馬を検出した場合に、そのメッセージを隔離するように InterScan を設定します。また、マスメーリング型ウイルスの検索を有効にして、マスメーリング型の活動を示すすべてのメッセージを削除するように InterScan を設定しています。InterScan が、MyDoom の変種などのワームを含むメッセージを受信します。このワームは、独自の SMTP エンジンを使用して、感染したコンピュータから収集したメールアドレスに自身を送信します。InterScan は MyDoom ワームを検出し、マスメーリング型の活動を認識すると、そのワームを含むメールを削除します。それに対して、マスメーリング型の活動を示さないワームには、隔離処理を実行します。

圧縮ファイル

圧縮とアーカイブは、特にメール添付ファイル、FTP、HTTP などのファイル転送では、最も一般的なファイル保存方法です。ただし、圧縮ファイルでウイルス検出を行う前には、まず解凍する必要があります。ウイルス検索 / 不正プログラムにおける解凍の根本的な重要性をふまえ、トレンドマイクロでは、主要な解凍ルーチンの多くをサポートしています。サポートしていないタイプの圧縮ファイルについては、圧縮ファイル内の個々のファイルにではなく、圧縮ファイル全体に対して処理を実行します。

InterScan では現在、以下の圧縮タイプをサポートしています。

- **抽出** — 次の種類の 1 つのファイルに複数のファイルが圧縮またはアーカイブされている場合に使用します。

PKZIP、LHA、LZH、ARJ、MIME、MSCF、TAR、GZIP、BZIP2、RAR、および ACE

- **展開** — 次の種類の 1 つのファイルにファイルが 1 つだけ圧縮またはアーカイブされている場合に使用します。

PKLITE、PKLITE32、LZEXE、DIET、ASPACK、UPX、MSCOMP、LZW、MACBIN、および Petite

- **復元** — ファイルがバイナリから ASCII に変換されている場合に使用します。メールシステムで広く使われている方法です。

UUENCODE および BINHEX

注意： InterScan では、サポートしていない圧縮タイプについては、第 1 圧縮階層より下の階層に含まれるウイルス / 不正プログラムを検出できません。

InterScan では、圧縮ファイルを検出すると、以下の操作を実行します。

1. 圧縮ファイルを抽出し、検索します。

InterScan ではまず、最初の圧縮階層の抽出から開始します。第 1 階層の抽出後、第 2 階層に進み、それ以降も最大 20 階層までのユーザが設定したすべての圧縮階層を検索します。

2. 感染ファイルに対してユーザが設定した処理を実行します。

InterScan では、圧縮形式で検出された感染ファイルに対しても、その他の感染ファイルと同じ処理を実行します。たとえば、感染ファイルに対する処理として「メッセージ全体の隔離」を選択すると、InterScan は感染ファイルが検出されたメッセージ全体を隔離します。

InterScan では、PKZIP と LHA の 2 種類の圧縮ルーチンからファイルを駆除できます。ただし、InterScan では、これらの圧縮ルーチンを使用して圧縮されたファイルの第 1 階層のみを駆除できます。

マクロウイルス / 不正プログラムについて

マクロウイルス / 不正プログラムは、アプリケーション固有のものです。Microsoft Word (.doc) や Microsoft Excel (.xls) などのアプリケーションに含まれるマクロユーティリティに感染します。したがって、.doc、.xls、.ppt など、マクロ対応のアプリケーションに共通する拡張子のファイルで検出されます。マクロウイルス / 不正プログラムは、アプリケーションのデータファイル間で伝染するため、阻止できない場合、最終的に膨大な数のファイルが感染する恐れがあります。

これらのファイルタイプはメールに添付されることが多いので、マクロウイルス / 不正プログラムはメールの添付ファイルに入り込み、インターネットを利用して簡単にまん延します。

InterScan では、次の方法で、Exchange サーバをマクロウイルス / 不正プログラムの感染から守ります。

- ヒューリスティック検索を使用して、不正なマクロコードを検出します。

ヒューリスティック検索とは、評価的なウイルス / 不正プログラム検出方法です。この方法は、既知のウイルスシグネチャを持たないウイルス / 不正プログラムおよび脅威の検出に優れています。

- 検索されたファイルのすべてのマクロコードを削除します。

スパイウェア / グレーウェア

クライアントは、ウイルス / 不正プログラム以外の潜在的な脅威の危険にもさらされています。グレーウェアは、ネットワーク上のコンピュータのパフォーマンスに悪影響を与え、セキュリティ上、機密保持上、および法律上の重大なリスクを組織にもたらしめます。

グレーウェア / グレーウェアの種類

InterScan では、以下のものを含む、複数の種類のグレーウェアを検出できます。

スパイウェア — アカウントユーザ名やパスワードなどのデータを収集し、そのデータを第三者に送信します。

アドウェア — 広告を表示し、ユーザのネットサーフィンの好みなどのデータを収集して、そのユーザを対象とする広告を Web ブラウザに表示します。

ダイヤラー — コンピュータのインターネット設定を変更して、あらかじめ設定された電話番号にモデムを通じて電話を掛けさせることができます。

ジョークプログラム — CD-ROM トレイを開閉したり、おびたどしい数のメッセージボックスを表示したりするなど、コンピュータの異常な動作を引き起こします。

ハッキングツール — ハッカーがコンピュータに侵入できるようにします。

リモートアクセスツール — ハッカーがリモートでコンピュータにアクセスし、制御できるようにします。

パスワード解読アプリケーション — ハッカーがアカウントユーザ名とパスワードを解読できるようにします。

潜在的なリスクと脅威

スパイウェア / グレーウェアがネットワーク上に存在すると、以下の事態を招く可能性があります。

- **コンピュータのパフォーマンスの低下** — スパイウェアまたはグレーウェアアプリケーションは、多くの場合、タスクを実行するために、CPU およびシステムメモリのリソースを大量に必要とします。
- **Web ブラウザ関連のクラッシュの増加** — アドウェアなど、ある種のグレーウェアアプリケーションは、多くの場合、ポップアップウィンドウを作成したり、ブラウザのフレームまたはウィンドウに情報を表示したりするように設計されています。そのアプリケーションのコードがシステムのプロセスとやり取りする方法によっては、グレーウェアがブラウザのクラッシュやフリーズを引き起こす場合や、システムの再起動が必要になる場合があります。
- **ユーザの能率の低下** — 頻繁に表示されるポップアップ広告を閉じたり、ジョークプログラムの悪影響に対処したりする必要があるために、ユーザが重要な仕事に集中できなくなる可能性があります。
- **ネットワーク帯域幅の減少** — スパイウェアまたはグレーウェアアプリケーションは、多くの場合、ネットワーク内で実行されている別のアプリケーションやネットワーク外の場所に、収集したデータを定期的送信します。
- **個人情報および企業情報の損失** — スパイウェアまたはグレーウェアアプリケーションが収集するデータは、ユーザが閲覧する Web サイトのリストのように無害なものばかりではありません。スパイウェアまたはグレーウェアは、ユーザが入力するユーザ名とパスワードを収集して、銀行口座やネットワークのリソースにアクセスする企業アカウントなどの個人アカウントにアクセスすることもあります。
- **法的責任のリスクの上昇** — ハッカーがネットワークのコンピュータリソースにアクセスできるようになれば、クライアントコンピュータが使用されて、ネットワーク外のコンピュータに対して攻撃が開始されたり、スパイウェアやグレーウェアがインストールされる可能性があります。その種の活動にネットワークリソースが否応なしに参加させられることにより、他者による被害に対して企業が法的責任を負うことになる場合があります。

InterScan による Exchange 環境の保護

トレンドマイクロでは、ウイルス / 不正プログラムなどが Microsoft Exchange サーバに及ぼす特異な危険を認識します。InterScan はこれらの数多くのさまざまな脅威から Exchange を保護するように設計されています。

InterScan は、トレンドマイクロのウイルス検索エンジンとスパムメール検索エンジンを使用して、ウイルス / 不正プログラムやその他のセキュリティ上の脅威を検出し、スパムメッセージを排除します。この 2 つのエンジンには、最新のパターンファイルが必要です。このパターンファイルは、TrendLabs によって提供され、アップデートサーバまたはユーザが設定したアップデート元から配信されます。

InterScan ではフィルタリング戦略により Exchange を保護します。メッセージが Exchange サーバに到着すると、InterScan は各メールに複数のフィルタを適用します。それぞれのフィルタでは、セキュリティ上の脅威や望ましくないコンテンツについて、メールが調べられます。ウイルス / 不正プログラム、トロイの木馬、ワーム、およびスパイウェア / グレーウェアが含まれるメールは、これらの InterScan のフィルタによって排除されます。

- **スパムメール対策**

各メールは、インフォメーションストアに送信される前に、スパムメールが含まれていないかどうか検査されます。

- **コンテンツフィルタ**

InterScan では、受信メールおよび送信メールをフィルタして、望ましくないコンテンツを排除できます。

- **添付ファイルブロック**

InterScan は、ユーザが定義するファイルタイプまたは特定のファイル名に基づいて添付ファイルをブロックできます。

- **ウイルス検索**

ウイルス検索は、ウイルス / 不正プログラム、ワーム、トロイの木馬、およびその他の脅威を検出します。InterScan ではまた、スパイウェア / グレーウェアを検出し、処理することもできます。

Windows イベントログコード

Windows のイベントログに記述される通知のイベント ID が、以前の InterScan のバージョンから大幅に変更されています。この変更が監視の実施に影響を与える場合があります。Windows のイベントログについては、次の表を参照してください。

イベント ID	機能部	種類 / 重要度	カテゴリ	説明
3	アプリケーション	エラー	なし	InterScan のサービス開始に失敗
4	アプリケーション	エラー	なし	InterScan のサービス停止に失敗
5	アプリケーション	警告	なし	ウイルス検索の通知
6	アプリケーション	警告	なし	添付ファイルのブロックの通知
7	アプリケーション	警告	なし	コンテンツフィルタの通知
16	アプリケーション	警告	なし	手動アップデートの失敗
17	アプリケーション	情報	なし	手動アップデートの完了
18	アプリケーション	警告	なし	最後のアップデート時期が指定時期以前
19	アプリケーション	情報	なし	手動検索の完了

表 A-1. InterScan 8.0 の Windows イベントログコード

イベント ID	機能部	種類 / 重要度	カテゴリ	説明
20	アプリケーション	エラー	なし	手動検索の失敗
21	アプリケーション	警告	なし	検索時間が指定時間を超過
22	アプリケーション	警告	なし	バックアップ、隔離、またはアーカイブディレクトリが含まれるドライブ (ボリューム) 上のディスク空き容量が指定サイズ未満
23	アプリケーション	警告	なし	隔離およびログ用のデータベースサイズが指定サイズを超過
24	アプリケーション	情報	なし	予約検索の完了
25	アプリケーション	エラー	なし	予約検索の失敗
32	アプリケーション	エラー	なし	予約アップデートの失敗
33	アプリケーション	情報	なし	予約アップデートの完了
80	アプリケーション	情報	なし	大規模感染予防モードの開始
82	アプリケーション	情報	なし	大規模感染予防モードの停止と設定の復元
257	アプリケーション	警告	なし	アウトブレイクアラート、ウイルスの検出
258	アプリケーション	警告	なし	アウトブレイクアラート、駆除不能なウイルスの検出
259	アプリケーション	警告	なし	アウトブレイクアラート、添付ファイルのブロック
513	アプリケーション	エラー	なし	フィルタロードの例外

表 A-1. InterScan 8.0 の Windows イベントログコード (続き)

イベント ID	機能部	種類 / 重要度	カテゴリ	説明
514	アプリケーション	エラー	なし	アダプタロードの例外
4097	アプリケーション	警告	なし	Exchange のトランザクションログの含まれるドライブ上のディスク空き容量が指定サイズ未満
4098	アプリケーション	警告	なし	Exchange のメールストアのサイズが指定サイズを超過
4099	アプリケーション	警告	なし	連続して待ち行列に格納される Exchange の SMTP メールが指定数を超過
4112	アプリケーション	エラー	なし	ディスク領域が不足しているため、InterScan Master Service が停止しました。空きディスク領域を増やして、InterScan Master Service を再開してください。
8193	アプリケーション	情報	なし	(エンドユーザメール隔離) 手動管理タスクの処理が開始。
8194	アプリケーション	情報	なし	(エンドユーザメール隔離) 手動管理タスクの処理が終了。
8195	アプリケーション	情報	なし	(エンドユーザメール隔離) 予約管理タスクの処理が開始。
8196	アプリケーション	情報	なし	(エンドユーザメール隔離) 予約管理タスクの処理の終了。
8197	アプリケーション	情報	なし	(エンドユーザメール隔離) 有効化タスクの処理の開始。
8198	アプリケーション	情報	なし	(エンドユーザメール隔離) 有効化タスクの処理の終了。
8199	アプリケーション	情報	なし	(エンドユーザメール隔離) 無効化タスクの処理の開始。
8200	アプリケーション	情報	なし	(エンドユーザメール隔離) 無効化タスクの処理の終了。

表 A-1. InterScan 8.0 の Windows イベントログコード (続き)

事前設定ファイル

事前設定ファイルは、サイレントインストールに使用されます。サイレントインストールを実行するには、新規の事前設定ファイルを記録します。各事前設定ファイルには、12 個のセクションがあります。次の表には、さまざまなセクションが一覧表示されています。事前設定ファイルを手動で変更する場合、次の表を参照用に使ってください。

セクション	内容
Log on	• LogonUserDomain= ユーザの設定 • LogonUserName= ユーザの設定 • LogonPassword= ユーザの設定 パスワードは暗号化する必要があります。
Directory	• TempDir=smex80temp • ShareName=C\$ 初期値は C\$ です。ユーザによる変更が可能です。 • TargetDir=C:\Program Files\Trend Micro\Isme これは初期設定です。ユーザによる変更が可能です。 • UseDefaultProgPath=0 または 1 0 の場合はユーザの設定を使用し、1 の場合は初期値を使用します。
Activation	MasterACCode= ユーザの設定

表 B-1. 事前設定ファイル

セクション	内容
Proxy	• UseProxy=0 または 1 0 の場合は無効、1 の場合は有効です。 • DoAUAfterInstall=0 または 1 0 の場合は無効、1 の場合は有効です。 • ProxyURL= ユーザの設定 • ProxyPort= ユーザの設定 範囲は 1 ～ 65535 です。 • ProxyUsername= ユーザの設定 • EnableSocks5=0 または 1 0 の場合は無効、1 の場合は有効です。
Web	• WebServerType=0 または 1 0 の場合は IIS、1 の場合は Apache です。 • IISSiteType=0 または 1 0 の場合は仮想 Web サイト、1 の場合は初期設定の Web サイトです。この設定は、ユーザが IIS サーバを選択した場合にのみ有効です。 • WebPort= ユーザの設定 範囲は 1 ～ 65535 です。 • EnableSSL=0 または 1 0 の場合は無効、1 の場合は有効です。 • SSLPort= ユーザの設定 範囲は 1 ～ 65535 です。 • SSLValidPeriodCertificate= ユーザの設定
WTC	WTCEnable=0 または 1 0 の場合は無効、1 の場合は有効です。
ServerManagement	• CreateNewConsoleAccount=0 または 1 0 の場合は既存のものを使用するかスキップし、1 の場合は新しいアカウントを作成します。 • ConsoleUsername= ユーザの設定 • ActivateServerManagement=0 または 1 0 の場合は非アクティベート、1 の場合はアクティベートです。
SMTP	EnableSMTPScanning=1 0 の場合は無効、1 の場合は有効です。

表 B-1. 事前設定ファイル

セクション	内容
EUQ	• ActivateEUQ=0 または 1 0 の場合は非アクティブ、1 の場合はアクティブです。 • IntegrateWithOutlook2K3JunkMailFolder=0 または 1 0 の場合は無効、1 の場合は有効です。 • UseDefaultSpamFolderName=0 または 1 0 の場合はユーザの設定を使用し、1 の場合は初期値を使用します。 • SpamFolderName=Spam Mail これは初期フォルダ名です。ユーザによる変更が可能です。 • SpamMsgRetainDay=14 これは初期設定です。ユーザによる変更が可能で、範囲は 0 ～ 30 です。
CMAgent	• RegisterCMAgent=0 または 1 0 の場合は無効、1 の場合は有効です。 • CMServerAddress= ユーザの設定 • CMServerPortNumber=443 これは初期設定です。ユーザによる変更が可能で、範囲は 1 ～ 65535 です。 • ConnectCMServerUsingHTTPS=0 または 1 0 の場合は無効、1 の場合は有効です。 • ConnectCMServerUsingProxy=0 または 1 0 の場合は無効、1 の場合は有効です。 • ConnectCMServerProxyAddress= ユーザの設定 • ConnectCMServerUseSOCKS5=0 または 1 0 の場合は無効、1 の場合は有効です。 • ConnectCMServerProxyUserName= ユーザの設定 • CMServerWebUserName= ユーザの設定 • ConnectCMServerProxyPortNumber=80 これは初期設定です。ユーザによる変更が可能で、範囲は 1 ～ 65535 です。

表 B-1. 事前設定ファイル

セクション	内容
Do NOT edit these settings	• LogonPassword= ユーザの設定 パスワードは暗号化する必要があります。 • ExchangeType=1、2、または 3 1 の場合は「Exchange 2007 エッジトランスポートサーバ」です。 2 の場合は「Exchange 2007 ハブトランスポート / メールボックスサーバ」です。 3 の場合は「Exchange 2000/2003 サーバ」です。 • ProxyPassword= ユーザの設定 パスワードは暗号化する必要があります。 • ConsolePassword= ユーザの設定 パスワードは暗号化する必要があります。 • EUQInstallLangID=1033 この設定は変更しないでください。 • EUQDefaultLangID=9 この設定は変更しないでください。 • ConnectCMServerProxyPassword= ユーザの設定 パスワードは暗号化する必要があります。 • CMServerWebPassword= ユーザの設定 パスワードは暗号化する必要があります。 • ConsoleGroup= 2000/2003 の場合は「SMEX Admin Group」（このグループ名は変更しないでください）です。 2007 の場合はユーザの設定（例：DomainName\Group。このグループ名は変更しないでください）です。 • ServerManagementGroupSid= (SID は変更しないでください)
InstallOption	WaitIISAdminToUnloadSMTPHook=-1 • この設定は、移行の場合のみ有効です。 • -1: これは初期設定です。InterScan インストールプログラムは、一般サーバのアップグレード時に IIS サービスを再開しますが、クラスタサーバの場合は 20 分待機します。移行には、ビルドおよびバージョンのアップグレードが含まれます。 • 0: 一般サーバおよびクラスタサーバの場合に 20 分待機せずに、IIS サービスを再開します。 • 1: 一般サーバおよびクラスタサーバの場合に 20 分待機します。

表 B-1. 事前設定ファイル

Trend Micro Control Manager について

Trend Micro Control Manager (以下、Control Manager) は、トレンドマイクロのゲートウェイ、メールサーバ、ファイルサーバ、デスクトップレベル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、およびサードパーティ製品を管理するための集中管理コンソールです。Control Manager の Web ベースの製品コンソールにより、ネットワーク全体のウイルス対策およびコンテンツセキュリティ製品やサービスを 1 か所から監視することができます。

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検出ポイントを監視し把握することができます。また、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。

- 188 ページの「Control Manager の基本機能」
- 189 ページの「Trend Micro Management Communication Protocol について」
- 194 ページの「Control Manager エージェントハートビート」
- 197 ページの「Control Manager への InterScan の登録」
- 198 ページの「Control Manager による InterScan の管理」

Control Manager の基本機能

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します。

Control Manager には主に次の機能があります。

- **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することができます。
- **大規模感染予防** - 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 では、SSL (Secure Socket Layer) プロトコルに基づいた通信技術を採用しています。
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することができます。
- **設定およびコンポーネントダウンロードの保護** - この機能により、管理コンソールへのアクセスとコンポーネントのダウンロードを保護できます。
- **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ーに異なる権限を持つアカウントを与えることができます。
ユーザーアカウントにより、ユーザーが 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することができます。
- **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することができます。

たとえば、ウイルスパターンファイルの更新や配信など、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。

-
- **リアルタイム / オンデマンドでの製品管理** - Control Manager は、管理コンソールで変更された設定を即座に InterScan for Microsoft Exchange (以下、InterScan) サーバに送信します。システム管理者は管理コンソールから手動検索を実行することができます。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一括して更新します。
 - **レポートの一元化** - 包括的なログや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 InterScan サーバ間の通信に使用されます。MCP には TMI と比べて、次のような利点があります。

- ネットワーク負荷とパッケージサイズの低減
- 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
- クラスタノードのサポート

ネットワーク負荷とパッケージサイズの低減

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。

- 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同一接続上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節約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環境のサポート

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) デバイスは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 IP アドレスが割り当てられます。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 の TMI ベース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放する必要がありません。
- 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。ユーザは、MCP エージェントに対して、一方向または双方向の通信の使用を設定できます。

一方向通信

NAT 通信環境は、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、Control Manager エージェントがサーバへの接続を開始し、サーバからのコマンドをポーリングします。それぞれの要求は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ンネルが追加されています。この追加チャンネルも HTTP プロトコルに基づいています。双方向通信では、Control Manager 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。Control Manager エージェント側には、CGI の要求を処理できる Web サーバまたは CGI 互換のプログラムが必要で、それによって Control Manager サーバからの通知が受信されます。

シングルサインオン (SSO) サポート

Control Manager との通信に MCP を使用する製品では、Control Manager 3.5 から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 にログオンすれば、他のトレンドマイクロ製品にログオンしなくてもそれらの製品のリソースにアクセスできます。

クラスタノードのサポート

さまざまな状況下で、管理者は特定の製品インスタンスを論理ユニットまたはクラスタとしてグループ化したい場合があります。たとえば、クラスタ環境でインストールされている製品が、1つのクラスタグループでインストールされているすべての製品インスタンスを表す場合などです。しかし、Control Manager サーバの観点から言うと、正式な登録プロセスを完了した各製品インスタンスは、独立した管理ユニットと見なされ、各管理ユニットは互いに区別されません。

Control Manager との通信に MCP を使用する製品では、Control Manager でクラスタノードがサポートされるようになりました。

Control Manager エージェントハートビート

InterScan サーバのステータスを監視するために、Control Manager 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、InterScan サーバのステータスを示したり、Control Manager からの InterScan サーバ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 の製品コンソールに InterScan サーバのステータスが表示されます。つまり、InterScan サーバのステータスは、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 InterScan サーバ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。InterScan サーバ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 InterScan サーバのステータスがオフラインに変更されます。

Control Manager による InterScan サーバ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 InterScan サーバのステータスが判断されます。

- Control Manager は InterScan サーバからログを受信します。Control Manager が、InterScan サーバ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、InterScan サーバ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、InterScan サーバ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 InterScan サーバに正常に接続されるということは、InterScan サーバ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せん。
 - 一方方向通信モードでは、Control Manager 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。

Control Manager エージェントハートビートは、次の方法で実装されます。

- **UDP:** InterScan サーバが 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 InterScan サーバ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。

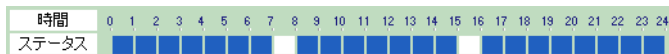
InterScan サーバのステータスを示すために単に接続ステータスを送信すると同時に、追加データを Control Manager にアップロードすることもできます。通常、追加データには、コンソールに表示される、InterScan サーバのアクティビティ情報が含まれます。

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、コミュニケーターから Control Manager サーバに情報が送信される稼働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、稼働中または停止中の時間帯を定義します。

コミュニケータースケジュールでは、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。



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 3:00、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

コミュニケーター接続ステータスの実行間隔を指定するときは、コミュニケーター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。

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ー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、コミュニケーター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ー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、コミュニケーターとの頻繁な通信によって帯域幅が多く消費されます。

表 C-1. 推奨される接続ステータス

Control Manager への InterScan の登録

InterScan サーバはスタンドアロン製品なので、Control Manager に登録する必要はありません。ただし、Control Manager に登録することにより、この付録で先に説明した機能を利用することができます。InterScan サーバの製品コンソールを使用して、すべての機能を管理します。

InterScan サーバを Control Manager に登録するには

1. InterScan 製品コンソールにログオンします。
2. [管理]→[Control Manager の設定] の順に選択します。[Control Manager の設定] 画面が表示されます。

注意：Control Manager は [エンティティ表示名] フィールドで指定された名前を使用して、InterScan サーバを識別します。この名前は Control Manager の製品ディレクトリに表示されます。

3. [接続設定] の [エンティティ表示名] フィールドに、InterScan サーバの名前を入力します。
4. [Control Manager サーバの設定] で、次の項目を指定します。
 - a. Control Manager サーバの IP アドレスまたはホスト名を [サーバの FQDN または IP アドレス] フィールドに入力します。
 - b. MCP エージェントが Control Manager と通信するために使用する、ポート番号を入力します。
 - c. Control Manager のセキュリティを「中」(Control Manager と管理下の製品の MCP エージェントとの間で、HTTPS 通信および HTTP 通信が許可されます) に設定した場合は、[HTTPS による接続] を選択します。
 - d. ネットワークで認証が必要な場合は、IIS サーバのユーザ名とパスワードを [ユーザ名] および [パスワード] フィールドに入力します。

- e. NAT デバイスを使用する場合は、[双方向通信ポート転送を有効にする] を選択して、NAT デバイスの IP アドレスを [IP アドレス] に、ポート番号を [ポート番号] に入力します。

Control Manager の製品管理の詳細については、「Control Manager 管理者ガイド」を参照してください。

5. Control Manager の管理コンソールのメインメニューで [製品] をクリックします。
6. 左端のメニューでリストから [管理下の製品] を選択して [表示] をクリックします。
7. InterScan サーバが表示されるのを確認します。

Control Manager による InterScan の管理

管理下の製品とは、製品ディレクトリ内の InterScan サーバ、ウイルス対策製品、コンテンツセキュリティ製品、またはサードパーティ製品を意味します。管理下の製品は、Control Manager の管理コンソールにアイコンで表示されます。これらのアイコンは、InterScan サーバ、その他の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、およびサードパーティ製品を表します。

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。製品ディレクトリ構成をカスタマイズするときには、ディレクトリ管理を使用します。

製品ディレクトリについて

製品ディレクトリは、管理下の製品を論理的にグループ化したものです。次のような影響があるため、製品ディレクトリの構造を慎重に計画する必要があります。

-
- **ユーザのアクセス権** : ユーザアカウントの作成時に、対象のユーザがアクセスできる製品ディレクトリの項目を指定するよう求められます。ユーザのアクセス権を割り当てることができるのは製品ディレクトリの 1 つの項目 (フォルダまたは製品) に対してのみです。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。一方、特定の InterScan サーバ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** : Control Manager は、配信計画に基づいて、ウイルス対策製品にパターンファイル、検索エンジン、スパムメール判定ルール、およびプログラムのアップデータを配信します。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。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することができます。
 - **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およびダメージクリーンナップサービスの配信は、大規模感染予防ポリシーとクリーンナップタスクの効率的な配分のための配信計画によって異なります。

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するアイコン

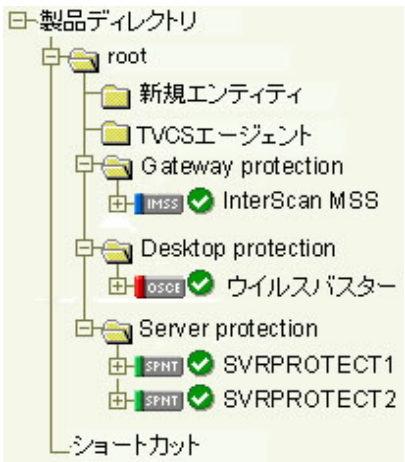
製品ディレクトリのツリー	アイコン	説明
製品ディレクトリ		
root		[新規エンティティ] フォルダまたはユーザ定義のフォルダの名前
新規エンティティ		
TVCSエージェント		InterScan eManager
Gateway protection		ウイルスバスター コーポレートエディション
IMSS  InterScan MSS		ServerProtect インフォメーションサーバ
Desktop protection		ServerProtect ドメイン
OSCE  ウイルスバスター Corp.		ServerProtect for Windows (一般サーバ)
Server protection		ServerProtect for NetWare (一般サーバ)
SPNT  SVRPROTECT1		InterScan Messaging Security Suite
SPNT  SVRPROTECT2		InterScan Web Security Suite
ショートカット		InterScan VirusWall for Windows
		InterScan VirusWall for UNIX
		InterScan for Microsoft Exchange
		InterScan for Lotus Notes
		Network VirusWall
		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

表 C-2. 管理下の製品を表すアイコン

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。InterScan サーバの保護タイプと Control Manager システムの管理モデルに従い、製品の種類を表すフォルダ名を使用して InterScan サーバ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。

InterScan の初期設定フォルダへのアクセス

新しく登録された InterScan サーバは、インストールの完了後、通常は InterScan フォルダに格納されます。このフォルダは、InterScan エージェントが Control Manager サーバに初めて登録するときに作成されます。ただし、TVCS エージェントフォルダの TVCS エージェントによって処理される管理下の製品は別のフォルダに格納されます。

 製品ディレクトリ ├── root │ ├── 新規エンティティ │ ├── TVCSエージェント │ ├── Gateway protection │ │ ├── IMSS ✓ InterScan MSS │ ├── Desktop protection │ │ ├── OSCE ✓ ウイルスバスター │ ├── Server protection │ │ ├── SPNT ✓ SVRPROTECT1 │ │ └── SPNT ✓ SVRPROTECT2 └── ショートカット	アカウントがアクセス権を持つ項目	管理下の製品の初期設定の配置場所
	root フォルダ	新規エンティティ
	Server protection	Server protection
	ウイルスバスター Corp.	新規エンティティ

ユーザアカウントに特定の管理下の製品へのアクセスを設定すると、そのアカウントは新しく登録された管理下の製品にはアクセスできなくなります。

表 C-3. 管理下の製品とユーザのアクセス権の関係

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 InterScan サーバを管理できます。

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、管理コンソールへのアクセスに使用するアカウントの種類とフォルダへ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

1. 上部のメニューで [製品] を選択します。
2. 左側のメニューでリストから [管理下の製品] を選択し、[表示] をクリックします。

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、InterScan サーバおよびその他の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。この機能は、ウイルス感染が急速に拡大している時に特に役立ちます。

特定またはグループ単位の InterScan サーバまたは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。
2. 左側のメニューでリストから [管理下の製品] を選択し、[表示] をクリックします。
3. 左側のメニューで、目的のフォルダまたは InterScan サーバを選択します。
4. 右側の画面で [タスク] タブをクリックします。
5. [タスク] リストから実行する処理を選択します。
6. [次へ] をクリックします。
7. [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。
8. [コマンド追跡] を使用して、進行状況を確認してください。
9. [配信開始] タスクの詳細を表示するには、[コマンド詳細] リンクをクリックします。

InterScan 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、およびスパイウェア / グレーウェア概要が表示されます。

InterScan サーバ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 InterScan サーバを選択します。
 - InterScan サーバまたは管理下の製品をクリックすると、その InterScan サーバまたは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、およびスパイウェア / グレーウェア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。

InterScan と管理下の製品の設定

管理下の製品の種類とエージェントのバージョンによって次のような違いがあります。

- デバイスまたは製品を個別に設定できる場合とフォルダごとにグループで設定できる場合があります。

グループ設定はフォルダの [設定] タブを使用して実行します。

注意： グループ設定は、1 つのグループに属する InterScan サーバすべてに同一の設定を適用する場合に実行します。グループ内の一部の製品に同一の設定を適用する場合は、対象のデバイスまたは管理下の製品をショートカットに追加して、その他の管理下の製品の設定が上書きされないようにします。

- [設定] タブをクリックすると、製品コンソールが表示されます。

管理下の製品を設定するには

1. 上部のメニューで [製品] を選択します。
2. 左側のメニューでリストから [管理下の製品] を選択し、[表示] をクリックします。
3. 左側のメニューで、目的の InterScan サーバ、管理下の製品またはフォルダを選択します。
4. 右側の画面で、[設定] タブをクリックします。
5. [製品] リストボックスから、設定する製品を選択します。

注意： 手順 4 はフォルダの [設定] タブを使用している場合に必要です。

6. [設定] リストボックスから、製品の設定メニューを選択します。
7. [次へ] をクリックします。InterScan 製品コンソールが表示されます。

InterScan と管理下の製品に対するタスクの実行

[タスク] タブを使用すると、グループ単位または特定の InterScan サーバまたは管理下の製品に対し、有効なタスクを実行できます。InterScan サーバでは、次のタスクを実行できます。

- 複製の設定
- スпамメール判定ルールの配信
- エンジンの配信
- ライセンスプロファイルの配信
- パターンファイル / クリーンナップテンプレートの配信
- リアルタイム検索の有効化
- 検索の開始

最新ではないコンポーネントを使用している InterScan サーバには、最新の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。

InterScan サーバ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. 左側のメニューで、目的の InterScan サーバまたはフォルダを選択します。
3. 右側の画面で [タスク] タブをクリックします。
4. [タスク] リストからタスクを選択します。
5. [次へ] をクリックします。
6. [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。

InterScan と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 InterScan サーバのログにクエリを実行してログを表示できます。

InterScan サーバ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. 左側のメニューで、目的の InterScan サーバまたはフォルダを選択します。
- 3. 右側の画面で [ログ] タブをクリックします。
- 4. クライアントのログの種類を選択します。

イベントログ

- a. 次の検索項目を指定します。

検索項目	説明
重大度	表示可能な情報の重大度を表します。[重大]、[警告]、[情報]、[エラー]、[不明] のオプションがあります。必要な項目のチェックボックスをオンにします。
イベント	イベントを表します。[すべて]、[ウイルス大規模感染]、[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] のオプションがあります。
製品	フォルダを選択した場合は、そのフォルダに属する管理下の製品のリストが表示されます。すべての製品に関する情報を表示するには、[すべて] を選択します。そうでない場合は、特定の管理下の製品のログにクエリを実行します。

表 C-4. イベントログの検索項目

検索項目	説明
対象期間	すべてのログを表示するか、特定の期間内に管理下の製品によって生成されたログだけを表示するかを選択します。 特定期間内のログだけを表示する場合は、過去 24 時間、今日、過去 7 日間、過去 14 日間、過去 30 日間、または指定する期間のログを指定できます。 [指定する期間] を選択した場合は、[開始日] と [終了日] で適切な年月日を選択します。
ソートの種類	日時、コンピュータ名、製品、イベント、または重大度を基準に結果を並べ替えます。
表示順序	結果を昇順または降順に並べ替えます。

表 C-4. イベントログの検索項目

- b. [ログ表示] をクリックして、クエリを開始し、クエリ結果を表示します。

セキュリティログ

- a. [すべてのウイルス / スパイウェアログイベント]、または特定のセキュリティログの種類を選択して、[クエリ] をクリックします。
- b. 次の検索項目を指定します。

検索項目	説明
対象期間	すべてのログを表示するか、特定の期間内に管理下の製品によって生成されたログだけを表示するかを選択します。 特定期間内のログだけを表示する場合は、過去 24 時間、今日、過去 7 日間、過去 14 日間、過去 30 日間、または指定する期間のログを指定できます。 [指定する期間] を選択した場合は、[開始日] と [終了日] で適切な年月日を選択します。
ソートの種類	日時、コンピュータ名、製品、イベント、または重大度を基準に結果を並べ替えます。
表示順序	結果を昇順または降順に並べ替えます。

表 C-5. セキュリティログの検索項目

- C. [ログ表示] をクリックして、クエリを開始します。

注意： eManager 製品では、コンテンツセキュリティ違反はウイルスログではなく、セキュリティログに記録されます。

5. [クエリ結果] 画面に結果が表形式で表示されます。
6. 結果の表の [生成日時] 列には、Control Manager サーバの時刻が表示されます。

製品ディレクトリから削除された InterScan の再登録

Control Manager では、次のような場合に、InterScan サーバ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] オプションを選択した場合
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、InterScan サーバを誤って削除した場合

InterScan サーバ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エージェント側で保持されています。製品のエージェントは、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。

製品ディレクトリから削除された InterScan サーバを再登録するには

- InterScan サーバを再起動します。
- InterScan エージェントを Control Manager サーバに再登録します。

InterScan、製品ディレクトリフォルダ、またはコンピュータの検索

次の操作は、[検索] ボタンを使用して簡単に実行できます。

- InterScan サーバを個別またはグループ単位でショートカットに追加
- 製品ディレクトリ内にある特定の InterScan サーバを検索

フォルダまたは InterScan サーバを検索するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで [検索] をクリックします。
3. 右側の画面で、次の検索項目を指定します。

検索項目	説明
管理下の製品の検索基準	リストボックスから検索対象を選択します。 検索は、管理下の製品またはコミュニケータの名前、フォルダ名、またはコンピュータ名に基づいて実行できます。
キーワード	検索対象の名前を指定します。 大文字と小文字を区別して検索するには、[大文字と小文字の区別] チェックボックスをオンにします。
管理下の製品ステータス	検索するコミュニケータ、または管理下の製品の適切な接続ステータスを指定します。 [すべて]、[稼動中]、[停止中]、[異常]、[製品稼動中]、および [製品停止中] のオプションがあります。接続ステータスに関係なくすべてのオブジェクトを検索する場合は [すべて] を選択します。
製品	リストから適切な管理下の製品を選択します。 すべての製品を検索する場合は [すべて] を選択します。

表 C-6. 検索項目

4. [検索開始] をクリックして検索を開始します。
5. 検索結果が表形式で表示されます。ショートカットサブフォルダを作成し、そこで検索結果をグループ化することもできます。

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 [更新] アイコンをクリックします。

ディレクトリ管理について

Control Manager に登録すると、InterScan サーバはまず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。

管理モデルの要件に合わせて製品ディレクトリの構成をカスタマイズするには、ディレクトリ管理を使用します。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 InterScan サーバ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 InterScan サーバを慎重に構成します。フォルダと InterScan サーバ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

InterScan サーバは、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 InterScan サーバ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。

グループ化の種類	長所	短所
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

表 C-7. 管理下の製品のグループ化の比較

ディレクトリ管理のオプションの使用

ディレクトリ管理には、[新規フォルダ]、[削除]、[名前の変更]、[元に戻す]、[やり直し]、[切り取り]、および [貼り付け]、[リセット] の 8 つのオプションが用意されています。

これら 7 つのオプションを使用して、Control Manager システム内の InterScan サーバを処理して構成します。

ディレクトリ管理でオプションを使用して変更を適用するには

- フォルダまたは InterScan サーバを右クリックすると、ポップアップメニューが開き、実行可能な処理のリストが表示されます。
- フォルダに属する InterScan サーバを表示するには、[+] またはそのフォルダをクリックします。
- フォルダの名前を変更する場合は、ポップアップメニューから [名前の変更] をクリックして名前を入力し、<Enter> キーを押すか、任意の場所をクリックします。
- 変更を適用して、ディレクトリ管理の構成を更新するには、[保存] をクリックします。
- まだ保存していない変更を破棄するには、[リセット] をクリックします。

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、InterScan サーバ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. 製品ディレクトリにアクセスします。
2. 左側のメニューで [ディレクトリ管理] を選択します。

フォルダの作成

Control Manager システムの管理モデルに応じて、InterScan サーバ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. ディレクトリ管理にアクセスします。
2. 右側の画面で、新規フォルダを作成する場所を右クリックします。はじめてサブフォルダを作成する場合は、root フォルダを右クリックします。ポップアップメニューが開きます。
3. ポップアップメニューから [新規フォルダ] を選択します。メインフォルダの下に新規サブフォルダが作成されます。
4. 新規フォルダの名前を入力するか、初期設定の名前を使用して、<Enter> キーを押します。
5. [保存] をクリックします。

フォルダまたは InterScan の名前変更

フォルダまたは InterScan サーバの名前を変更するには

1. ディレクトリ管理にアクセスします。

-
2. 右側の画面で、名前を変更するフォルダまたは InterScan サーバを右クリックし、ポップアップメニューから [名前の変更] をクリックします。フォルダまたは InterScan サーバの名前が編集可能になります。
 3. 新規フォルダの名前を入力するか、初期設定の名前を使用して、<Enter> キーを押します。
 4. [保存] をクリックします。

注意： InterScan サーバ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。製品自体に影響はありません。

フォルダまたは InterScan の移動

フォルダまたは InterScan サーバを別の場所に移動するには

1. ディレクトリ管理にアクセスします。
2. 右側の画面で、移動するフォルダまたは InterScan サーバを選択します。
3. 次のいずれかを実行します。
 - フォルダまたは InterScan サーバを、移動先にドラッグアンドドロップします。
 - フォルダまたは InterScan サーバを切り取り、移動先に貼り付けます。
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。InterScan サーバを誤って削除し、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

1. ディレクトリ管理にアクセスします。

2. 右側の画面で、削除するフォルダを右クリックし、ポップアップメニューから [削除] をクリックします。
3. [保存] をクリックします。

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。

ショートカットについて

ショートカットには、InterScan サーバへのショートカットが作成されます。ショートカットを使用して、製品ディレクトリの構成を変更せずに特定の製品に対する作業を集中的に実行できます。ショートカット機能の最も効果的な利用法として、期限切れのコンポーネントを持つ製品をショートカットに追加し、最新コンポーネントを一括して配信する例があります。

ショートカット機能を使用する際は、次の点に注意してください。

- InterScan サーバへのショートカットはすべて、管理コンソールからログオフしたときに Control Manager によって削除されます。
- ショートカットに追加できる InterScan サーバは、製品ディレクトリに表示されている InterScan サーバだけです。アクセスが許可されていない InterScan サーバのショートカットを作成することはできません。

ショートカットとは

ショートカット内の InterScan サーバは、製品ディレクトリ内の InterScan サーバと同じように扱うことができます。ショートカット内のフォルダや InterScan サーバを選択すると、ディレクトリと同様、右側の画面に [ステータス]、[設定]、[タスク]、[ログ] のタブが表示されます。ただし、InterScan サーバに対して実行できる処理は、ユーザアカウントのアクセス権に基づいて、Control Manager によって決められます。

ショートカットは次の目的に使用できます。

- フォルダレベルのアクセス権を使用して InterScan サーバのグループにコマンドを発行します。

-
- 特定の InterScan サーバを選択し、アクセス可能な製品ディレクトリのタブを使用して処理を実行します。

ショートカットへのアクセス

ショートカットを使用すると、InterScan サーバへのアクセスを容易にすることができます。

ショートカットにアクセスするには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで [ショートカット] をクリックします。

ショートカットへの InterScan の追加

ショートカットに InterScan サーバを追加するには、次の 3 つの方法があります。

- 検索結果から追加
- 製品ディレクトリから追加
- [ステータス概要] 画面に基づいて、期限切れのコンポーネントを持つ InterScan サーバを追加

3 つ目の方法を使用して、複数の InterScan サーバを一度にショートカットに追加することをお勧めします。[ステータス概要] 画面には、期限切れのコンポーネントを使用している InterScan サーバに関する情報が表示されます。これにより、異なるフォルダグループに属する複数の InterScan サーバに対し、まとめて簡単にウイルスパターンと検索エンジンのアップデートを実行できるようになります。

注意： ショートカットに InterScan サーバを追加する操作では、期限切れのコンポーネントを持つ InterScan サーバが 1 か所に集められるというだけで、自動配信が開始されるわけではありません。

検索結果から追加するには

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 [検索] をクリックします。
3. 右側の画面で、InterScan サーバまたはフォルダを検索します。
4. InterScan サーバのショートカットを格納するショートカットサブフォルダの名前を [検索結果用ショートカットサブフォルダ] フィールドに指定します。

注意：手順 4 は任意です。ショートカットフォルダの下にさらにフォルダ階層を作成するには、[検索結果用ショートカットサブフォルダ] フィールドに「¥{ フォルダ名レベル 1}¥{ サブフォルダ名レベル 2}」の形式で名前を指定します。たとえば、「Pattern(1)¥VB_Corp」と指定した場合、ショートカットフォルダの構造は次のようになります。



-
5. [追加] をクリックします。検索結果から InterScan サーバがショートカットに追加されます。

製品ディレクトリから追加するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで、ショートカットに追加する InterScan サーバを選択します。
3. キーボードの <+> (プラス) キーを押します。

[ステータス概要] 画面に基づいて、期限切れのコンポーネントを持つ InterScan サーバを追加するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで、目的の製品ディレクトリフォルダを選択します。
3. 右側の画面で、[製品ステータス] タブをクリックします。
4. [コンポーネントのステータス] 表で、期限切れのコンポーネントを使用している InterScan サーバを示す数値のリンクを 1 つクリックします。クリックしたリンクに応じて [パターンファイルのステータス (期限切れ)]、[検索エンジンのステータス (期限切れ)]、または [スパムメール判定ルール of ステータス (期限切れ)] 画面が表示され、その画面に、コンピュータ名、製品名、製品バージョン、および期限切れコンポーネントバージョンが表示されます。
5. ステータスの画面で [ショートカットに追加] をクリックします。追加元の画面名と同じ名前前のフォルダを使用して、InterScan サーバがショートカットに配置されます。たとえば、[検索エンジンのステータス (期限切れ)] 画面から追加された InterScan サーバは、[検索エンジンのステータス (期限切れ)] フォルダに配置されます。

注意： [ショートカットに追加] をクリックしたときに追加されるのは、ステータスの画面に表示されている InterScan サーバだけです。InterScan サーバのリストが複数ページにわたる場合は、すべてのページで [ショートカットに追加] をクリックして、期限切れコンポーネントを持つ InterScan サーバをすべて追加してください。

6. [戻る] をクリックして、[ステータス概要] 画面に戻り、次の期限切れコンポーネントに進みます。期限切れのコンポーネントを使用している InterScan サーバすべてがショートカットに追加されるまで、この操作を繰り返します。

ショートカットからの InterScan の削除

ショートカットから InterScan サーバを削除するには

1. 製品ディレクトリにアクセスします。

2. 左側のメニューで [ショートカット] をクリックして展開します。
3. [ショートカットリスト] 内の有効な InterScan サーバから、削除するフォルダまたは InterScan サーバのショートカットを選択します。
4. キーボードの <-> (マイナス) キーを押します。

注意：管理コンソールからログオフすると、Control Manager によってショートカットにある InterScan サーバのショートカットが削除されます。

ショートカットから InterScan サーバを削除しても、ウイルス対策 / コンテンツセキュリティ製品のサービスが停止したり、Control Manager エージェントが Control Manager サーバからアンインストールされたりすることはありません。

Control Manager からの新しいコンポーネントのダウンロードと配信

アップデート管理は、Control Manager システム上で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をアップデートするための機能をまとめたものです。トレンドマイクロでは、最新のウイルスおよび不正コード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、ダメージクリーンアップテンプレート、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、ダメージクリーンアップテンプレート、脆弱性診断パターンファイル、ネットワーク大規模感染監視ルール、パターンファイルリリース履歴、ネットワークウイルスパターンファイル

-
- **スパムメール判定ルール** - スパムメール判定およびコンテンツフィルタ用のインポートファイルおよびルールファイル
 - **エンジン** - ウイルス検索エンジン、ダメージクリーンナップエンジン、脆弱性診断エンジン、およびネットワークウイルス検索エンジン
 - **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。詳細については、Control Manager オンラインヘルプの「製品のアクティベーションについて」を参照してください。

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。

アップデート管理について

アップデート管理は、Control Manager のネットワーク上の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をアップデートするための機能です。

Control Manager のネットワークのアップデート作業は、次の 2 つの手順に分かれます。

- コンポーネントのダウンロード - 手動または予約によって実行できます。
- コンポーネントの配信 - 手動または予約によって実行します。

手動ダウンロードについて

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、最新コンポーネントを手動でダウンロードします。

コンポーネントの手動ダウンロード

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. メインメニューで [運用管理] をクリックします。
2. 左側のメニューの [アップデート管理] 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. 右側の画面で、[新規配信計画の追加] をクリックします。

新規配信計画の追加

手動ダウンロードまたは予約ダウンロードのいずれかで自動配信が選択されている場合、配信は次のスケジュールに従って実行されます。

配信計画名:

スケジュール:

No.	配信時刻	編集	削除
新規スケジュールの追加			

注意: 新規配信計画およびスケジュールを保存するには、[保存] をクリックしてください。

4. [新規配信計画の追加] 画面で、[配信計画名] フィールドに配信計画名を入力します。
5. [新規スケジュールの追加] 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。

新規スケジュールの追加

配信計画名: Schedule 1

配信時刻: ☒ 保留時間: 0 時間 5 分
☐ 開始時刻: 00 : 00 (hh:mm)

フォルダの選択:
 設定を適用するフォルダは、スケジュールごとに選択してください。複数のフォルダに対しては、フォルダ数に応じて複数のスケジュールを作成してください。表示されるフォルダは、設定するユーザの持つ権限によって異なります。

製品ディレクトリ
 root
 新規エンティティ

OK キャンセル

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]→[システム設定] の順に選択します。[システム設定] 画面が表示されます。

システム設定

Control Manager では、さまざまな通信機能を使用できます。あらかじめ必要な情報を入力してください。

保存

アップデート設定

ローカル環境のWindows認証

ユーザー名:

パスワード:

リモート環境のUNG認証

ユーザー名:

パスワード:

ダウンロードに使用するプロキシ設定

☐ インターネットからアップデートファイルをダウンロードするのにプロキシサーバを使用する

ホスト名: ポート番号:

例: proxy.company.comまたは10.21.254.30

プロトコル: ☒ HTTP ☐ Socks

認証情報

ログイン名:

パスワード:

TVCSエージェントとの接続に使用するプロキシ設定

☐ TVCSエージェントとの接続にプロキシサーバを使用する

ホスト名: ポート番号:

例: proxy.company.comまたは10.21.254.30

プロトコル: ☒ HTTP ☐ Socks

認証情報

ログイン名:

パスワード:

通知設定

SMTPサーバ

ホスト名: ポート番号:

例: proxy.company.comまたは10.21.254.30

送信者アドレス:

注意: SMTPサーバによって、送信者アドレスがないメールは配信されない場合があります。

ポケットベルのCOMポート

ポケットベル通知に ☐ を使用する

SNMPトラップ通知

コミュニティ名:

サーバIPアドレス:

アプリケーション

☐ 指定したユーザがアプリケーションを起動

ユーザー名:

パスワード:

MSN Messenger通知

MSNアカウント:

パスワード:

☐ MSNサーバとの接続にプロキシサーバを使用する

ホスト名: ポート番号:

例: proxy.company.comまたは10.21.254.30

プロトコル: ☒ Socks 4 ☐ Socks 5

認証情報

ログイン名:

パスワード:

保存

2. [ダウンロードに使用するプロキシ設定] で、[インターネットからアップデートファイルをダウンロードするのにプロキシサーバを使用する] チェックボックスをオンにします。
3. [ホスト名] フィールドに、サーバのホスト名または IP アドレスを入力します。
4. [ポート番号] フィールドに、ポート番号を入力します。

5. プロトコルを選択します。
 - HTTPS
 - SOCKS
6. 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。
7. [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. [運用管理]→[アップデート管理]→[手動ダウンロード] の順に選択します。[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 ?

手動ダウンロードを実行して、アップデートファイルを取得します。

コンポーネント	
☒	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

ダウンロード設定

ダウンロード元:

☒ トrendマイクロのアップデートサーバ
☐ その他のアップデートサーバ

例: http://DownloadServer.Antivirus.com/AU または
 c:\ActiveUpdate\ または %Updatesource

再試行間隔: ☐ ダウンロードに失敗した場合、再試行を 回まで、 分ごとに繰り返す

プロキシ: [編集](#)

自動配信設定

自動配信を設定するには、配信計画を選択してください。

スケジュール:
☐ 配信しない
☐ ただちに配信
☒ 配信計画に従う

☒ 新しいコンポーネントが利用可能になったとき

配信計画:

2. [コンポーネント] 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. 次のダウンロードするコンポーネントを選択します。

パターンファイル/テンプレート

- スпамメール判定ルール

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、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、[システム設定] 画面でプロキシを設定します。

手順 5 - 自動配信の設定

1. [スケジュール] 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
 - **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** : 管理下の製品に必要なコンポーネントが Control Manager で更新された場合のみ、設定されている計画に基づいて配信されます。

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] 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. [ダウンロード開始] 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。

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。

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. メインメニューで [運用管理] をクリックします。
2. 左側のメニューの [アップデート管理] で、[予約ダウンロードの除外設定] をクリックします。
3. 次のいずれかを実行します。
 - **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。
 - **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。
4. [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. メインメニューで [運用管理] をクリックします。
2. 左側のメニューの [アップデート管理] 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. 右側の画面で、[新規配信計画の追加] をクリックします。

新規配信計画の追加

手動ダウンロードまたは予約ダウンロードのいずれかで自動配信が選択されている場合、配信は次のスケジュールに従って実行されます。

配信計画名:

スケジュール:

No.	配信時刻	編集	削除
新規スケジュールの追加			

注意: 新規配信計画およびスケジュールを保存するには、[保存] をクリックしてください。

4. [新規配信計画の追加] 画面で、[配信計画名] フィールドに配信計画名を入力します。
5. [新規スケジュールの追加] 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]→[システム設定] の順に選択します。[システム設定] 画面が表示されます。

システム設定

Control Managerで、さまざまな通信機能を使用できます。あらかじめ必要な情報を入力してください。

保存

アップデート設定

ローカル環境のWindows認証

ユーザ名:

パスワード:

リモート環境のUNC認証

ユーザ名:

パスワード:

ダウンロードに使用するプロキシ設定

- ☐ インターネットからアップデートファイルをダウンロードするのにプロキシサーバを使用する

ホスト名: ポート番号:

例: proxy.company.comまたは10.21.254.30

プロトコル: ☒ HTTP ☐ Socks

認証情報

ログオン名:

パスワード:

TVCSエージェントとの接続に使用するプロキシ設定

- ☐ TVCSエージェントとの接続にプロキシサーバを使用する

ホスト名: ポート番号:

例: proxy.company.comまたは10.21.254.30

プロトコル: ☒ HTTP ☐ Socks

認証情報

ログオン名:

パスワード:

2. [ダウンロードに使用するプロキシ設定] で、[インターネットからアップデートファイルをダウンロードするのにプロキシサーバを使用する] チェックボックスをオンにします。
3. [ホスト名] フィールドに、サーバのホスト名または IP アドレスを入力します。
4. [ポート番号] フィールドに、ポート番号を入力します。
5. プロトコルを選択します。
 - HTTPS
 - SOCKS
6. 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。
7. [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. [運用管理]→[アップデート管理]→[予約ダウンロード] の順に選択します。[予約ダウンロード] 画面が表示されます。

予約ダウンロード



予約設定に従って、コンポーネントを自動的にダウンロードすることができます。

コンポーネント	実行間隔	有効	ダウンロード元
☒ パターンファイル/テンプレート	1日		トレンドマイクロのアップデートサーバ
☒ スпамメール判定ルール	1日		トレンドマイクロのアップデートサーバ
☒ エンジン	1日		トレンドマイクロのアップデートサーバ
☐ 製品プログラム	1週間		トレンドマイクロのアップデートサーバ

2. [コンポーネント] 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. 次のダウンロードするコンポーネントを選択します。

パターンファイル/テンプレート

- スпам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。

パターンファイル/テンプレート

設定したスケジュールに従って自動的にコンポーネントをダウンロードすることができます。

☒ 予約ダウンロードを有効にする

スケジュール(実行間隔)

ダウンロード間隔: ☐ 5分
☐ 毎時
☒ 毎日
☐ 毎週 ☐ 日曜日
 開始時刻: 00 : 26 (hh:mm)

ダウンロード設定

ダウンロード元: ☒ トレンドマイクロのアップデートサーバ
☐ その他のアップデートサーバ

 例: http://DownloadServer.Antivirus.com/AU または
 c:\ActiveUpdate¥ または ¥¥updatesource
 再試行間隔: ☐ ダウンロードに失敗した場合、再試行を 2 回まで、2 分ごとに繰り返す
 プロキシ: (編集)

自動配信設定

自動配信を設定するには、配信計画を選択してください。

スケジュール: ☐ 配信しない
☐ ただちに配信
☒ 配信計画に従う
☒ 新しいコンポーネントが利用可能になったとき
 配信計画: すべての製品にただちに配信(通常時)

保存 キャンセル リセット

手順 4 - ダウンロードスケジュールの設定

1. [予約ダウンロードを有効にする] 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。[ダウンロード間隔] 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] にて、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、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、[システム設定] 画面でプロキシを設定します。

手順 6 - 自動配信の設定

1. [スケジュール] 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
- **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**：管理下の製品に必要なコンポーネントが Control Manager で更新された場合のみ、設定されている計画に基づいて配信されます。

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] 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。

レポートの使用

Control Manager のレポートは、Control Manager システムで発生したウイルスイベント、スパイウェアイベント、およびコンテンツセキュリティイベントの件数をオンライン集計したものです。Control Manager のエンタープライズ版に、レポート機能が搭載されています。

Control Manager では、次の種類に従ってレポートが分類されます。

- ローカルレポート
- 広域レポート

注意： 上位サーバの管理コンソールからは、[広域レポート] オプションのみを設定できます。

ローカルレポート

ローカルレポートは、上位サーバの管理下の製品に関するレポートです。ローカルレポートには、下位サーバによって作成されたレポートは含まれません。上位サーバに登録されている下位サーバの管理下の製品に関するレポートを表示するときは、[広域レポート] オプションを使用します。

[ローカルレポート] 画面を使用して、利用可能な 1 回限りのローカルレポートおよび予約ローカルレポートを表示できます。

[ローカルレポート] にアクセスするには

1. 上部のメニューで [レポート] を選択します。
2. 左側のメニューで [レポート]→[ローカルレポート] の順に選択します。

注意： 複数のレポートが表示される場合には、[レポートプロファイル] の名前または [前回の作成日時] の日付に基づいてレポートを並べ替えます。

広域レポート

広域レポートは、上位サーバと下位サーバの管理下の製品に関するレポートです。

[広域レポート] 画面を使用して、利用可能な 1 回限りの広域レポートおよび予約広域レポートを表示できます。

[広域レポート] にアクセスするには

1. 上部のメニューで [レポート] を選択します。
2. 左側のメニューで [レポート]→[広域レポート] の順に選択します。
3. 複数のレポートが表示される場合には、[レポートプロファイル] または [作成日時] の日付に基づいてレポートを並べ替えます。

注意： 広域レポートを表示できるのは、上位サーバだけです。また、レポート機能を使用できるのは、エンタープライズ版の Control Manager のみです。

複数のレポートが表示される場合には、[レポートプロファイル] の名前または [前回の作成日時] の日付に基づいてレポートを並べ替えます。

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。特に、レポートテンプレートではレポートに表示される次のセクションが定義されます。

- ヘッダ
- レポート本文
- フッタ

本バージョンの Control Manager では、Control Manager 3.0 Service Pack 3 以降利用可能な 77 個のレポートテンプレートに、新たに 3 つのレポートテンプレートが追加されました。Control Manager 3.0 Service Pack 3 で追加されたレポートは、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、および管理下の全製品の 5 つのカテゴリに分類されます。本バージョンで追加されたレポートは、ネットワーク製品という 6 番目のカテゴリに属します。このカテゴリでは、Network VirusWall Enforcer 2500 に関連するレポートを作成できます。

注意： 本バージョンの Control Manager では、スパイウェアはウイルス / 不正プログラム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。

レポートを生成するには、上部のメニューで [レポート] をクリックし、左側のメニューで [ローカルレポート] の下の [レポートプロファイルの作成]、または [広域レポート] の下の [広域レポートの作成] をクリックします。右側の画面に表示される [コンテンツ] タブで、[レポート名]、[レポートタイトル] (任意)、[説明] (任意) を入力できます。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、[レポートのカテゴリ] リストを使用します。チェックボックスをオンにすると、出力されるレポートファイルに、該当するレポートを含めることができます。

本バージョンの Control Manager には、このほかに次のような 18 種類のテンプレートが用意されています。これらのテンプレートは、C:\Program Files\Trend Micro\Control Manager\Reports に、Crystal Report 9 のファイル (*.rpt) として保存されています (インストール先に応じて異なる場合があります)。これらのテンプレートをローカルレポートおよび広域レポートに適用することができます。

レポートプロファイルについて

プロファイルによって、レポートのコンテンツ (テンプレートと形式)、対象、実行間隔、および受信者がレイアウトされます。次のファイル形式でレポートを表示することができます。

- **RTF:** リッチテキスト形式。*.RTF レポートを表示するときは、Microsoft Word などのワードプロセッサを使用します。
- **PDF:** Portable Document Format。*.PDF レポートを表示するときは、Adobe Reader を使用します。
- **ActiveX:** ActiveX ドキュメント。ActiveX 形式のレポートを表示するときは、Web ブラウザを使用します。

注意: Control Manager では、ActiveX 形式のレポートをメールの添付ファイルとして送信することはできません。

- **RPT:** Crystal Reports 形式。*.RPT レポートを表示するときは、Crystal Smart Viewer を使用します。

レポートサーバでレポートの作成が完了すると、作成されたレポートのファイル形式に対応する初期設定のビューアが起動します。Crystal Reports 形式のレポートの場合、Crystal Smart Viewer をインストールしておく必要があります。

レポートプロファイルの作成

レポートプロファイルの作成プロセスは、5 段階の手順で構成されます。ローカルレポートと広域レポートでは、作成プロセスが非常に似ています。レポートプロファイルの作成プロセスは、次のとおりです。

手順 1: ローカルレポートと広域レポートのどちらを作成するか選択します。

手順 2: [コンテンツ] タブの設定を指定します。

手順 3: [対象] タブの設定を指定します。

手順 4: [実行間隔] タブの設定を指定します。

手順 5: [受信者] タブの設定を指定します。

ローカルまたは広域レポートプロファイルを作成するには

手順 1: ローカルレポートと広域レポートのどちらを作成するか選択します。

1. 上部のメニューで [レポート] を選択します。
2. 次のいずれかの処理を実行します。
 - ローカルレポートプロファイルを作成する場合は、[レポート]→[ローカルレポート] の順に選択します。
 - 広域レポートプロファイルを作成する場合は、[レポート]→[広域レポート] の順に選択します。
3. 左側のメニューで [ローカルレポート] または [広域レポート]→[レポートプロファイルの作成] の順に選択します。

レポートプロファイルの作成



1. コンテンツ 2. 対象 3. 実行間隔 4. 受信者 5. 概要

テンプレートを選択して、新規レポートを作成します。

レポート名

レポートタイトル (オプション)

説明 (オプション)

Control Manager レポート レポートのカテゴリ: 管理下の全製品

スパイウェア検出レポート:	推移レポート:
☐ スパイウェア検出	☐ スパイウェア検出数 日ごと
☐ スパイウェア検出数 上位 10	☐ ウイルス検出数 日ごと
☐ スパイウェア検出一覧	☐ ダメージクリーンナップ 日ごと
ウイルス検出レポート:	☐ スпамメール検出数 日ごと
☐ ウイルス検出	脆弱性レポート:
☐ ウイルス検出数 上位 10	☐ リスクレベル別 脆弱なコンピュータの割合
☐ ウイルス検出一覧	☐ リスクレベル別 脆弱性の割合
	☐ ウイルス/スパイウェア感染駆除 上位 10
	☐ 危険性の高い脆弱性 上位 10
	☐ リスクレベル別 脆弱性

手順 2: [コンテンツ] タブの設定を指定します。

1. 右側の画面の [コンテンツ] タブで、[レポート名] フィールドにレポートの名前を入力します。この名前が、[ローカルレポート] 画面、[広域レポート] 画面のレポートプロファイルに表示されます。
2. [レポートタイトル] フィールドにレポートのタイトルを入力します (任意)。
3. [説明] フィールドにレポートプロファイルの説明を入力します (任意)。
4. [レポートテンプレート] リストボックスから [ネットワーク製品] を選択します。
5. レポートの出力形式を選択します。
6. [次へ>] をクリックして、[対象] タブに進みます。

レポートプロファイルの作成

1. コンテンツ **2. 対象** 3. 実行間隔 4. 受信者 5. 概要

レポート対象とする製品または製品グループを指定します。

複数の製品またはディレクトリフォルダを選択することができます。

製品ディレクトリ

- ☒ root
- ☒ 新規エンティティ

<戻る 次へ> キャンセル

手順 3: [対象] タブの設定を指定します。

1. 右側の画面の [対象] タブで、ローカルまたは広域レポートプロファイルの対象を選択します。
 - InterScan サーバまたはフォルダを選択します。プロファイルには、選択した InterScan サーバまたはフォルダに関する情報だけが含まれます。
 - 下位サーバを選択します。プロファイルには、選択した下位サーバに関する情報だけが含まれます。プロファイルにすべての下位サーバの管理下の製品を含めるときは、上位サーバを選択してください。
2. レポートの対象とするコンピュータを選択します。
 - **すべてのクライアント** : 選択した InterScan サーバの保護対象のすべてのクライアント
 - **IP 範囲** : レポートの対象とするクライアントの IP 範囲を選択します。
 - **セグメント** : レポートの対象とするクライアントの IP 範囲とセグメントを選択します。
3. [次へ>] をクリックして、[実行間隔] タブに進みます。

レポートプロファイルの作成

1. コンテンツ

2. 対象

3. 実行間隔

4. 受信者

5. 概要

レポート作成のスケジュールを設定します。

☒ 1回限り

レポートの範囲:
開始日: 2006 年 6 月 2 日
終了日: 2006 年 6 月 2 日

☐ 毎日

予約開始:
☒ ただちに開始
☐ 開始日時
2006 年 6 月 2 日
10 : 42 (hh:mm)

☐ 毎週
日曜日

☐ 毎月
1日

☐ カレンダー日を使用する

☒ 保存するレポートの数: 10

<戻る

次へ>

キャンセル

手順 4: [実行間隔] タブの設定を指定します。

1. 右側の画面の [実行間隔] タブで、このレポートを作成する間隔を指定します。次のオプションから選択できます。
 - **1 回限り**：開始日と終了日で指定した情報が含まれます。
 - **毎日**：作成時 (前日の午前 12 時) から現在の時刻までの情報が含まれます。
 - **毎週または隔週**：7 日間または 14 日間の情報が含まれます。レポートサーバがレポートの作成を開始する曜日を選択します。
 - **毎月**：30 日間の情報が含まれます。レポートサーバがレポートの作成を開始する日 (1 日、15 日、または月末日) を選択します。
 - **カレンダー日を使用する**：このチェックボックスをオンにすると、開始時刻は初日の 00:00:00 で、終了時刻は作成日の 00:00:00 になります。
このチェックボックスをオフにすると、開始時刻は初日における作成時刻と同じ時刻で、終了時刻は作成実行日の作成時刻になります。
2. [予約開始] で、レポートサーバがこのレポートの情報収集を開始する日時を指定します。次のいずれかを選択します。
 - **ただちに開始**：レポートプロファイルを保存後、ただちに情報が収集されます。
 - **開始日時**：指定した日時に情報収集が実行されます。
3. 予約レポートの場合は、[保存するレポートの数] をオンにして、サーバ上に保持するレポートの数を指定します。

注意： Control Manager では、予約レポートプロファイルが自動的に有効になります。レポートの作成を一時的に無効にするには、[予約レポート] または [予約広域レポート] 画面に移動し、予約レポートプロファイルの隣にあるチェックボックスをオフにします。

4. [次へ>] をクリックして、[受信者] タブに進みます。

レポートプロフィールの作成

1. コンテンツ 2. 対象 3. 実行間隔 4. 受信者 5. 概要

このレポートの生成時に送信するメール通知の受信者:

ユーザおよびグループ		受信者リスト
--- グループリスト ---	>>	--- グループリスト ---
Unexpected_Event		
Update_Event	<<	
Virus_Event		
--- ユーザリスト ---		--- ユーザリスト ---
root		

☒ レポートを添付ファイルとして送信する

< 戻る 次へ> キャンセル

手順 5: [受信者] タブの設定を指定します。

1. 右側の画面の [受信者] タブで、Control Manager のユーザおよびグループから受信者を選択します。
 -  を使用して、受信者を [ユーザおよびグループ] リストから [受信者] リストに追加します。
 -  を使用して、受信者を [受信者] リストから削除します。
2. レポートを添付ファイルとして送信する場合は、[レポートを添付ファイルとして送信する] をクリックします。添付ファイルの送信を指定しない場合、受信者は、作成されたレポートについてのメール通知のみを受信します。
3. [次へ>] をクリックして、[概要] タブに進みます。

レポートプロファイルの作成

1. コンテンツ	2. 対象	3. 実行間隔	4. 受信者	5. 概要
プロフィール作成日時: 2006/06/02 10:43:29 作成者: root コンテンツ レポート名: test1 レポートタイトル: Spyware report 説明: 出力形式: RTF レポートテンプレート: 1. スパイウェア検出 一覧レポート (管理下の全製品) 2. スパイウェア検出 上位レポート (管理下の全製品) 3. スパイウェア検出レポート (管理下の全製品)				
対象 - 製品ディレクトリ - root ☒ - 新規エンティティ ☒				

4. 右側の画面の [概要] タブで、プロフィール設定を確認し、[実行] をクリックしてプロフィールを保存します。

レポートプロフィールの設定の確認

プロフィールの設定を確認するには、[プロフィールの概要] 画面を使用します。

[プロフィールの概要] 画面にアクセスしてレポートプロフィールを確認するには

- [ローカルレポート] 画面または [広域レポート] 画面にアクセスします。
右側の画面の [プロフィール] 列で、[プロフィール表示] をクリックします。
- [予約レポート] 画面または [予約広域レポート] 画面にアクセスします。
右側の画面の [プロフィール] 列で、[プロフィール表示] をクリックします。

予約レポートプロファイルの有効化

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、データベースまたはエージェントの移行中) は、[予約レポート] 画面または [予約広域レポート] 画面を使用して再度有効にすることができます。

予約レポートプロファイルを有効にするには

1. [予約レポート] 画面または [予約広域レポート] 画面にアクセスします。
2. 右側の画面の [レポートプロファイル] 列で、プロファイルのチェックボックスをオンにします。

すべてのプロファイルを選択または選択解除するには、[レポートプロファイル] の隣にあるチェックボックスをオンまたはオフにします。
3. [有効] をクリックします。

注意： 実行間隔が「1 回限り」のレポートは 1 度しか生成されないため、これらのレポートプロファイルを有効化、無効化、および編集するオプションは使用できません。

オンデマンド予約レポートの作成

レポートサーバでは、ユーザによって指定された日時に基づいて予約レポートを作成します。予約した作成日時よりも以前にレポートを出力したい場合は、[生成開始] をクリックして、オンデマンドでレポートを作成できます。

オンデマンド予約レポートを作成するには

1. 上部のメニューで [レポート] を選択します。

2. 次のいずれかを実行します。
 - ローカルレポートプロファイルを作成するには、[レポート] の左側のメニューの [ローカルレポート] をクリックします。
 - 広域レポートプロファイルを作成するには、[レポート] の左側のメニューの [広域レポート] をクリックします。
3. 右側の画面の [レポート] 列で、対応する [表示] リンクをクリックします。
4. [開始日] に年、月、日を入力してください。
5. [生成] をクリックします。

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 [レポート表示] リンクが使用できるようになります。

作成されたレポートの表示

レポートをメールの添付ファイルとして送信して表示する以外に、[ローカルレポート] または [広域レポート] 画面を使用して、ローカルレポートまたは広域レポートを表示することもできます。

レポートを表示するには

1. 上部のメニューで [レポート] を選択します。
2. 次のいずれかを実行します。
 - ローカルレポートプロファイルを作成するには、[レポート] の左側のメニューの [ローカルレポート] をクリックします。
 - 広域レポートプロファイルを作成するには、[レポート] の左側のメニューの [広域レポート] をクリックします。
3. 右側の画面の [レポート] 列で、対応する [表示] リンクをクリックします。
[レポート]:{プロファイル名} では、[作成要求の送信日時] や [生成完了日時] の順にレポートを並べ替えることができます。

-
4. [ステータス] 列で、[レポート表示] をクリックします。そのレポートのファイル形式を開くように初期設定で指定されているプログラムが起動します。

用語集

以下は、本ガイドで使用する用語のリストです。

用語	説明
DHCP (Dynamic Host Control Protocol)	コンピュータやスイッチなどのデバイスは、ネットワークに接続するために IP アドレスを持つ必要がありますが、そのアドレスは静的である必要はありません。Dynamic Host Control Protocol を使用する DHCP サーバは、デバイスがネットワークに接続されるたびに、IP アドレスを動的に割り当て、管理できます。
DNS	ドメインネームシステム — 主にインターネットで、ホスト名を IP アドレスに変換するために使用する、汎用データクエリサービス。
DNS 解決	DNS クライアントが DNS サーバにホスト名とアドレスデータを要求するとき、その処理を解決と呼びます。基本的な DNS の構成は、初期設定の解決を実行するサーバとなります。たとえば、リモートサーバが別のサーバに対して、現在のゾーンにあるコンピュータ上のデータについてのクエリを実行します。リモートサーバのクライアントソフトウェアは、リゾルバにクエリを実行します。リゾルバは、内部のデータベースファイルを基に要求に応えます。
DoS 攻撃 (Denial of Service Attack)	ネットワーク接続を不能にする、コンピュータまたはネットワークに対する攻撃。典型的な DoS 攻撃は、ネットワーク帯域幅に悪影響を及ぼしたり、メモリなどのコンピュータリソースに過度の負荷を掛けたりします。
FTP (File Transfer Protocol)	FTP とは、インターネットを介してサーバからクライアントにファイルを転送するための、標準的なプロトコルです。詳細については、Network Working Group の RFC 959 を参照してください。
HotFix と Patch	お客さまに関連する問題や、新たに発見されたセキュリティの脆弱性に対する回避策。トレンドマイクロの Web サイトからダウンロードして、InterScan サーバおよびクライアントプログラム、またはそのいずれかに展開できます。
HTML ウイルス、VBScript ウイルス、または JavaScript ウイルス	Web ページに存在するウイルスで、ブラウザを介してダウンロードされます。

用語	説明
HTTP (Hypertext Transfer Protocol)	HTML ドキュメントをやり取りするために World Wide Web で使用される、クライアントサーバ型の TCP/IP プロトコル。通常はポート 80 を使用します。
HTTPS (Hypertext Transfer Protocol Secure)	HTTP から派生した、保護されたトランザクションの処理に使用するプロトコル。
IP (インターネット プロトコル)	「インターネットプロトコルは、データグラムと呼ばれるデータのブロックを、送信元から宛先へ送信します。この場合、送信元と宛先は、固定長アドレスで識別されるホストとなります。」(RFC 791)。
LAN (Local Area Network)	地理的に制限されたデータ通信ネットワーク。これを使用することにより、同じ建物の中のコンピュータを簡単に相互接続できます。
Ping	ICMP エコーリクエストを IP アドレスに送信し、応答を待つユーティリティ。Ping ユーティリティを使用すると、特定の IP アドレスを持つコンピュータがオンライン状態であるかどうかを判断できます。
Ping of Death	ハッカーが対象のコンピュータに既定サイズを超える ICMP パケットを送信する DoS 攻撃。これにより、コンピュータのバッファオーバーフローが発生し、コンピュータがフリーズしたり再起動する可能性があります。
POP3 (Post Office Protocol 3)	POP3 は、サーバからクライアントのメールアプリケーションにメールを転送および保存するための標準的なプロトコルです。
メッセージ部分の隔離	メール本文または添付ファイルをアクセス制限付きのフォルダに移動し、Exchange 環境に対するセキュリティリスクとして削除します。メッセージ部分が、指定したテキスト / ファイルに置き換えられます。
SMTP (Simple Mail Transfer Protocol)	インターネットを介してサーバからサーバ、クライアントからサーバへメールを送信するために使用される、標準的なプロトコル。
SOCKS 4	内部ネットワークまたは LAN のクライアントと、LAN 外のコンピュータまたはサーバとの間の接続を確立するために、プロキシサーバで使用される TCP プロトコル。SOCKS 4 プロトコルでは、接続要求を行い、プロキシ回路を設定して、OSI モデルのアプリケーション層でデータをリレーします。
SSL (Secure Socket Layer)	Netscape Communications Corporation が提案したスキームで、RSA 公開鍵の暗号方式を使用して、HTTP、NNTP、FTP など、上位のプロトコルで転送されるコンテンツを暗号化し、認証します。
SSL 証明書	ポリシーサーバと ACS サーバ間にセキュリティで保護された HTTPS 通信を確立する電子証明書。

用語	説明
TCP (Transmission Control Protocol)	端末間の通信路を確保したコネクション型の信頼性のあるプロトコルで、マルチネットワークアプリケーションをサポートするプロトコルの階層に合わせて設計されています。TCP は、アドレス解決を IP データグラムに依存しています。詳細については、DARPA Internet Program の RFC 793 を参照してください。
Telnet	Telnet とは、「ネットワーク仮想端末」を作成することにより、TCP を介して端末デバイスを操作できるようにする標準的な方法です。詳細については、Network Working Group の RFC 854 を参照してください。
TrendLabs	TrendLabs は、トレンドマイクロのウイルス対策調査と製品サポートセンターのグローバルネットワークで、世界中のトレンドマイクロのお客さまに週 7 日 24 時間のサポートを提供しています。
UDP (User Datagram Protocol)	アプリケーションプログラムから別のプログラムにメッセージを送信するために IP と共に使用される、コネクションレス型の通信プロトコル。詳細については、DARPA Internet Program の RFC 768 を参照してください。
zip ファイル	WinZip などのアーカイブプログラムを使用して、1 つ以上のファイルを圧縮したアーカイブ。
アクティベーションコード	ハイフンを含む 37 文字のコードで、InterScan のアクティベートに使用します。アクティベーションコードの例は、SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 です。「レジストレーションキー」も参照してください。
アップデート	ウイルスパターンファイルやウイルス検索エンジン、さらにスパムメール判定ルールやスパムメール検索エンジンを、オンデマンドまたはバックグラウンドでアップデートできるようにする、トレンドマイクロ製品の機能です。
アドウェア	アドウェアは、スパイウェアと同様に、ネットサーフィンの好みなどのユーザデータを収集します。そのデータは、広告目的で使用される可能性があります。
ウイルス	コンピュータウイルスはプログラム、つまり実行可能なコードで、感染という独特の機能を備えています。生物学上のウイルスと同様に、コンピュータウイルスは急速に広がり、多くの場合、撲滅するのが困難です。 一部のコンピュータウイルスは、増殖することに加えて、別の共通点も持っています。それは、ウイルスのペイロード（発病機能を担う部分）を運ぶダメージルーチンです。ウイルスのペイロードは、メッセージや画像を表示するだけの場合がありますが、ファイルを破壊したり、ハードディスクを再フォーマットしたり、その他の被害を引き起こしたりする可能性もあります。ウイルスにダメージルーチンが含まれていない場合でも、ストレージ領域やメモリを消費し、コンピュータの全体的なパフォーマンスを低下させて、問題を引き起こすことがあります。

用語	説明
ウイルス検索エンジン	ホスト製品に組み込まれて、ウイルス対策検索および検出を実行するモジュール。
ウイルス作成者	ウイルスコードを記述する者。
エンドユーザメール隔離	エンドユーザメール隔離は、InterScan に特別なスパムメール管理機能を追加するツールです。インストールの際、InterScan は各エンドユーザのサーバ側のメールボックスにフォルダを追加します。スパムメッセージが届くと、システムは InterScan により事前に定義されているスパムメールフィルタルールに従って、メッセージをこのフォルダに隔離します。エンドユーザはこのスパムメールフォルダを参照して、疑わしいメールを開いたり、参照したり、削除したりすることができます。
スパイウェア / グレーウェア	ネットワーク上のコンピュータのパフォーマンスに悪影響を与えるファイルおよびプログラム。ウイルスではありません。スパイウェア、アドウェア、ダイヤラ、ジョークプログラム、ハッキングツール、リモートアクセスツール、パスワード解読アプリケーションなどが該当します。InterScan のウイルス検索エンジンでは、ウイルスと同様にグレーウェアも検索します。
ゲートウェイ	異なるネットワーク間でデータを移動できるようにするデバイス。
コンテンツフィルタ	メールについて、組織の従業員メッセージポリシーまたは IT メッセージポリシーで禁止されている脅迫メール、下品な言葉、ポルノなどのコンテンツ (語または句) を検索することです。
サポート契約	該当する料金の支払いの対価としてテクニカルサポートおよび製品アップデートを受ける権利に関して、お客さまとトレンドマイクロとの間で結ばれる契約です。 トレンドマイクロのソフトウェアライセンスには、通常、ユーザ登録完了日から 1 年間を対象としたコンポーネントアップデート、および基本的なテクニカルサポート (「保守」) が含まれています。契約期間終了後には、サポート契約を更新する必要があります。
システム領域感染型ウイルス	ウイルスの一種で、パーティションまたはディスクのブートセクタに感染します。
ジョークプログラム	コンピュータに、画面を震わせるなどの異常な動作をさせるソフトウェア。

用語	説明
スパイウェア / グレーウェア	グレーウェアの一種で、主にマーケティングのためにネットサーフィンの傾向を記録することを目的として、コンピュータにコンポーネントをインストールします。スパイウェアは、コンピュータがオンラインになったときに、その情報をスパイウェアの作成者またはその他の関係者に送信します。スパイウェアは、多くの場合、「無料ダウンロード」とされるアイテムと共にダウンロードされますが、ユーザはスパイウェアの存在を知らされず、コンピュータへインストールする許可も求められません。スパイウェアコンポーネントが収集する情報には、ユーザのキーストロークが含まれることがあります。つまり、ログイン名、パスワード、クレジットカード番号などの個人情報が盗まれやすいことを意味します。
スパムメール	製品またはサービスを売り込むために、求められていないのに送信されるメール。
スパムメール対策	フィルタメカニズムとも呼ばれ、要求していない広告、ポルノ、およびその他の「迷惑」メールの配信を識別し、回避するためのものです。
タグ	メールの件名フィールドに、「Spam:」などの識別子を入れることです。
ダイヤラー	クライアントのインターネット設定を変更して、あらかじめ設定された電話番号にモデムを通じて電話を掛けさせることが可能なソフトウェア。
テストウイルス	本物のウイルスのように動作し、ウイルス検索ソフトウェアで検出される感染しないファイル。EICAR テストスクリプトなどのテストファイルを使用して、インストールしたウイルス対策ソフトウェアで検索が正常に実行されていることを確認します。
トラフィック	インターネットとネットワークとの間の、受信および送信双方向のデータの流れ。
トレンドマイクロの推奨設定	トレンドマイクロの推奨設定はトレンドマイクロの検索技術で、実際のファイルタイプを認識する機能を使用してファイルのヘッダを調べ、不正コードが隠れている可能性があると判明したファイルタイプのみを検索することにより、パフォーマンスを最適化します。実際のファイルタイプの認識は、無害な拡張子名を装う可能性がある不正コードの識別に役立ちます。
トロイの木馬	実行可能なプログラムで、増殖はしませんが、システムに潜伏して、ハッカーが侵入するためのポートを開くなど、不正な動作を行います。
ドメイン名	ローカルホスト名とドメイン名から成る、システムの完全名。たとえば、tellsital.com などです。ドメイン名は、インターネットのすべてのホストの中で一意のインターネットアドレスを特定できることが必要です。この処理は「名前解決」と呼ばれ、DNS (Domain Name System) を使用します。

用語	説明
ハッカー	「ウイルス作成者」を参照してください。
ハッキングツール	ハッカーが、多くの場合空きポートから、コンピュータに侵入するために使用するツール。
パスワード解読アプリケーション	ハッカーがユーザ名とパスワードの解読に使用するソフトウェア。
パターンファイル	パターンファイルは、オフィシャルパターンリリース (OPR) と呼ばれ、特定済みのウイルスのパターンを集めたコンポーネントです。最新のウイルスの脅威から最適な保護を確実に受けられるように、一連の厳しいテストをパスしたことが保証されています。このパターンファイルは、最新のウイルス検索エンジンと併用した場合に最も効果を発揮します。
ファイルタイプ	ファイルに格納されているデータの種類。ほとんどの OS では、ファイル拡張子を使用してファイルタイプを特定します。ファイルタイプは、ユーザインタフェースでファイルを表す適切なアイコンと、そのファイルを表示、編集、または印刷する適切なアプリケーションを選択するために使用されます。
フィッシングサイト	ユーザをおびき寄せて、クレジットカード情報などの個人の詳細情報を提供させる Web サイト。フィッシングサイトへのリンクは、多くの場合、知名度のある企業からの正規のメッセージを装った偽のメールで送信されます。
ブロックする送信者	この送信者からのメッセージは、常に削除されます。
ホスト名	ASCII 文字から成る一意の名前で、この名前によりコンピュータがネットワーク上で認識されます。
マクロウイルス	マクロウイルスは、他の種類のウイルスとは異なり、特定の OS に固有のものではありません。メールの添付ファイル、Web でのダウンロード、ファイル転送、グループウェアを介して感染する可能性があります。
マスメーリング型の活動	大量のネットワークトラフィックを発生させることにより被害を引き起こす可能性が高い、不正プログラム。
メッセージサイズ	メッセージとそのすべての添付ファイルが占めるバイト数。
メッセージ全体の隔離	InterScan の検索機能で、分離したディレクトリ、つまり隔離ディレクトリにメールを置くこと。隔離ディレクトリに置かれたアイテムは、InterScan のデータベースに登録されます。
ライセンス	製品を使用するための法的な使用許諾。
リモートアクセスツール	ハッカーがコンピュータに対してリモートでアクセスしたり、制御したりするために使用するツール。

用語	説明
ワーム	自己完結型のプログラムまたはプログラムのセットで、多くの場合メールで、自己の機能の複製または自己の一部を他のコンピュータシステムに感染させます。ワームは、ネットワークウイルスとも呼ばれます。
ワイルドカード	InterScan では、アスタリスク (*) が任意の文字を表します。たとえば、*ber という表現で、barber、number、plumber、timberなどを示すことができます。
圧縮ファイル	1 つ以上の個別のファイルと、WinZip などの適切なプログラムで解凍できるようにするための情報を含む、単一のファイル。
外部受信	ネットワーク内にルーティングされるメール。
外部送信	ルーティングされてネットワーク外に出て行くメールまたはその他のデータ。
駆除	ファイルまたはメッセージからウイルスコードを削除します。
件名 (メッセージの件名)	メールの題名またはトピック。InterScan では、メッセージヘッダの件名を使用して、メッセージの内容を判断します。
検索	ファイル内のアイテムを順に調べて、特定の条件に合致するものを見つけること。
誤検出	スパムメールフィルタで「捕捉」され、スパムメールであると特定されたが、実際はスパムメールではないメール。
使用許諾契約書 (EULA)	使用許諾契約書つまり EULA は、ソフトウェアの販売元とソフトウェアユーザの間の法的契約書です。通常は、ユーザ側の制限の大意が述べられています。ユーザはインストールの際に「同意する」をクリックしないことにより、契約を結ぶことを拒否できます。「同意しない」をクリックすれば、ソフトウェア製品のインストールは終了します。 ある種のフリーソフトウェアのインストール時に表示される EULA で「同意する」をクリックすることによって、多くのユーザが、意識しないままスパイウェアやその他のグレーウェアがコンピュータにインストールされることに同意しています。
実行可能ファイル	そのまますぐに実行できる、機械言語で記述されたプログラムを含むバイナリファイル。
実際のファイルタイプ	ファイル名の拡張子は見せかけの場合があるので、拡張子に関係なく、ファイルのヘッダを調べてファイルの情報の種類を判断するウイルス検索技術。
初期設定	管理コンソールのインタフェースのフィールドにあらかじめ設定されている値。初期設定値は、1 つの適切な選択を表し、便宜を図るために提示されます。初期設定値をそのまま使用するか、または変更します。

用語	説明
承認する送信者	この送信者からのメッセージは、スパムメールフィルタで処理しません。
設定	InterScan の機能についてのオプションを選択することです。たとえば、ウイルスに感染したメールを隔離するか、削除するかを選択します。
通知	次の宛先のうちの 1 つまたは複数に送信されるメッセージ。 - システム管理者 - メッセージの送信者 - メッセージの受信者 - その他のメールアドレス - SNMP および Windows イベントログ 通知の目的は、メッセージからウイルスが検出されたなどのイベントの発生を伝えることです。
添付ファイル	メールに添付されている (一緒に送信されてくる) ファイル。
動的 IP アドレス (DIP)	動的 IP アドレスとは、DHCP サーバによって割り当てられる IP アドレスです。コンピュータの MAC アドレスは変わりません。しかし、動的 IP アドレスでは、IP アドレスが使用可能であるかどうかに応じて、新しい IP アドレスが DHCP サーバからコンピュータに割り当てられる場合があります。
不正な Java コード	Java で記述された、または Java に埋め込まれた、OS に依存しないウイルスコード。
望ましくないコンテンツ	メッセージや添付ファイルに記述されている、下品な言葉、性的嫌がらせ、人種差別に基づく嫌がらせ、または脅迫メールなどの、他者を不快にさせると思われる語句。
本文 (メール本文)	メールのコンテンツ。
迷惑メール	「スパムメール」を参照してください。

索引

英数字

Control Manager 187

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 218、219

基本機能 188

レポート 235

レポートの種類 235

Control Manager の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

スパムメール判定ルール 219

パターンファイル/テンプレート 218

InterScan

クイックスタートガイド 12

ドキュメント

表記規則 13

InterScan が生成するネットワークトラフィック

38

InterScan 管理コンソール

構成要素の説明 141

リモートサーバの表示 144

ローカルサーバの表示 144

InterScan コンポーネント 129

InterScan の削除

コンポーネント 110

InterScan の導入

ネットワークトラフィックへの影響 38

バックエンドサーバ 39

フロントエンドサーバ 39

Java

不正コード

定義 256

Management Communication Protocol

「MCP」を参照 189

MCP

一方向通信 193

概要 189

双方向通信 193

SSO

「シングルサインオン」を参照 193

Trend Micro InterScan for Microsoft Exchange

印刷ドキュメント 12

ドキュメント 12

対象読者 13

TrendLabs 167

URL

ウイルス検索エンジンのバージョン 25

あ

アカウント 権限、インストール時に必要 46

アクティベーションコード

アドバンス版 127

通常版 127

圧縮タイプ

サポート対象 174

アップグレード

クラスタサーバ 49

- サポートされるバージョン 48
- アップデート 129
 - アップデート前 159
 - 仕組み 27
 - 手動アップデート 132
 - ダウンロード元の設定 134
 - パターンファイルの差分アップデート 27
 - 予約アップデート 133
 - ロールバック 136
- アップデート管理 218
- アドウェア
 - 定義 176
- アドバンス版アクティベーションコード 127
- アンインストール 110
- 一方向通信 193
- 移動
 - 管理下の製品 213
 - フォルダ 213
- インストール
 - インストール前のチェックリスト 46
 - クラスタサーバ 103
 - 正常なインストールの確認 103
- インストール、InterScan
 - サービスの停止 / 再開、不要 46
 - 設定、プロキシサーバ 46
 - 登録キーの要求 46
- インストール、InterScan アクティベーションコード、入力 46
- ウイルス
 - スクリプト 171
 - 定義 170

- ファイル感染型 171
- ブート 171
- ウイルス検索エンジン
 - アップデート 25
 - アップデートを起動するイベント 25
 - 現在のバージョンを調べるための URL 25
 - テクノロジーの説明 24
- オンデマンド予約レポート 245

か

- 仮想サーバの表示 145
- 管理下の製品
 - 移動 213
 - 検索 209
 - 実行、タスク 205
 - 設定 204
 - 名前変更 212
 - 表示、ステータス 203
 - 表示、ログ 206

InterScan

- クイックスタートガイド 12
- クイックスタートガイド 12
 - 説明 12
- クラスタサーバ
 - コンポーネントのアップデート 131
- 検索
 - 管理下の製品 209
- 広域レポート 235
- コンポーネント
 - ダウンロード 218
- コンポーネントの手動ロールバック 136

コンポーネントのダウンロードと配信 218

さ

サーバ管理

サーバ設定の複製 149

最小システム要件 32

削除、InterScan 110

クラスタサーバ 122

作成

フォルダ 212

作成、オンデマンド予約レポート 245

サポート契約

製品版 127

システム要件 32

手動ダウンロード、コンポーネント 220

ジョークプログラム

定義 173

ショートカット 214

除外、フォルダ

ファイルベースのウイルス対策ソフトウェア

除外、フォルダ 158

処理 173

シングルサインオン 193

推奨システム要件 32

スパイウェア

その他のグレーウェア、定義 176

製品ディレクトリ 198

配信、コンポーネント 202

製品版 127

設定

管理下の製品 204

予約ダウンロード 228

予約ダウンロードの除外設定 227

双方向通信 193

た

体験版 127

対象読者 13

ダイヤラー、定義 176

ダウンロード、コンポーネント

手動 220

ダウンロード元 134

選択 134

ローカルサーバへのコピー 135

ダウンロード元のコピー 135

通常版アクティベーションコード 127

ディレクトリ管理 210

テクニカルサポート 164

ドキュメントの表記規則 13

トレンドマイクロの推奨処理

仕組み 29

トレンドマイクロの推奨設定

仕組み 28

トロイの木馬

定義 172

な

名前変更

管理下の製品 212

フォルダ 212

は

バージョンの比較 23

パスワード解読アプリケーション

定義 176

パターンファイル

差分アップデート 27

ハッキングツール

定義 176

バックエンドサーバ、InterScan の導入 39

表記規則 13

表示

管理下の製品のステータス 203

管理下の製品ログ 206

表示、作成されたレポート 246

フェイルオーバー、コンポーネントに対する影響 131

フォルダ

移動 213

作成 212

名前変更 212

複数のサーバ、管理、InterScan 管理コンソール 140

プロキシサーバ

設定 131

必要な InterScan 機能 131

プロファイル「レポートプロファイル」を参照

フロントエンドサーバ、InterScan の導入 39

本書の対象読者

対象読者 13

ま

マクロウイルス

説明 175

マスメーリング型ウイルス

InterScan の処理 173

定義 173

や

有効化、コンポーネントの予約ダウンロード 228

用語の説明 170

予約ダウンロード 227

設定 228

予約ダウンロードの除外設定

設定 227

予約レポート 245

ら

リアルタイムモニタ

概要 145

リモートサーバの表示方法 146

リモートアクセスツール

定義 176

リモートサーバ

リアルタイムモニタでの表示 146

レポート 235

オンデマンド予約 245

広域 235

表示、作成されたレポート 246

レポートプロファイル 238

ActiveX 238

PDF 238

RPT 238

RTF 238

コンテンツ 240

作成 238

実行間隔 242

受信者 243

対象 241

ローカル 235

レポートテンプレート 236

ローカルレポート 235

ロールバック、コンポーネント 136

ロックダウンツール、削除、インストールの前
46

わ

ワーム

定義 172

