TREND MICRO

InterScan™ for Microsoft Exchange 14.0

インストールおよびアップグレードガイド

Messaging Security

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

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

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

商標について

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

P/N: SMEM148568/190103_JP_R2 (2023/05)

プライバシーと個人データの収集に関する規定

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

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

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

重要

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

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

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

目次

はじめに

第 1 章：InterScan のインストールとアップグレードの計画

第 6 章：InterScan のアンインストール

第 7 章：テクニカルサポート

付録 A：事前設定ファイル

付録 B：用語集

索引

はじめに

InterScan for Microsoft Exchange (以下、InterScan) インストールおよびアップグレードガイドへようこそ。本書には、InterScan を導入して Exchange サーバを保護するために実行する必要があるタスクの基本情報を示します。本書は、InterScan の管理を行う、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。

ドキュメント

本製品には、次のドキュメントが付属しています。

- Readme: 基本的なインストール方法と既知の制限事項に関する説明
- オンラインヘルプ: 各種作業を実行するための詳細な手順の説明
- インストールガイド: 製品の概要、インストール計画、インストール、設定、起動方法に関する説明
- 管理者ガイド: 製品の概要、インストール計画、インストール、設定、および製品環境を管理するために必要な詳細情報の説明

最新の情報については弊社の「最新版ダウンロード」サイトをご参照ください。https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

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
- スパムメール保護
- 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)
- ネットワークトポロジ
- Microsoft Exchange Server 管理
- Microsoft Exchange Server 2019、2016、2013 サーバの役割の設定
- メッセージ形式

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 1. ドキュメントの表記規則

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

第 1 章

InterScan のインストールとアップグレードの計画

セットアッププログラムを使用して 1 台以上のサーバにローカルまたはリモートで InterScan をインストールします。

この章の内容は次のとおりです。

システム要件

最新のシステム要件については、次の Web サイトを参照してください。

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

注意

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

Exchange Server 2019 での InterScan の使用

次の表に、Exchange Server 2019 に対して InterScan を実行するためのシステム要件を示します。

表 1-1. Microsoft Exchange Server 2019 に対して InterScan を使用する場合のシステム要件

リソース	要件
プロセッサ	• Intel 64 アーキテクチャ (旧 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	InterScan 用として 4GB の RAM
ディスク空き容量	5GB のディスクの空き容量 30GB 以上のディスク空き容量 (インストール時)

リソース	要件
OS	MicrosoftWindows Server 2022 Standard または Datacenter (64 ビット) Microsoft Windows Server 2019 Standard または Datacenter (64 ビット) **注意** InterScan を Server Core にインストールする場合は、デスクトップエクスペリエンス搭載の Windows Server でインストールパッケージを実行して、InterScan のインストールをリモートで行うことをお勧めします。
メールサーバ	Microsoft Exchange Server 2019 以上
Web サーバ	• Microsoft Internet Information Services (IIS) 10.0
ブラウザ	• Microsoft Internet Explorer 7.0 以上 • Mozilla Firefox 3.0 以上
MSXML	4.0 Service Pack 2 以上
.NET framework	4.7.2

Exchange Server 2016 での InterScan の使用

次の表に、Exchange Server 2016 に対して InterScan を実行するためのシステム要件を示します。

表 1-2. Microsoft Exchange Server 2016 に対して InterScan を使用する場合のシステム要件

リソース	要件
プロセッサ	• Intel 64 アーキテクチャ (旧 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

リソース	要件
メモリ	InterScan 用として 1GB の RAM (2GB の RAM を推奨)
ディスク空き容量	5GB のディスクの空き容量
OS	• Microsoft Windows Server 2016 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2012 R2 Standard または Datacenter (64 ビット) 重要 また、Microsoft Windows Server 2012 R2 に Windows Server 2012 R2 Update (KB2919355 および KB2919442) をインストールする必要があります。 • Microsoft Windows Server 2012 Standard または Datacenter (64 ビット)
メールサーバ	Microsoft Exchange Server 2016 以上
Web サーバ	• Microsoft Internet Information Services (IIS) 10.0 • Microsoft Internet Information Services (IIS) 8.5 • Microsoft Internet Information Services (IIS) 8.0
ブラウザ	• Microsoft Internet Explorer 7.0 以上 • Mozilla Firefox 3.0 以上
MSXML	4.0 Service Pack 2 以上
.NET framework	4.5 以降

Exchange Server 2013 での InterScan の使用

次の表に、Exchange Server 2013 に対して InterScan を実行するためのシステム要件を示します。

表 1-3. Microsoft Exchange Server 2013 に対して InterScan を使用する場合のシステム要件

リソース	要件
プロセッサ	• Intel 64 アーキテクチャ (旧 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	InterScan 用として 1GB の RAM (2GB の RAM を推奨)
ディスク空き容量	5GB のディスクの空き容量
OS	• Microsoft Windows Server 2012 R2 Standard または Datacenter (64 ビット) **重要** また、Microsoft Windows Server 2012 R2 に Windows Server 2012 R2 Update (KB2919355 および KB2919442) をインストールする必要があります。 • Microsoft Windows Server 2012 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2008 R2 Standard Service Pack 1 以上 (64 ビット) • Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 以上 (64 ビット) • Microsoft Windows Server 2008 R2 Datacenter RTM Service Pack 1 以上 (64 ビット) **注意** Microsoft Windows Server 2008 R2 はサポートされません。
メールサーバ	Microsoft Exchange Server 2013 SP1 以上

リソース	要件
Web サーバ	• Microsoft Internet Information Services (IIS) 8.5 • Microsoft Internet Information Services (IIS) 8.0 • Microsoft Internet Information Services (IIS) 7.5
ブラウザ	• Microsoft Internet Explorer 7.0 以上 • Mozilla Firefox 3.0 以上
MSXML	4.0 Service Pack 2 以上
.NET framework	4.5 以降

SQL Server Express の要件

アップグレードインストールの 場合は、セットアッププログラムを実行する前に、現在の SQL Server Express のバージョンを次のようにアップグレードしてください。

- SQL Server Express 2005:SQL Server Express 2014 32 ビットにアップグレード
- SQL Server Express 2008: SQL Server Express 2014 64 ビットにアップグレード

クラスタ環境でのインストール

クラスタ環境をサポートするモデルは次のとおりです。

- Exchange Server 2019: データベース可用性グループ (DAG) モデル
- Exchange Server 2016: データベース可用性グループ (DAG) モデル
- Exchange Server 2013: データベース可用性グループ (DAG) モデル

トレンドマイクロ製品との InterScan の統合

InterScan は、必要に応じて他のトレンドマイクロ製品と統合できます。次の表は、サポートされる製品とバージョンの概要を示しています。

表 1-4. 統合可能なトレンドマイクロ製品サポート

トレンドマイクロ製品	サポートされるバージョン
Trend Micro Control Manager	• 2019
Trend Micro Smart Protection Server	• 3.0 以上 • ウイルスバスター コーポレートエディションのサーバ統合 Smart Protection Server
Deep Discovery Advisor	• 3.0 以上
Deep Discovery Analyzer	• 5.0 以上 • 6.0 以上

パイロットインストールの実行

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。

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、以下を参照してください。

- 22 ページの「手順 1 - 適切なテストサイトの作成」
- 22 ページの「手順 2 - ロールバック計画の準備」
- 23 ページの「手順 3 - パイロットインストールの実行と評価」

手順 1 - 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 Apex Central™、Trend Micro Apex One™、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トポロジ。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の Web サイトからダウンロードできます。

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

---

手順 2 - ロールバック計画の準備

セットアップ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

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。

手順

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 for Microsoft Exchange Master Service と SQL Server (SCANMAIL) Service を停止します。
2. データベースファイルをコピーします。インストールに応じて、次のいずれかのファイルのセットがあります。

- `Conf.mdf`、`Log.mdf`、`Report.mdf`
- `ScanMail.mdf`

InterScan の設定の復元

必要に応じて、次の手順を使用して InterScan の設定を復元します。

手順

1. 設定の復元先の対象サーバ上の InterScan for Microsoft Exchange Master Service と SQL Server (SCANMAIL) Service を停止します。
2. `Conf.mdf`、`Log.mdf`、`Report.mdf`、または `ScanMail.mdf` を削除します。
3. `Conf.mdf`、`Log.mdf`、`Report.mdf`、または `ScanMail.mdf` を置き換えます。
4. InterScan for Microsoft Exchange Master Service と SQL Server (SCANMAIL) Service を開始します。

注意

バックアップしていたファイルをリストアする場合は、バックアップ時に適用していた修正モジュール (Service Pack/Patch/Hotfix/Critical Patch) をあらかじめインストールしておく必要があります。

手順 3 - 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、セキュリティの適用とネットワークパフォーマンスの点から評価します。パイロットインストール中に発生した成功と問題のリストを作成します。潜在的な「落とし穴」を特定し、それに従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 セットアッププログラムでは、1 台または複数のローカルサーバ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。

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の計画

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

InterScan で CPU の負荷が増加するのは、メールを検索するときです。InterScan ではマルチスレッド検索が使用されるため、CPU の負荷が軽減されます。

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、26 ページの表 1-5：Exchange Server に対する InterScan の導入に示す点を考慮してください。

もう 1 つの戦略は、InterScan をネットワークの非武装地帯 (DMZ) にある Exchange サーバに導入する方法ですが、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。

表 1-5. Exchange Server に対する InterScan の導入

サーバの役割	考慮する点
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。 • 25 番ポートによる SMTP の中継。 • 分散管理。 • 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を果たすプライマリデプロイサーバとしては、(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と、(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の 2 つがあります。	• リアルタイムのセキュリティリスク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。 • スパムメール対策機能を有効にします。 • Web レピュテーション機能を有効にします。

サーバの役割	考慮する点
メールボックスサーバ 2013、2016、および 2019: • 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、カテゴライ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。 • 25 番ポートによる SMTP およびメッセージの中継。 • 負荷分散が可能です。 • ローカルネットワーク内のネットワークの周辺部、インターネットから遮断され場所に配置されます。 • メールボックスデータベースをホストします。 • メールをクライアントのメールボックスに配信し、インフォメーションストアに保存します。	• リアルタイムのセキュリティリスク検索を実行するように、サーバを設定します。 • エッジサーバがある場合、アップデートのダウンロード元としてエッジサーバを使用するように、このサーバを設定します。それ以外の場合は、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のアップデートサーバを設定します。 • Active Directory と統合された添付ファイルブロックルールおよびコンテンツフィルタポリシーを有効にします。 • Exchange メールボックスに対して定期的に予約検索を実行し、設定でカバーされていない想定外のソースからセキュリティリスクが侵入しないようにします。

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トレンドマイクロ Apex One™や、ネットワークの周辺を保護するトレンドマイクロ InterScan VirusWall™、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

インストールをスムーズに準備するには、事前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。このインストールプロセスは、サポートされているすべての Windows サーバのバージョンで同じです。

Microsoft Exchange サーバごとに 1 つの Trend Micro InterScan をインストールすることをお勧めします。InterScan では、1 つのセットアップ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セットアップ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。

表 1-6. 新規インストールに最低限必要な権限

EXCHANGE の役割	最低限必要な権限
Exchange Server 2013/2016/2019 (メールボックスサーバの役割)	ローカル管理者およびドメインユーザ Exchange Organization Management グループ
Exchange Server 2013/2016/2019 (エッジトランスポートサーバの役割)	ローカル管理者

アップグレード時の設定の例外

InterScan 12.5 Service Pack 1 から InterScan 14.0 にアップグレードする場合、セットアッププログラムはインストールに以前の設定を使用します。ただし、一部の設定は、InterScan 14.0 に引き継がれません。

表 1-7. 設定の例外

設定	説明
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。新しいアクティベーションコードを入力しない場合、元のアクティベーションコードが使用されます。
Web サーバ	InterScan では、常に新しい Web サーバの設定が使用されます。HTTPS サービスを使用した新しい Web サーバを使用するよう、Web サーバの設定をアップデートします。HTTP サービスを使用した前のバージョンの IIS サイトは、使用されなくなります。

Internet Information Services を含まないインストール

InterScan では、Internet Information Services (IIS) をサーバにインストールする必要はありません。InterScan 管理コンソールがサーバに必要ない場合は、IIS の要件を除外して InterScan をインストールすることができます。

手順

1. `cmd.exe` を実行します。
2. `InterScan` フォルダに移動し、コマンドプロンプトの後に次のコマンドを入力します。

   ```
   setup /skipwebconsole
   ```

3. 最初の画面が表示され、通常のインストールと同様にインストールプロセスが進みます。IIS の要件はチェックされず、このサーバには管理コンソールがインストールされません。

リモート SQL Server に対するインストール

InterScan では、サポートされるバージョンの Exchange Server での新規インストール時に、InterScan データベースをリモート SQL Server へ格納できます。これを行うには、InterScan をインストールする前にリモート SQL Server を準備してください。

注意

InterScan は、自動的にリモート SQL Server を検出することはできません。インストール時にリモート SQL Server を手動で設定します。インストール時にこの設定が行われない場合、InterScan はローカルの SQL Server Express にデータベースをインストールします。

手順

1. リモート SQL Server を準備します。
2. InterScan をインストールする SQL インスタンス内に dbcreator の役割としてアカウントを作成します。

注意

InterScan は、SQL Server アカウントと Windows アカウントの両方をサポートします。Windows アカウントを使用する場合は、次の権限が必要です。

- ローカル管理者
- Exchange の ApplicationImpersonation の役割
- Exchange Organization Management グループ

インストール時に EUQ をアクティベートするには、ユーザアカウントのドメイン管理者権限を有効にする必要があります。インストールが完了したら、アカウントのドメイン管理者権限を無効にすることができます。

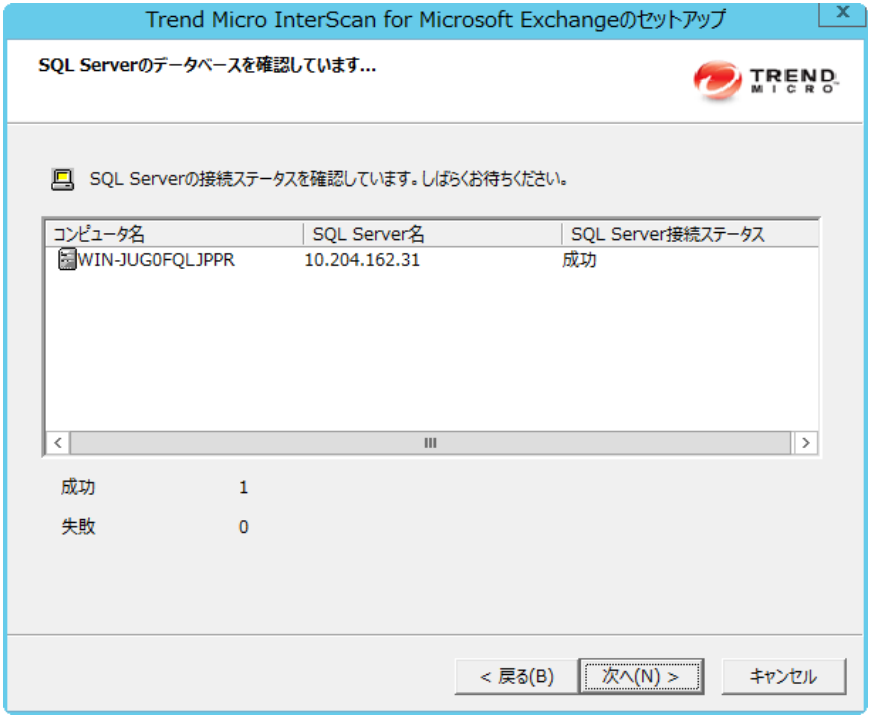
3. インストール時に、SQL Server データソースと、手順 2 で準備した SQL または Windows のアカウントを [SQL の設定] 画面に入力します。

注意

リモート SQL Server を使用して InterScan をインストールする場合、サーバへの接続が使用できないときは、データベースへの再接続が実行されます。InterScan は、Windows イベントログにエラーを記録し、サーバが使用できない間、1 時間ごとにエントリを追加します。サーバが使用できない間も InterScan はメッセージの検索を続行し、ローカルサーバにログデータを格納します。初期設定では、InterScan は 1 分ごとにデータベースサーバへの再接続を試行します。データベースへの接続が復旧すると、Windows イベントログエントリが追加され、InterScan はローカルに格納されたデータを使用してデータベースをアップデートします。

4. [次へ] をクリックします。

SQL Server データベースの確認の画面が開きます。



5. インストールプロセスの残りの手順を完了します。

Windows Server 2008 および 2012 に対してリモートインストールを行うための追加要件

これは、複数の Exchange サーバをリモートでインストールする場合の Windows Server 2008 R2 SP1、Windows Server 2012、Windows Server 2012 R2 OS にのみ適用されます。

次の準備を行います。

- 次の権限が付与されたアカウントが必要です。

- Exchange Server 2013/2016/2019 メールボックスの場合:
  - ローカル管理者
  - ドメインユーザ
  - Exchange Organization Management グループ
- Exchange Server 2013/2016/2019 エッジトランスポートの場合:
  - ローカル管理者

注意

ドメインユーザ権限を持つアカウントの場合は、各 Exchange サーバでローカル管理者権限を持つアカウントである必要があります。

- リモートインストール中は、Windows ファイアウォールでファイルとプリンターの共有を許可にするか、各 Exchange サーバ上で Windows ファイアウォールを無効にします。

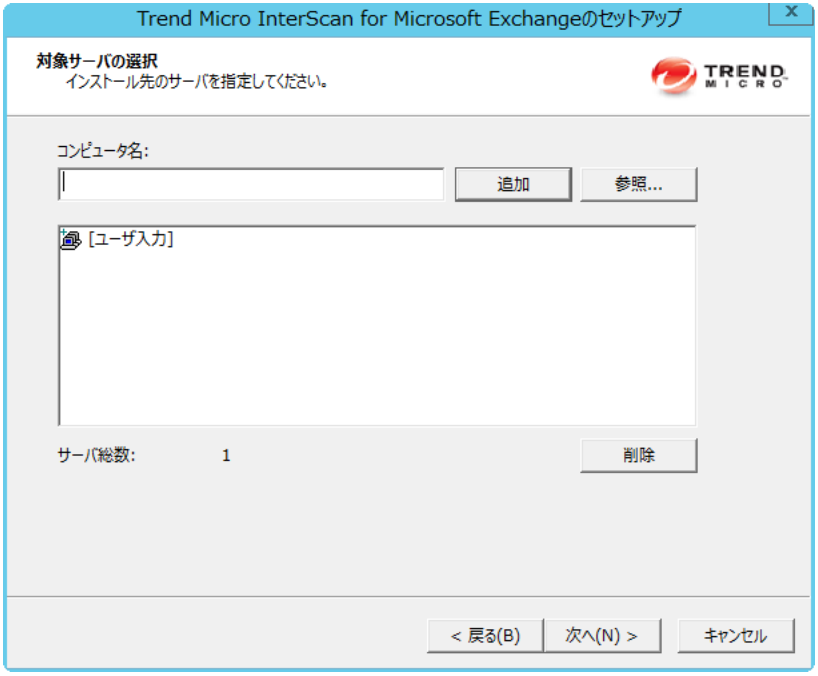
注意

インストールの完了後、元の設定に戻すことをお勧めします。

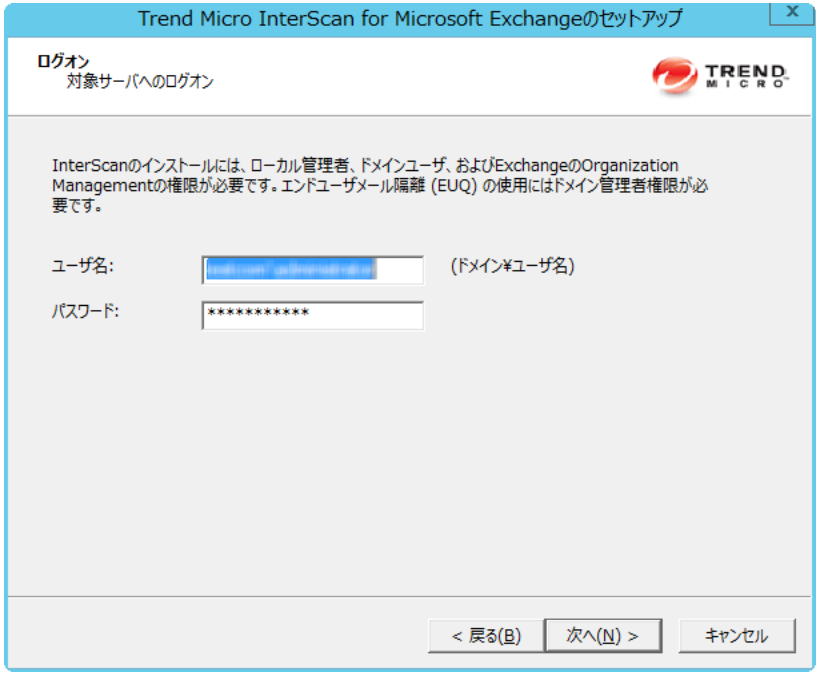
- 各 Exchange サーバ上で管理共有が使用可能であることを確認します。

手順

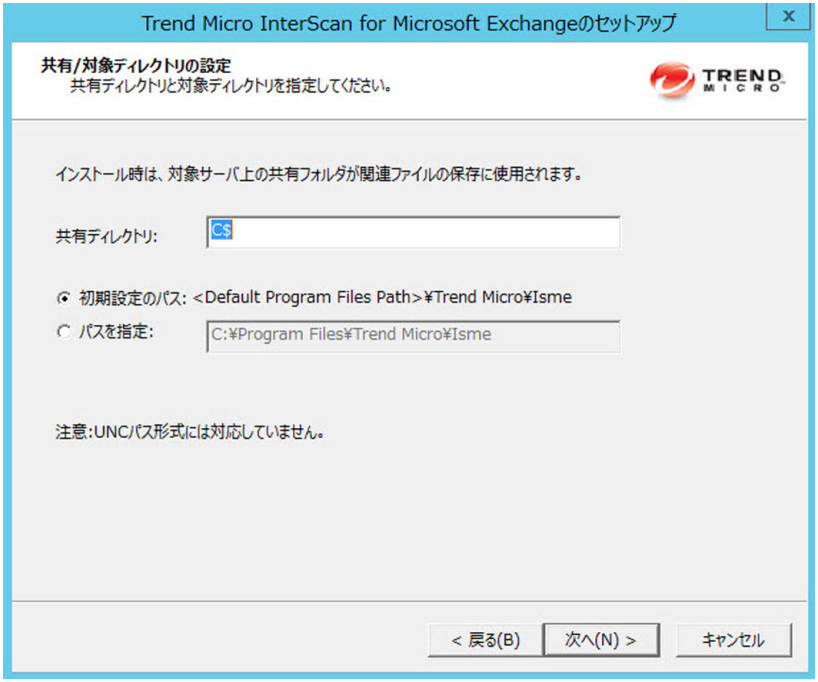
1. ドメイン管理者権限を持つアカウントで OS にログオンし、InterScan のセットアッププログラムを起動します。
2. 次の画面でオプションを指定します。
   a. インストールプロセスの [対象サーバの選択] 画面で、[追加] または [参照] をクリックして、同じドメインに属する複数の対象 InterScan サーバを追加します。



b. インストールプロセスの [ログオン] 画面で、手順 1 で OS にログオンする際に使用したのと同じアカウントを入力します。



c. インストールプロセスの [共有/対象ディレクトリの設定] 画面で、ADMIN$、C$、D$などの管理共有を入力します。



3. インストールプロセスの残りの手順を完了します。

インストール前のチェックリスト

次の表に、InterScan のインストールを開始する前に注意が必要な重要な項目の概要を示します。

表 1-8. インストール前のチェックリスト

項目	備考
最低限必要なアカウント権限	• Exchange メールボックスの場合、必要な権限はローカル管理者権限と Exchange の Organization Management グループ権限です。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 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。
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。InterScan に付属のレジストレーションキーを使用して、アクティベーションコードをトレンドマイクロの Web サイトからオンラインで入手できます。セットアッププログラムに、トレンドマイクロの Web サイトへのリンクが示されます。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。
CGI コンポーネント	Windows Server 2008、2012、2012 R2 では、InterScan をインストールする前に CGI 役割サービスをインストールしてください。Windows のサーバーマネージャーで、[役割の追加] > [Web サーバー (IIS)] > [役割サービスの追加] > [アプリケーション開発] > [CGI] の順にクリックして、CGI 役割サービスを追加します。
SQL Server Express	アップグレードインストールの場合は、SQL Server Express の現在のバージョンを 2014 以降にアップグレードしてください。

新規インストールについて

InterScan を初めてインストールする場合は、新規インストールを実行します。インストールを開始する前に、インストール前のチェックリスト (37 ページの「インストール前のチェックリスト」) を参照してください。

注意

このインストール手順は、サポートされているすべての Windows バージョンで同じです。

InterScan へのアップグレードについて 14.0

インストールを開始する前に、インストール前のチェックリスト (38 ページの表 1-8：インストール前のチェックリスト) を参照してください。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。

InterScan 14.0 は、InterScan 12.5 Service Pack 1 からのアップグレードに対応しています。

アップグレードの際、InterScan 14.0 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、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

本バージョンの InterScan 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も 、アップグレード時に維持されます。

クラスタ環境でのインストールについて

Exchange Server 2013、2016、および 2019 の場合のクラスタ環境でのインストール

DAG を備えた Exchange 2013、2016、または 2019 クラスタに InterScan をインストールする手順は、通常のサーバにインストールする手順と同じです。全部の DAG ノードに InterScan が自動でインストールされるわけではありません。InterScan は、[対象サーバの選択] 画面で設定したノードにのみインストールされます。インストール時に、[対象サーバの選択] 画面で対象サーバに DAG クラスタのすべてのノードを手動で追加してください。

第 2 章

Exchange Server 2013/2016/2019 に対する InterScan のインストール

セットアッププログラムを使用して 1 台以上のサーバにローカルまたはリモートで InterScan をインストールします。

この章の内容は次のとおりです。

必要な権限

次の表に、メールボックスの役割の Exchange 2013/2016/2019 に InterScan をインストールするために必要な権限を示します。

表 2-1. メールボックスの役割の Exchange 2013/2016/2019 に InterScan をインストールするために必要な権限

InterScan データベースのオプション	セットアップアカウントの権限	データベースアクセスアカウントの権限
ローカルデータベース	• ローカル管理者 • ドメインユーザ • Exchange Organization Management グループ [エンドユーザメール隔離のアクティベーション] セットアップアカウントは、ドメイン管理者アカウントである必要があります。	該当なし
SQL Windows 認証を使用するリモート SQL Server	• ローカル管理者 • ドメインユーザ • Exchange Organization Management グループ インストール中、[エンドユーザメール隔離のアクティベーション] セットアップアカウントを一時的にドメイン管理者に昇格させる必要があります。	dbcreator の役割および次の権限: • ローカル管理者 • Exchange Organization Management グループ • Exchange の ApplicationImpersonation の役割 インストール中、[エンドユーザメール隔離のアクティベーション] データベースアクセスアカウントを一時的にドメイン管理者に昇格させる必要があります。

InterScan データベースのオプション	セットアップアカウントの権限	データベースアクセスアカウントの権限
SQL Server 認証を使用するリモート SQL Server	• ローカル管理者 • ドメインユーザ • Exchange Organization Management グループ [エンドユーザメール隔離のアクティベーション] セットアップアカウントは、ドメイン管理者である必要があります。	dbcreator の役割

注意

[SQL Windows 認証を使用するリモート SQL Server] オプションを使用する場合は、セットアップアカウントとデータベースアクセスアカウントに同じドメインアカウントを使用することをお勧めします。

Exchange Server 2019/2016/2013 に対するインストール

以下に、Exchange Server 2019/2016/2013 メールボックスサーバおよびエッジサーバに対して InterScan をインストールするための手順を示します。

注意

ここでは Exchange Server 2016 の手順を紹介していますが、Exchange Server 2013 および 2019 でも手順は同じです。

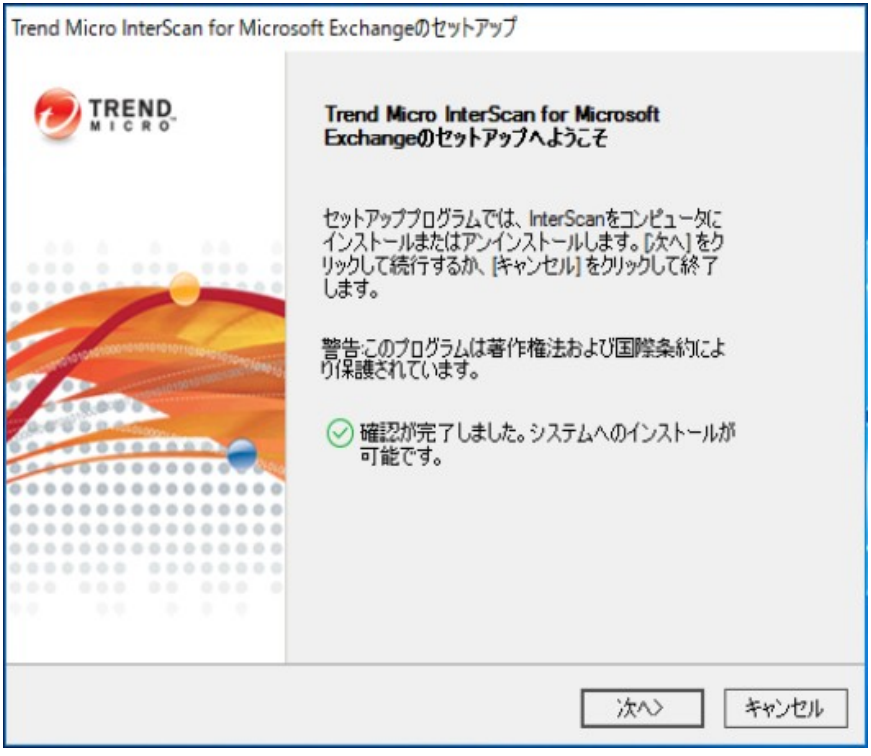
手順

1. セットアッププログラムを入手します。
   a. 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。

b. ファイルを一時ディレクトリに解凍します。

c. `setup.exe` を実行して InterScan をインストールします。

[Trend Micro InterScan for Microsoft Exchange のセットアップへようこそ] 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。

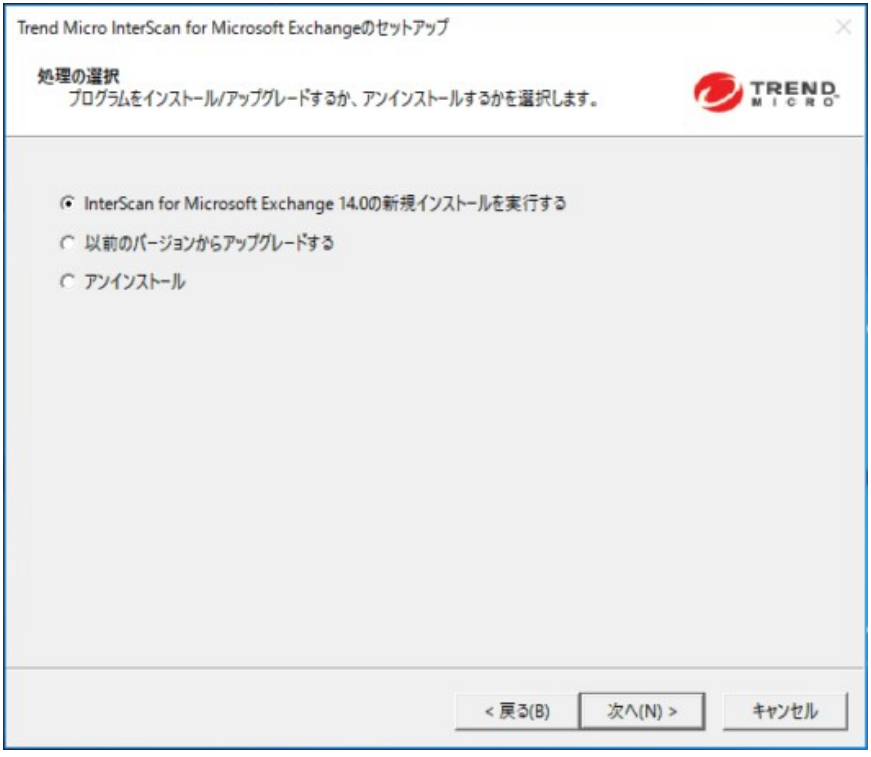
[使用許諾契約書] 画面が表示されます。

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。

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、インストールが終了します。

[処理の選択] 画面が表示されます。



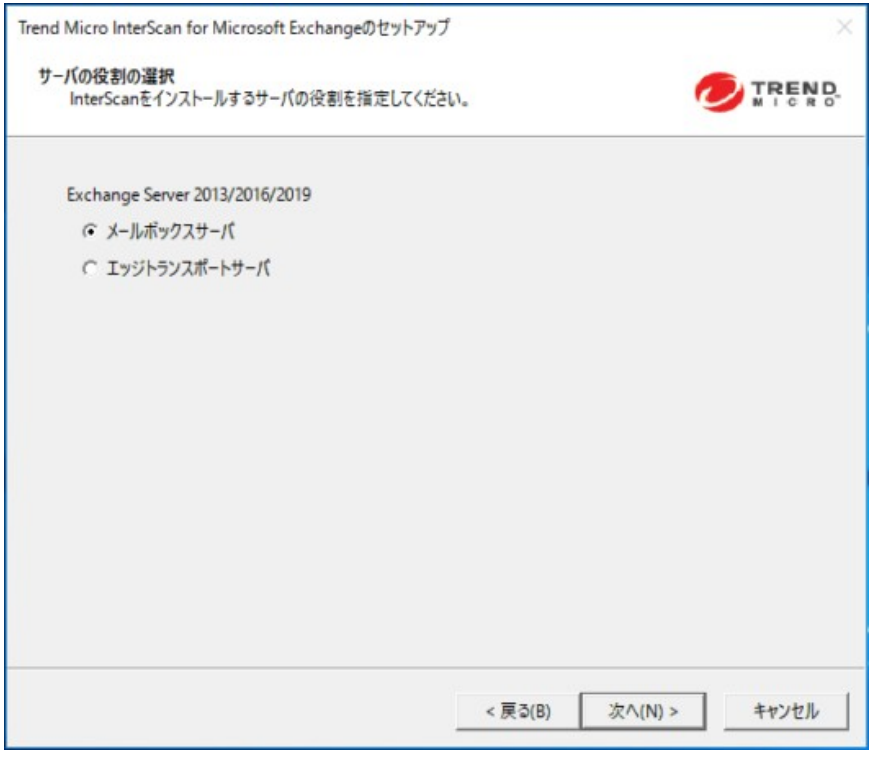
4. 処理を選択します。

   a. 新規インストールを実行するには、[InterScan for Microsoft Exchange 14.0 の新規インストールを実行する] を選択します。

   b. InterScan の既存のバージョンをアップグレードするには、[以前のバージョンからアップグレードする] を選択します。アップグレードの詳細については、39 ページの「InterScan へのアップグレードについて 14.0」を参照してください。

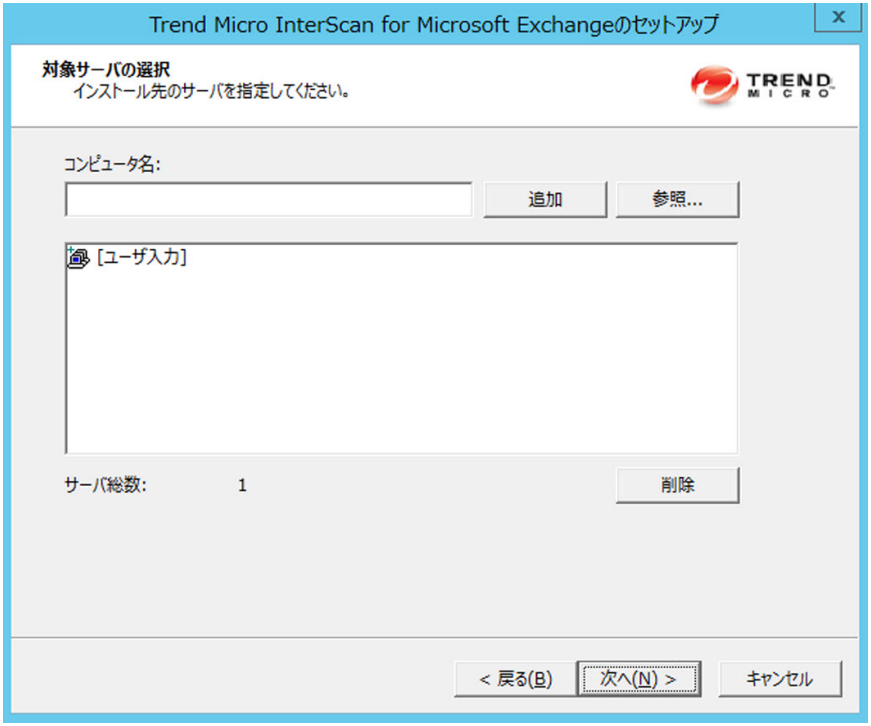
   c. [次へ] をクリックして続行します。

[サーバのバージョンの選択] 画面が表示されます。



5. InterScan をインストールする Exchange Server の種類を [Exchange Server 2013 / 2016 / 2019] で選択し ([メールボックスサーバ] または [エッジトランスポートサーバ])、[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。



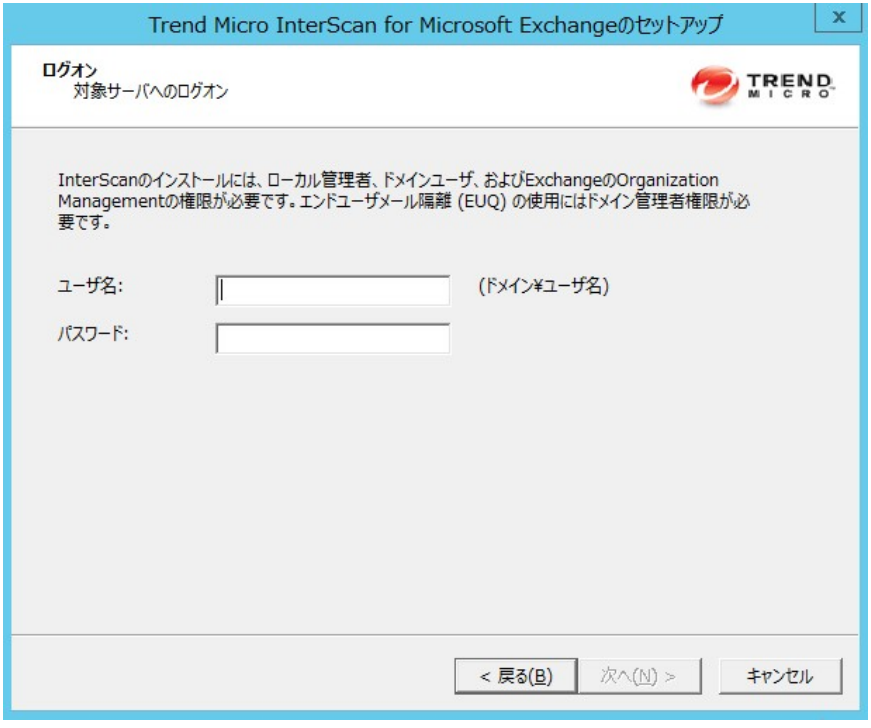
6. InterScan のインストール先コンピュータを選択します。

   a. 次のいずれかを実行します。

      - [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。
      - 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。



注意

セットアッププログラムでは、InterScan を複数のサーバに個々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。本バージョンの InterScan は、IPv6 をサポートしています。

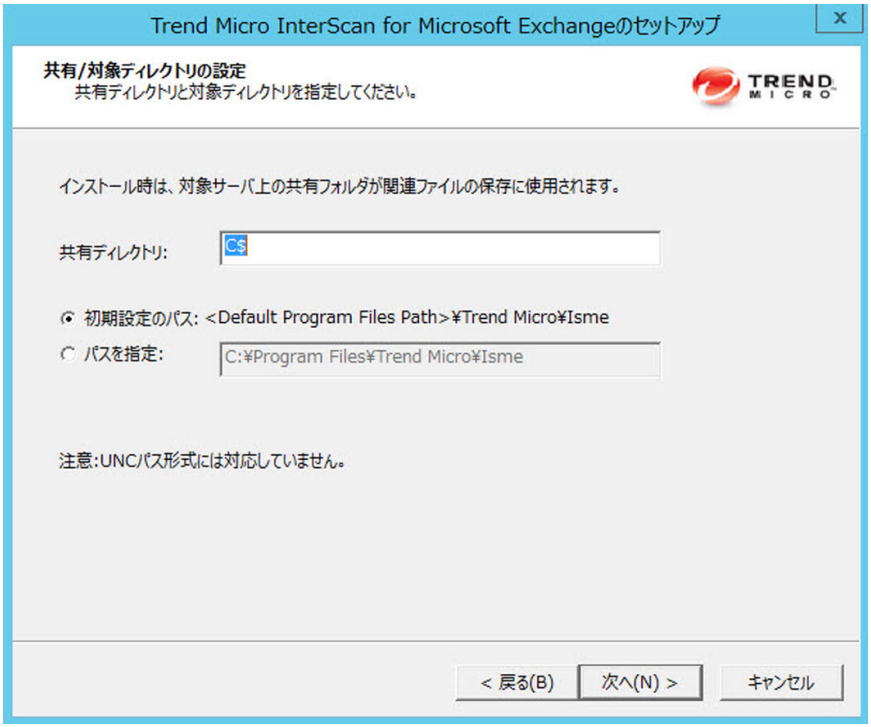
7. InterScan をインストールする対象サーバにログオンします。InterScan をインストールする対象サーバにログオンするためのユーザ名とパスワードを入力します。[次へ] をクリックして続行します。

注意

Exchange Server の役割に応じて、InterScan では次の権限が必要になります。

- メールボックスサーバ: ローカル管理者、ドメインエンドユーザ、および Exchange の Organization Management
- エッジトランスポートサーバ: ローカル管理者

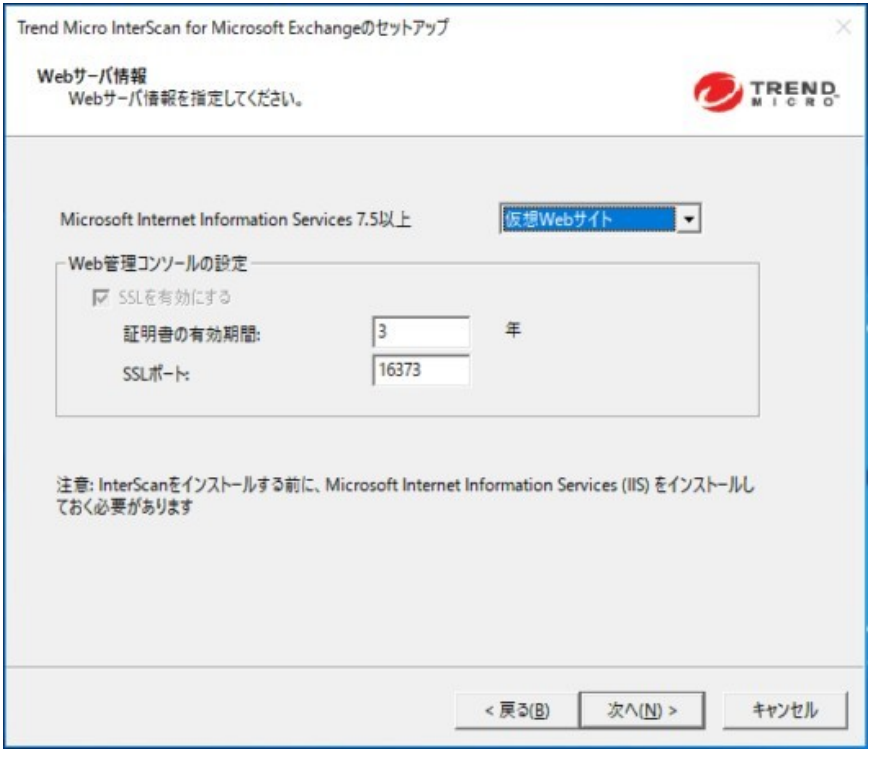
[共有/対象ディレクトリの設定] 画面が表示されます。



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。この共有ディレクトリには管理

者のみがアクセスできます。[初期設定のパス] または [パスを指定] を選択し、InterScan をインストールする対象サーバのディレクトリパスを入力します。[次へ] をクリックして続行します。

[Web サーバ情報] 画面が表示されます。



重要

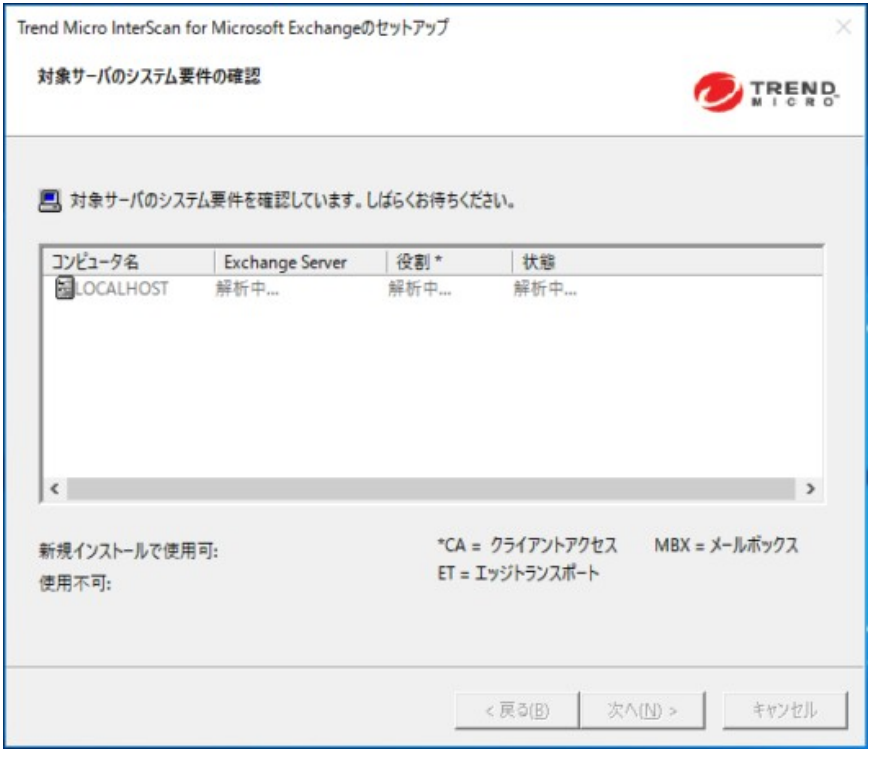
本バージョンでは、管理コンソールの SSL を無効化することはできません。

9. [既定の Web サイト] (IIS の場合) または [仮想 Web サイト] を選択します。[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。[次へ] をクリックして続行します。

注意

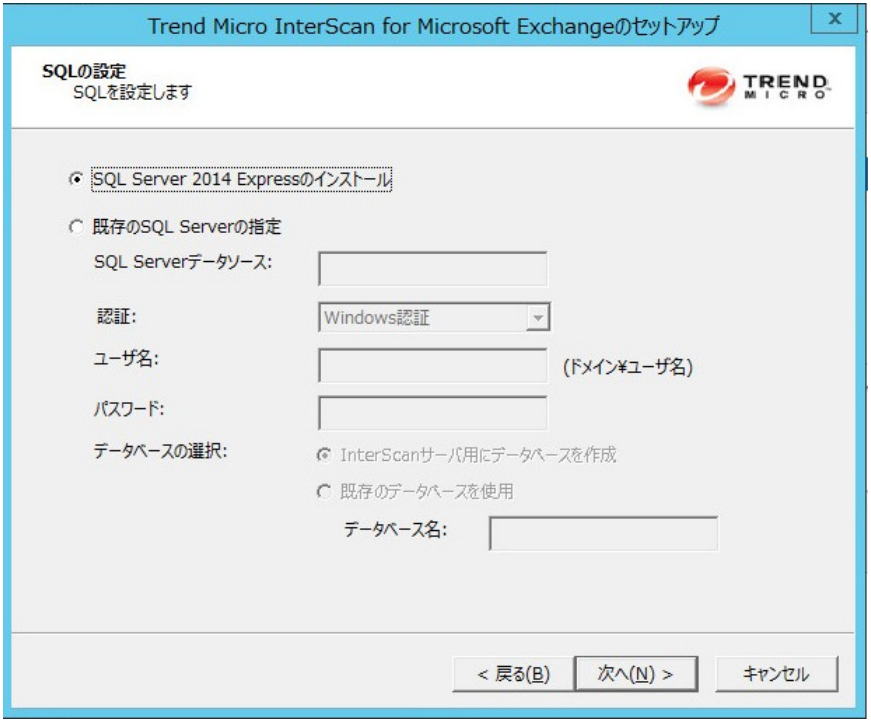
Web 管理コンソールの SSL を無効にすることはできません。

[対象サーバのシステム要件の確認] 画面が表示されます。



10. 設定を確認します。[次へ] をクリックします。

[SQL の設定] 画面が表示されます。



11. 次のいずれかを選択します。

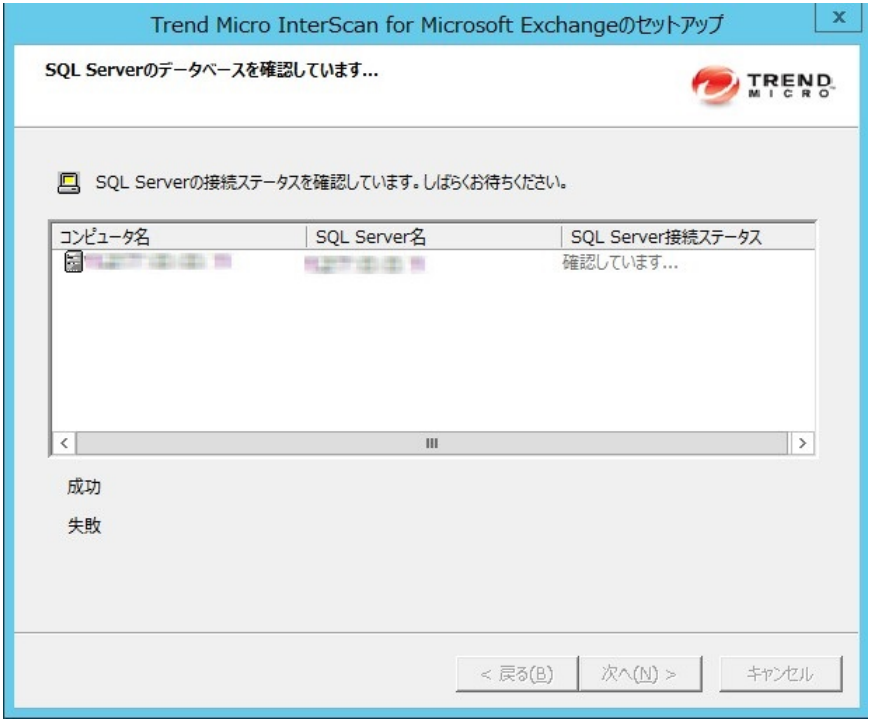
    - ローカルコンピュータに SQL Server 2014 Express をインストールするには、[SQL Server 2014 Express のインストール] を選択します。
    - 既存のデータベースサーバを使用するには、[既存の SQL Server の指定] を選択します。SQL Server データソース、ユーザ名、およびパスワードを入力します。

    注意

    InterScan のデータ保存に一元管理の SQL Server を使用すると、単一点障害のリスクが増し、パフォーマンスが低下します。高可用性リモート SQL Server のための手順を実行してください。

12. [次へ] をクリックします。

    SQL Server データベースの確認の画面が開きます。

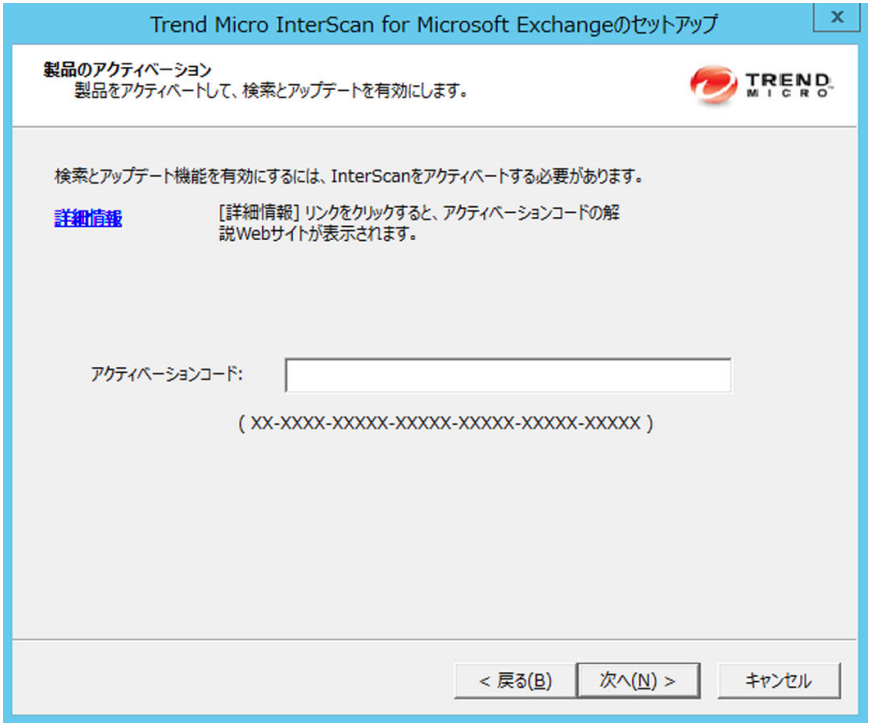


13. [次へ] をクリックして続行します。

[接続設定] 画面が表示されます。

14. プロキシサーバによって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る場合は、[プロキシサーバを使用する] を選択し、プロキシのホスト名またはアドレス、およびプロキシで使用される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。プロキシ経由の通信を SOCKS 5 を使用して保護する場合は、[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。



15. アクティベーションコードを入力します。

> **注意**
> アクティベーションコードをコピーし、この画面の [アクティベーションコード] に貼り付けることができます。

16. [次へ] をクリックします。
17. [スパムメール対策設定] 画面で、次の処理を行います。

a. 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。

ヒント

エンドユーザメール隔離機能を使用する場合は、インストール時にアクティベートすることをお勧めします。また、次のような環境ではエンドユーザメール隔離を使用しないことをお勧めします。

- ドメインコントローラに Exchange メールボックスサーバの役割がインストールされている
- ドメインコントローラに Exchange クライアントアクセスサーバの役割がインストールされている (メンバーサーバにメールボックスサーバの役割がインストールされている場合も含む)

- 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、[エンドユーザメール隔離との統合] を選択します。

重要

エンドユーザメール隔離は Exchange Server 2016 および 2019 ではサポートされていません。

---

i. インストールプロセスでスパムメールフォルダを作成するには、[エンドユーザメール隔離のアクティベーション] を選択します。

ii. 初期設定のスパムメールフォルダ名をそのまま使用するか、新しいスパムメールフォルダ名を指定します。

iii. [スパムメールを保管する日数] で日数を指定します。

b. [次へ] をクリックして続行します。

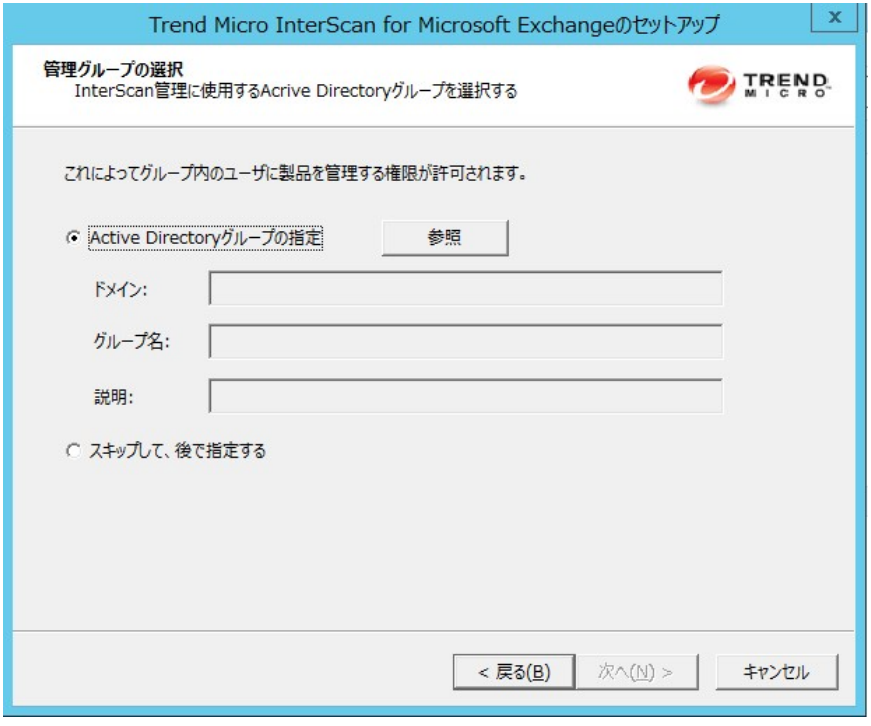
注意

Exchange メールボックスサーバまたはコンボサーバの役割がインストールされているサーバの Microsoft Outlook では、エンドユーザメール隔離はサポートされません。

[Apex Central サーバの設定] 画面が表示されます。

18. Apex Central サーバの設定を指定します。また、InterScan サーバと Apex Central 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。



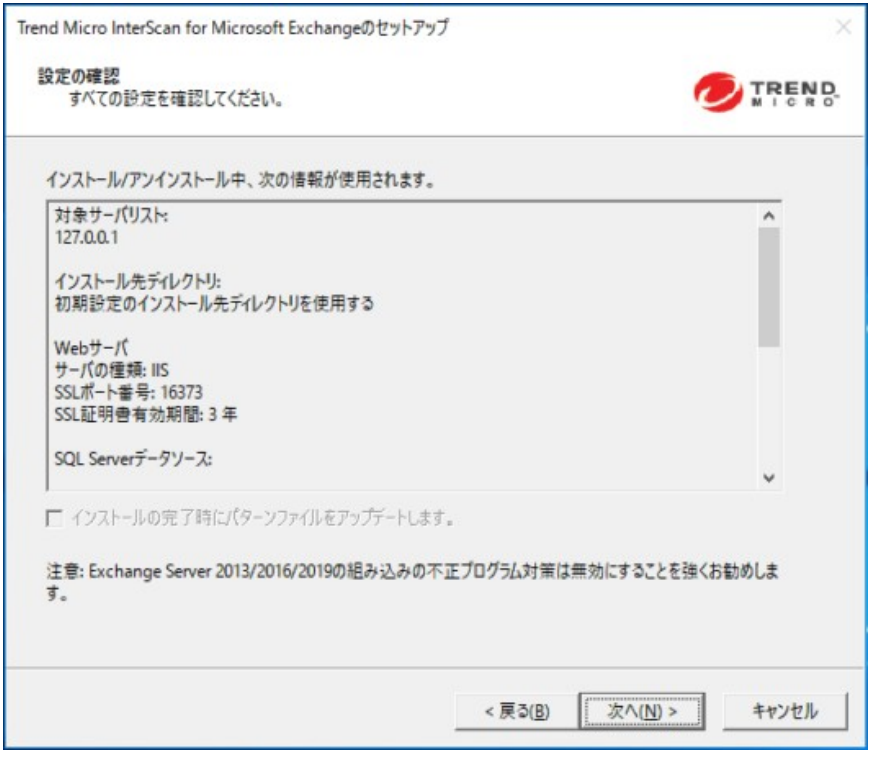
19. [管理グループの選択] 画面で、次の処理を行います。

    a. 次のいずれかの方法で、InterScan の管理権限を持つ Active Directory グループを設定します。

        - [Active Directory グループの指定] をクリックします。
        - この機能をインストール後に設定する場合は、[スキップして、後で指定する] を選択します。

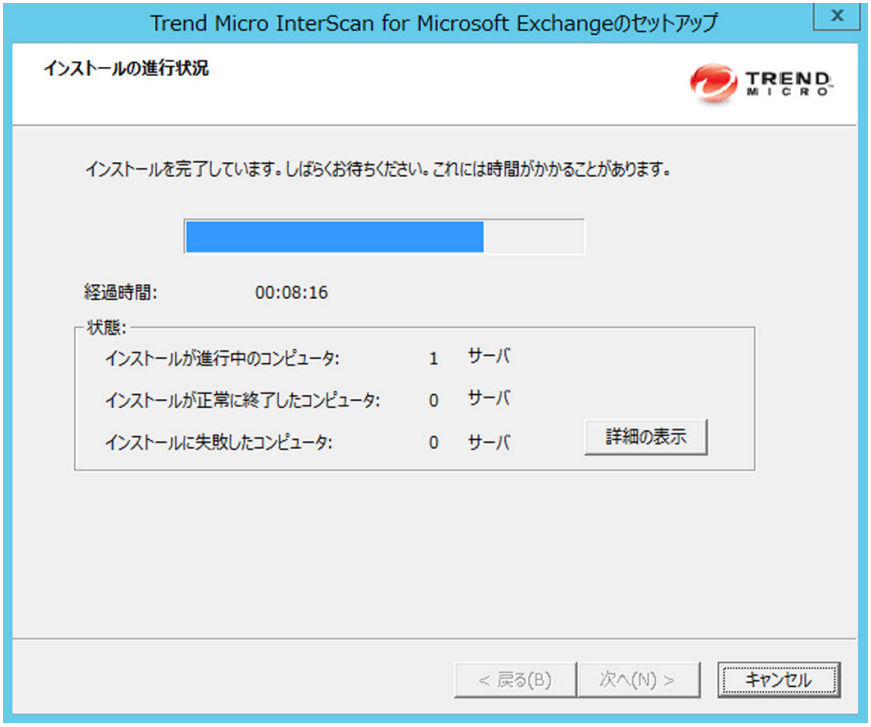
    b. [次へ] をクリックして続行します。

[設定の確認] 画面が表示されます。



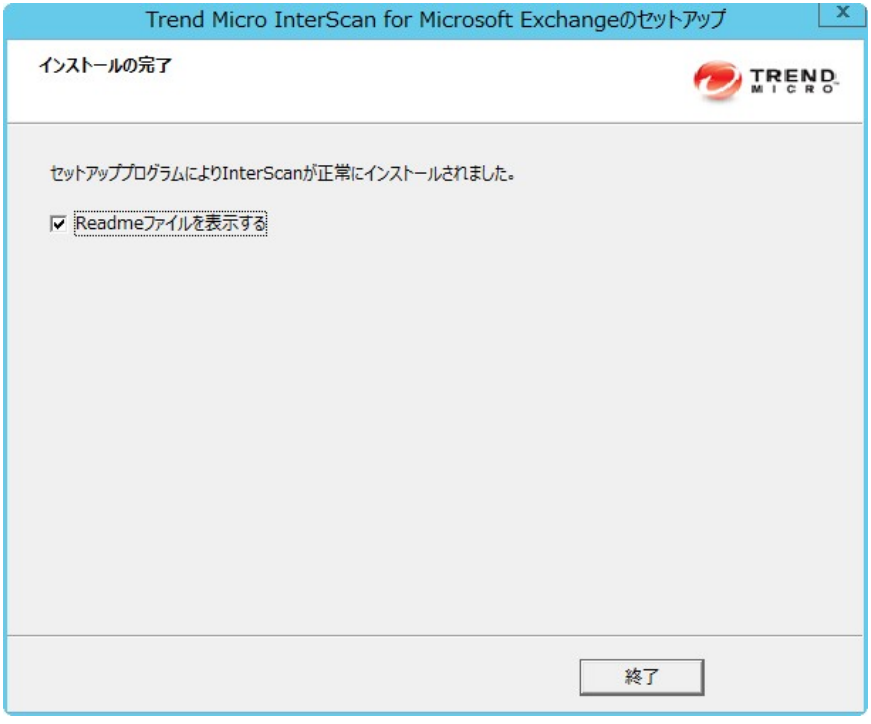
20. 設定を確認し、インストールの直後にパターンファイルをアップデートする場合は、[インストールの完了時にパターンファイルをアップデートします。]チェックボックスをオンにします。[次へ] をクリックして続行します。

[インストールの進行状況] 画面が表示されます。



21. [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。



22. 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。

第 3 章

Exchange Server 2013/2016 に対する InterScan のアップグレード

セットアッププログラムを使用して 1 台以上のサーバにローカルまたはリモートで InterScan をインストールします。

この章の内容は次のとおりです。

InterScan のアップグレードのサポート対象 Exchange プラットフォーム

次の表に、InterScan のアップグレードがサポートされる Exchange プラットフォームを示します。

表 3-1. InterScan のアップグレードのサポート対象 Exchange プラットフォーム

プラットフォーム	アップグレード元
Exchange Server 2016 以降	InterScan 12.5 Service Pack 1 以降
Exchange Server 2013 Service Pack 1 以降	InterScan 12.5 Service Pack 1 以降

Exchange Server 2013/2016 での InterScan のアップグレード

以下に、Exchange Server 2013/2016 に対して InterScan をインストールするための手順を示します。アップグレード前に、SQL Server サービスが開始されており、InterScan がデータベースに適切に接続できることを確認してください。

注意

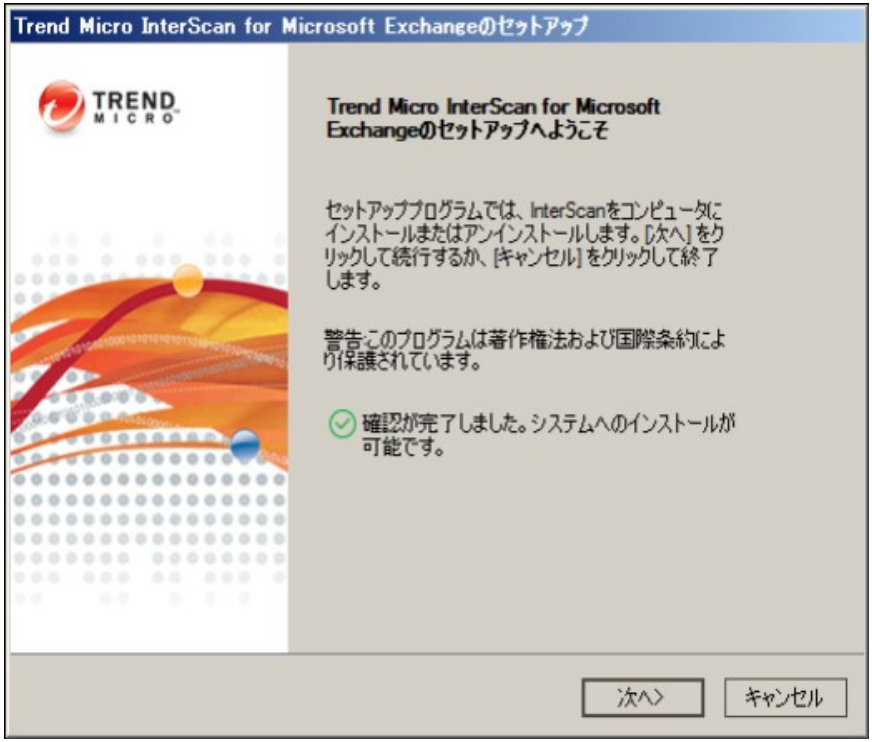
ここでは Exchange Server 2013 の手順を紹介していますが、Exchange Server 2016 でも手順は同じです。

手順

1. セットアッププログラムを入手します。
   a. 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。
   b. ファイルを一時ディレクトリに解凍します。

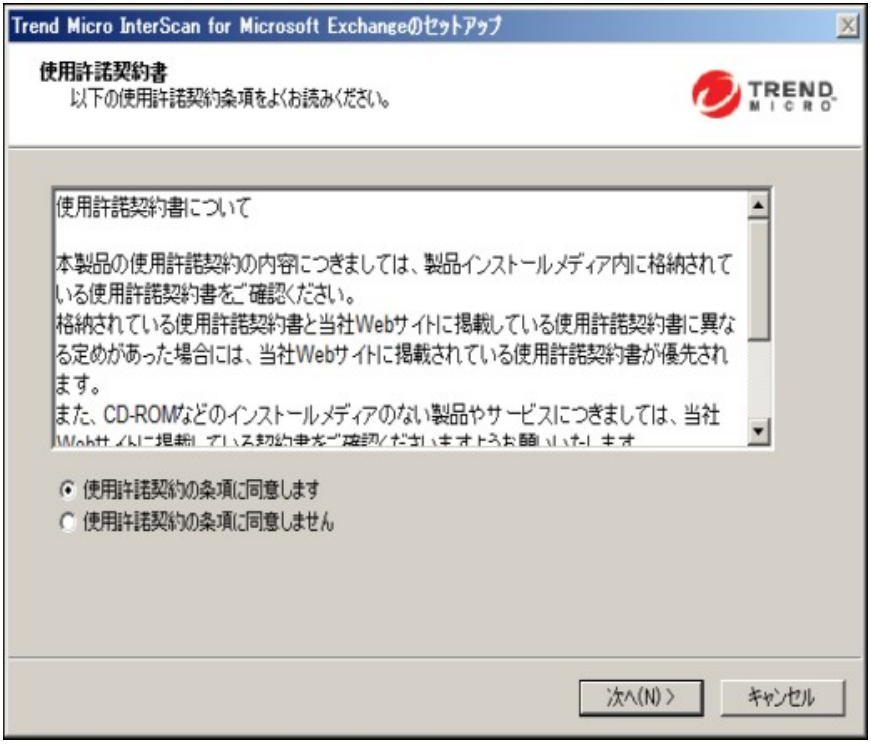
c. `setup.exe` を実行して InterScan をインストールします。

[Trend Micro InterScan for Microsoft Exchange のセットアップへようこそ] 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。

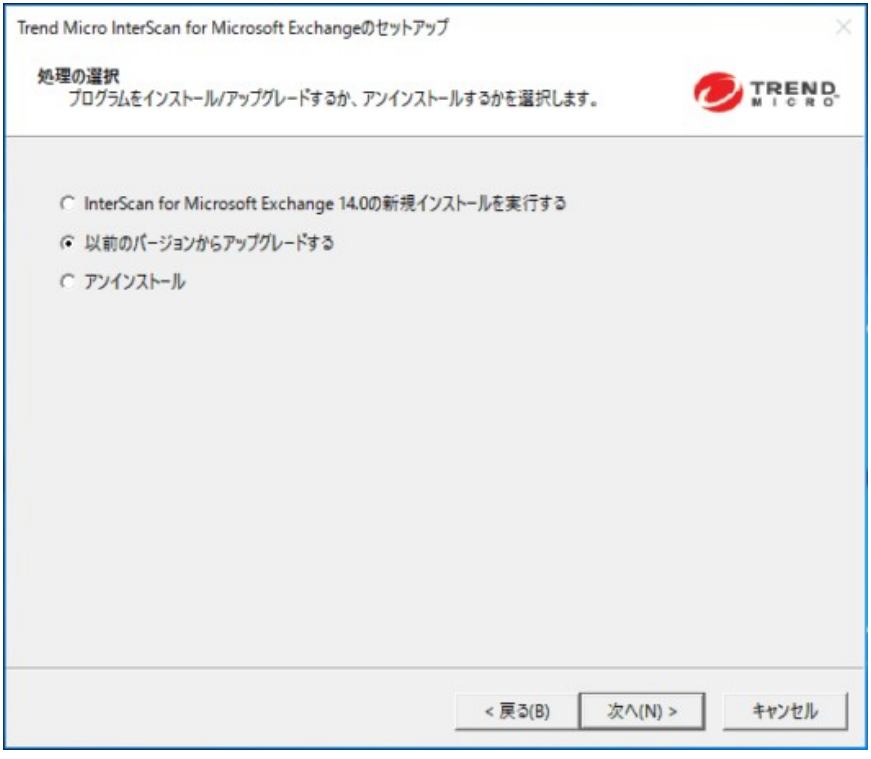


3. 契約の条件に同意して、インストールを続行するには、[使用許諾契約の条項に同意します] をクリックします。[次へ] をクリックして続行します。

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、インストールが終了します。

[処理の選択] 画面が表示されます。

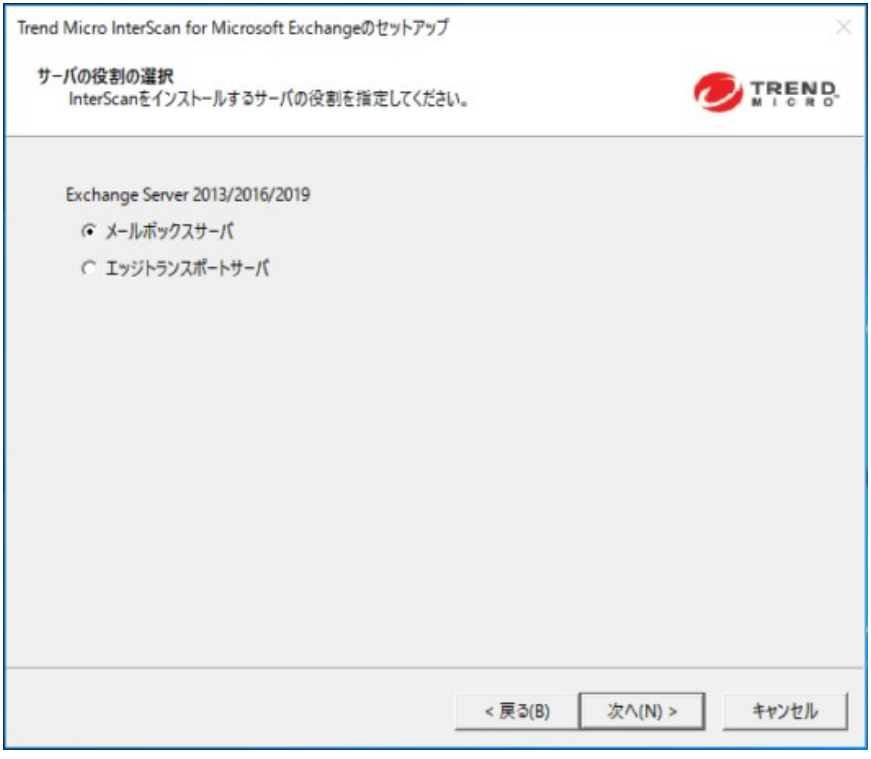


4. 処理を選択します。

   a. InterScan の既存のバージョンをアップグレードするには、[以前のバージョンからアップグレードする] を選択します。アップグレードの詳細については、39 ページの「InterScan へのアップグレードについて 14.0」を参照してください。

   b. [次へ] をクリックして続行します。

[サーバのバージョンの選択] 画面が表示されます。



5. InterScan をアップグレードするには、[メールボックスサーバ]または [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。

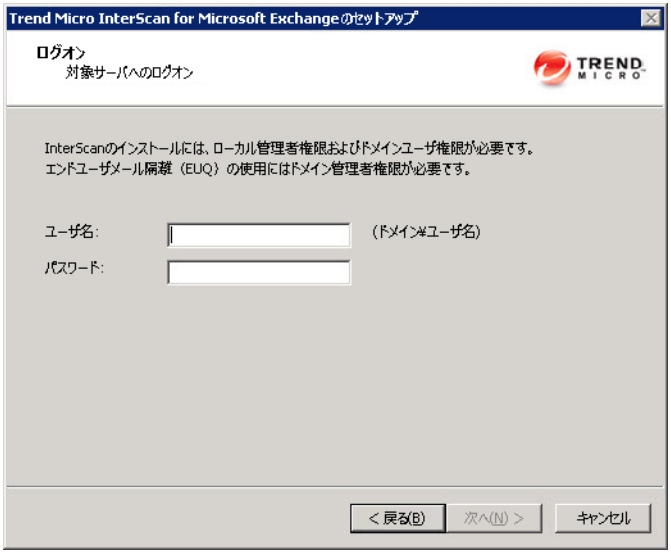
6. InterScan のインストール先コンピュータを選択します。

   a. 次のいずれかを実行します。

      - [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。
      - 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。

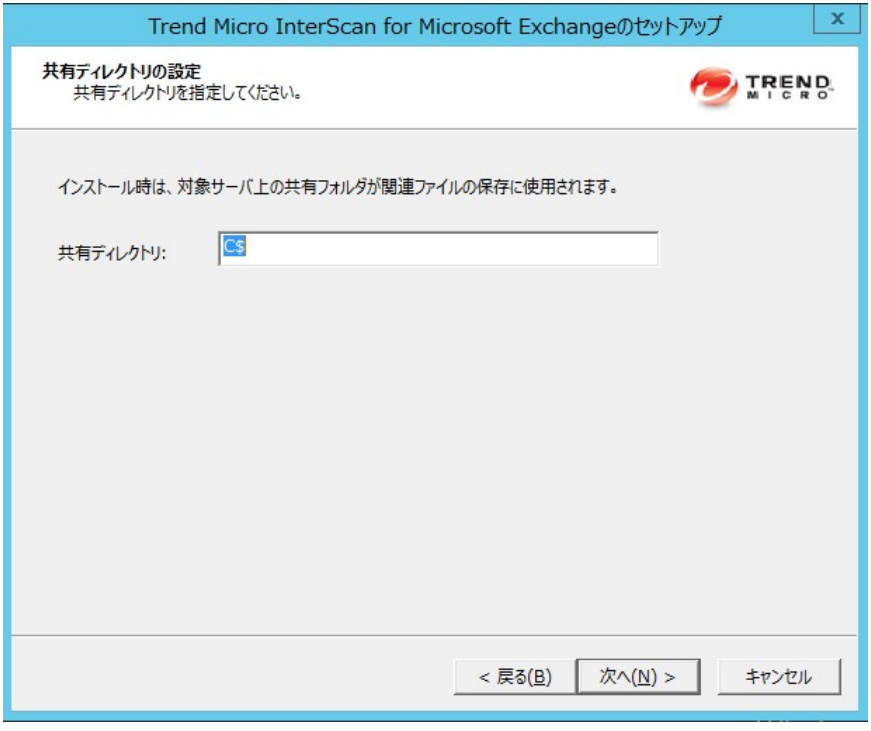


注意

セットアッププログラムでは、InterScan を複数のサーバに個々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。本バージョンの InterScan は、IPv6 をサポートしています。

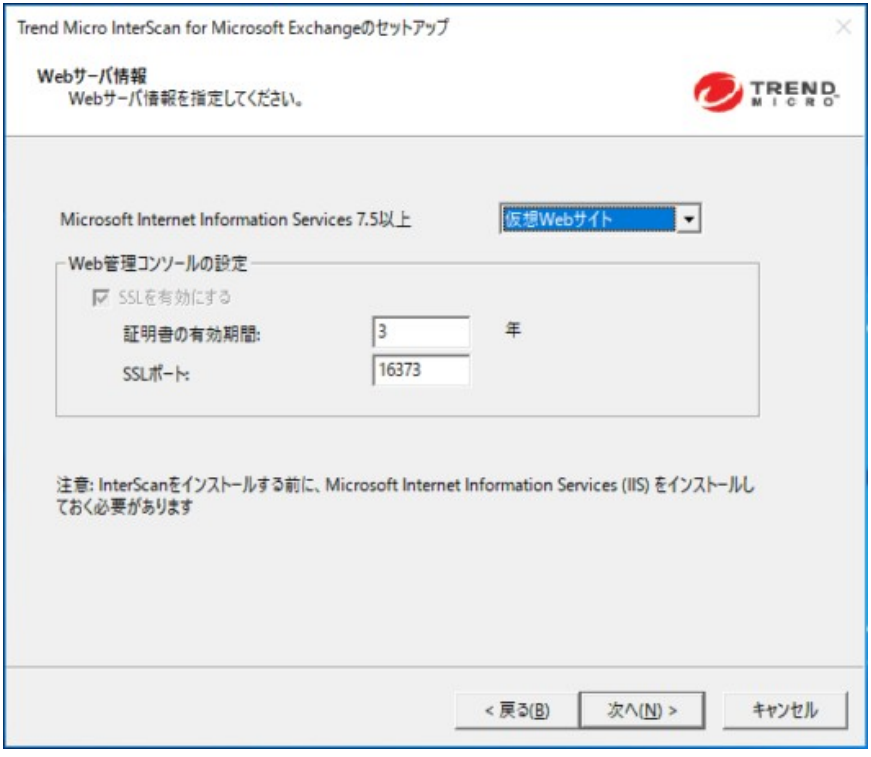
7. InterScan をインストールする対象サーバにログオンします。メールボックスサーバ環境では、Exchange 組織管理者権限とローカル管理者権限を持つアカウントを使用します。InterScan をインストールする対象サーバにログオンするためのユーザ名とパスワードを入力します。[次へ] をクリックして続行します。

[共有/対象ディレクトリの設定] 画面が表示されます。



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。この共有ディレクトリには管理者のみがアクセスできます。[初期設定のパス] または [パスを指定] を選択し、InterScan をインストールする対象サーバのディレクトリパスを 入力します。[次へ] をクリックして続行します。

[Web サーバ情報] 画面が表示されます。



重要

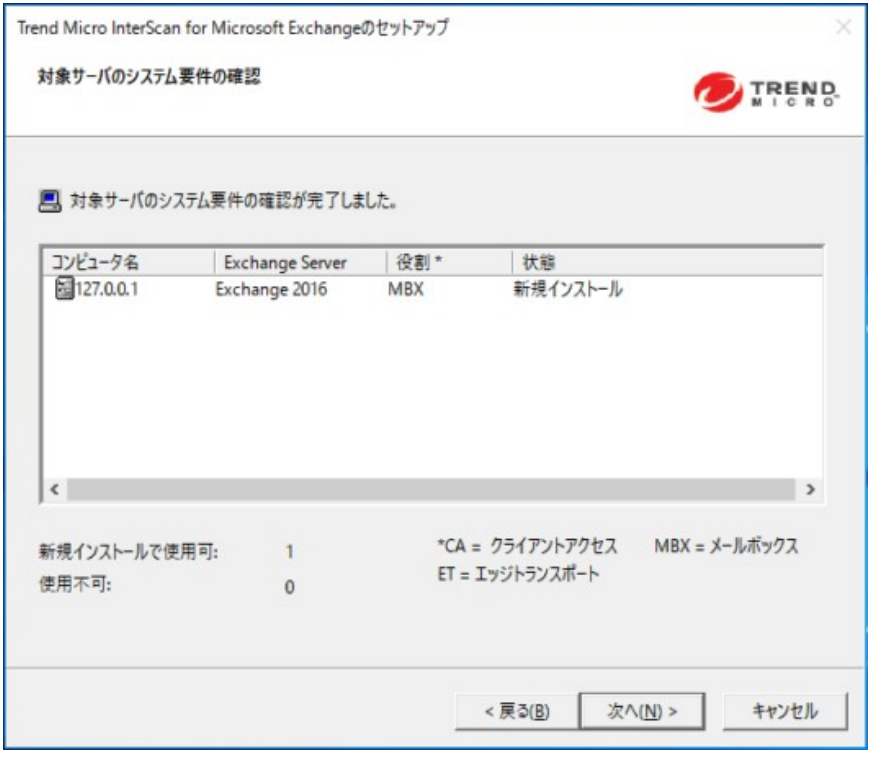
本バージョンでは、管理コンソールの SSL を無効化することはできません。

9. [既定の Web サイト] (IIS の場合) または [仮想 Web サイト] を選択します。[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。[次へ] をクリックして続行します。

注意

Web 管理コンソールの SSL を無効にすることはできません。

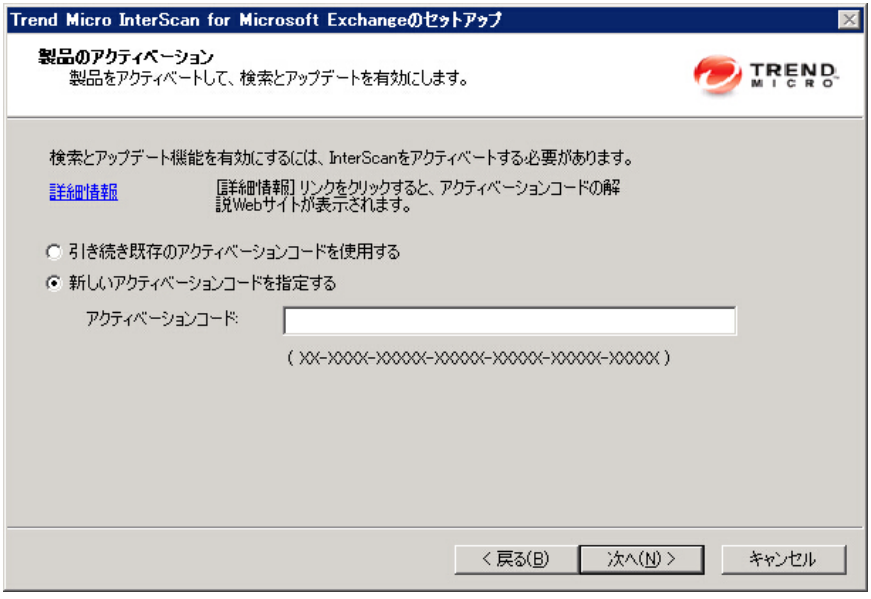
[対象サーバのシステム 要件の確認] 画面が表示されます。



10. 設定を確認します。
11. [次へ] をクリックして続行します。

    Windows ドメインアカウントを使用する場合は、ドメインのパスワードを入力する必要があります。

[製品のアクティベーション] 画面が表示されます。



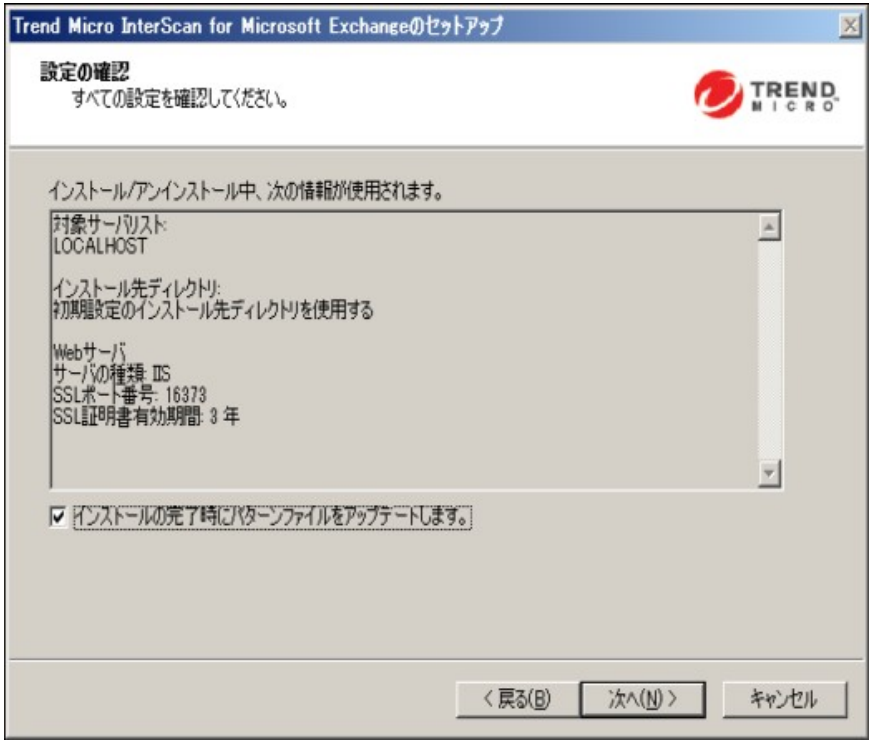
12. 次のいずれかのオプションを実行します。
    - [引き続き既存のアクティベーションコードを 使用する] を選択します。
    - [新しいアクティベーションコードを 指定する] を選択して、アクティベーションコードを入力します。

      注意

      アクティベーションコードをコピーし、この画面の [アクティベーションコード] に貼り付けることができます。

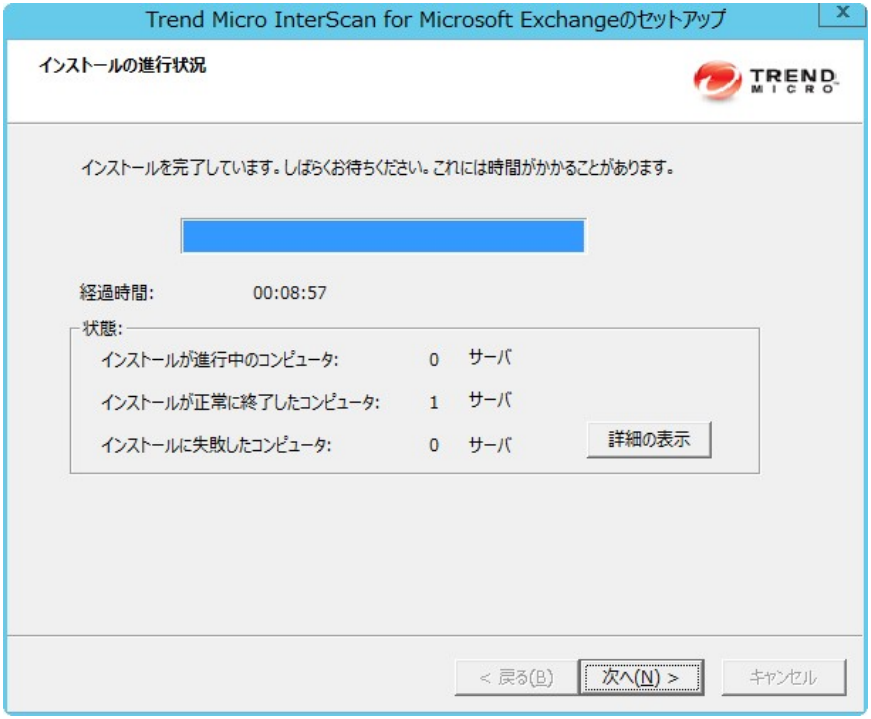
13. [次へ] をクリックします。

[設定の確認] 画面が表示されます。



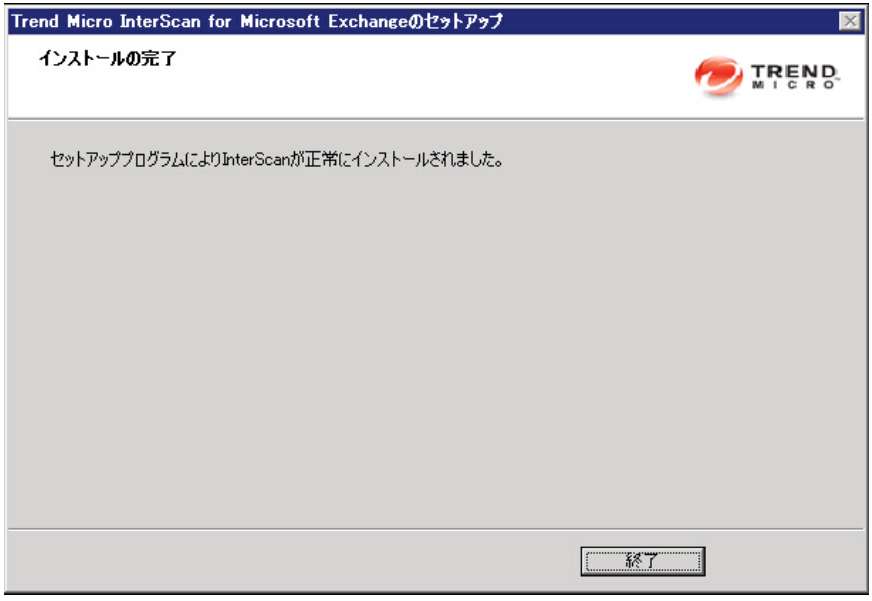
14. 設定を確認し、インストールの直後にパターンファイルをアップデートする場合は、[インストールの完了時にパターンファイルをアップデートします。]チェックボックスをオンにします。[次へ] をクリックして続行します。

[インストールの進行状況] 画面が表示されます。



15. [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。



16. 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ます。

第 4 章

インストール後の処理の実行

インストール後の処理を実行して、InterScan が正常にインストールされたことを確認します。

この章の内容は次のとおりです。

正常にインストールされたことの確認

InterScan フォルダ、サービス、およびレジストリキーをチェックして、正常にインストールされたことを確認します。

表 4-1. 正常にインストールされたことの確認

項目	設定
インストールフォルダ	`C:¥Program Files¥Trend Micro¥Isme¥`
サービス	• InterScan for Microsoft Exchange Master Service • InterScan EUQ Monitor Service **注意** このサービスは、Exchange Server 2016 と Exchange Server 2019 の環境では無効です。 • InterScan for Microsoft Exchange Remote Configuration Server **注意** このサービスは、Exchange Server エッジトランスポートサーバの役割には追加されません。 • InterScan for Microsoft Exchange System Watcher
レジストリキー (すべてのバージョン)	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange`

項目	設定
レジストリキー • メールボックスサーバ	• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-Name>\Private-<MDB-GUID>\VirusScanEnabled • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-Name>\Private-<MDB-GUID>\VirusScanBackgroundScanning • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-Name>\Public-<MDB-GUID>\VirusScanEnabled • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-Name>\Public-<MDB-GUID>\VirusScanBackgroundScanning 注意 これらのキーは、エッジトランスポートサーバまたはハブトランスポートサーバには追加されません。

InterScan 管理パックについて

InterScan は、Systems Center Operations Manager (SCOM) 2012 および 2016 に対応しています。InterScan のインストールパッケージの 次のパスから System Center Operations Manager (SCOM) に InterScan 管理パックをインポートして、InterScan を Systems Center Operations Manager (SCOM) で使用できます。

```
¥Management Pack
¥Trend.Micro.ScanMail.for.Microsoft.Exchange.xml
```

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。

手動検索のテスト

手順

1. テスト対象の Exchange Server に有効なメールクライアントを接続します。
2. リアルタイムウイルス検索の処理を [放置] に変更して、すべてのメールと添付されているテキストファイルが、手動検索の対象として選択したデータベースに送信されるようにします。
3. メールクライアントを起動し、「Test InterScan」という件名のテストメールを作成します。そのメールに EICAR テストスクリプトを添付し、テスト用メールボックス宛てに送信します。

4. 手動検索を設定するか、トレンドマイクロの初期設定の設定を使用します。初期設定のウイルス検索設定では、すべてのファイルが検索され、ウイルスが駆除されます。
5. 手動検索を実行します。InterScan によって EICAR ウイルスが検出され、それに対して設定した処理が実行されます。
6. InterScan のログまたは [今日の検索概要] 画面で結果を表示します。

リアルタイム検索のテスト

手順

1. テスト対象の Exchange Server に有効なメールクライアントを接続します。
2. テスト用に、業界標準の EICAR テストファイルのコピーを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るか確認します。
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てに送信します。
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 製品コンソールのウイルスログでセキュリティリスクの 検出結果を確認できます。

通知のテスト

手順

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セキュリティリスク検索を設定します。
   a. [セキュリティリスク検索] > [対象] の順にクリックします。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[送信する]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。

スパムメールフォルダの設定

重要

エンドユーザメール隔離のスパムメールフォルダは、Exchange Server 2013 環境でのみ使用できます (迷惑メールフォルダも 使用可能)。Exchange Server 2016 および 2019 では、迷惑メールフォルダのみを使用できます。

- トレンドマイクロのスパムメールフォルダ

  InterScan をインストールした Exchange サーバ上のすべてのメールボックスに、スパムメールフォルダが作成されます。InterScan のインストール時に、インストールプログラムによって、このフォルダの名前を指定するように指示され、指定した名前のフォルダが作成されます。

  インストール後に、Microsoft Outlook を使用してスパムメールフォルダの名前を変更できます。トレンドマイクロでは、このフォルダをフォルダ名ではなく ID で識別しています。

- スパムメール検出レベル

  InterScan では、スパムメール検出レベルの初期設定も行われます。スパムメール検出レベルは、Exchange サーバに着信するスパムメールをフィルタ処理するレベルです。

  - 高 — 最も厳しいスパムメール検出レベルです。InterScan は不審ファイルやテキストについてすべてのメールを監視しますが、誤検出の可能性が高くなります。誤検出とは、実際は正当なメールが InterScan によってスパムメールとしてフィルタされることです。
  - 中 — InterScan は高いスパムメール検出レベルで監視し、誤検出となる可能性は中程度になります。
  - 低 — これが初期設定になります。これは最も緩やかなスパムメール検出レベルです。InterScan は最も明確で一般的なスパムメールだけをフィルタします。誤検出の可能性は非常に低くなります。

第 5 章

サイレントインストール

サイレントインストールを 利用して InterScan を 1 台以上のサーバにインストールします。

この章の内容は次のとおりです。

サイレントインストールについて

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 手順は通常のインストールの手順と基本的に同じです。

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 のセットアップ画面に、インストールプロセスが事前に設定した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が記録されるだけで、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 [対象サーバの選択] 画面は表示されません。

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でのみサポートされています。
- 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_these_settings」セクションの設定は変更しないでください。
- バージョン/ビルドのアップグレードの場合、新しいパッケージを使用して設定を記録します。アップグレードの実行時、サイレントインストールでは以前の設定が保持されます。

- 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

手順

1. Windows のコマンドプロンプトを起動します。
2. InterScan for Microsoft 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 Microsoft 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。

既存の事前設定ファイルの使用

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。

表 5-1. 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 /H |Help| ?`	ヘルプ画面を表示します。
`Setup /R <設定ファイルのパス>`	記録モードを開始します。パスを指定しない場合、初期設定パスとして Windows ディレクトリ `C:¥Windows¥temp¥setup-silent-config.dat` が使用されます。
`Setup /S <設定ファイル>`	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。

パラメータ	説明
`Setup /output <出力ファイル>`	出力ファイルの名前を指定します。初期設定パスは、Windows ディレクトリ `C:¥Windows¥temp ¥ScanMail_SilentOutput.txt` です。

第 6 章

InterScan のアンインストール

この章では、InterScan をアンインストールする 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。

InterScan をアンインストールする前に

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
- レジストリに追加されたエントリ

Exchange Server で InterScan を使用している場合、InterScan 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++ 2015 再頒布可能パッケージ
- Microsoft Visual C++ 2015 再頒布可能パッケージ (X64)

警告!

- 単一サーバの場合、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 InterScan をアンインストールしてください。

権限の要件

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。

表 6-1. InterScan のアンインストールに最低限必要な権限

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 Server 2016/2019 メールボックスサーバ	• ローカル管理者 • ドメインユーザ • ExchangeOrganization Management グループ	該当なし
Exchange Server 2013 メールボックスサーバ	• ローカル管理者 • ドメインユーザ • ExchangeOrganization Management グループ	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 2019、2016、2013 エッジトランスポート	ローカル管理者	該当なし

セットアッププログラムの使用

setup.exe プログラムを使用して、InterScan をアンインストールできます。

手順

1. InterScan をアンインストールするには、setup.exe を実行します。

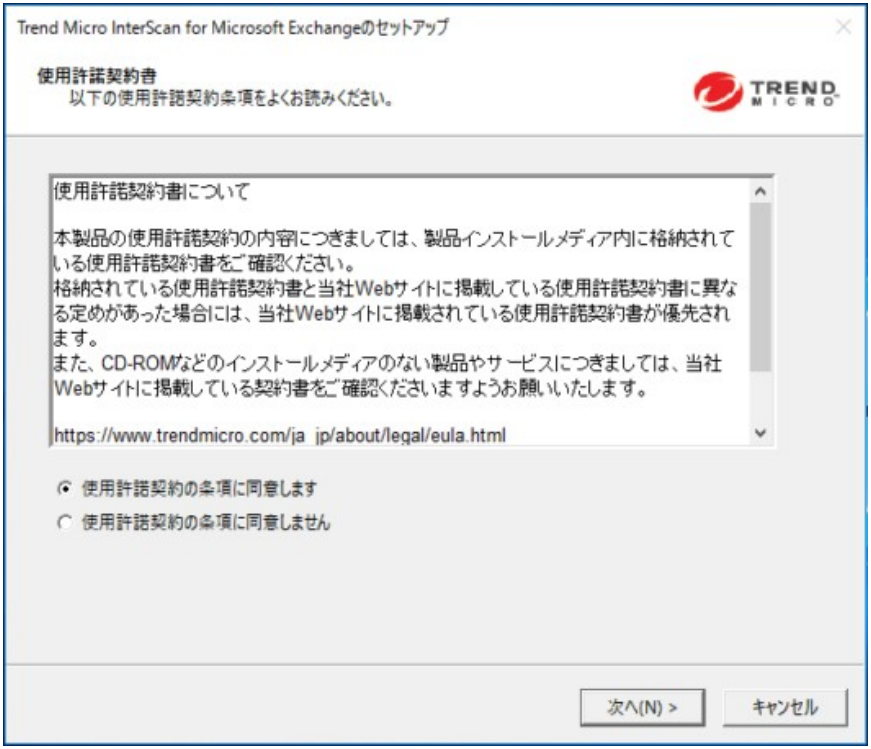
   注意

   アン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。

   [Trend Micro InterScan for Microsoft Exchange のセットアップへようこそ] 画面が表示されます。

2. [次へ] をクリックします。

[使用許諾契約書] 画面が表示されます。

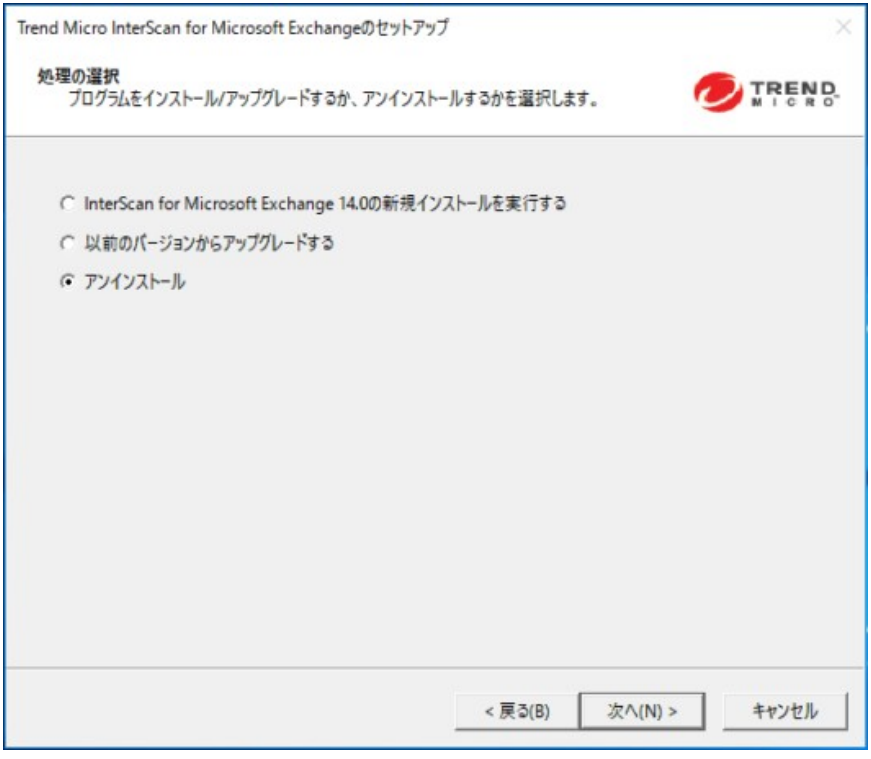


3. 契約の条件に同意して、インストールを続行するには、[使用許諾契約の条項に同意します] をクリックします。[次へ] をクリックして続行します。

注意

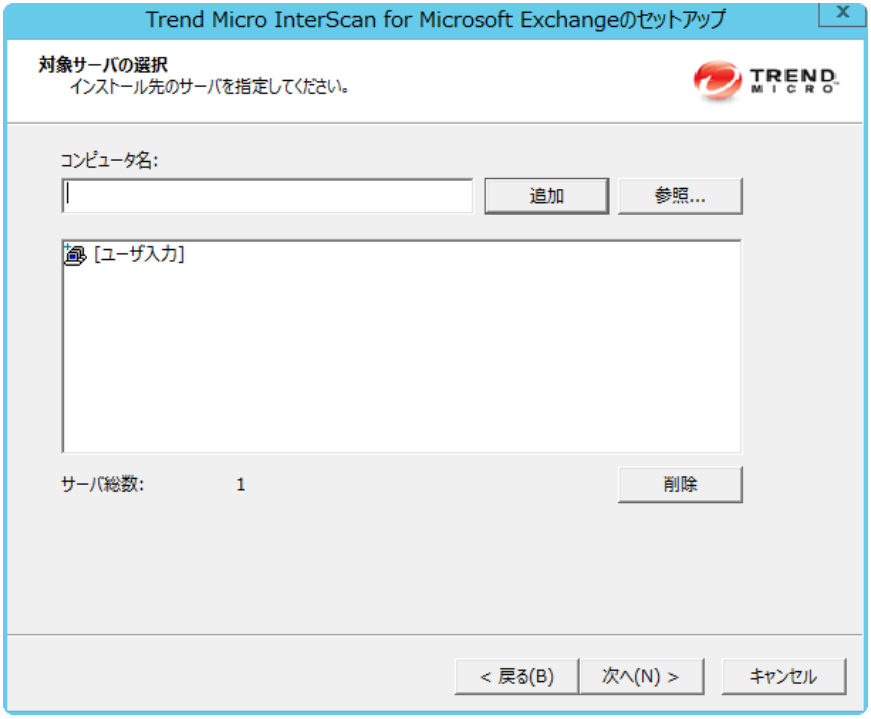
契約の条件に同意しない場合は、[使用許諾契約の条項に同意しません] をクリックします。これを選択すると、システムが変更されることなく、インストールが終了します。

[処理の選択] 画面が表示されます。



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。



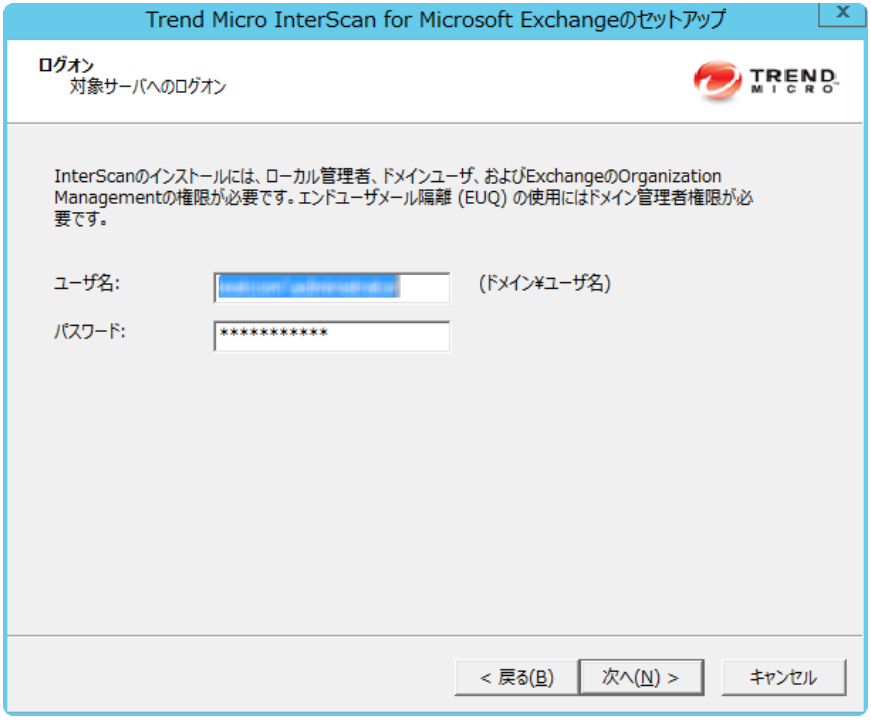
5. サーバから InterScan をアンインストールするには、次の手順に従ってください。

   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] に対象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。
      - 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。

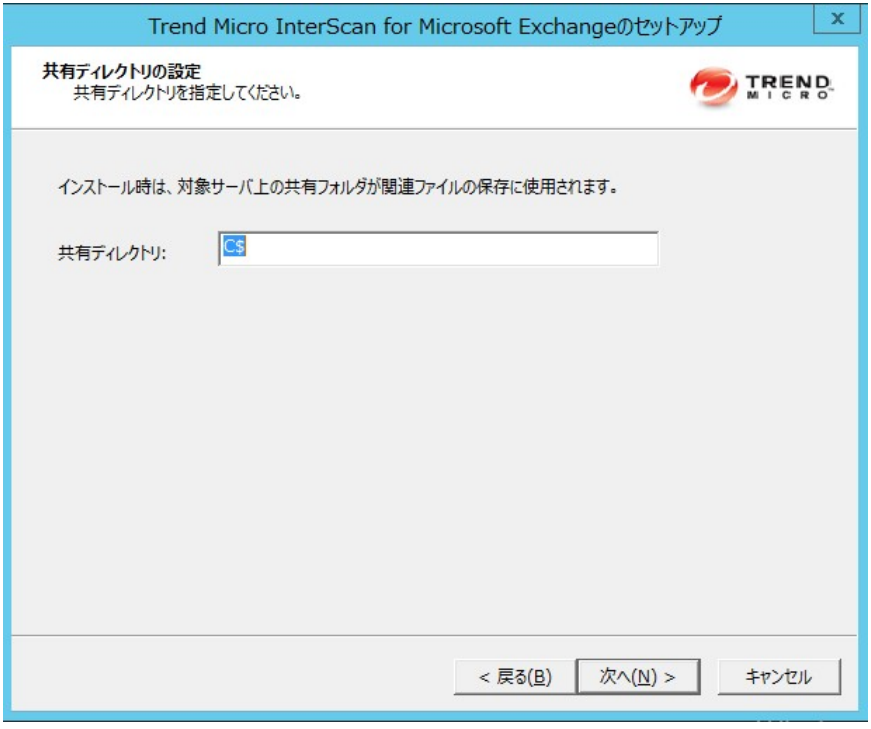
b. [次へ] をクリックします。

[ログオン] 画面が表示されます。



6. 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。
7. [次へ] をクリックします。

[共有/対象ディレクトリの設定] 画面が表示されます。

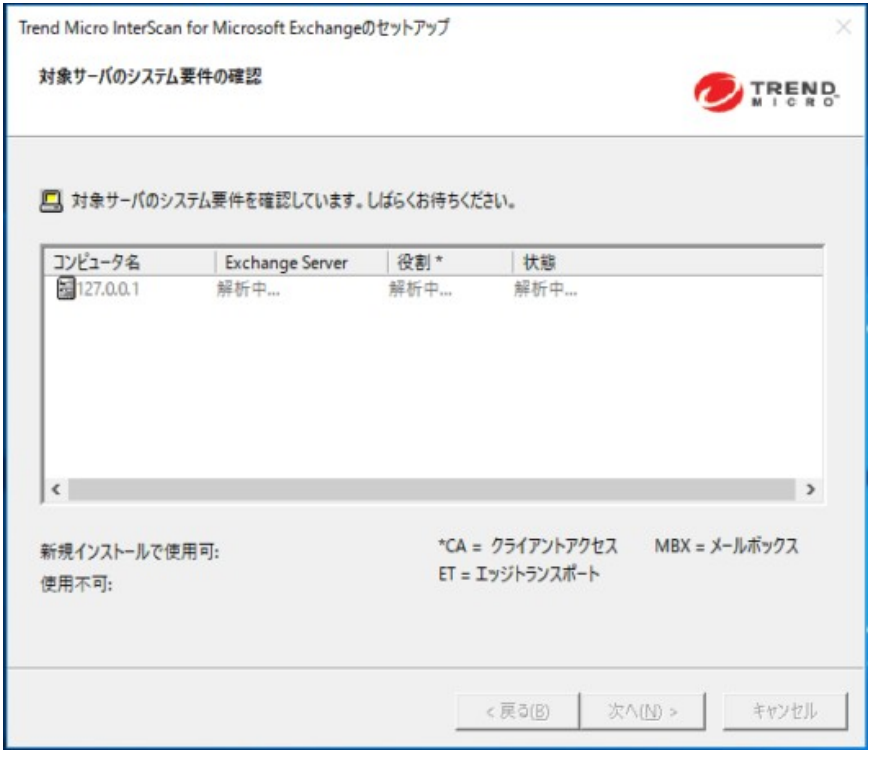


8. この画面で、InterScan をアンインストールする 対象サーバの共有ディレクトリを指定します。

   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。

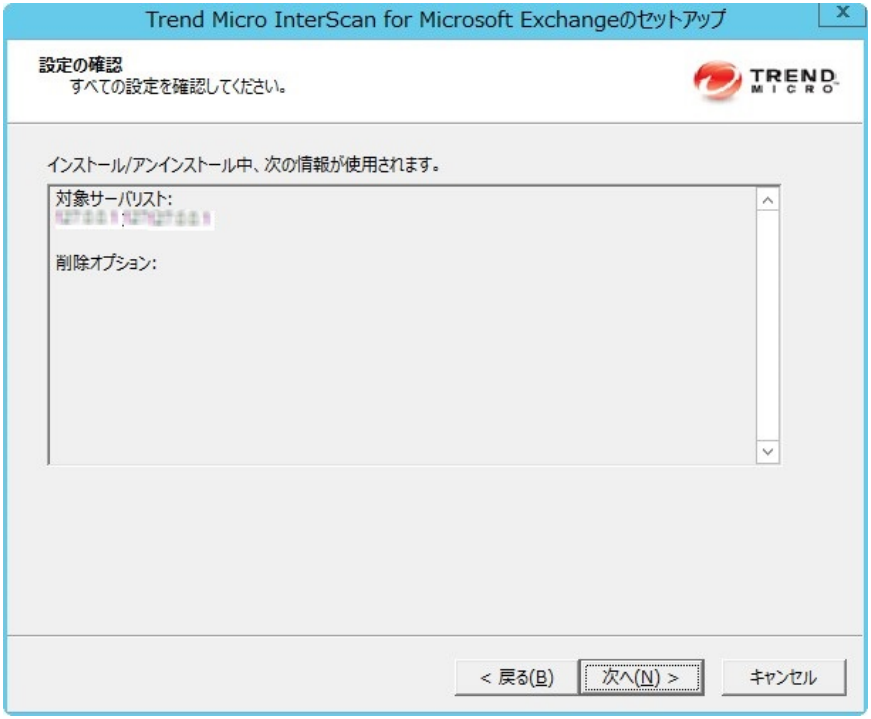
   b. [次へ] をクリックします。

[対象サーバのシステム 要件の確認] 画面が表示されます。



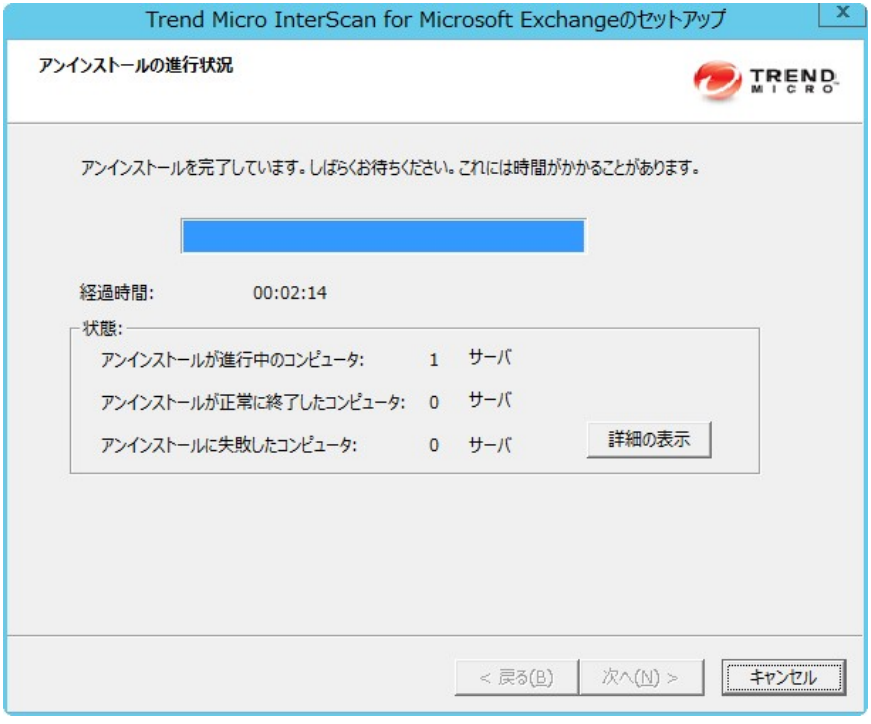
9. 画面を参照してアンインストールの設定が正しいことを確認します。
10. [次へ] をクリックします。

[設定の確認] 画面が表示されます。



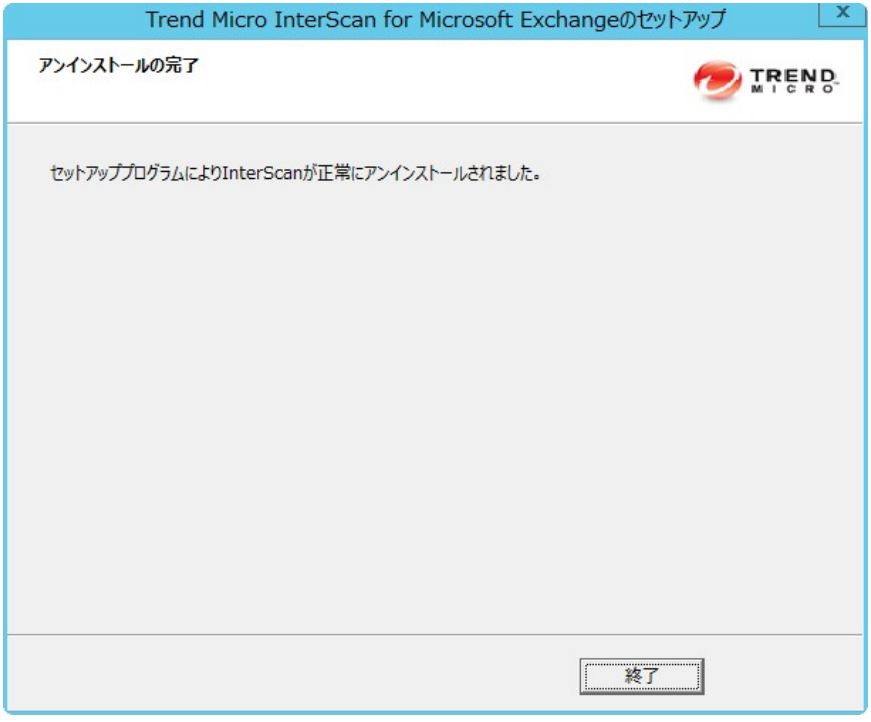
11. 設定を確認します。
12. [次へ] をクリックします。

[アンインストールの 進行状況] 画面が開きます。



13. アンインストールが完了したら、[次へ] をクリックして続行します。

[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。



14. [完了] をクリックして、セットアッププログラムを終了します。

    選択したサーバから InterScan がアンインストールされます。

Windows コントロールパネルの使用

InterScan は Microsoft™ Windows™のコントロールパネルを使用してアンインストールできます。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。

手順

1. Windows で [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 プログラムをクリックし、[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 により、Microsoft Visual C++ 2015 再頒布可能パッケージおよび Microsoft Visual C++ 2015 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。

Exchange サーバからの InterScan の手動アンインストール

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

重要

アンインストールの実行中は、アンインストールツールによって Microsoft Exchange Transport (MsExchangeTransport) サービスが停止されます。アンインストールが完了すると自動的に再開されます。

手順

1. アンインストールツールを取得するには、トレンドマイクロのテクニカルサポートにお問い合わせください。
2. Exchange 2019、2016、および 2013 サーバから InterScan を削除するには、付属の readme ファイルの手順に従ってください。

3. リモート SQL Server データベースをインストールしている環境では、InterScan データベースを Microsoft SQL Server からアンインストールしてください。

   a. SQL Server Management Studio Express を使用して、InterScan がインストールされているリモート SQL Server に接続します。

   b. 次の InterScan データベースを削除します。

      - アップグレード版をアンインストールする場合は次を削除します。
        - `Conf_HostName_UUID`
        - `Log_HostName_UUID`
        - `Report_HostName_UUID`
      - 新規インストール版をアンインストールする場合は次を削除します。
        - `ScanMail_UUID`

4. エンドユーザ隔離 (EUQ) が有効化されている環境では、次のデータベースを Exchange サーバから手動で削除してください。

   `EUQ_[サーバ名]`

第 7 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの 送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

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

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録 A

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。次の表に各セクションを表示します。事前設定ファイルを手動で変更する場合は、次の表を参照してください。

表 A-1. 事前設定ファイル

セクション	内容
Logon	• LogonUserDomain=<ユーザの設定> • LogonUserName=<ユーザの設定>
Directory	• TempDir=smextemp • ShareName=C$ 注意 これは初期設定ですが、変更可能です。 • TargetDir=C:\Program Files\Trend Micro\Isme 注意 これは初期設定ですが、変更可能です。

セクション	内容
	• `UseDefaultProgPath=0` または `1` **注意** 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>`
Proxy	• `UseProxy=0` **注意** 0 の場合は無効、1 の場合は有効です。 • `DoAUAfterInstall=0` **注意** 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>` **注意** 範囲は 1〜65535 です。 • `ProxyUsername=<ユーザの設定>` • `EnableSocks5=0` または `1` **注意** 0 の場合は無効、1 の場合は有効です。
Web	• `IISSiteType=0` または `1`

セクション	内容
	注意 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、IIS が選択されている場合にのみ適用されます。 • WebPort=<ユーザの設定> 注意 範囲は 1〜65535 です。 • SSLPort=<ユーザの設定> 注意 範囲は 1〜65535 です。 • SSLValidPeriodCertificate=<ユーザの設定>
ServerManagement	• CreateNewConsoleAccount=0 または 1 注意 0 の場合は現在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 注意 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 注意 0 の場合は無効、1 の場合は有効です。

セクション	内容
EUQ	• `ActivateEUQ=0` または `1` 注意 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。 • `IntegrateWithOutook2K3JunkMailFolder=0` または `1` 注意 0 の場合は無効、1 の場合は有効です。 • `UseDefaultSpamFolderName=0` または `1` 注意 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` 注意 これは初期値のフォルダ名ですが、変更可能です。 • `SpamMsgRetainDay=14` 注意 これは初期設定ですが、変更可能です。範囲は 0〜30 です。
CMAgent	• `RegisterCMAgent=0` または `1` 注意 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`

セクション	内容
	注意 範囲は 1〜65535 です。 • ConnectCMServerUsingHTTPS=0 または 1 注意 0 の場合は無効、1 の場合は有効です。 • ConnectCMServerUsingProxy=0 または 1 注意 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 注意 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 注意 範囲は 1〜65535 です。
Do NOT edit these settings	• LogonPassword=<ユーザの設定> 注意 パスワードは表示されません。 • ExchangeType=1、2、3、または 4

セクション	内容
	注意 • 1 は Exchange 2010 エッジトランスポートサーバ • 2 は Exchange 2010 ハブトランスポートサーバ/メールボックスサーバ • 3 は Exchange 2013/2016/2019 メールボックスサーバ • 4 は Exchange 2013/2016/2019 エッジトランスポートサーバ • ProxyPassword=<ユーザの設定> 注意 パスワードは表示されません。 • ConsolePassword=<ユーザの設定> 注意 パスワードは表示されません。 • EUQInstallLangID=1033 注意 この設定は変更しないでください。 • EUQDefaultLangID=9 注意 この設定は変更しないでください。 • ConnectCMServerProxyPassword=<ユーザの設定> 注意 パスワードは表示されません。

セクション	内容
	• CMServerWebPassword=<ユーザの設定> **注意** パスワードは表示されません。 • ConsoleGroup=<ユーザの設定> **注意** 次に例を示します。DomainName\Group。このグループ名は変更しないでください。 • ServerManagementGroupSid= **注意** SID は変更しないでください。
RemoteSQL with Windows Authentication	• RemoteSQLWindowsAuthentication **注意** 0 は SQL アカウント認証を示し、1 は Windows 認証を示します。 • RemoteSQLUserName=<ユーザの設定> **注意** Windows 認証を使用するように RemoteSQLWindowsAuthentication を設定した場合、ユーザ名は Windows アカウントです。 • RemoteSQLPassword=<ユーザの設定> **注意** リモート SQL のパスワードは暗号化されます。

セクション	内容
RemoteSQL with SQL Authentication	• `RemoteSQLServerDataSource=<ユーザの設定>` • `RemoteSQLUserName=<ユーザの設定>` **注意** dbcreator の役割が必要です。 Windows 認証を使用するように `RemoteSQLWindowsAuthentication` を設定した場合、ユーザ名は Windows アカウントです。 • `RemoteSQLPassword=<ユーザの設定>` **注意** リモート SQL のパスワードは暗号化されます。 • `RemoteSQLWindowsAuthentication` **注意** 0 は SQL アカウント認証を示し、1 は Windows 認証を示します。 • `RemoteSQLExistingDatabase=<ユーザの設定>` **注意** 空白のままにすると、InterScan によって新しいデータベースが作成されます。

付録 B

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
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対策エンジンを、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。
スパムメール対策	フィルタメカニズムとも呼ばれ、未承諾の広告、ポルノ、およびその他の「迷惑」メールを識別し、配信を防止するためのものです。
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。
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。
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。
本文 (メール本文)	メールのコンテンツ。

用語	説明
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。
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。
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。
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。
コンテンツフィルタ	メールに含まれる組織のポリシーなどで禁止されている嫌がらせ、中傷、セクシャルハラスメントなどの内容 (語句) を検索することです。
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。
DNS (Domain Name System)	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 (Domain Name System) 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。
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。

用語	説明
ドメイン名	ローカルホスト名とドメイン名 (tellsital.com など) から成るシステムの完全名。 ドメイン名は、インターネット上にあるすべてのホストについて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。
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。
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。
使用許諾契約書 (EULA)	使用許諾契約書 (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、ユーザ側の制限の概要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中止されます。 フリーソフトウェアのインストール時に表示される EULA に安易に「同意する」ことによって、意図しない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があります。

用語	説明
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。スパムメールが届くと、システムは InterScan であらかじめ定義されているスパムメールフィルタルールに従って、メール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。
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。
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。
FTP (File Transfer Protocol)	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。 詳細については、Network Working Group の RFC 959 を参照してください。
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。
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。
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。スパイウェア、アドウェア、ダイヤラー、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。
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。

用語	説明
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。
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解決策。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。
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。
外部受信	ネットワーク内にルーティングされるメール。
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。
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)。
Java の不正コード	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。
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。
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。

用語	説明
ライセンス	InterScan for Microsoft Exchange 製品を使用するための法的な使用許諾。
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。
製品の種類	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 (「スタンダードサポート」) 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。
マスメーリング型ウイルス	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。
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。
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。
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。

用語	説明
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) とも呼ばれ、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受けられるように、一連の厳しいテストをパスしています。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。
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フローが発生し、コンピュータがフリーズしたり再起動したり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。
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。
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。
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。

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。
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。
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。
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。
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。

用語	説明
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。
テストウイルス	本物のウイルスのように動作し、セキュリティリスク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。
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。
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。
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。
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。
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。
迷惑メール	「スパムメール」を参照してください。

用語	説明
ウイルス	コンピュータウイルスはプログラム (実行可能なコード) で、特有の感染能力があります。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。
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。
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。
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。

索引