TREND MICRO™

ウイルスバスター™ ビジネスセキュリティ 10.0

Service Pack 1

管理者ガイド

※注意事項

複数年契約について

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

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

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

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、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、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

P/N: WFEM108677_190617_JP_R4 (2024/02)

目次

はじめに

第 1 章：ウイルスバスター ビジネスセキュリティについて

第 2 章：使用の開始

第 3 章：エージェントのインストール

第 4 章：デバイスの管理

第 6 章：検索の管理

第 7 章：アップデートの管理

第 8 章：最新ステータスの利用

第 12 章：管理タスクの実行

第 13 章：管理ツールの使用

付録 D：製品の用語と概念

索引

はじめに

『ウイルスバスター ビジネスセキュリティ 管理者ガイド』にようこそ。このドキュメントでは、使用開始にあたっての情報、ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) エージェントのインストール手順、およびビジネスセキュリティサーバとエージェントの 管理について説明します。

ビジネスセキュリティのドキュメント

ビジネスセキュリティ のドキュメントには次のものがあります。

表 1. ビジネスセキュリティのドキュメント

ドキュメント	説明
インストールガイド	ビジネスセキュリティサーバのインストール要件と手順、およびサーバとエージェントのアップグレード要件と手順について説明しているドキュメントです (PDF または冊子)。
管理者ガイド	使用開始にあたっての情報、エージェントのインストール手順、およびビジネスセキュリティサーバとエージェントの管理について説明しているドキュメントです (PDF)。
ヘルプ	WebHelp (HTML ファイル) で、「使用方法」、使用に関するアドバイス、およびフィールド固有の情報を提供します。
Readme ファイル	既知の問題のリストと基本的なインストール手順が含まれています。ヘルプや印刷されたドキュメントには記載されていない最新の製品情報が含まれている場合もあります。
製品 Q&A	問題の解決策およびトラブルシューティング情報を提供するオンラインデータベースです。製品の既知の問題に関する最新情報を参照できます。製品 Q&A には、次の Web サイトからアクセスできます。 http://tmqa.jp/biz

最新版の PDF ドキュメントと Readme は次のサイトからダウンロードできます。

http://tmqa.jp/biz10_dlcenter

対象読者

ビジネスセキュリティ のドキュメントは、次のユーザを対象としています。

- セキュリティ 管理者: ビジネスセキュリティサーバおよびエージェントのインストールと管理をはじめ、ビジネスセキュリティ の管理責任を持つユーザ。 これらのユーザには、ネットワークとサーバ管理に関する高度な知識を備えていることが求められます。

- エンドユーザ: コンピュータにセキュリティエージェントがインストールされているユーザ。個々のコンピュータスキルのレベルは初心者から上級者まで広範にわたります。

ドキュメントの表記規則

情報を簡単に見つけ理解できるように、ビジネスセキュリティ のドキュメントでは次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記規則	説明
 注意	設定に関する注意事項または推奨事項を示します。
 ヒント	ベストプラクティス情報およびトレンドマイクロの推奨事項を示します。
 警告!	ネットワーク上のコンピュータに害を及ぼす可能性のあるアクティビティについて 警告を示します。

第 1 章

ウイルスバスター ビジネスセキュリティについて

本章では、ウイルスバスタービジネスセキュリティ (以下、ビジネスセキュリティ) の概要について説明します。

ビジネスセキュリティの概要

ビジネスセキュリティは、データや個人情報の盗難、危険な Web サイトから中小企業のユーザおよび資産を保護します。

ビジネスセキュリティは、Trend Micro Smart Protection Network を備えることにより、次の点が強化されています。

- 安全性 — ウイルス、スパイウェア、および Web からの脅威がクライアントに到達しないよう阻止します。URL フィルタによって、危険な Web サイトへのアクセスがブロックされ、ユーザの生産性向上に役立ちます。
- 高性能 — 迅速な検索と継続的なアップデートにより、新しい脅威を阻止してクライアントに対する影響を最小限に抑えます。
- 利便性 — インストールが簡単で、管理の必要性がありません。ビジネスセキュリティは脅威をより効率的に検出するため、ユーザはセキュリティ以外の業務に専念できます。

新機能

次の表に、ビジネスセキュリティの本リリースの新機能と拡張機能を示します。

機能/拡張機能	説明
アグレッシブ検索	ビジネスセキュリティにアグレッシブ検索が追加され、さらに詳細な検索および感染したデバイスのクリーンナップが可能になりました。 詳細については、64 ページの「デバイスツリーを使用する」および 66 ページの「デバイスコマンドを使用する」を参照してください。
ファイルレスマルウェア対策の強化	ファイルレス攻撃からエンドポイントを保護するために、ビジネスセキュリティに最新のファイルレスマルウェア対策技術が導入されました。

機能/拡張機能	説明
OS のサポート	ビジネスセキュリティでは、次の OS へのビジネスセキュリティサーバおよびエージェントのインストールがサポートされるようになりました。 • Windows 10 May 2019 Update • Windows Server 2019

主要機能と利点

ビジネスセキュリティには、次の機能と利点があります。

Trend Micro Smart Protection Network

Trend Micro Smart Protection Network は、顧客をセキュリティリスクや Web の脅威から保護する目的で設計された、次世代のクラウドクライアント型コンテンツセキュリティ基盤です。オンプレミスのソリューションとトレンドマイクロのホステッドソリューションの両方の機能を強化して、企業ネットワーク内、自宅、または外出先などどこでもユーザを保護します。Smart Protection Network は、軽量クライアントを使用して、独自のインターネットクラウドで提供されているメールレピュテーション、Web レピュテーション、およびファイルレピュテーションの相関分析テクノロジおよび脅威データベースにアクセスします。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ顧客の保護機能が自動的に更新および強化され、ユーザにとってのリアルタイムのネイバーフッドウォッチ (近隣監視活動) 保護サービスが形成されます。

Trend Micro Smart Protection Network 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サービス

ファイルレピュテーションサービスでは、大規模なクラウド型データベースを照合して、各ファイルの評価情報が確認されます。不正プログラムに関する情報がクラウドに保存されるため、すべてのユーザが即座に利用できます。高性能のコンテンツ配信ネットワークおよび社内ネットワーク内のスキャン

サーバによって、確認プロセス時の遅延が最小限に抑えられます。このクラウドクライアントアーキテクチャによって、より迅速な保護が実現され、クライアント全体のフットプリントが大幅に軽減されるとともにパターンファイル配信の負担が取り除かれます。

セキュリティエージェントでファイルレピュテーションサービスを使用する場合は、スマートスキャンモードにする必要があります。このドキュメントでは、このようなエージェントをスマートスキャンエージェントと呼んでいます。スマートスキャンモードでないエージェントは、ファイルレピュテーションサービスを使用せず、従来型スキャンエージェントと呼ばれます。ビジネスセキュリティの管理者は、すべてまたはいくつかのエージェントをスマートスキャンモードに設定できます。

Web レピュテーションサービス

トレンドマイクロの Web レピュテーションテクノロジでは、世界最大級のドメインレピュテーションデータベースを使用して、Web サイトの古さ、位置の履歴的変化、および不正プログラム挙動分析から検出される不審な活動の兆候などの要素に基づいて、レピュテーションスコアを割り当てることによって、Web ドメインの信用性が探知されます。また、引き続きサイトが検索され、感染サイトにユーザがアクセスしないようブロックされます。Web レピュテーション機能により、ユーザがアクセスするページが安全で、不正プログラム、スパイウェア、およびユーザをだまして個人情報を入力させるよう設計されたフィッシング詐欺といった Web からの脅威が存在しないことを確認できます。正確性を向上し、誤検出を減らすために、Web レピュテーションテクノロジでは、サイト全体を分類してブロックするのではなく、サイト内の特定のページやリンクにレピュテーションスコアが割り当てられます。これは、多くの場合、正規サイトの一部のみがハッキングされていて、レピュテーションが時間の経過とともに動的に変化する可能性があるためです。

Web レピュテーションポリシーの対象となるセキュリティエージェントは、Web レピュテーションサービスを使用します。ビジネスセキュリティの管理者は、すべてまたは一部のセキュリティエージェントを Web レピュテーションポリシーの対象にすることができます。

スマートフィードバック

トレンドマイクロスマートフィードバックは、トレンドマイクロのテクノロジおよび 24 時間体制の TrendLabs の運用によって、トレンドマイクロの製品

間での継続的な情報交換を実現しています。ユーザの 1 回の定期的なレピュテーションチェックによって新しい脅威が特定されるたびに、トレンドマイクロの脅威に関するデータベースがすべて自動的にアップデートされ、これ以降ユーザで所定の脅威が発生することがないようブロックされます。

顧客およびパートナーの広範囲にわたる世界的なネットワークを通して収集された脅威に関する情報を継続的に処理することによって、トレンドマイクロは、最新の脅威に対して自動的なリアルタイムの保護を提供し、住民を保護するために地域で行われる自動化された自警組織と同様に、「団結」することによるセキュリティの強化を実現しています。脅威に関して収集される情報は、特定の通信のコンテンツではなく、送信元の評価に基づいています。

トレンドマイクロに送信される情報のサンプルを次に示します。

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

プログラムへの参加は、Web コンソールからいつでも終了できます。

詳細については、218 ページの「スマートフィードバックプログラムに参加する」を参照してください。

ヒント

ご使用のエンドポイントを保護するためにスマートフィードバックに参加することは必須ではありません。参加は任意であり、いつでも参加の取り消しができます。トレンドマイクロ製品のすべてのお客さまに対する全体的な保護の強化に役立つので、スマートフィードバックへの参加をお勧めします。

Trend Micro Smart Protection Network 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

URL フィルタ

URL フィルタを使用すると、Web サイトへのアクセスを制御して、従業員の非生産的な時間を削減し、インターネット帯域幅の使用率を軽減して、より安全なインターネット環境を確立できます。URL フィルタの保護レベルを選択したり、スクリーニングを行う Web サイトの種類をカスタマイズしたりできます。

保護機能

次の表は、ビジネスセキュリティのさまざまなコンポーネントが、各種の脅威からコンピュータをどのように保護しているのかを示しています。

表 1-1. 保護機能

セキュリティ上の脅威	保護
ウイルス/不正プログラム – ウイルス、トロイの木馬、ワーム、バックドア、ルートキット スパイウェア/グレーウェア – スパイウェア、ダイヤラ、ハッキングツール、パスワード解析アプリケーション、アドウェア、ジョークプログラム、キーロガー	ファイルベースの検索 (リアルタイム検索、手動検索、予約検索)
メールメッセージを介して送信されるセキュリティ上の脅威	セキュリティエージェントでの POP3 メール検索
ネットワークワーム/ウイルスおよび侵入	セキュリティエージェントのファイアウォール
有害と考えられる Web サイト/フィッシングサイト	セキュリティエージェントの Web レピュテーションおよび URL フィルタ
USB などの外部デバイスを介して広がるセキュリティ上の脅威	セキュリティエージェントのデバイスコントロール
不正挙動	セキュリティエージェントの挙動監視
エンドポイント上の文書を標的とするランサムウェアプログラム	セキュリティエージェントの挙動監視と機械学習型検索

脅威について

インターネット上にはさまざまな脅威が存在します。効果的なセキュリティ対策を実現するには、脅威についての理解も必要です。

ウイルスと不正プログラム

ウイルス/不正プログラムの数は何万にも上り、その数は日々増え続けています。以前は一般的に DOS または Windows が攻撃されていましたが、今日のコンピュータウイルスは、企業のネットワーク、メールシステム、Web サイトの脆弱性を悪用することによって、莫大な損害を引き起こすことがあります。

- ジョークプログラム:ウイルスに似たプログラムで、多くの場合コンピュータのモニタの表示内容を操作します。
- 潜在的なウイルス/不正プログラム:ウイルス/不正プログラムの何らかの特徴を持つ不審ファイルです。詳細については、次の場所からトレンドマイクロの脅威データベースを参照してください。

  https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/
- ルートキット:ユーザが同意も認識もしないうちにシステムにインストールされ実行される、1 つのプログラムまたはプログラムの集合です。このプログラムは、コンピュータ上に検出されずに常駐するために、ステルス技術を使用します。ルートキットはコンピュータに影響を与えませんが、不正コードを実行するための検出されない環境を作り出すことを目的とします。ルートキットは、不正プログラムの実行時に、または不正な Web サイトを閲覧しただけで、ソーシャルエンジニアリングによりシステムにインストールされます。いったんインストールされると、攻撃者はリモートアクセスや傍受を行ったり、プロセス、ファイル、レジストリキーや通信チャネルを隠すといったあらゆる機能をシステム上で実行できるようになります。
- トロイの木馬:この種類の脅威は、多くの場合ポートを使用してコンピュータに侵入し、プログラムを実行します。トロイの木馬プログラムは自己増殖はしませんが、システムに常駐し、ハッカーが侵入できるようにポートを開くなどの不正処理を実行します。従来のウイルス対策ソリューションでは、ウイルスの検出と駆除はできますが、トロイの木馬 (特に、システム上ですでに実行されているもの) の検出/駆除はできません。

- ウイルス:自己増殖するプログラムです。ウイルスは別のプログラムファイルに寄生することによって増殖し、次のようなホストプログラムの実行に付随して動作します。
  - ActiveX 不正コード:Web ページに内在し、ActiveX™コントロールを実行するコードです。
  - システム領域感染型ウイルス:パーティションまたはディスクのシステム領域に感染するウイルスです。
  - COM および EXE ファイル感染型ウイルス:.com または.exe 拡張子を持つ実行可能プログラムです。
  - Java 不正コード:OS 独自のウイルスで、Java™で書かれ、埋め込まれています。
  - マクロウイルス:多くの場合ドキュメントに組み込まれている、アプリケーションマクロとしてエンコードされたウイルスです。
  - パッカー:圧縮、暗号化、またはその両方が適用された Windows または Linux™の実行可能プログラムを指し、その多くのものはトロイの木馬プログラムです。実行可能ファイルの圧縮によって、ウイルス対策製品でのパッカーの検出がより難しくなります。
  - 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索可能な、実行機能を持たないファイルです。EICAR テストスクリプトなどのテストウイルスを使用して、ウイルス対策製品が正常に機能しているかどうかを検証できます。
  - VBScript、JavaScript または HTML ウイルス:Web ページ上に存在し、ブラウザからダウンロードされるウイルスです。
  - ワーム:多くの場合メールを介して、自己またはその一部の動作可能なコピーを他のコンピュータシステムにばらまくことができる自己完結型プログラムまたはプログラムセットです。
  - その他:上記のどの種類にも該当しないウイルス/不正プログラムです。

スパイウェアとグレーウェア

エンドポイントは、ウイルス/不正プログラム以外の潜在的な脅威からの危険性にもさらされています。スパイウェア/グレーウェアはウイルスやトロイの

木馬とは異なりますが、不正な処理を実行する可能性のあるソフトウェアです。ネットワーク上のクライアントのパフォーマンスに悪影響を与えたり、セキュリティ、機密性、および法律に関する重大なリスクを企業に与える可能性があります。多くの場合、スパイウェア/グレーウェアは、煩わしいポップアップウィンドウの表示、ユーザのキー入力の記録、クライアントの脆弱性を露呈させ攻撃を受けやすくするなど、さまざまな好ましくない脅威につながる動作を実行します。

種類	説明
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、第三者に送信します。
アドウェア	広告を表示して、ユーザの Web サーフィンの嗜好などのデータを収集します。このデータは、Web ブラウザによるそのユーザへの広告内容の設定に使用されることがあります。
ダイヤラ	クライアントのインターネット設定を変更し、あらかじめ設定された電話番号にクライアントからモデム経由でダイヤルするよう強制します。この番号は、多くの場合、ペイパーコール (pay-per-call) や国際電話の番号となっており、企業に多大な費用を負わせる可能性があります。
ジョークプログラム	CD-ROM トレイの開閉、多数のメッセージボックスを表示するなどクライアントに異常な挙動をさせます。
ハッキングツール	ハッカーがコンピュータに入るのを助けます。
リモートアクセスツール	ハッカーがリモートアクセスしてコンピュータをコントロールするのを助けます。
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やパスワードを解読するのを助けます。
その他	上記のどの種類にも該当しないスパイウェア/グレーウェアです。

スパムメール

スパムメールとは、複数のメーリングリスト、個人、またはニュースグループに一方的に送信されるメール (迷惑メール) のことで、商業目的のものも多数あります。スパムメールには 2 種類あり、1 つは一方的に送信される宣伝用

メールメッセージ、もう 1 つは一方的に送信される大量のメールメッセージです。

侵入

侵入とは、ネットワークまたはクライアントに力ずくで、または許可を得ずに入り込むことを指します。ネットワークまたはクライアントに対するセキュリティを避けることを意味する場合もあります。

不正挙動

不正挙動とは、ソフトウェアが、OS、レジストリエントリ、他のソフトウェア、またはファイルおよびフォルダを許可なく変更することを指します。

Web からの脅威

Web からの脅威には、インターネットで発生する広範囲にわたる脅威が含まれます。Web からの脅威はその手法が巧妙化しており、単独のファイルや手法ではなく、さまざまなファイルやテクニックが併用されています。たとえば、Web からの脅威の作成者は、使用するバージョンや亜種を絶えず変えています。Web からの脅威は、感染したクライアント上ではなく Web サイトの一定の場所に存在するため、作成者は検出を逃れるために定期的にそのコードを変更しています。

かつて、ハッカー、ウイルスライター、スパムメール送信者、スパイウェア作成者と呼ばれていた人たちは、最近ではサイバー犯罪者と呼ばれるようになりました。Web からの脅威は、このような犯罪者が 2 つの目的のいずれかを達成するために利用されます。目的の 1 つは、今後の営業に関する情報を盗難することです。これにより、個人情報の損失という形で、機密情報の漏えいが発生します。また、感染したクライアントは、フィッシング攻撃やその他の情報収集活動を拡大するための媒介物として利用される場合もあります。さらに、この脅威によって、Web 商取引での信用を喪失し、インターネット取引に必要な信頼関係が崩壊してしまう危険性もあります。第 2 の目的は、ユーザの CPU の処理能力を奪い取って、金儲け活動の道具として利用することです。この活動には、分散型のサービス拒否攻撃やペイパークリック活動という形を取った、スパムメールの送信や支払いの強要などがあります。

第 2 章

使用の開始

本章では、ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) を起動して実行する方法について説明します。

ビジネスセキュリティネットワーク

ビジネスセキュリティは次のコンポーネントで構成されます。

- 12 ページの「ビジネスセキュリティサーバ」
- 14 ページの「エージェント」
- 14 ページの「Web コンソール」

ビジネスセキュリティサーバ

ビジネスセキュリティの中核になるのはビジネスセキュリティサーバです。ビジネスセキュリティサーバは Web コンソールをホストします。この Web コンソールは、ビジネスセキュリティを集中管理する Web ベースのコンソールです。ビジネスセキュリティサーバは、エージェントをネットワーク上のクライアントにインストールし、エージェント/サーバの関係を形成します。ビジネスセキュリティサーバでは、セキュリティステータス情報の表示、エージェントの表示、システムセキュリティの設定、およびコンポーネントのダウンロードを集中管理できます。ビジネスセキュリティサーバにはデータベースも配置されており、エージェントから報告されたインターネット脅威の検出ログがこのデータベースに格納されます。

ビジネスセキュリティサーバには次の重要な機能があります。

- コンピュータにエージェントをインストールし、監視および管理します。
- エージェントが必要とするコンポーネントをダウンロードします。ビジネスセキュリティサーバは、初期設定で、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てエージェントに配信します。

スキャンサーバ

ビジネスセキュリティサーバにはスキャンサーバと 呼ばれるサービスがあり、ビジネスセキュリティサーバのインストール 時に自動的にインストールされます。このため、別途インストールする必要はありません。スキャンサーバは、`iCRCService.exe` という名前のプロセスで実行され、Microsoft 管理コンソールには Trend Micro Smart Scan Service と表示されます。

セキュリティエージェントがスマートスキャンという検索方法を使用しているとき、スキャンサーバが、このエージェントで検索をより効率良く実行できるように支援します。スマートスキャンプロセスの説明を次に示します。

- セキュリティエージェントは、従来のウイルスパターンファイルの軽量版であるスマートスキャンエージェントパターンファイルを使用してクライアントでセキュリティ上の脅威を検索します。スマートスキャンエージェントパターンファイルには、ウイルスパターンファイルにある脅威のシグネチャのほとんどが含まれています。
- 検索時にファイルのリスクを特定できない場合、セキュリティエージェントはスキャンサーバに検索クエリを送信して、リスクを検証します。スキャンサーバは、スマートスキャンパターンファイルを使用してリスクを検証します。このパターンファイルにはスマートスキャンエージェントパターンファイルにない脅威のシグネチャが含まれています。
- セキュリティエージェントは、検索のパフォーマンスを向上するために、スキャンサーバにより提供される検索クエリの結果を「キャッシュ」します。

スキャンサーバは、脅威の定義の一部を保持することで、セキュリティエージェントでのコンポーネントのダウンロードによる帯域幅の消費を削減します。ウイルスパターンファイルをダウンロードする代わりに、セキュリティエージェントでは、大幅にサイズが削減されたスマートスキャンエージェントパターンファイルをダウンロードします。

セキュリティエージェントがスキャンサーバに接続できない場合、スキャンサーバと同じ機能を持つ Trend Micro Smart Protection Network に検索クエリを送信します。

ビジネスセキュリティサーバからスキャンサーバを個別にアンインストールすることはできません。スキャンサーバを使用する必要がない場合は、次の手順を実行します。

1. ビジネスセキュリティサーバコンピュータで、Microsoft 管理コンソールを開き、Trend Micro Smart Scan Service を無効にします。
2. Web コンソールで、[管理] > [グローバル設定] > [デスクトップ/サーバ] タブに移動し、[スマートスキャンサービスを無効にする] オプションを選択して、セキュリティエージェントを従来型スキャンに切り替えます。

エージェント

エージェントはセキュリティ上の脅威からクライアントを保護します。クライアントには、デスクトップおよびサーバが含まれます。ビジネスセキュリティエージェントは次のとおりです。

表 2-1. ビジネスセキュリティエージェント

エージェント	説明
セキュリティエージェント	デスクトップとサーバをセキュリティ上の脅威および侵入から保護します。

エージェントはレポートを作成し、そのエージェントのインストール元となるビジネスセキュリティサーバにレポートを送信します。エージェントは、イベントのステータス情報をリアルタイムでビジネスセキュリティサーバに送信し、最新のクライアント情報を提供します。エージェントがレポートするイベントは、脅威の検出、起動、停止、検索の開始、アップデートの完了などです。

Web コンソール

Web コンソールは、企業ネットワーク全体におけるセキュリティエージェント監視の中枢です。このコンソールの初期設定と初期値は、セキュリティ要件や仕様に応じて変更できます。Web コンソールでは、Java、CGI、HTML、HTTP などの標準的なインターネット技術が使用されています。

Web コンソールを使用して、次のタスクを実行できます。

- セキュリティエージェントをエンドポイントにインストールする。
- 同時設定や同時管理を目的として、エージェントを論理グループ化する。
- エンドポイントに対してウイルス検索およびスパイウェア検索を設定し、手動検索を開始する。
- 脅威に関連した活動についての通知を受信したり、ログレポートを表示したりする。
- エンドポイントで脅威が検出された場合は、通知を受信し、メールメッセージ、SNMP トラップ、または Windows イベントログを介してウイルス大規模感染の警告を送信する。

Web コンソールを開く

Web コンソールは、ネットワーク上の任意のエンドポイントからサポート対象の Web ブラウザを使用して開くことができます。ブラウザの要件の詳細については、システム要件を参照してください。

https://www.trendmicro.com/ja_jp/small-business/worry-free-standard.html#requirement

手順

1. Web コンソールを開くには、次のいずれかの方法を使用します。
   - ビジネスセキュリティサーバをホストするエンドポイント上で、デスクトップに移動してビジネスセキュリティのショートカットをクリックします。
   - ビジネスセキュリティサーバをホストするエンドポイント上で、Windows の [スタート] メニュー > [ウイルスバスター ビジネスセキュリティサーバ] > [ビジネスセキュリティ] の順にクリックします。
   - ネットワーク上の任意のエンドポイントで、Web ブラウザを開いてアドレスバーに次のアドレスを入力します。

     `https://{ビジネスセキュリティサーバ名または IP アドレス}:{ポート番号}/SMB`

     例を以下に示します。

     `https://my-test-server:4343/SMB`

     `https://192.168.0.10:4343/SMB`

     `http://my-test-server:8059/SMB`

     `http://192.168.0.10:8059/SMB`

ヒント

SSL を使用していない場合は、「`https`」ではなく「`http`」と入力します。ポートの初期設定値は、HTTP 接続の場合は 8059、HTTPS 接続の場合は 4343 です。

DNS によるサーバ名の解決ができない環境では、IP アドレスの代わりにサーバ名を使用してください。

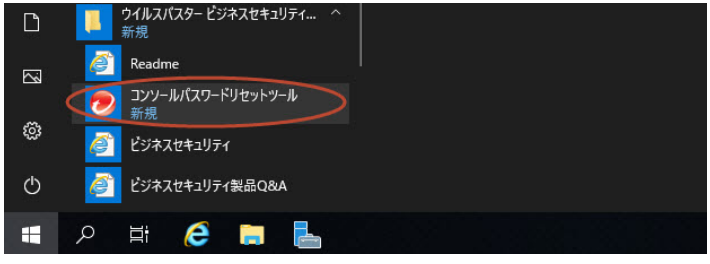
ブラウザにビジネスセキュリティ のログオン画面が表示されます。

2. パスワードを入力して、[ログオン] をクリックします。

   ブラウザに、[最新ステータス] 画面が表示されます。

次に進む前に

Web コンソールにアクセスできない場合は、次のことを確認してください。

確認項目	詳細
パスワード	パスワードを忘れた場合は、コンソールパスワードリセットツールを使用してパスワードをリセットしてください。このツールには、Windows [スタート] メニューの [ウイルスバスター ビジネスセキュリティサーバ] フォルダにあるビジネスセキュリティサーバからアクセスします。 

確認項目	詳細
ブラウザのキャッシュ	以前のバージョンのビジネスセキュリティからアップグレードした場合は、Web ブラウザおよびプロキシサーバのキャッシュファイルが原因で Web コンソールをロードできないことがあります。ブラウザのキャッシュファイルをクリアしてください。また、Web コンソールへのアクセスに使用するエンドポイントとビジネスセキュリティサーバとの間にプロキシサーバが設定されている場合は、プロキシサーバのキャッシュファイルもクリアしてください。
SSL 証明書	Web サーバが正常に機能していることを確認します。SSL を使用する場合は、SSL 証明書が有効であることも確認します。詳細については、Web サーバのドキュメントを参照してください。

確認項目	詳細
仮想ディレクトリの設定	Web コンソールを IIS サーバ上で実行しているときに、次に示すメッセージが表示される場合は、仮想ディレクトリの設定に問題がある可能性があります。 ページを表示できません。 HTTP エラー 403.1 - 許可されていません:実行のアクセスが拒否されました。 インターネット インフォメーション サービス (IIS) このメッセージは、次のいずれかのアドレスを使用して Web コンソールにアクセスしたときに表示される可能性があります。 http://{サーバ名}/SMB/ http://{サーバ名}/SMB/default.htm ただし、次のアドレスを使用した場合には、Web コンソールは問題なく開きます。 http://{サーバ名}/SMB/console/html/cgi/cgichkmasterpwd.exe この問題を解決するには、SMB 仮想ディレクトリの実行アクセス許可を確認してください。 スクリプトを実行できるようにするには 1. インターネット インフォメーション サービス (IIS) マネージャを起動します。 2. SMB 仮想ディレクトリで、[プロパティ] を選択します。 3. [仮想ディレクトリ] タブを選択し、[なし] から [スクリプト] に実行アクセス許可を変更します。クライアントのインストール仮想ディレクトリの実行アクセス許可も変更します。

Web コンソールのナビゲーション

Web コンソールには、次の主要なセクションがあります。

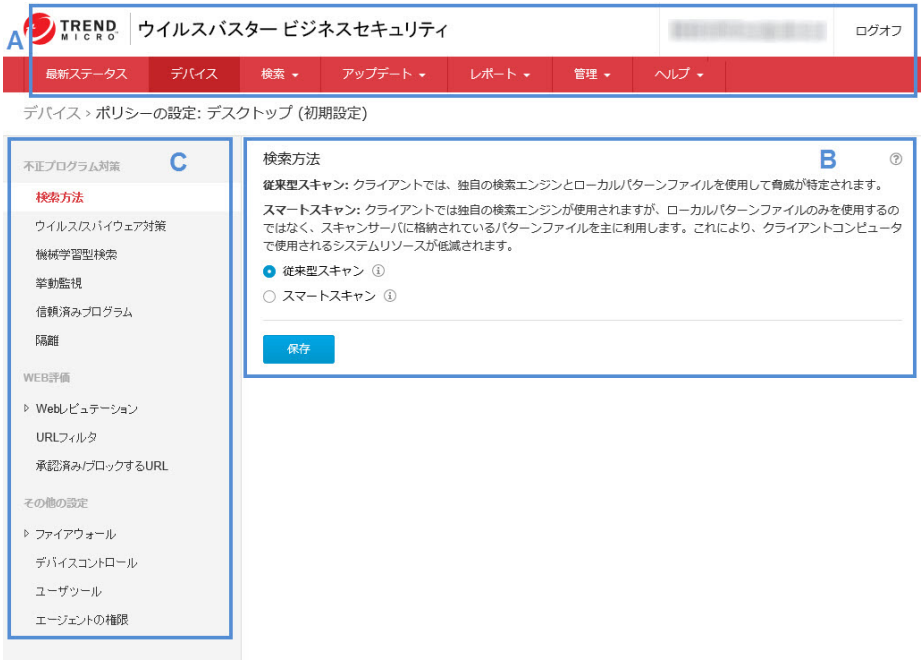


表 2-2. Web コンソールの主なセクション

セクション	説明
A. メインメニュー	Web コンソールの最上部に表示されるのがメインメニューです。 [ログオフ] をクリックすると、現在のセッションを終了できます。
B. 設定領域	メインメニュー項目の下には設定領域が表示されます。この領域では、選択したメニュー項目に応じて設定を行います。

セクション	説明
C. メニューサイドバー (一部の画面上のみ)	[デバイス] 画面でセキュリティエージェントのグループを 選択し、[ポリシーの設定] をクリックすると、メニューサイドバーが表示されます。このサイドバーを使用して、そのグループに属するデスクトップとサーバのセキュリティおよび検索を設定します。

表 2-3. メインメニューセクション

メニュー項目	説明
最新ステータス	セキュリティエージェントの全体的なセキュリティ状況とビジネスセキュリティサーバの動作状況を監視します。
デバイス	• エージェントのセキュリティ設定をカスタマイズします。 • グループ間の設定を複製します。
検索	• エンドポイントで脅威を検索します。 • 時間を指定した検索を設定できます。
アップデート	• トレンドマイクロのアップデートサーバ (またはその他のアップデート元) に、最新のコンポーネント (ウイルスパターンファイル、検索エンジン、クリーンナップコンポーネント、エージェントプログラムなど) があるかどうかを調べます。 • アップデート元を設定します。 • セキュリティエージェントをアップデートエージェントとして設定します。
レポート	脅威およびその他のセキュリティ関連のイベントを追跡するレポートを生成します。

メニュー項目	説明
管理	• 脅威またはシステムに関連した異常なイベント発生についての通知を設定します。 • プロキシサーバやメールサーバなどといった、ビジネスセキュリティ全般に関連する設定項目があります。 • ネットワークおよびクライアントのセキュリティの管理に役立つ管理ツールに関する情報を表示します。 • 製品ライセンス情報の表示、管理者パスワードの設定、およびスマートフィードバックプログラムへの参加の可否などを設定します。 • 新しい修正プログラムが利用可能になったときに製品に自動的に適用してユーザに通知します。
ヘルプ	• 特定の目次やトピックを検索します。 • 管理者ガイドを表示します。 • 製品 Q&A の最新情報にアクセスします。 • セキュリティ情報、購入情報、テクニカルサポート、およびバージョン情報を表示します。

Web コンソールのアイコン

次の表は、Web コンソールに表示されるアイコンとその用途を示しています。

表 2-4. Web コンソールのアイコン

アイコン	説明
	[ヘルプ] アイコン。オンラインヘルプを開きます。
	[表示更新] アイコン。現在の画面の情報を更新します。
	セクションの展開と折り畳みアイコン。セクションの表示または非表示を切り替えます。一度に展開できるセクションは 1 つのみです。
	[情報] アイコン。特定の項目に関連する情報を表示します。
	[通知のカスタマイズ] アイコン。さまざまな通知オプションを表示します。

第 3 章

エージェントのインストール

本章では、セキュリティエージェントのインストールに必要な手順について説明します。また、これらのエージェントの削除についても説明します。

セキュリティエージェントのインストール

Windows クライアント (デスクトップおよびサーバ) にセキュリティエージェントの新規インストールを実行します。要件に合ったインストール方法を使用してください。

セキュリティエージェントのインストールを開始する前に、クライアント上で起動中のアプリケーションをすべて終了してください。他のアプリケーションの実行中にインストールした場合、インストールプロセスに通常より長い時間がかかることがあります。

注意

このバージョンへのセキュリティエージェントのアップグレードについては 、『インストールガイド』を参照してください。

セキュリティエージェントのインストール要件

インストール要件および互換性のあるサードパーティ製品の全リストについては、次の Web サイトを参照してください。

https://www.trendmicro.com/ja_jp/small-business/worry-free-standard.html#requirement

セキュリティエージェントのインストールに関する考慮事項

セキュリティエージェントをインストールする 前に、次の点について考慮してください。

- エージェントの機能: セキュリティエージェントの機能の一部は、Windows プラットフォームによっては使用できません。詳細については、25 ページの「使用可能なセキュリティエージェントの 機能」を参照してください。
- 64 ビットプラットフォーム : セキュリティエージェントは、64 ビットプラットフォームで使用できます。しかし、現在 IA-64 プラットフォームでは使用できません。
- IPv6 のサポート: セキュリティエージェントは、デュアルスタックまたはシングルスタックの IPv6 エンドポイントにインストールできます。た

だし、インストール方法によっては特別な要件が適用される場合があります。

詳細については、27 ページの「セキュリティエージェントのインストールと IPv6 のサポート」を参照してください。

- 除外リスト: 次の機能の除外リストが適切に設定されていることを確認してください。
  - 挙動監視: 重要なクライアントアプリケーションは、セキュリティエージェントでブロックされないように承認済みプログラムリストに追加します。詳細については、91 ページの「挙動監視を設定する」を参照してください。
  - Web レピュテーション: 安全であることが判明している Web サイトは、セキュリティエージェントでアクセスをブロックされないように承認済み URL リストに追加します。詳細については、101 ページの「セキュリティエージェントの Web レピュテーションを設定する」を参照してください。
- エージェントのインストールディレクトリ : ビジネスセキュリティサーバのインストール時、セットアッププログラムでは、ィエージェントのインストールディレクトリを指定するよう求められます。このディレクトリは、初期設定では`$ProgramFiles¥Trend Micro¥Security Agent`になります。セキュリティエージェントを別のディレクトリにインストールする場合は、[管理] > [グローバル設定] > [システム] > [セキュリティエージェントのインストール] で新しいディレクトリを指定します。

使用可能なセキュリティエージェントの機能

クライアント上で使用可能なセキュリティエージェントの機能は、クライアントの OS によって異なります。エージェントを特定の OS にインストールした場合、サポートされない機能に注意してください。

表 3-1. セキュリティエージェントの機能

機能	Windows OS		
	10	SBS 2011	Server 2012/2012 R2/2016/2019
手動検索 (通常/アグレッシブ)、リアルタイム検索、および予約検索	○	○	○
ファイアウォール	○	○	○
Web レピュテーション	○	○	○
URL フィルタ	○	○	○
挙動監視	○	○	○
デバイスコントロール	○	○	○
ダメージクリーンナップサービス	○	○	○
POP3 メール検索	○	○	○
手動アップデートと自動アップデート	○	○	○
アップデートエージェント	○	○	○
プラグインマネージャ	○	○	○
スマートフィードバック	○	○	○
迷惑メール対策ツールバー	○ サポートされるメールクライアント (32 ビットおよび 64 ビット): • Outlook 2010 • Outlook 2013 • Outlook 2016	×	×

セキュリティエージェントのインストールと IPv6 のサポート

ここでは、セキュリティエージェントをデュアルスタックまたは IPv6 シングルスタッククライアントにインストールする 際の考慮事項について説明します。

OS

セキュリティエージェントは、IPv6 アドレス指定をサポートする次の OS にのみインストールできます。

- Windows SBS 2011
- Windows 10 (すべてのエディション)
- Windows Server 2012/2012 R2 (すべてのエディション)
- Windows Server 2016 (Standard、Datacenter、Essentials)
- Windows Server 2019 (Standard、Datacenter、Essentials)

システム要件の全リストについては、次の Web サイトを参照してください。

https://www.trendmicro.com/ja_jp/small-business/worry-free-standard.html#requirement

サポートされるインストール方法

利用可能なすべてのインストール方法を使用して、IPv6 またはデュアルスタッククライアントにセキュリティエージェントをインストールできます 。インストール方法によっては、セキュリティエージェントを 正常にインストールするための特別な要件があります。

表 3-2. インストール方法と IPv6 のサポート

インストール方法	要件/考慮事項
インストール用 Web ページおよびメール通知によるインストール	IPv6 シングルスタッククライアントにインストールする場合、ビジネスセキュリティサーバがデュアルスタックまたは IPv6 シングルスタックであることと、そのホスト名または IPv6 アドレスが URL の一部であることが必要です。 デュアルスタッククライアントの場合、インストール状況画面に表示される IPv6 アドレスは、[管理] > [グローバル設定] > [デスクトップ/サーバ] タブの [優先される IP アドレス] で選択した内容によって異なります。
脆弱性検索ツールおよびリモートインストール	IPv6 シングルスタックのビジネスセキュリティサーバは、IPv4 シングルスタッククライアントにセキュリティエージェントをインストールできません。同様に、IPv4 シングルスタックのビジネスセキュリティサーバは、IPv6 シングルスタッククライアントにエージェントをインストールできません。

セキュリティエージェントの IP アドレス

IPv6 アドレス指定をサポートする環境にインストールされたビジネスセキュリティサーバは、次のセキュリティエージェントを管理できます。

- IPv6 シングルスタッククライアントにインストールされたビジネスセキュリティサーバは、IPv6 シングルスタックのセキュリティエージェントを管理できます。
- デュアルスタッククライアントにインストールされ、IPv4 と IPv6 の両方のアドレスを割り当てられているビジネスセキュリティサーバは、IPv6 シングルスタック、デュアルスタック、および IPv4 シングルスタックのセキュリティエージェントを管理できます。

セキュリティエージェントは、インストールまたはアップグレード後に、IP アドレスを使用してビジネスセキュリティサーバに登録されます。

- IPv6 シングルスタックのセキュリティエージェントは、IPv6 アドレスを使用して登録されます。
- IPv4 シングルスタックのセキュリティエージェントは、IPv4 アドレスを使用して登録されます。
- デュアルスタックのセキュリティエージェントは、IPv4 または IPv6 のいずれかのアドレスを使用して登録されます。これらのエージェントで使

用する IP アドレスは、[管理] > [グローバル設定] > [デスクトップ/サーバ] タブの [優先される IP アドレス] で選択できます。

セキュリティエージェントのインストール方法

ここでは、セキュリティエージェントの新規インストールを実行するさまざまな方法の概要を説明します。すべてのインストール方法で、インストール先エンドポイントのローカル管理者権限が必要となります。

セキュリティエージェントをインストールし、IPv6 のサポートを有効にする場合は、27 ページの「セキュリティエージェントのインストールと IPv6 のサポート」のガイドラインをお読みください。

表 3-3. インストール方法

インストール方法/OS でのサポート	インストールについての考慮事項					
	WAN 経由のインストールに適している	集中管理に適している	ユーザの介入が必要	IT リソースが必要	大量インストールに適している	帯域幅の消費量
インストール用 Web ページ すべての OS でサポート	○	○	○	×	×	少ない (予約される場合)
メール通知 すべての OS でサポート	○	○	○	×	×	多い (インストールが同時に開始される場合)
リモートインストール すべての OS でサポート	×	○	×	○	○	少ない (予約される場合)

インストール方法/OS でのサポート	インストールについての考慮事項					
	WAN 経由のインストールに適している	集中管理に適している	ユーザの介入が必要	IT リソースが必要	大量インストールに適している	帯域幅の消費量
ログオンスクリプトウィザード すべての OS でサポート	×	○	×	○	○	多い (インストールが同時に開始される場合)
Client Packager すべての OS でサポート	○	×	○	○	×	少ない (予約される場合)
脆弱性検索ツール (TMVS) Windows 10 を除くすべての OS でサポート	×	○	×	○	○	少ない (予約される場合)

単一サイトにインストールする場合、または IT ポリシーが厳格に施行されている組織の場合は、リモートインストールまたはログオンスクリプトウィザードによるインストールを選択できます。

組織内で IT ポリシーがそれほど厳格に施行されていない場合は、インストール用 Web ページを使用してセキュリティエージェントをインストールすることをお勧めします。ただし、この方法では、エンドユーザに、セキュリティエージェントをインストールするための管理者権限が必要になります。

リモートインストールは、Active Directory を使用するネットワークに適しています。Active Directory を使用していない場合は、インストール用 Web ページを使用してください。

インストール用 Web ページを使用したインストール

始める前に

インストール用 Web ページを使用してインストールするには、次のことが必要です。

確認項目	要件
ビジネスセキュリティサーバ	ビジネスセキュリティサーバが、システム要件を満たしている必要があります。詳細は次の Web サイトを参照してください。https://www.trendmicro.com/ja_jp/small-business/worry-free-standard.html#requirement
対象エンドポイント	• 対象エンドポイントは、Windows 10、Windows Server 2012、2012 R2、2016、2019、または SBS 2011 にインストールされている必要があります。 • 対象エンドポイントには、Internet Explorer 9.0 以降がインストールされている必要があります。 • ユーザは、管理者アカウントを使用してエンドポイントにログオンする必要があります。 注意 対象エンドポイントがデスクトップ OS で実行されている場合は、最初にビルトイン管理者アカウントを有効にします。 詳細については、Microsoft のサポートサイト (https://msdn.microsoft.com/ja-jp/library/windows/hardware/dn898563(v=vs.85).aspx) を参照してください。

確認項目	要件
Internet Explorer のセキュリティ設定	ユーザは次の手順を実行する必要があります。 1. Internet Explorer を起動し、ビジネスセキュリティサーバの URL (`https://<ビジネスセキュリティサーバの 名前>:4343/SMB/console/html/client`) を信頼済みサイトのリストに追加します。[ツール] > [インターネット オプション] > [セキュリティ] タブの順に移動し、[信頼済みサイト] アイコンを選択して、[サイト] をクリックします。 2. [ActiveX コントロールに対して自動的にダイアログを表示] を有効にして、Internet Explorer のセキュリティ設定を変更します。[ツール] > [インターネット オプション] > [セキュリティ] タブの順に移動して、[レベルのカスタマイズ] をクリックします。
IPv6	IPv4 シングルスタック、IPv6 シングルスタック、およびデュアルスタックエンドポイントで構成される混合型の環境の場合は、すべてのエンドポイントがビジネスセキュリティサーバのインストール用 Web ページに接続できるように、ビジネスセキュリティサーバに IPv4 と IPv6 の両方のアドレスを指定する必要があります。

インストール用 Web ページからセキュリティエージェントをインストールするための次の手順をユーザに送信してください。インストール通知をメールで送信するには、54 ページの「メール通知を使用したインストール」を参照してください。

手順

1. 管理者アカウントでエンドポイントにログオンします。
2. Internet Explorer を起動して、次のいずれかを入力します。
   - SSL を使用するビジネスセキュリティサーバ:

     `https://<ビジネスセキュリティサーバの 名前または IP アドレス>:4343/SMB/console/html/client`
   - SSL を使用しないビジネスセキュリティサーバ:

     `http://<ビジネスセキュリティサーバの 名前または IP アドレス>:8059/SMB/console/html/client`
3. [インストール] をクリックして、セキュリティエージェントのインストールを開始します。

インストールが開始します。ActiveX コントロールのインストールを求めるメッセージが表示されたら、インストールを許可します。インストール後、Windows のタスクバーにセキュリティエージェントのアイコンが表示されます。

注意

Windows タスクバーに表示されるアイコンのリストについては、234 ページの「セキュリティエージェントのステータスを確認する」を参照してください。

次に進む前に

インストール用 Web ページからインストールできないとユーザから報告があった場合は、次の方法を試します。

- ping コマンドおよび telnet コマンドを使用してエンドポイント/サーバ間が接続されているかどうかを確認します。
- エンドポイントで TCP/IP が有効になっているか、またその設定が正しいかを確認します。
- エンドポイント/サーバ間の通信にプロキシサーバを使用している場合は、プロキシ設定が正しいかどうかを確認します。
- Web ブラウザで、トレンドマイクロのアドオンおよび表示履歴を削除します。

ログオンスクリプトウィザードによるインストール

ログオンスクリプトウィザードを使用すると、ウイルス対策が実施されていないクライアントがネットワークにログオンした際、そのクライアントにセキュリティエージェントを自動的にインストールできます。ログオンスクリプトウィザードを実行すると、サーバのログオンスクリプトに `AutoPcc.exe` というプログラムが追加されます。

`AutoPcc.exe` は、ウイルス対策が実施されていないクライアントにセキュリティエージェントをインストールし、プログラムファイルとコンポーネントをアップデートします。ログオンスクリプトの AutoPcc を使用するには、クライアントはドメインに属している必要があります。

既存のログオンスクリプトがある場合は、ログオンスクリプトウィザードにより、AutoPcc.exe を実行するコマンドが追加されます。それ以外の場合は、AutoPcc.exe を実行するコマンドを含む ofcscan.bat というバッチファイルが作成されます。

ログオンスクリプトウィザードでは、スクリプトの末尾に次のものが追加されます。

¥¥<サーバ名>¥ofcscan¥autopcc

説明:

- <サーバ名>は、ビジネスセキュリティサーバコンピュータの 名前または IP アドレスです。
- 「ofcscan」は、ビジネスセキュリティサーバの 共有フォルダ名です。
- 「autopcc」は、セキュリティエージェントをインストールする autopcc 実行可能ファイルへのリンクです。

Windows Server のすべてのバージョンで、ログオンスクリプトは次の場所にあります (ネットログオンの共有フォルダ経由)。

¥¥Windows server¥system drive¥windir¥sysvol¥domain¥scripts ¥ofcscan.bat

---

手順

1. サーバインストールの実行に使用したコンピュータで、<ビジネスセキュリティサーバのインストールフォルダ >¥PCCSRV¥Admin を開きます。
2. SetupUsr.exe をダブルクリックします。

   ログオンスクリプトウィザードが起動します。コンソールには、ネットワーク上のすべてのドメインを示すツリーが表示されます。
3. ログオンスクリプトを変更するサーバを探して選択し、[選択] をクリックします。サーバがプライマリドメインコントローラであることと、そのサーバへの管理者のアクセス権限があることを確認してください。

   ログオンスクリプトウィザードで、ユーザ名とパスワードの入力が求められます。

4. ユーザ名とパスワードを入力します。[OK] をクリックして続行します。

   [ユーザの選択] 画面が表示されます。[ユーザ] リストには、このサーバにログオンするユーザのプロファイルが表示されます。[選択したユーザ] リストには、ログオンスクリプトを変更するユーザのプロファイルが表示されます。

5. ユーザプロファイルのログオンスクリプトを変更するには、[ユーザ] リストからユーザプロファイルを選択し、[追加] をクリックします。

6. すべてのユーザのログオンスクリプトを変更するには、[すべて追加] をクリックします。

7. すでに選択したユーザプロファイルを除外するには、[選択したユーザ] リストで名前を選択し、[削除] をクリックします。

8. 選択内容をリセットするには、[すべて削除] をクリックします。

9. 対象となるすべてのユーザプロファイルが [選択したユーザ] リストに追加されたら、[適用] をクリックします。

   サーバのログオンスクリプトが正常に変更されたことを知らせるメッセージが表示されます。

10. [OK] をクリックします。

    ログオンスクリプトウィザードが最初の画面に戻ります。

11. ログオンスクリプトウィザードを閉じるには、[終了] をクリックします。

Client Packager を使用したインストール

Client Packager は、CD-ROM などの従来型メディアを使用するユーザに送付可能なインストールパッケージを作成します。ユーザはクライアントでパッケージを実行して、セキュリティエージェントのインストールやアップグレード、およびコンポーネントのアップデートを実行します。

Client Packager は、次の場合に特に便利です。

- セキュリティエージェントまたはコンポーネントを、遠隔地にある帯域幅の狭いオフィスのクライアントにインストールする 場合
- インターネットへの接続に関して制限が設けられている環境、つまりクローズド LAN の場合やインターネット接続ができない環境の場合

Client Packager を使用してインストールされたセキュリティエージェントは、パッケージ作成元のサーバにレポートを送信します。

手順

1. ビジネスセキュリティサーバコンピュータで、<サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥ClientPackager に移動します。
2. ClnPack.exe をダブルクリックします。

   Client Packager のコンソールが開きます。
3. パッケージの作成対象の OS を選択します。パッケージは、対象となる種類の OS を実行するクライアントにのみインストールします。別の種類の OS には、別のパッケージを作成してインストールします。
4. パッケージの検索方法を選択します。

   検索方法の詳細については、83 ページの「検索方法」を参照してください。

   パッケージに含まれるコンポーネントは、選択した検索方法に応じて異なります。スマートスキャンでは、ウイルスパターンファイル以外のすべてのコンポーネントが含まれます。従来型スキャンでは、スマートスキャンエージェントパターンファイル以外のすべてのコンポーネントが含まれます。
5. 作成するパッケージの種類を選択します。

表 3-4. クライアントパッケージの種類

パッケージの種類	説明
セットアップ	[セットアップ] を選択すると、パッケージは MSI ファイルで作成されます。このファイルは、Microsoft インストーラパッケージ形式に準拠しています。このパッケージでは、セキュリティエージェントのプログラムと、ビジネスセキュリティサーバで現在使用可能なコンポーネントがインストールされます。 対象クライアントに以前のバージョンのセキュリティエージェントがインストールされており、それをアップグレードする場合は、そのエージェントを管理するビジネスセキュリティサーバから MSI ファイルを作成します。それ以外の場合、エージェントはアップグレードされません。
アップデート	[アップデート] を選択すると、ビジネスセキュリティサーバで現在使用可能なコンポーネントを含むパッケージが作成されます。このパッケージは、実行可能ファイルで作成されます。セキュリティエージェントがインストールされたクライアントで、コンポーネントのアップデートに問題がある場合、このパッケージを使用します。

6. [サイレントモード] をクリックすると、バックグラウンドでクライアントにインストールするパッケージが作成されます。バックグラウンドでのインストールは、クライアントユーザを煩わせることがなく、インストール状況ウィンドウも表示されません。このオプションは、遠隔地のクライアントにパッケージをインストールする 場合に選択します。

7. [インストール前のウイルス検索の無効化 (新規インストールのみ)] は、セキュリティエージェントをインストールする 前にクライアントで脅威の検索を実行しない場合に選択します。これは、そのクライアントが 脅威にさらされていないことが確かな場合に実行します。

   事前検索が有効な場合、セットアップでは、次に示すようなコンピュータの最も脆弱な領域でウイルスおよび不正プログラムが検索されます。

   - システム領域とシステムフォルダ (システム領域感染型ウイルスの検索)
   - Windows フォルダ
   - Program Files フォルダ

8. [ソースファイル] の横に表示されている ofcscan.ini ファイルの場所が正しいことを確認します。パスを変更するには、(...) をクリックして ofcscan.ini ファイルを参照します。初期設定で、このファイルは<サーバのインストールフォルダ>¥PCCSRV にあります。
9. [出力ファイル] で、(...) をクリックしてパッケージの作成場所を指定し、パッケージのファイル名を入力します (たとえば、ClientSetup.exe)。
10. [作成] をクリックします。

    パッケージが作成されると、「パッケージは正常に作成されました。」というメッセージが表示されます。前の手順で指定したディレクトリにパッケージがあることを確認します。

次に進む前に

パッケージをクライアントにインストールします。

クライアントの要件:

- ディスク容量
  - 従来型スキャン: 1.5GB 以上 (2GB を推奨)
  - スマートスキャン: 500MB

  パッケージの検索方法が従来型スキャンの場合は 1GB、スマートスキャンの場合は 500MB の空きディスク領域
- Windows インストーラ 4.5 以降 (MSI パッケージを実行する場合)

パッケージによるインストールのガイドライン:

- パッケージをユーザに送付して、そのファイル (.msi または.exe) をダブルクリックしてパッケージを実行するよう指示します。

  注意

  パッケージは、パッケージ作成元のサーバにレポートを送信するセキュリティエージェントのユーザにのみ送信します。
- パッケージファイルを右クリックして [管理者として実行] を選択するようにユーザに指示します。

- Active Directory を使用している場合は、各ユーザにセキュリティエージェントをインストールするよう求めなくても、.msi ファイルを使用して、セキュリティエージェントをすべてのクライアントに 同時かつ自動的にインストールできます。クライアントにログオンするユーザに関係なくセキュリティエージェントをインストールできるように、[ユーザの構成] ではなく [コンピュータの構成] を使用します。
- 新規インストールしたセキュリティエージェントがビジネスセキュリティサーバに接続できない場合、セキュリティエージェントは初期設定を保持しています。セキュリティエージェントは、ビジネスセキュリティサーバに接続する際に Web コンソールで自分のグループの設定を取得します。
- Client Packager を使用したセキュリティエージェントのアップグレードの際に問題が発生した場合は、まず前のバージョンのセキュリティエージェントをアンインストールしてから 新しいバージョンをインストールすることをお勧めします。アンインストール手順の詳細については、58 ページの「エージェントを削除する」を参照してください。

リモートインストールを使用したインストール

始める前に

ネットワークに接続された 1 台以上の遠隔地のエンドポイントにセキュリティエージェントをインストールします。

リモートインストールを 使用してインストールするには、次のことが必要です。

確認項目	要件
対象エンドポイント	• 各対象エンドポイントにログオンするには、管理者アカウントを使用します。

確認項目	要件
	注意 • 対象エンドポイントがデスクトップ OS で実行されている場合は、最初にビルトイン管理者アカウントを有効にします。 詳細については、Microsoft のサポートサイト (https://msdn.microsoft.com/ja-jp/library/windows/hardware/dn898563(v=vs.85).aspx) を参照してください。 • Windows 10 でリモートインストールを実行する場合、Microsoft アカウントで対象クライアントにログインすることはできません。 • 対象エンドポイントにビジネスセキュリティサーバがインストールされていないことを確認してください。リモートインストールでは、ビジネスセキュリティサーバをすでに実行しているエンドポイントにはセキュリティエージェントはインストールされません。
ファイルとプリンタの共有	エンドポイントで、[ファイルとプリンタの共有] を一時的に有効にします。 注意 社内のセキュリティポリシーで Windows ファイアウォールが無効になっている場合は、Remote Registry に関するセクションに進んでください。 1. コントロールパネルで Windows ファイアウォールを開きます。 2. [Windows ファイアウォールによるプログラムの許可] をクリックします。管理者パスワードまたは確認を求められたら、パスワードを入力するか、確認します。[Windows ファイアウォール設定] 画面が表示されます。 3. [例外] タブのプログラムまたはポートリストの下で [ファイルとプリンタの共有] チェックボックスがオンになっていることを確認します。 4. [OK] をクリックします。

確認項目	要件
	5. セキュリティエージェントのインストールが完了したら、必要に応じて元の設定に戻します。
ユーザーアカウント制御	ユーザーアカウント制御を無効にします。 **注意** 次のレジストリキーを変更してユーザーアカウント制御を無効にします。[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System] “EnableLUA”=dword:00000000. セキュリティエージェントのインストールが完了したら、必要に応じて元の設定に戻します。
Remote Registry	Remote Registry サービスを一時的に有効にします。 1. **注意** Microsoft 管理コンソールを起動するには、[ファイル名を指定して実行] で「`services.msc`」と入力します。 2. [Remote Registry] を右クリックして、[開始] を選択します。 3. セキュリティエージェントのインストールが完了したら、必要に応じて元の設定に戻します。
IPv6	デュアルスタックのビジネスセキュリティサーバは、セキュリティエージェントを任意のエンドポイントにインストールできます。IPv6 シングルスタックのビジネスセキュリティサーバは、IPv6 シングルスタックまたはデュアルスタックのエンドポイントにのみセキュリティエージェントをインストールできます。

手順

1. [デバイス] に移動します。
2. [デバイスの追加] をクリックします。
3. [コンピュータの種類] セクションで、[デスクトップまたはサーバ] を選択します。

4. [クライアントのインストール方法] で、[リモートインストール] を選択します。
5. [次へ] をクリックします。

   新しい画面が表示されます。
6. [グループとコンピュータ] ボックスのクライアントリストからクライアントを選択して、[追加] をクリックします。クライアントのユーザ名とパスワードを入力するよう求められます。
7. ユーザ名とパスワードを入力して、[ログオン] をクリックします。[選択したコンピュータ] リストボックスにクライアントが表示されます。
8. これらの手順を繰り返して、すべてのクライアントを [選択したコンピュータ] リストボックスに追加します。
9. [インストール] をクリックします。

   確認ボックスが表示されます。
10. [はい] をクリックして、エージェントをクライアントコンピュータにインストールすることを確認します。

    セキュリティエージェントのファイルが各クライアントにコピーされている間、進行状況画面が表示されます。

    ビジネスセキュリティサーバによるクライアントへのインストールが 完了すると、[選択したコンピュータ] リストボックスの [ステータス] フィールドにインストール状況が表示され、クライアント名に緑色のチェックマークが表示されます。

次に進む前に

リモートインストールを使用したインストールが正常に完了しない場合は、次のタスクを実行します。

- ping コマンドおよび telnet コマンドを使用してクライアント/サーバ間が接続されているかどうかを確認します。
- クライアントで TCP/IP が有効になっているか、またその設定が正しいかを確認します。
- クライアント/サーバ間の通信にプロキシサーバを使用している場合は、プロキシ設定が正しいかどうかを確認します。

- Web ブラウザで、トレンドマイクロのアドオンおよび表示履歴を削除します。

脆弱性検索ツールを使用したインストール

始める前に

インストール済みのウイルス対策製品の検出、ネットワーク上のウイルス対策が実施されていないクライアントの検索、およびセキュリティエージェントのクライアントへのインストールを行うには、脆弱性検索を実行します。

脆弱性検索ツールを使用してインストールするには、次のことが必要です。

確認項目	要件
脆弱性検索ツールの起動場所	脆弱性検索ツールは、ビジネスセキュリティサーバまたはネットワーク上の任意のクライアントで起動できます。ターミナルサーバを実行しているクライアントでは使用できません。
対象クライアント	• 対象クライアントにビジネスセキュリティサーバがインストールされていないことを確認してください。脆弱性検索ツールでは、ビジネスセキュリティサーバをすでに実行中のクライアントにはセキュリティエージェントはインストールされません。 • ユーザは、管理者アカウントを使用してクライアントにログオンする必要があります。 注意 対象クライアントがデスクトップ OS で実行されている場合は、最初にビルトイン管理者アカウントを有効にします。詳細については、Microsoft のサポートサイト (https://msdn.microsoft.com/ja-jp/library/windows/hardware/dn898563(v=vs.85).aspx) を参照してください。

脆弱性検索を実行するには、いくつかの方法があります。

- 44 ページの「手動での脆弱性検索の実行」
- 45 ページの「DHCP 検索の実行」
- 47 ページの「脆弱性検索の予約設定」

手動での脆弱性検索の実行

必要に応じて脆弱性検索を実行します。

手順

1. 脆弱性検索ツールを起動します。

脆弱性検索ツールの起動場所	手順
ビジネスセキュリティサーバ	a. <サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動します。 b. TMVS.exe をダブルクリックします。
ネットワーク上のクライアント	a. ビジネスセキュリティサーバで、<サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility に移動します。 b. TMVS フォルダを別のクライアントにコピーします。 c. コピー先のクライアントで TMVS フォルダを開き、TMVS.exe をダブルクリックします。

2. [Manual Scan] に移動します。
3. 対象となるクライアントの IP アドレス範囲を入力します。
   a. IPv4 のアドレス範囲を入力します。

      注意
      IPv4 シングルスタックまたはデュアルスタッククライアント 上で実行されている脆弱性検索ツールは、IPv4 のアドレス範囲のみでクエリを実行できます。脆弱性検索ツールでは、168.212.1.1～168.212.254.254 などクラス B の IP アドレス範囲のみがサポートされます。

   b. IPv6 のアドレス範囲については、IPv6 のプレフィックスと長さを入力します。

注意

IPv6 シングルスタックまたはデュアルスタッククライアント 上で実行されている脆弱性検索ツールは、IPv6 のアドレス範囲のみでクエリを実行できます。

4. [Settings] をクリックします。

   [Settings] 画面が表示されます。

5. 脆弱性検索設定を指定します。詳細については、50 ページの「脆弱性検索の設定」を参照してください。

6. [OK] をクリックします。

   [Settings] 画面が閉じます。

7. [Start] をクリックします。

   [Manual Scan] タブの [Results] テーブルに脆弱性検索の結果が表示されます。

注意

コンピュータで Windows Server 2008 が実行されている場合は、MAC アドレス情報が [Results] テーブルに表示されません。

8. 結果を CSV ファイルに保存するには、[Export] をクリックし、ファイルを保存するフォルダを参照してファイル名を入力し、[保存] をクリックします。

DHCP 検索の実行

DHCP サーバに IP アドレスをリクエストしているクライアントに対して脆弱性検索を実行します。

脆弱性検索ツールは 67 番ポートで待機します。このポートは、DHCP サーバの DHCP リクエスト用の待機ポートです。クライアントからの DHCP リクエストが検出されると、脆弱性検索がクライアントで実行されます。

注意

脆弱性検索ツールは、Windows Server 2008 または Windows 7 上で起動されると DHCP リクエストを検出できません。

手順

1. 次のフォルダにある TMVS.ini ファイルで DHCP の設定を行います。<サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS.

表 3-5. TMVS.ini ファイルでの DHCP 設定

設定	説明
DhcpThreadNum=x	DHCP モードのスレッド数を指定します。最小値は 3、最大値は 100、初期設定値は 3 です。
DhcpDelayScan=x	リクエストを行っているコンピュータにインストールされているウイルス対策製品を確認するまでの遅延時間 (秒) です。 最小値は 0 (待機しない)、最大値は 600、初期設定値は 60 です。
LogReport=x	ログ記録を無効にする場合は 0、有効にする場合は 1 にします。 脆弱性検索ツールでは、検索結果をビジネスセキュリティサーバに送信します。ログは Web コンソールの [システムイベントログ] 画面に表示されます。
OsceServer=x	ビジネスセキュリティサーバの IP アドレスまたは DNS 名です。
OsceServerPort=x	ビジネスセキュリティサーバの Web サーバポートです。

2. 脆弱性検索ツールを起動します。

脆弱性検索ツールの起動場所	手順
ビジネスセキュリティサーバ	a. <サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動します。 b. TMVS.exe をダブルクリックします。

脆弱性検索ツールの起動場所	手順
ネットワーク上のクライアント	a. ビジネスセキュリティサーバで、<サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility に移動します。 b. TMVS フォルダを別のクライアントにコピーします。 c. コピー先のクライアントで TMVS フォルダを開き、TMVS.exe をダブルクリックします。

3. [Manual Scan] の横にある [Settings] をクリックします。

   [Settings] 画面が表示されます。

4. 脆弱性検索設定を指定します。詳細については、50 ページの「脆弱性検索の設定」を参照してください。

5. [OK] をクリックします。

   [Settings] 画面が閉じます。

6. [Results] テーブルで、[DHCP Scan] タブをクリックします。

   注意

   [DHCP Scan] タブは、Windows Server 2008 および Windows 7 を実行しているコンピュータでは使用できません。

7. [DHCP Start] をクリックします。

   脆弱性検索ツールは DHCP リクエストの待機を開始し、クライアントコンピュータがネットワークにログオンしたら、そのコンピュータに対して脆弱性検索を実行します。

8. 結果を CSV ファイルに保存するには、[Export] をクリックし、ファイルを保存するフォルダを参照してファイル名を入力し、[保存] をクリックします。

脆弱性検索の予約設定

脆弱性検索をスケジュールに応じて自動的に実行します。

手順

1. 脆弱性検索ツールを起動します。

脆弱性検索ツールの起動場所	手順
ビジネスセキュリティサーバ	a. <サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動します。 b. TMVS.exe をダブルクリックします。
ネットワーク上のクライアント	a. ビジネスセキュリティサーバで、<サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility に移動します。 b. TMVS フォルダを別のクライアントにコピーします。 c. コピー先のクライアントで TMVS フォルダを開き、TMVS.exe をダブルクリックします。

2. [Scheduled Scan] に移動します。
3. [Add/Edit] をクリックします。

   [Scheduled Task] 画面が表示されます。
4. 予約する脆弱性検索の名前を入力します。
5. 対象となるコンピュータの IP アドレス範囲を入力します。
   a. IPv4 のアドレス範囲を入力します。

      注意
      使用可能な IPv4 アドレスがある IPv4 シングルスタックまたはデュアルスタックのホストマシン上で実行されている脆弱性検索ツールは、IPv4 のアドレス範囲のみでクエリを実行できます。脆弱性検索ツールでは、168.212.1.1～168.212.254.254 などクラス B の IP アドレス範囲のみがサポートされます。

   b. IPv6 のアドレス範囲については、IPv6 のプレフィックスと長さを入力します。

注意

使用可能な IPv6 アドレスがある IPv6 シングルスタックまたはデュアルスタックのホストマシン上で実行されている脆弱性検索ツールは、IPv6 のアドレス範囲のみでクエリを実行できます。

6. 24 時間形式で開始時刻を指定して、検索を実行する頻度を選択します。毎日、毎週、または毎月のいずれかを選択します。
7. 指定済みの手動による脆弱性検索の設定を使用する場合は、[Use current settings] を選択します。手動による脆弱性検索の設定の詳細については、44 ページの「手動での脆弱性検索の実行」を参照してください。

   手動による脆弱性検索を設定していない場合、または別の設定を使用する場合は、[Modify settings] を選択し、[Settings] をクリックします。[Settings] 画面が表示されます。検索設定を指定し、[OK] をクリックします。詳細については、50 ページの「脆弱性検索の設定」を参照してください。
8. [OK] をクリックします。

   [Scheduled Task] 画面が閉じます。予約した脆弱性検索は [Scheduled Scan] に表示されます。通知を有効にしている場合は、脆弱性検索ツールによって予約した脆弱性検索の結果が送信されます。
9. 予約した脆弱性検索をただちに実行するには、[Run Now] をクリックします。

   [Schedule Scan] タブの [Results] テーブルに脆弱性検索の結果が表示されます。

注意

コンピュータで Windows Server 2008 が実行されている場合は、MAC アドレス情報が [Results] テーブルに表示されません。

10. 結果を CSV ファイルに保存するには、[Export] をクリックし、ファイルを保存するフォルダを参照してファイル名を入力し、[保存] をクリックします。

11. 予約した脆弱性検索の実行を停止するには、[Scheduled Scan] に移動して、予約した検索を選択し、[Delete] をクリックします。

脆弱性検索の設定

脆弱性検索を実行する場合は、次の設定を行います。各種の脆弱性検索の詳細については、43 ページの「脆弱性検索ツールを使用したインストール」を参照してください。

設定	説明および手順
Product Query	脆弱性検索ツールでは、対象クライアントでのセキュリティソフトウェアの有無を確認できます。 1. 確認するセキュリティソフトウェアを選択します。 2. 脆弱性検索ツールでは、画面に表示される初期設定ポートを使用してソフトウェアの有無が確認されます。ソフトウェア管理者が初期設定ポートを変更した場合、必要に応じて変更を行わないと、脆弱性検索ツールでそのソフトウェアが検出されません。 3. Norton Antivirus Corporate Edition については、[Settings] をクリックしてタイムアウト設定を変更できます。

設定	説明および手順
	その他の製品のクエリ設定 脆弱性検索ツールでセキュリティソフトウェアの有無を同時に確認できるクライアント数を設定するには 1. <サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、メモ帳などのテキストエディタを使用して TMVS.ini を開きます。 2. 確認するクライアント数を設定するには、次の手順を実行します。 • 手動による脆弱性検索の場合は、ThreadNumManual の値を変更します。8〜64 の値を指定します。 たとえば、脆弱性検索ツールが同時に 60 のクライアントを確認するように指定するには、「ThreadNumManual=60」と入力します。 • 予約による脆弱性検索の場合は、ThreadNumSchedule の値を変更します。8〜64 の値を指定します。 たとえば、脆弱性検索ツールが同時に 50 のクライアントを確認するように指定するには、「ThreadNumSchedule=50」と入力します。 3. TMVS.ini を保存します。
Description Retrieval Settings	脆弱性検索ツールでクライアントの「ping」が可能な場合、クライアントの追加情報を取得できます。情報を取得する方法は 2 つあります。 • Normal retrieval:ドメインとコンピュータの両方の情報を取得します。 • Quick retrieval:コンピュータ名のみを取得します。

設定	説明および手順
Alert Settings	脆弱性検索の結果を管理者に自動的に送信するには 1. [Email results to the system administrator] を選択します。 2. [Configure] をクリックして、メールを設定します。 3. [To] テキストボックスに、受信者のメールアドレスを入力します。 4. [From] テキストボックスに、送信者のメールアドレスを入力します。 5. [SMTP server] テキストボックスに、SMTP サーバのアドレスを入力します。 たとえば、「`smtp.example.com`」と入力します。SMTP サーバ情報は必須です。 6. [Subject] テキストボックスに新しい件名を入力するか、または初期設定を適用します。 7. [OK] をクリックします。 コンピュータにセキュリティソフトウェアがインストールされていないことをユーザに通知するには 1. [Display a notification on unprotected computers] を選択します。 2. [Customize] をクリックして、通知メッセージを設定します。 3. [Notification Message] 画面で新しいメッセージを入力するか、または初期設定を適用します。 4. [OK] をクリックします。
Save as CSV File	脆弱性検索の結果を CSV ファイルに保存します。 このファイルは、脆弱性検索ツールを起動したクライアントに保存されます。初期設定のファイルパスを適用するか、または必要に応じて変更します。

設定	説明および手順
Ping Settings	クライアントの存在を検証し、その OS を判別するには、「ping」の設定を使用します。これらの設定が無効な場合、脆弱性検索ツールは指定された IP アドレス範囲のすべての IP アドレスを (どのクライアントにも使用されていないアドレスであっても) 検索するため、検索に必要以上の時間がかかります。 1. [Packet size] フィールドおよび [Timeout] フィールドで、初期設定値を適用するか変更します。 2. [Detect the type of operating system using ICMP OS fingerprinting] を選択します。 このオプションを選択すると、脆弱性検索ツールは、クライアントが実行しているのが Windows か別の OS かを判別します。Windows を実行しているクライアントの場合は、脆弱性検索ツールで Windows のバージョンを識別できます。
	その他の ping の設定 脆弱性検索ツールによって ping を同時に実行するクライアントの数を設定するには 1. <サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、メモ帳などのテキストエディタを使用して TMVS.ini を開きます。 2. EchoNum の値を変更します。1〜64 の値を指定します。 たとえば、脆弱性検索ツールが同時に 60 のクライアントに ping コマンドを実行するように指定するには、「EchoNum=60」と入力します。 3. TMVS.ini を保存します。

設定	説明および手順
Security Server settings	1. 脆弱性検索ツールで検索するクライアントにセキュリティエージェントをインストールするには、[Auto-install Security Agent on unprotected computers] を選択します。 2. ビジネスセキュリティサーバのホスト名または IPv4/IPv6 アドレス、およびポート番号を入力します。脆弱性検索ツールによってインストールされたセキュリティエージェントは、このサーバにレポートを送信します。 3. [Install Account] をクリックして、クライアントへのログオン時に使用する管理者の資格情報を設定します。[Account Information] 画面でユーザ名とパスワードを入力し、[OK] をクリックします。

メール通知を使用したインストール

インストーラへのリンクのあるメールメッセージを送信するには、このインストール方法を使用します。

手順

1. [デバイス] に移動します。
2. [デバイスの追加] をクリックします。
3. [コンピュータの種類] セクションで、[デスクトップまたはサーバ] を選択します。
4. [クライアントのインストール方法] で、[メール通知によるインストール] を選択します。
5. [次へ] をクリックします。

   新しい画面が表示されます。
6. メールの件名と受信者を入力します。
7. [適用] をクリックします。初期設定のメールクライアントで、受信者、件名、およびインストーラへのリンクのあるメールが開きます。

セキュリティエージェントに移行する

セキュリティエージェントのインストール時、セットアップによって対象クライアントにトレンドマイクロまたは他社製のエンドポイントセキュリティソフトウェアがインストールされているかどうかが確認されます。

セットアップでは次の処理を実行できます。

- 現在インストールされている他のエンドポイントセキュリティソフトウェアを削除して、セキュリティエージェントに置き換える
- 他のエンドポイントセキュリティソフトウェアを検出するが削除しない

クライアント上のソフトウェアを自動的に削除できなかったり、検出できても削除できない場合は、最初に手動でアンインストールします。ソフトウェアのアンインストール手順によっては、アンインストール後にクライアントの再起動が必要な場合があります。

移行時の問題と解決策

他社製のエンドポイントセキュリティソフトウェアの自動アンインストールは、次の理由により失敗することがあります。

- 他社製ソフトウェアのバージョン番号またはプロダクトキーが不整合である
- 他社製ソフトウェアのアンインストールプログラムが動作しない
- 他社製ソフトウェアの特定のファイルがないか破損している
- 他社製ソフトウェアのレジストリキーを削除できない
- 他社製ソフトウェアにアンインストールプログラムがない

これらの問題に対する解決策として、次のものが考えられます。

- 他社製ソフトウェアを手動で削除する
- 他社製ソフトウェアのサービスを停止する
- 他社製ソフトウェアのサービスまたはプロセスをアンロードする

セキュリティエージェントでインストール後の作業を実行する

手順

1. 次のことを確認します。
   - エンドポイントの Windows の [スタート] メニューにセキュリティエージェントへのショートカットが表示されています。
   - エンドポイントのコントロールパネルの [プログラムの追加と削除] または [プログラムと機能] リストに、[ウイルスバスター ビジネスセキュリティエージェント] が表示されています。
   - セキュリティエージェントが Web コンソールの [デバイス] 画面に表示され、エンドポイントの OS の種類に応じて [サーバ (初期設定)] または [デスクトップ (初期設定)] にグループ化されています。

     注意

     セキュリティエージェントが表示されない場合は、[管理] > [グローバル設定] > [システム] タブ > [クライアントの接続状態の確認] から接続状態の確認タスクを実行します。

   - Microsoft「サービス」に、次のセキュリティエージェントサービスが表示されています。
     - Trend Micro Security Agent Listener (`tmlisten.exe`)
     - Trend Micro Security Agent RealTime Scan (`ntrtscan.exe`)
     - Trend Micro Security Agent Firewall (`TmPfw.exe`) (インストール時にファイアウォールを有効にした場合)
     - Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`) (インストール時に挙動監視またはデバイスコントロールを有効にした場合)
     - Trend Micro Common Client Solution Framework (`TmCCSF.exe`)

2. セキュリティエージェントが Web コンソールに表示されない場合は、サーバにステータスを送信できなかった可能性があります。次のいずれかの操作を実行します。

   - クライアントで Web ブラウザを開き、アドレスボックスに「`https://{ビジネスセキュリティサーバ名}:{ポート番号}/SMB/cgi/cgionstart.exe`」と入力して <ENTER> キーを押します。

     次の画面に「-2」が表示されている場合、エージェントはサーバと通信できることを意味しています。また、これはサーバのデータベースにエージェントの記録がなく、サーバデータベース側に問題がある可能性を示しています。

   - ping コマンドおよび telnet コマンドを使用してクライアント/サーバ間が接続されているかどうかを確認します。
   - 帯域幅が制限されている場合、それによってサーバ/クライアント間に接続タイムアウトが発生していないかを確認します。
   - サーバの`¥PCCSRV` フォルダに共有権限があるかどうか、およびすべてのユーザにこのフォルダのフルコントロール権限が付与されているかどうかを確認します。
   - ビジネスセキュリティサーバのプロキシ設定が正しいことを確認します。

3. EICAR テストスクリプトを使用してセキュリティエージェントをテストします。

   EICAR (European Institute of Computer Anti-virus Research) は、ウイルス対策ソフトウェアのテストに利用できる、テスト用の「ウイルス」スクリプトを開発しています。このスクリプトは、実行機能を持たないテキストファイルです。このファイルのバイナリパターンは、大部分のウイルス対策ソフトウェアベンダーのウイルスパターンファイルに含まれています。EICAR テストスクリプトは、ウイルスではないのでプログラムコードがありません。

   EICAR テストスクリプトは、次の URL からダウンロードできます。

   http://www.eicar.org/anti_virus_test_file.htm

EICAR テストスクリプトは、自分で作成することもできます。その場合は、下記のテキストをテキストファイルに入力して、「eicar.com」という名前を付けて保存します。

(実際の文字列では、改行は不要です。文字列中に改行があると検知されません。)

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS
-TEST-FILE!$H+H*
```

注意

テストの前に、キャッシュサーバおよびローカルブラウザのキャッシュをクリアしてください。

エージェントを削除する

[エージェントのアンインストール] コマンドを使用し、次の方法でセキュリティエージェントを削除できます。

- 59 ページの「Web コンソールからエージェントを削除する」

  この方法は、オフラインのエージェントに対して使用します。オフラインのエージェントは、Web コンソールにオフラインと表示され続けます。これは、エージェントがインストールされたクライアントコンピュータが長期間にわたって電源オフになっているか、エージェントをアンインストールできるようになる前に、ハードディスクが再フォーマットされた可能性があります。

  Web コンソールからエージェントを削除する場合:

  - エージェントが、クライアントにまだ存在する場合には、アンインストールされません。
  - サーバがエージェントの管理を停止します。
  - エージェントがサーバと通信を再開すると (クライアントでの電源投入後など)、再度 Web コンソールにエージェントが追加されます。セキュリティエージェントには、元のグループの設定が適用されます。そのグループが存在しない場合には、クライアントの OS に応じ

て [サーバ (初期設定)] または [デスクトップ (初期設定)] にグループ化され、そのグループの設定が適用されます。

ヒント

ビジネスセキュリティには、その他にもオフラインのエージェントをチェックし、Web コンソールから削除する機能があります。この機能は、エージェントの削除作業を自動化します。この機能を使用するには、[管理] > [グローバル設定] > [システム] タブに移動し、[オフラインセキュリティエージェントの削除] に移動します。

- 60 ページの「Web コンソールからエージェントをアンインストールする」

エージェントのプログラムに問題が発生した場合には、エージェントをアンインストールできます (同時に、Web コンソールからも削除できます)。クライアントを脅威から保護するために、エージェントをただちに再インストールすることをお勧めします。

Web コンソールからエージェントを削除する

手順

1. [デバイス] に移動します。
2. セキュリティエージェントを削除するには、グループを選択してからエージェントを選択します。

ヒント

隣接する複数のセキュリティエージェントを選択するには、選択範囲内の最初のエージェントをクリックして、<Shift> キーを押しながら選択範囲内の最後のエージェントをクリックします。隣接していないエージェントの範囲を選択するには、選択範囲内の最初のエージェントをクリックして、<Ctrl> キーを押しながら選択するエージェントをクリックします。

3. [詳細] > [エージェントのアンインストール] をクリックします。

   新しい画面が表示されます。

4. [選択したエージェントを削除] をクリックします。
5. [適用] をクリックします。

Web コンソールからエージェントをアンインストールする

手順

1. [デバイス] に移動します。
2. セキュリティエージェントをアンインストールするには、グループを選択してからエージェントを選択します。

   ヒント

   隣接する複数のセキュリティエージェントを選択するには、選択範囲内の最初のエージェントをクリックして、<Shift> キーを押しながら選択範囲内の最後のエージェントをクリックします。隣接していないエージェントの範囲を選択するには、選択範囲内の最初のエージェントをクリックして、<Ctrl> キーを押しながら選択するエージェントをクリックします。

3. [詳細] > [エージェントのアンインストール] をクリックします。

   新しい画面が表示されます。
4. [選択したエージェントをアンインストール] をクリックします。
5. [適用] をクリックします。

   ポップアップ画面が表示され、サーバが送信したアンインストール通知の数と、通知を受信したエージェントの数が示されます。
6. [OK] をクリックします。
7. エージェントがアンインストールされたことを確認するには、[セキュリティ設定] 画面を更新します。そのエージェントは、セキュリティ設定のグループツリーには表示されなくなります。

エンドポイントからセキュリティエージェントをアンインストールする

アンインストールする 際、設定によってパスワードが必要な場合と必要ない場合があります。パスワードが必要な場合は、アンインストールプログラムを実行するユーザのみとパスワードを共有し、他のユーザにそのパスワードが流出した場合には、ただちにそのパスワードを変更してください。

このパスワードは、[管理] > [グローバル設定] > [デスクトップ/サーバ] タブ > [セキュリティエージェント アンインストール用パスワード] で設定または無効化できます。

手順

1. [コントロール パネル] > [プログラムの追加と削除] または [プログラムと機能] をクリックします。
2. [ウイルスバスター ビジネスセキュリティエージェント] を探し、[アンインストール] をクリックします。
3. 画面の指示に従います。
4. アンインストールパスワードを 要求された場合には入力します。

   ユーザにアンインストールの 進行状況と完了が通知されます。ユーザが、アンインストールを 完了するためにコンピュータを再起動する必要はありません。

第 4 章

デバイスの管理

ビジネスセキュリティ の [デバイス] 画面は、2 つの主要なセクションに分かれています。

- デバイスツリー

  デバイスツリーは論理グループのリストで、展開することができます。エンドポイントの種類に基づいてグループを管理できるほか、要件に応じて手動でグループを設定してセキュリティエージェントを割り当てることもできます。

  詳細については、64 ページの「デバイスツリーを使用する」を参照してください。

- グループ情報テーブル

  デバイスツリーからグループを 選択すると、そのグループに属するセキュリティエージェントのリストが右側に表示されます。

  詳細については、66 ページの「デバイスコマンドを使用する」を参照してください。

デバイスツリーを使用する

図 4-1. デバイスツリーコマンドメニューの使用

デバイスツリーのメニューを開くには、次の手順を実行します。

- デバイスツリーからグループを選択し、グループ名の横にある歯車アイコンをクリックします。

選択したグループの種類に応じて、特定の種類のグループでしか使用できないコマンドや無効になるコマンドがあります。

表 4-1. デバイスツリーコマンド

コマンド	説明
グループの追加	デバイスツリーに新しいグループを追加します。 詳細については、69 ページの「グループの追加」を参照してください。
[通常検索の開始]	通常検索を開始します。

コマンド	説明
[アグレッシブ検索の開始]	アグレッシブ検索を開始します (通常検索実行後に不審な挙動が見られる場合などに実行してください)。 **注意** アグレッシブ検索を実行すると、エンドポイントのパフォーマンスに影響する可能性があるほか、誤検出が多くなることもあります。検索に要する時間は、エンドポイントのハードウェアリソースと検索するファイル数によって異なります。
[検索停止]	検索を停止します。
グローバル設定	セキュリティ検索、承認済み/ブロックリスト、セキュリティエージェントコントロール、デバイス管理など、セキュリティエージェント全体の設定を行います。 詳細については、184 ページの「グローバル設定」を参照してください。
[ポリシーの設定]	選択したグループに属するすべてのセキュリティエージェントのセキュリティ設定を指定します。 詳細については、82 ページの「セキュリティエージェントの基本的なセキュリティ設定の概要」を参照してください。
名前の変更	選択したグループの名前を変更します。
設定の複製	グループの設定を別のグループにコピーします。コピー先のグループに属するセキュリティエージェントでコピー元のグループと同じ設定が適用されます。 詳細については、77 ページの「設定を複製する」を参照してください。
ポリシーの設定のインポート	別のグループから取得した設定をインポートします。 詳細については、78 ページの「セキュリティエージェントグループの設定をインポートおよびエクスポートする」を参照してください。

コマンド	説明
ポリシーの設定のエクスポート	選択したグループの設定をエクスポートします。 詳細については、78 ページの「セキュリティエージェントグループの設定をインポートおよびエクスポートする」を参照してください。
削除	デバイスツリーからグループを削除します。

デバイスコマンドを使用する

図 4-2. デバイスコマンドメニューの使用

デバイスツリーからグループを選択すると、そのグループに属するセキュリティエージェントのリストが表の右側に表示されます。表の上部にあるメニューバーのコマンドを使用して、セキュリティエージェントを管理できます。選択したグループの種類に応じて、特定の種類のグループでしか使用できないコマンドや無効になるコマンドがあります。

名前、ラベル、または IP アドレスでエンドポイントを検索するには、[デバイス] 画面の上部にある検索バーを使用します。

ヒント

ネットワーク内のエンドポイントについては、IP アドレスの一部を入力して検索できます。たとえば、「192」と入力して検索すると「192」を含むすべての IP アドレスが返され、「192.」と入力して検索すると「192」で始まるすべての IP アドレスが返されます。ただし、エンドポイントの名前の検索では、ワイルドカードや特殊文字 (*、+、(、)、-、&) は使用できません。

表 4-2. デバイスコマンド

コマンド	説明
[デバイスの追加]	次のインストールを実行します。 • セキュリティエージェントをエンドポイントへ (デスクトップまたはサーバ) 詳細については、68 ページの「エージェントをグループに追加する」を参照してください。
[ポリシーの設定]	選択したグループに属するすべてのセキュリティエージェントのセキュリティ設定を指定します。 詳細については、82 ページの「セキュリティエージェントの基本的なセキュリティ設定の概要」を参照してください。
[通常検索の開始]	通常検索を開始します。
[アグレッシブ検索の開始]	アグレッシブ検索を開始します (通常検索実行後に不審な挙動が見られる場合などに実行してください)。  注意 アグレッシブ検索を実行すると、エンドポイントのパフォーマンスに影響する可能性があるほか、誤検出が多くなることもあります。検索に要する時間は、エンドポイントのハードウェアリソースと検索するファイル数によって異なります。
[検索停止]	検索を停止します。

コマンド	説明
[エージェントのアンインストール]	選択したデバイスからセキュリティエージェントを削除します。 詳細については、58 ページの「エージェントを削除する」を参照してください。
[カウンタのリセット]	ネットワーク上のすべてのセキュリティエージェントのセキュリティリスク検出数をリセットします。関連するログの情報はログクエリで引き続き参照できます。
[列のカスタマイズ]	表に表示する列を選択します。 詳細については、70 ページの「デバイスリストの列をカスタマイズする」を参照してください。
[セキュリティエージェントの移動]	選択したセキュリティエージェントを別のグループまたは別のビジネスセキュリティサーバに移動します。 詳細については、72 ページの「エージェントを移動する」を参照してください。

エージェントをグループに追加する

エージェントがインストールされ、ビジネスセキュリティサーバに通知が行われると、サーバはそのエージェントを下記グループに自動的に追加します。

- サーバプラットフォームにインストールされたセキュリティエージェントは、[サーバ (初期設定)] グループに追加されます。
- デスクトッププラットフォームにインストールされたセキュリティエージェントは、[デスクトップ (初期設定)] グループに追加されます。

注意

セキュリティエージェントは、それらを移動することで他のグループに割り当てることができます。詳細については、72 ページの「エージェントを移動する」を参照してください。

セキュリティ設定のグループツリーに正しいエージェント数が反映されていない場合は、サーバに通知されずにエージェントが削除された可能性があります (たとえば、エージェントの削除中にクライアント/サーバ間の通信が失わ

れたなど)。このような場合、サーバはエージェント情報をデータベースに保持し、Web コンソール上でそのエージェントをオフラインとして表示します。エージェントを再インストールすると、サーバはデータベースに新しいレコードを作成し、エージェントを新規として扱うため、セキュリティ設定のグループツリーにエージェントが重複して表示されます。重複したエージェントレコードがないかを確認するには、[管理] > [グローバル設定] > [システム] で [エージェントの接続状態の確認] 機能を使用します。

セキュリティエージェントのインストール

次の項目を参照してください。

- 24 ページの「セキュリティエージェントのインストール 要件」
- 24 ページの「セキュリティエージェントのインストールに 関する考慮事項」
- 29 ページの「セキュリティエージェントのインストール 方法」
  - 31 ページの「インストール用 Web ページを使用したインストール」
  - 33 ページの「ログオンスクリプトウィザードによるインストール」
  - 35 ページの「Client Packager を使用したインストール」
  - 39 ページの「リモートインストールを 使用したインストール」
  - 43 ページの「脆弱性検索ツールを使用したインストール」
  - 54 ページの「メール通知を使用したインストール」
- 56 ページの「セキュリティエージェントでインストール 後の作業を実行する」

グループの追加

サーバグループまたはデスクトップグループを 追加して、1 つ以上のセキュリティエージェントを 含めることができます。

手順

1. [デバイス] に移動します。

2. [グループの追加] をクリックします。

   新しい画面が表示されます。

3. グループの種類を選択します。

   - デスクトップ
   - サーバ

4. グループの名前を入力します。

5. 追加するグループに既存グループの設定を適用するには、[次のグループから設定をインポートする] をクリックして、グループを選択します。選択した「グループの種類」に該当するグループだけが表示されます。

6. [保存] をクリックします。

デバイスリストの列をカスタマイズする

デバイスリスト上部の [詳細] > [列のカスタマイズ] をクリックして、表示する列を選択することができます。

列	表示される情報
クライアント	
IP アドレス	エージェントがインストールされているクライアントの IP アドレス
ステータス	• オンライン: エージェントはビジネスセキュリティサーバに接続されています • オフライン: エージェントはビジネスセキュリティサーバに接続されていません
エージェントのバージョン	エージェントのバージョン
OS	エージェントがインストールされているクライアントの OS
アーキテクチャ	• x64:64 ビット OS • x86: 32 ビット OS

列	表示される情報
検索	
スマートスキャンサービス 注意 この列は検索方法がスマートスキャンの場合にのみ表示されます。	• 接続されました: エージェントはスマートスキャンサービスに接続されています • 切断されました: エージェントはスマートスキャンサービスから切断されています 注意 スマートスキャンサービスは、ビジネスセキュリティサーバでホストされています。エージェントが切断されている場合は、ビジネスセキュリティサーバに接続できない、またはスマートスキャンサービスが機能していない (たとえば、サービスが停止されている) ことを意味しています。 • 無効: エージェントは従来型スキャンを使用します
スマートスキャンエージェントパターンファイル/ウイルスパターンファイル	スマートスキャンエージェントパターンファイルまたはウイルスパターンファイルのバージョン
検索方法	• スマート: ローカル検索およびクラウド型クエリ • 従来型: ローカルの検索のみ 詳細については、83 ページの「検索方法」を参照してください。
通常検索	前回の通常検索の日付と時刻
POP3 検索	• 有効 • 無効
予約検索	前回の予約検索の日付と時刻
アグレッシブ検索	前回のアグレッシブ検索の日付と時刻
脅威	

列	表示される情報
検出されたウイルス	検出されたウイルス/不正プログラムの数
検出されたスパイウェア	検出されたスパイウェア/グレーウェアの数
検出されたスパムメール	スパムメールメッセージの数
URL フィルタ違反	禁止された URL へのアクセス数
ウイルス検索エンジン	ウイルス検索エンジンのバージョン
ウイルスパターンファイル 注意 この列は検索方法が従来型スキャンの場合にのみ表示されます。	ウイルスパターンファイルのバージョン

エージェントを移動する

エージェントは、次に示す複数の方法で移動できます。

移動対象	詳細	移動方法
セキュリティエージェント	セキュリティエージェントをグループ間で移動します。移動後、エージェントは新しいグループの設定を継承します。	Web コンソールを使用して、1 つ以上のエージェントを移動します。73 ページの「セキュリティエージェントをグループ間で移動する」を参照してください。

移動対象	詳細	移動方法
	複数のビジネスセキュリティサーバがある場合に、セキュリティエージェントをサーバ間で移動します。 移動後、エージェントは、その OS に応じて移動先のビジネスセキュリティサーバの [デスクトップ (初期設定)] または [サーバ (初期設定)] の下にグループ化されます。エージェントは新しいグループの設定を継承します。	• Web コンソールを使用して、1 つ以上のエージェントを移動します。74 ページの「Web コンソールを使用してビジネスセキュリティサーバ間でエージェントを移動する」を参照してください。 • クライアント移動ツールを実行して、クライアントにインストールされているエージェントを移動します。75 ページの「クライアント移動ツールを使用してビジネスセキュリティサーバ間でセキュリティエージェントを移動する」を参照してください。

セキュリティエージェントをグループ間で移動する

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. 移動するエージェントを選択します。

ヒント

隣接する複数のセキュリティエージェントを選択するには、選択範囲内の最初のエージェントをクリックして、<Shift> キーを押しながら選択範囲内の最後のエージェントをクリックします。隣接していないエージェントの範囲を選択するには、選択範囲内の最初のエージェントをクリックして、<Ctrl> キーを押しながら選択するエージェントをクリックします。

4. エージェントを新しいグループにドラッグします。

Web コンソールを使用してビジネスセキュリティサーバ間でエージェントを移動する

始める前に

ビジネスセキュリティサーバ 間でエージェントを移動するときは、次のことに注意してください。

- 以前のバージョンのエージェントを最新バージョンのビジネスセキュリティサーバに移動すると、エージェントは自動的にアップグレードされます。
- 最新バージョンのエージェントを以前のバージョンのセキュリティサーバに移動すると、そのエージェントを管理できなくなるため、この移動は行わないでください (エージェントは移動元のサーバから登録解除されますが、新しいサーバに登録できないため、いずれの Web コンソールにも表示されなくなります)。
- 移動元と移動先のビジネスセキュリティサーバの 言語は同じである必要があります。
- 移動先のビジネスセキュリティサーバのサーバ 名とポート番号を記録します。サーバ名とポート番号は、ビジネスセキュリティサーバの [タスク] パネル上部にある [セキュリティ 設定] 画面に表示されています。

手順

1. 移動元のエージェントを管理しているビジネスセキュリティサーバの Web コンソールで、[デバイス] に移動します。
2. セキュリティエージェントを移動するには、グループを選択してからエージェントを選択します。
3. [詳細] > [セキュリティエージェントの 移動] をクリックします。

   新しい画面が表示されます。
4. 移動先のビジネスセキュリティサーバのサーバ 名とポート番号を入力します。

5. [移動] をクリックします。
6. エージェントの接続先が移動先のセキュリティサーバになっていることを確認するには、移動先のサーバの Web コンソールを開き、セキュリティ設定のグループツリーに目的のエージェントが表示されていることを確認します。

注意

セキュリティ設定のグループツリーにセキュリティエージェントが 表示されない場合、サービスから Trend Micro Security Server Master Service を再起動します。

クライアント移動ツールを使用してビジネスセキュリティサーバ間でセキュリティエージェントを移動する

始める前に

ビジネスセキュリティサーバ 間でエージェントを移動するときは、次のことに注意してください。

- 以前のバージョンのエージェントを最新バージョンのビジネスセキュリティサーバに移動すると、エージェントは自動的にアップグレードされます。
- 最新バージョンのエージェントを以前のバージョンのセキュリティサーバに移動すると、そのエージェントを管理できなくなるため、この移動は行わないでください (エージェントは移動元のサーバから登録解除されますが、新しいサーバに登録できないため、いずれの Web コンソールにも表示されなくなります)。
- 移動元と移動先のビジネスセキュリティサーバの 言語は同じである必要があります。
- 移動先のビジネスセキュリティサーバのサーバ 名とポート番号を記録します。サーバ名とポート番号は、ビジネスセキュリティサーバの [タスク] パネル上部にある [セキュリティ 設定] 画面に表示されています。
- 管理者アカウントでクライアントにログオンします。

手順

1. クライアントでコマンドプロンプトを開きます。

   注意

   コマンドプロンプトは管理者として開く必要があります。

2. 「cd」と入力し、続けてセキュリティエージェントのインストールフォルダのパスを入力します。例を以下に示します。`cd C:\Program Files\Trend Micro\Security Agent`

3. 次の構文を使用してクライアント移動ツールを実行します。

   <実行可能ファイル名> -s <サーバ名> -p <サーバ待機ポート> -c <クライアント待機ポート> -pwd <エージェントの「アンロードとロック解除」の権限のパスワード>

   表 4-3. クライアント移動ツールのパラメータ

パラメータ	説明
<実行可能ファイル名>	IpXfer.exe (32 ビット) IpXfer_x64.exe (64 ビット)
<サーバ名>	移動先ビジネスセキュリティサーバ (エージェントの転送先のサーバ) の名前
<サーバ待機ポート>	移動先ビジネスセキュリティサーバの待機ポート (信頼するポート) 番号
<クライアント待機ポート>	セキュリティエージェントがサーバとの通信に使用するポート番号
<エージェントの「アンロードとロック解除」の権限のパスワード>	セキュリティエージェントのアンロードとロック解除に使用するパスワード

   例:

   ```
   ipXfer.exe -s Server01 -p 8080 -c 21112 -pwd Password
   ```

4. セキュリティエージェントの接続先が移動先のセキュリティサーバになっていることを確認するには、移動先のサーバの Web コンソールを開

き、セキュリティ設定のグループツリーに目的のエージェントが表示されていることを確認します。

注意

セキュリティ設定のグループツリーにセキュリティエージェントが 表示されない場合、サービスから Trend Micro Security Server Master Service を再起動します。

設定を複製する

セキュリティエージェントグループ 間で設定を複製します。

セキュリティエージェントのグループ設定を複製する

この機能は、特定のデスクトップグループまたはサーバグループの 設定を同じタイプの別のグループに適用するために使用します。サーバグループの設定をデスクトップグループに 複製することや、その逆の複製を行うことはできません。

特定のグループタイプに 1 つのグループしかない場合、この機能は無効になります。

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. グループ名の横にある歯車アイコンをクリックします。
4. [設定の複製] をクリックします。

   新しい画面が表示されます。
5. 設定を継承する対象グループを選択します。
6. [適用] をクリックします。

セキュリティエージェントグループの設定をインポートおよびエクスポートする

デスクトップまたはサーバグループの設定を.dat ファイルにエクスポートして、設定をバックアップします。また、その.dat ファイルを使用して、設定を別のグループにインポートできます。

注意

デスクトップおよびサーバのグループ間で、設定のインポートとエクスポートができます。設定はグループの種類に依存しません。[設定の複製] 機能も使用できますが、この機能はグループの種類に依存します。[設定の複製] 機能の詳細については、77 ページの「設定を複製する」を参照してください。

表 4-4. インポートおよびエクスポート可能な設定

選択内容	設定が含まれる画面	エクスポートまたはインポート可能な設定
デスクトップグループ ( ) またはサーバグループ ( )	デバイス ([デバイス] > [ポリシーの設定])	• ウイルス/スパイウェア対策 • 機械学習型検索 • 挙動監視 • 信頼済みプログラム • 隔離 • Web レピュテーション • URL フィルタ • ファイアウォール • デバイスコントロール • ユーザツール (デスクトップグループでのみ使用可能) • エージェントの権限
	手動検索 ([検索] > [手動検索])	すべての設定
	予約検索 ([検索] > [予約検索])	すべての設定

設定をエクスポートする

手順

1. [デバイス] に移動します。
2. デスクトップ/サーバグループを選択します。
3. グループ名の横にある歯車アイコンをクリックします。
4. [ポリシーの設定のエクスポート] をクリックします。

   新しい画面が表示されます。
5. [エクスポート] をクリックします。

   ダイアログボックスが表示されます。
6. [保存] をクリックして保存する場所を参照し、[保存] をクリックします。

設定をインポートする

手順

1. [デバイス] に移動します。
2. デスクトップ/サーバグループを選択します。
3. [ポリシーの設定のインポート] をクリックします。

   新しい画面が表示されます。
4. [ファイルの選択] をクリックしてファイルを検索し、[インポート] をクリックします。

第 5 章

セキュリティエージェントの基本的なセキュリティ設定の管理

本章では、セキュリティエージェントの基本的なセキュリティ設定方法について説明します。

セキュリティエージェントの基本的なセキュリティ設定の概要

表 5-1. セキュリティエージェントの基本的なセキュリティ設定の概要

オプション	説明	初期設定
検索方法	スマートスキャンを有効にするか無効にするかを設定します。	ビジネスセキュリティサーバのインストール時に従来型スキャン、スマートスキャンを選択します
ウイルス/スパイウェア対策	ウイルス対策、スパイウェア対策のリアルタイム検索におけるオプションを設定します。	有効 (リアルタイム検索)
機械学習型検索	機械学習型検索オプションを設定します。	無効
挙動監視	挙動監視オプションを設定します。	デスクトップグループの場合: 有効 サーバグループの場合: 無効
信頼済みプログラム	不審な挙動についての監視対象から除外する必要のあるプログラムを指定します。	なし
隔離	隔離ディレクトリを指定します。	http://<セキュリティサーバ名または IP アドレス>
Web レピュテーション	オフィス内外の Web レピュテーションに関するオプションを設定します。	オフィス内:有効、低 オフィス外:有効、中
URL フィルタ	URL フィルタによって、設定されているポリシーに違反する Web サイトがブロックされます。	有効、低
承認済み/ブロックする URL	承認済み/ブロックする URL のリストを設定します。	無効

オプション	説明	初期設定
ファイアウォール	ファイアウォールオプションを設定します。	無効
デバイスコントロール	自動実行、USB、およびネットワークアクセスを設定します。	無効
ユーザツール	迷惑メール対策ツールバーを設定します。	無効: サポート対象のメールクライアントの迷惑メール対策ツールバー
エージェントの権限	エージェントのコンソールから各種設定にアクセスできるかどうかを設定します。 自動でのビルドのバージョンアップ、HotFix、Critical Patch、Patch、Service Pack を無効にします。	なし

検索方法

セキュリティエージェントでは、脅威を検索するときに、次の 2 種類の検索方法のいずれかを使用できます。

- スマートスキャン:本書では、スマートスキャンを使用するセキュリティエージェントをスマートスキャンエージェントと呼びます。スマートスキャンエージェントは、ローカル検索と、ファイルレピュテーションサービスで提供されるクラウド型クエリを利用できます。
- 従来型スキャン:スマートスキャンを使用しないセキュリティエージェントは、従来型スキャンエージェントと呼びます。従来型スキャンエージェントでは、ウイルスパターンファイルを使用して、脅威を検索します。

次の表は、2 つの検索方法を比較しています。

表 5-2. 従来型スキャンとスマートスキャンの比較

比較基準	従来型スキャン	スマートスキャン
検索の動作	従来型スキャンエージェントは、クライアント上でスキャンを実行します。	• スマートスキャンエージェントは、クライアント上でスキャンを実行します。 • 検索時にファイルのリスクを特定できない場合、セキュリティエージェントは、スキャンサーバ (セキュリティサーバに接続されたセキュリティエージェントの場合) または Trend Micro Smart Protection Network (セキュリティサーバに接続されていないセキュリティエージェントの場合) に検索クエリを送信して、リスクを検証します。 注意 スキャンサーバは、スマートスキャンサーバで実行されるサービスです。 • セキュリティエージェントは、検索のパフォーマンスを向上するために検索クエリの結果を「キャッシュ」します。
使用およびアップデートされるコンポーネント	アップデート元にある、利用可能なすべてのセキュリティエージェントコンポーネント (スマートスキャンエージェントパターンファイルを除く)	コンポーネントは、ウイルスパターンファイルを除き、すべてアップデート元からダウンロードできます。
通常のアップデート元	アップデートサーバ	アップデートサーバ

検索方法を設定する

始める前に

ビジネスセキュリティサーバをインストールすると 、スマートスキャンを有効にするオプションを選択できるようになります。このオプションを有効にすると、初期設定の検索方法がスマートスキャンになります。つまり、すべてのセキュリティエージェントがスマートスキャンを 使用するようになります。有効にしない場合、初期設定は従来型スキャンになります。エージェントでは、現在の要求に従ってこれらの検索方法を切り替えることができます。例を以下に示します。

- エージェントで現在従来型スキャンを使用しており、検索処理が完了するまでに著しく長い時間がかかっている場合、高速で効率が良くなるように設計されたスマートスキャンに切り替えることができます。スマートスキャンに切り替える状況には他にも、エージェントのディスク容量が不足している場合があります。これは、スマートスキャンクライアントがダウンロードするパターンファイルのサイズが 少ないためで、したがって必要なディスク容量も少なくなります。

  スマートスキャンに切り替える前に、[管理] > [グローバル設定] に移動して [デスクトップ/サーバ] タブをクリックし、[一般検索] に移動します。[スマートスキャンサービスを無効にする] が無効になっていることを確認します。

- ビジネスセキュリティサーバでのパフォーマンスが 低下した場合には、エージェントを従来型スキャンに切り替えてください。エージェントからの検索クエリをすべて迅速に処理できないことを示している可能性があります。

次の表に、検索方法を切り替える際のいくつかの考慮事項を示します。

表 5-3. 検索方法を切り替える際の考慮事項

考慮事項	詳細
ビジネスセキュリティサーバの接続	セキュリティエージェントがビジネスセキュリティサーバに接続できることを確認します。別の検索方法に切り替えたとき、オンラインのエージェントのみに通知されます。オフラインのエージェントは、オンラインになったときに通知されます。 また、エージェントではビジネスセキュリティサーバから新しいコンポーネントをダウンロードする必要があるため、ビジネスセキュリティサーバに最新のコンポーネントがあることを確認してください。具体的には、スマートスキャンエージェントパターンファイル (スマートスキャンに切り替わるエージェントの場合) およびウイルスパターンファイル (従来型スキャンに切り替わるエージェントの場合) です。
切り替わるセキュリティエージェントの数	一度に切り替わるセキュリティエージェントの数が比較的少数である場合は、ビジネスセキュリティサーバのリソースを効率的に使用することが可能です。ビジネスセキュリティサーバでは、エージェントが検索方法を変更する間も、その他の重要なタスクを実行できます。
タイミング	セキュリティエージェントを初めて切り替えるとき、エージェントでは、スマートスキャンエージェントパターンファイル (スマートスキャンに切り替わるエージェントの場合) またはウイルスパターンファイル (従来型スキャンに切り替わるエージェントの場合) を全部ダウンロードする必要があります。 ダウンロード処理が短い時間で終了するように、切り替えをオフピーク時に行うことを検討してください。また、ユーザが開始するアップデートを回避するために一時的にエージェントでの「今すぐアップデート」を無効にして、エージェントが検索方法の切り替えを完了した後で再度有効にしてください。 **注意** それ以降エージェントでは、高い頻度でアップデートを実行するたびに、スマートスキャンエージェントパターンファイルまたはウイルスパターンファイルのサイズの小さな増分がダウンロードされます。

考慮事項	詳細
IPv6 のサポート	IPv6 シングルスタックのスマートスキャンエージェントがオフラインである場合、Trend Micro Smart Protection Network にクエリを直接送信できません。 このような場合にスマートスキャンクライアントでクエリを送信できるようにするために、IP アドレスを変換可能なデュアルスタックプロキシサーバ (DeleGate など) が必要です。

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [検索方法] に移動します。
5. 必要な検索方法を選択します。
6. [保存] をクリックします。

セキュリティエージェントのリアルタイム検索

リアルタイム検索は、セキュリティエージェントで、ファイルが開かれたり、ダウンロード、コピー、または変更されたりするたびに、ファイルを検索し脅威が含まれていないかどうかを確認します。

セキュリティエージェントのリアルタイム検索の設定

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。

4. [ウイルス/スパイウェア対策] をクリックします。

   新しい画面が表示されます。

5. [リアルタイムのウイルス 対策/スパイウェア対策を有効にする] を選択します。

6. 検索設定を指定します。詳細については、124 ページの「セキュリティエージェントの検索対象と処理」を参照してください。

   注意

   ユーザに自分の検索設定を指定できる権限を付与している場合は、そのユーザの指定した設定が検索で使用されます。

7. [保存] をクリックします。

機械学習型検索

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジを使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどのファイル機能を使用した詳細なファイル分析により未知のセキュリティリスクを検出します。また、不明なプロセスやあまり普及していないプロセスの挙動分析を実行して、ネットワークへの侵入を試みる未知の新しい脅威がないかどうかを判定します。

機械学習型検索は、未知の脅威およびゼロデイ攻撃から環境を保護するのに役立つ強力な検索方法です。

検出の種類	説明
ファイル	不明なファイルやあまり普及していないファイルを検出すると、セキュリティエージェントは、高度な脅威検索エンジン (ATSE) でファイルを検索してファイル特性を抽出し、Trend Micro Smart Protection Network でホストされる機械学習型検索エンジンにレポートを送信します。機械学習型検索では、不正プログラムモデリングにより、サンプルを不正プログラムモデルと比較し、可能性スコアを割り当て、ファイルに含まれる潜在的な不正プログラムの種類を判別します。 機械学習型検索の設定に応じて、ネットワークへの脅威の拡散を防ぐために、セキュリティエージェントは該当するファイルの「隔離」を試みます。
プロセス	不明なプロセスやあまり普及していないプロセスを検出すると、セキュリティエージェントは、CI エンジンを使用してプロセスを監視し、動作レポートを機械学習型検索エンジンに送信します。 機械学習型検索では、不正プログラムの動作モデリングにより、サンプルをモデルと比較し、可能性のスコアを割り当て、プロセスが実行する潜在的な不正プログラムの種類を判別します。 機械学習型検索の設定に応じて、セキュリティエージェントは該当するプロセスまたはスクリプトを「終了」し、プロセスまたはスクリプトを実行したファイルの駆除を試みます。

機械学習型検索を設定する

注意

機械学習型検索では下記についての確認が必要です。

- [ポリシーの設定] > [挙動監視] で挙動監視が有効になっていること
- Smart Protection Network に接続できること

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。

3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。

4. [機械学習型検索] をクリックします。

5. [機械学習型検索を有効にする] を選択します。

6. 機械学習型検索で実行する検出の種類とそれに対する処理を選択します。

検出の種類	処理
ファイル	• 隔離: 機械学習型検索による分析で不正プログラムに似た特性を示すと判定されたファイルを自動的に隔離する場合に選択します。 • ログのみ: 脅威について内部で詳しく調査するために、不明なファイルを検索して機械学習型検索による分析をログに記録する場合に選択します。
プロセス	• 終了: 機械学習型検索による分析で不正プログラムに似た挙動を示すと判定されたプロセスまたはスクリプトを自動的に終了する場合に選択します。 **重要** 機械学習型検索は、不正なプロセスまたはスクリプトを実行したファイルの駆除を試みます。駆除に失敗した場合、該当するファイルはセキュリティエージェントによって隔離されます。 • ログのみ: 脅威について内部で詳しく調査するために、不明なプロセスまたはスクリプトを検索して機械学習型検索による分析をログに記録する場合に選択します。

7. [保存] をクリックします。

挙動監視

セキュリティエージェントは常にクライアントを監視し、OS やインストール済みのソフトウェアに異常な変更が加えられていないかどうかを確認します。管理者またはユーザは、監視対象の変更に違反する場合に特定のプログラムを起動できるように除外リストを作成するか、または特定のプログラムをブロックすることができます。また、有効なデジタル署名を持つプログラムは常に起動が許可されます。

挙動監視のもう 1 つの機能は、EXE および DLL ファイルが削除または変更されないよう保護することです。挙動監視が有効な場合、ユーザは、除外設定を作成して、特定のプログラムを承認するかブロックできます。

挙動監視を設定する

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [挙動監視] をクリックします。
5. 必要に応じて次の項目を設定します。
   - 挙動監視の有効化

     注意

     ユーザが自分の挙動監視設定をカスタマイズできるようにするには、[デバイス] > {グループ名} > [ポリシーの設定] > [エージェントの権限] > [挙動監視] の順に進んで、[ユーザに挙動監視設定の変更を許可する] にチェックを入れます。
   - [不正プログラムの挙動ブロックを有効にする]: 不正プログラム挙動ブロックは、パターンファイルに定義されている一連の内部ルールを使用して実行されます。これらのルールは、不正プログラムに共

通する既知の不審な脅威の挙動を識別します。不審な挙動の例として、突然説明できない動作をするサービスの追加、ファイアウォールの変更、システムファイルの改ざんなどが挙げられます。

不正プログラム挙動監視は次の脅威レベルの検索オプションを提供します。

- [既知の脅威]: 既知の脅威に関連付けられた挙動をブロックします。
- [既知および潜在的な脅威]: 既知の脅威に関連付けられた挙動をブロックし、潜在的に不正な挙動に対して処理を実行します。

- HTTP またはメールアプリケーションを介してダウンロードされた新しいプログラムを実行する前にユーザに確認する (サーバプラットフォームは除く):挙動監視では、Web レピュテーションサービスと連携し、HTTP チャネル経由でダウンロードされたファイルの利用状況を検証します。新しいファイルが検出された場合、管理者は、ユーザがファイルを実行する前にその旨を通知するかどうかを選択できるます。トレンドマイクロの Smart Protection Network では、ファイルの検出数またはファイル作成からの存続期間などから、検出数の少ない特定のプログラムを「新しく検出されたプログラム」として分類します。

注意

HTTP チャネルの場合は、実行可能ファイル (.exe) が検索されます。メールアプリケーション (Outlook および Windows Live Mail のみ) の場合は、パスワード保護されていないアーカイブファイル (zip/rar) 内の実行可能ファイル (.exe) が検索されます。

- ランサムウェア対策:「ランサムウェア」の脅威によるコンピュータ上のファイルの不正な変更または暗号化を防止します。ランサムウェアは不正プログラムの一種で、ファイルへのアクセスを制限し、ファイルの復元と引き換えに金銭を要求してきます。
  - [不正な暗号化や変更から文書を保護]: 不正な変更から文書を保護します。
    - 不審なプログラムによって変更されたファイルを自動的にバックアップして復元:文書の保護が有効に設定されている

場合に、不審なプログラムによって変更されたファイルのバックアップを自動的に作成します。

- [ランサムウェアに関連付けられていることの多いプロセスをブロック]: ハイジャックに関連していることが多いプロセスをブロックすることで、ランサムウェアの攻撃からエンドポイントを保護します。
- (デスクトップグループのみ) [プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック]: ランサムウェアに似た挙動をするプロセスがないかを監視することで、検出を強化します。
- 脆弱性攻撃に関連する異常な挙動を示すプログラムを終了: 脆弱性対策とプログラム検査が連携してプログラムの挙動を監視し、プログラムの脆弱性を利用した攻撃が疑われる異常な挙動を検出します。検出されると、挙動監視によってプログラムのプロセスが終了されます。

注意

脆弱性対策を使用するには、[プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック] を選択する必要があります。

注意

ビジネスセキュリティによって安全なプロセスが不正なプロセスとして検出される率を下げるには、コンピュータをインターネットに接続し、トレンドマイクロサーバによる追加の確認プロセスを実行できるようにする必要があります。

- [除外設定]: 除外設定には、承認済みプログラムリストとブロックするプログラムリストが含まれます。承認済みプログラムリスト内のプログラムは、監視対象の変更に違反する場合でも起動できます。一方、ブロックするプログラムリスト内のプログラムはいかなる場合でも起動することはできません。
  - [プログラムのフルパスを入力]: プログラムの Windows または UNC のフルパスを入力します。複数のエントリはセミコロン

(;) で区切ります。[承認済みリストに追加する] または [ブロックリストに追加する] をクリックします。必要に応じて、環境変数を使用してパスを指定します。

- [承認済みプログラムリスト]: このリスト内のプログラムは起動できます。エントリを削除するには、削除アイコンをクリックします。

  承認済みプログラムリストでは、ワイルドカードと環境変数がサポートされます。

  サポートされる環境変数については、94 ページの「サポートされている環境変数」を参照してください。

- [ブロックするプログラムリスト]: このリスト内のプログラムは起動できません。エントリを削除するには、削除アイコンをクリックします。

  ブロックするプログラムリストでは、ワイルドカードのみがサポートされます。

6. [保存] をクリックします。

サポートされている環境変数

次の表は、ファイルおよびフォルダをリストに追加する際に使用できる環境変数を示しています。

環境変数	例	対応するパス
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe

環境変数	例	対応するパス
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{現在のユーザアカウント}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

信頼済みプログラム

信頼済みプログラムリスト内のプログラムは、不審なファイルアクセスの監視対象から除外されます。

信頼済みプログラムを設定する

注意

信頼済みプログラムリストでは、ワイルドカードと環境変数はサポートされません。

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [信頼済みプログラム] をクリックします。

   新しい画面が表示されます。

5. 不審なファイルアクセスの監視対象からプログラムを除外するには、そのファイルの特定の完全パスを入力して [信頼済みプログラムリストに追加] をクリックします。

   <ドライブ名>:¥<パス>¥<ファイル名>

   例 1:C:¥Windows¥system32¥regedit.exe

   例 2:D:¥backup¥tool.exe

   完全パスを入力するのは、信頼済みプログラムリストに追加されているプログラム名がハッカーに悪用されないよう防止するためです。

6. [保存] をクリックします。

隔離ディレクトリ

感染ファイルの処理が「隔離」の場合、セキュリティエージェントはファイルを暗号化して、一時的に次の場所にある隔離ディレクトリに移動します。

- <セキュリティエージェントインストールフォルダ >¥quarantine(エージェントをバージョン 6.x 以前からアップグレードした場合)
- <セキュリティエージェントインストールフォルダ >¥SUSPECT¥Backup (エージェントを初めてインストールしたか、バージョン 7.x 以降からアップグレードした場合)

セキュリティエージェントは、感染したファイルをビジネスセキュリティサーバで設定した隔離ディレクトリに送付します。このディレクトリは Web コンソールの [デバイス] > {グループ名} > [ポリシーの設定] > [隔離] で設定できます。

初期設定の隔離ディレクトリ

初期設定の隔離ディレクトリは、ビジネスセキュリティサーバにあります。このディレクトリは URL 形式で、http://server のようにビジネスセキュリティサーバのホスト名または IP アドレスを含みます。対応するビジネスセキュリティサーバ内での保管場所は <ビジネスセキュリティサーバインストールフォルダ>¥PCCSRV¥Virus になります。

- サーバで IPv4 および IPv6 エージェントの両方を管理している場合、すべてのエージェントが隔離ファイルをサーバに送信できるようにホスト名を使用してください。

- サーバが、IPv4 アドレスしか与えられていないか、IPv4 アドレスのみで識別可能な場合には、IPv4 シングルスタックのエージェントとデュアルスタックのエージェントのみで隔離ファイルをサーバに送信できます。
- サーバが、IPv6 アドレスしか与えられていないか、IPv6 アドレスのみで識別可能な場合には、IPv6 シングルスタックのエージェントとデュアルスタックのエージェントのみで隔離ファイルをサーバに送信できます。

代替の隔離ディレクトリ

URL、UNC パス、または絶対ファイルパスの形式で場所を入力することで、代替の隔離ディレクトリを指定できます。セキュリティエージェントからは、このディレクトリに接続できる必要があります。たとえば、このディレクトリが、隔離ファイルをデュアルスタックやシングルスタックの IPv6 エージェントから受信する場合、IPv6 アドレスを与える必要があります。デュアルスタックディレクトリを指定し、そのディレクトリをホスト名で識別して、さらにディレクトリを入力するときは UNC パスを使用することをお勧めします。

隔離ディレクトリの指定に関するガイドライン

次の表に、URL、UNC パス、絶対ファイルパスを使用する際の参考情報を示します。

表 5-4. 隔離ディレクトリ

隔離ディレクトリ	使用可能形式	例	注意
ビジネスセキュリティサーバの初期設定ディレクトリ	URL	`http://` <サーバホスト名または IP>	初期設定ディレクトリをそのまま使用する場合は、隔離フォルダのサイズなど、そのディレクトリの管理設定を [管理] > [グローバル設定] > [システム] タブ > [隔離フォルダ設定] で指定してください。
	UNC パス	¥¥<サーバホスト名または IP>¥ofcscan¥Virus	

隔離ディレクトリ	使用可能形式	例	注意
ビジネスセキュリティサーバのその他のディレクトリ	UNC パス	¥¥<サーバホスト名または IP>¥ D$ ¥Quarantined Files	初期設定ディレクトリを使用しない場合 (たとえばディスクス容量が不足しているなど)、別のディレクトリへの UNC パスを入力します。これを行う場合は、対応する絶対パスを [管理] > [グローバル設定] > [システム] タブ > [隔離フォルダ設定] で入力して、管理設定が反映されるようにします。
他のビジネスセキュリティサーバコンピュータのディレクトリ (ネットワークに他のビジネスセキュリティサーバがある場合)	URL	http:// <サーバ 2 ホスト名または IP>	エージェントから、このディレクトリに接続できるようにしてください。間違ったディレクトリを指定した場合、エージェントは正しい隔離ディレクトリが指定されるまで隔離ファイルを保持します。サーバのウイルス/不正プログラムログでは、検索結果が「隔離のためのビジネスセキュリティサーバへのファイルアップロードが実行できません。」となります。 UNC パスを使用する場合、隔離ディレクトリフォルダを「Everyone」グループに加えて、このグループに読み取りと書き込みの権限を割り当ててください。
	UNC パス	¥¥<サーバ 2 ホスト名または IP>¥ ofcscan¥Virus	
ネットワークのその他のコンピュータ	UNC パス	¥¥<コンピュータ名>¥temp	
クライアントの別のディレクトリ	絶対パス	C:¥temp	次の場合には絶対パスを指定してください。 • 隔離されたファイルをクライアントのみで保持する場合。 • クライアントの初期設定ディレクトリにファイルを格納することが望ましくない場合。 このパスが存在しない場合、セキュリティエージェントにより自動的に作成されます。

隔離ディレクトリを設定する

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [隔離] をクリックします。

   新しい画面が表示されます。
5. 隔離ディレクトリを設定します。詳細については、96 ページの「隔離ディレクトリ」を参照してください。
6. [保存] をクリックします。

Web レピュテーション

Web レピュテーションでは、セキュリティリスクの危険性のある Web の URL またはメールに埋め込まれている URL へのアクセスを防止します。Web レピュテーションは、URL の評価をトレンドマイクロの Web レピュテーションサーバに照会し、その評価とクライアントに適用されている特定の Web レピュテーションポリシーを関連付けます。実行する処理は、適用されているポリシーに応じて異なります。

- セキュリティエージェントでは、Web サイトへのアクセスがブロックまたは許可されます。

Web レピュテーションでは、検出された Web 脅威を、管理者には通知設定に基づいてメールで、ユーザにはオンラインで通知します。

セキュリティエージェントに対して、クライアントの場所 (オフィス内/オフィス外) に応じた異なるレベルのセキュリティを設定します。

Web レピュテーションが URL をブロックしても、その URL が安全であると判断した場合は、承認済み URL リストにその URL を追加します。

ヒント

ネットワーク帯域幅を節約するには、企業の内部 Web サイトを Web レピュテーションの承認済み URL リストに追加することをお勧めします。

評価スコア

URL が Web からの脅威かどうかは、その URL の「評価スコア」によって判定されます。このスコアは、トレンドマイクロ独自の基準値を使用して計算されます。

トレンドマイクロでは、スコアが定義済みのしきい値内にある URL を Web からの脅威と見なし、しきい値を超えている URL を安全であるとみなします。

セキュリティエージェントには、URL へのアクセスを許可するかブロックするかを判定するための次の 3 つのセキュリティレベルがあります。

- 高 – ブロックするページは次のとおりです。
  - 危険: 詐欺サイトや脅威の既知の送信元であることが確認されました
  - 極めて不審: 詐欺サイトまたは脅威の送信元である可能性があります
  - 不審: スパムメールに関連付けられている、またはセキュリティ侵害の可能性があります
  - 未評価: トレンドマイクロは、安全のために Web ページを積極的にテストしていますが、ユーザが新しい Web サイトやあまり利用されない Web サイトにアクセスすると、未評価のページに遭遇する可能性があります。未評価のページへのアクセスをブロックすると、安全性は向上しますが、安全なページへのアクセスもブロックされる場合があります。
- 中 – ブロックするページは次のとおりです。
  - 危険: 詐欺サイトや脅威の既知の送信元であることが確認されました
  - 極めて不審: 詐欺サイトまたは脅威の送信元である可能性があります

- 低 – ブロックするページは次のとおりです。
  - 危険: 詐欺サイトや脅威の既知の送信元であることが確認されました

セキュリティエージェントの Web レピュテーションを設定する

Web レピュテーションは、HTTP/HTTPS リクエストごとにトレンドマイクロの脅威データベースにクエリを実行し、要求された各 URL のセキュリティリスクを評価します。

注意

[ロケーション認識] が無効な場合は、オフィス外の接続にオフィス内の設定が適用されます。ロケーション認識の詳細については、187 ページの「デスクトップ/サーバの設定」を参照してください。

Web レピュテーションとブラウザ脆弱性対策の両方が有効な場合、Web レピュテーションによってブロックされない URL は、その後、ブラウザ脆弱性対策によって検索されます。ブラウザ脆弱性対策は、jar、class、pdf、swf、html、js など、URL の Web ページに埋め込まれたオブジェクトを検索します。

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [Web レピュテーション] > [オフィス内] または [Web レピュテーション] > [オフィス外] をクリックします。

   新しい画面が表示されます。
5. 必要に応じて次の項目をアップデートします。
   - Web レピュテーションを有効にする

- セキュリティレベル:[高]、[中]、または [低]
- ブラウザ脆弱性対策:不正スクリプトを含むページをブロックする

6. [保存] をクリックします。

URL フィルタ

URL フィルタを使用すると、Web サイトへのアクセスを制御して、従業員の非生産的な時間を削減し、インターネット帯域幅の使用率を軽減して、より安全なインターネット環境を確立できます。URL フィルタの保護レベルを選択したり、スクリーニングを行う Web サイトの種類をカスタマイズしたりできます。

注意

顧客を保護するため、トレンドマイクロは、世界の多くの場所で違法と考えられるコンテンツを含むすべての URL を自動的にブロックします。

URL フィルタを設定する

[カスタム] を選択すると、1 日のさまざまな時間帯でブロックする特定の種類の Web サイトを選択できます。

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [URL フィルタ] をクリックします。

   新しい画面が表示されます。
5. 必要に応じて次の項目をアップデートします。
   - URL フィルタを有効にする

- フィルタ強度
  - 高 — 既知のまたは潜在的なセキュリティ上の脅威、不適切なコンテンツまたは攻撃的な可能性のあるコンテンツ、生産性または帯域幅に影響を与える可能性のあるコンテンツ、および評価のないページをブロックします。
  - 中 — 既知のセキュリティ上の脅威および不適切なコンテンツをブロックします。
  - 低 — 既知のセキュリティ上の脅威をブロックします。
  - カスタム — 独自でカテゴリを選択し、業務時間または業務時間外にそれらのカテゴリをブロックするかどうかを指定します。
- 業務時間 — [業務時間] で指定されていない曜日または時間は、すべて業務時間外と見なされます。

6. [保存] をクリックします。

承認済み/ブロックする URL

URL の自動的な承認およびブロック機能は、Web サイトへのアクセスを制御し、より安全なインターネット環境を構築するために役立ちます。承認済み URL やブロックする URL は [グローバル設定] で識別できます。

カスタマイズした URL の承認およびブロックリストを特定のグループに対して作成することもできます。[このグループの承認済み/ブロックする URL をカスタマイズする] オプションが選択されている場合、セキュリティエージェントはグループのカスタマイズされた承認済み URL またはブロックする URL のリストを使用して、Web サイトへのアクセスを制御します。

承認済み/ブロックする URL を設定する

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

[ポリシーの設定: <グループ名>] 画面が表示されます。

4. [承認済み/ブロックする URL] をクリックします。

   新しい画面が表示されます。

5. 必要に応じて次の設定を更新します。

   - [このグループの承認済み/ブロックする URL をカスタマイズする]: この URL リストの設定は、他のすべての設定に優先されます。
   - [承認済み URL] ボックスで、Web レピュテーションと URL フィルタの検証から除外する Web サイトの URL を入力します。複数の URL を指定する場合は、セミコロン (;) で区切って入力してください。[追加] をクリックします。

     ヒント

     グローバル設定で登録したすべての URL を使用するには、[グローバル設定からインポート] をクリックします。この URL をグループ用にカスタマイズできます。

   - [ブロックする URL] ボックスで、URL フィルタ中にブロックする Web サイトの URL を入力します。複数の URL を指定する場合は、セミコロン (;) で区切って入力してください。[追加] をクリックします。

     ヒント

     グローバル設定で登録したすべての URL を使用するには、[グローバル設定からインポート] をクリックします。この URL をグループ用にカスタマイズできます。

6. [保存] をクリックします。

ファイアウォール

ファイアウォールを使用すると、クライアントとネットワークの間に障壁を作成することにより、特定の種類のネットワークトラフィックを拒否または許可できます。また、クライアントに対する攻撃が疑われるネットワークパケットのパターンを特定できます。

ビジネスセキュリティでは、ファイアウォールを設定する際、簡単モードと詳細モードの 2 つのオプションのいずれかを選択できます。簡単モードでは、推奨されている初期設定でファイアウォールを使用できます。詳細モードは、ファイアウォールの設定をカスタマイズするために使用します。

ヒント

ファイアウォールをインストールして有効化する前に、その他のファイアウォールソフトウェアをアンインストールすることをお勧めします。

ファイアウォールの簡単モードの初期設定

ファイアウォールの初期設定によって、クライアントのファイアウォールによる保護を開始するための基本的な設定が提供されます。初期設定は、インターネットにアクセスする必要性や FTP を使用したファイルのダウンロードまたはアップロードなど、クライアント上で生じる可能性のある一般的な状況に対応することを目的としています。

注意

ビジネスセキュリティの初期設定では、すべての新しいグループとセキュリティエージェント上でファイアウォールは無効になっています。

表 5-5. ファイアウォールの初期設定

設定	ステータス
セキュリティレベル	低 受信トラフィックと送信トラフィックが許可され、ネットワークウイルスだけがブロックされます。
IDS (侵入検知システム)	無効
警告メッセージ	無効

表 5-6. ファイアウォールの除外設定の初期設定

除外設定	処理	方向	プロトコル	ポート番号
DNS	許可	送受信	TCP/UDP	53
NetBIOS	許可	送受信	TCP/UDP	137, 138, 139, 445
HTTPS	許可	送受信	TCP	443
HTTP	許可	送受信	TCP	80
Telnet	許可	送受信	TCP	23
SMTP	許可	送受信	TCP	25
FTP	許可	送受信	TCP	21
POP3	許可	送受信	TCP	110
MSA	許可	送受信	TCP	16372, 16373
LDAP	許可	送受信	TCP/UDP	389

表 5-7. 場所に応じたファイアウォールの初期設定

場所	ファイアウォール設定
オフィス内	オフ
オフィス外	オフ

トラフィックのフィルタリング

ファイアウォールは、次の条件に基づいて特定の種類のトラフィックをブロックする機能を備えており、すべての送受信トラフィックをフィルタします。

- 方向 (受信/送信)
- プロトコル (TCP/UDP/ICMP/ICMPv6)
- ポート
- コンピュータ

ネットワークウイルスの検索

ファイアウォールはネットワークウイルスについても 各パケットを調べます。

ステートフルインスペクション

ファイアウォールは、ステートフルインスペクションファイアウォールであり、クライアント上のすべての接続を監視します。ファイアウォールは、接続内の特定の状況を識別し、どの処理を追跡する必要があるかを予測して、通常の接続から逸脱した時点でそれを検出します。そのため、ファイアウォールの効果的な使用には、プロファイルやポリシーの作成だけでなく、接続の分析やファイアウォールを通過するパケットのフィルタも 必要となります。

ファイアウォールドライバ

ファイアウォールドライバは、ユーザ定義のファイアウォール設定と連動して、大規模感染時にポートをブロックします。また、ネットワークウイルスパターンファイルを使用して、ネットワークウイルスを検出します。

ファイアウォールを設定する

オフィス内およびオフィス外に対してファイアウォールを設定します。[ロケーション認識] が無効な場合は、オフィス外の接続にオフィス内の設定が適用されます。

ロケーション認識の詳細については、187 ページの「デスクトップ/サーバの設定」を参照してください。

初期設定ではファイアウォールは無効になっています。

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。

4. [ファイアウォール] > [オフィス内] または [オフィス外] をクリックします。
5. [ファイアウォールを有効にする] をオンにします。
6. 次のいずれかを選択します。
   - 簡単モード ― ファイアウォールを初期設定で有効にします。

     詳細については、104 ページの「ファイアウォール」を参照してください。
   - 詳細モード ― ファイアウォールをカスタム設定で有効にします。
7. [詳細モード] を選択した場合は、必要に応じて次のオプションをアップデートします。
   - セキュリティレベル ― セキュリティレベルは、除外リストにないポートに適用されるトラフィックルールを制御します。
     - 高 ― 除外リストで許可されているトラフィックを除き、すべての受信および送信トラフィックをブロックします。
     - 中 ― 除外リストで許可またはブロックされているトラフィックを除き、すべての受信トラフィックをブロックしてすべての送信トラフィックを許可します。
     - 低 ― 除外リストでブロックされているトラフィックを除き、すべての受信および送信トラフィックを許可します。これは、簡単モードの初期設定です。
   - 設定
     - IDS (侵入検知システム) を有効にする ― 侵入検知システムが、攻撃すると疑われるネットワークパケットのパターンを特定します。

       詳細については、255 ページの「侵入検知システム (IDS)」を参照してください。
     - 警告メッセージを有効にする ― ビジネスセキュリティが違反を検出すると、クライアントは通知を受け取ります。
   - 除外設定 ―除外リストで許可するように指定したポートはブロックされません。

詳細については、109 ページの「ファイアウォールの除外設定を使用する」を参照してください。

8. [保存] をクリックします。

ファイアウォールの除外設定を使用する

ファイアウォール除外リストには、クライアントのポート番号と IP アドレスに基づいてさまざまな種類のネットワークトラフィックを許可またはブロックするように設定できる項目が含まれています。

たとえば、大規模感染が発生したときに、HTTP ポート (80 番ポート) を含むすべてのクライアントトラフィックをブロックするように 選択したとします。この場合でも、ブロック設定を適用したクライアントに対してインターネットへのアクセスを許可したい場合は、除外リストにその Web プロキシサーバを追加できます。

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [ファイアウォール] > [オフィス内] または [オフィス外] をクリックします。

   新しい画面が表示されます。
5. [ファイアウォールを有効にする] をオンにします。
6. [詳細モード] を選択します。
7. 除外設定を追加するには
   a. [追加] をクリックします。

      新しい画面が表示されます。
   b. 除外設定の名前を入力します。

c. [処理] の隣で、次のいずれかをクリックします。

- ネットワークトラフィックを許可
- ネットワークトラフィックを拒否

d. [方向] の隣の [受信] または [送信] チェックボックスをオンにして、除外設定を適用するトラフィックの種類を選択します。

e. [プロトコル] リストから、ネットワークプロトコルの種類を選択します。

- すべて
- TCP/UDP (初期設定)
- TCP
- UDP
- ICMP
- ICMPv6

f. 次のいずれかを選択して、クライアントポートを指定します。

- すべてのポート (初期設定)
- 範囲 — ポートの範囲を入力します。
- 指定ポート — 個々のポートを指定します。ポート番号を区切るには、カンマ「,」を使用します。

g. [コンピュータ] で、クライアントの IP アドレスを選択し、除外設定に追加します。たとえば、[ネットワークトラフィックを拒否] ([受信] および [送信]) を選択し、ネットワーク上のクライアントの IP アドレスを入力した場合、ポリシーにこの除外設定があるクライアントは、その IP アドレスに対するデータの送受信を実行できません。次のいずれかを選択します。

- すべての IP アドレス (初期設定)
- 単一 IP — IPv4 アドレスまたは IPv6 アドレス、もしくはホスト名を入力します。ホスト名から IP アドレスを解決するには、[名前解決] をクリックします。

- IP 範囲 (IPv4 または IPv6) — [開始値] および [終了値] フィールドに、2 つの IPv4 アドレスまたは IPv6 アドレスのいずれかを入力します。一方のフィールドに IPv6 アドレスを入力し、もう一方のフィールドに IPv4 アドレスを入力することはできません。
- IP 範囲 (IPv6) — IPv6 アドレスのプレフィックスと 長さを入力します。

h. [保存] をクリックします。

8. 除外設定を編集するには、[編集] をクリックして、表示される画面の設定を変更します。
9. 除外設定をリスト内で上または下に移動するには、除外設定を選択して、目的の位置まで [上に移動] または [下に移動] をクリックします。
10. 除外設定を削除するには、除外設定を選択し、[削除] をクリックします。

エージェントグループのファイアウォールを無効にする

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [ファイアウォール] > [オフィス内] または [オフィス外] をクリックします。

   新しい画面が表示されます。
5. [ファイアウォールを有効にする] をオフにします。
6. [保存] をクリックします。

すべてのエージェントでファイアウォールを 無効にする

手順

1. [管理] > [グローバル設定] に移動します。
2. [デスクトップ/サーバ] をクリックします。
3. [ファイアウォール] で、[ファイアウォールを無効にしてドライバをアンインストールする] をオンにします。
4. [保存] をクリックします。

デバイスコントロール

デバイスコントロールは、デバイスに接続された外部ストレージデバイスへのアクセスを調整します。特に、USB インターフェースで 接続されたあらゆる種類のストレージデバイスへのアクセスが制限されます。ただし、モバイルデバイスとデジタルカメラは例外です。

デバイスコントロールを設定する

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [デバイスコントロール] をクリックします。
5. 必要に応じて次の項目をアップデートします。
   - デバイスコントロールを有効にする
   - USB 自動実行防止を有効にする
   - 権限: USB デバイスとネットワークリソースの両方に設定します。

表 5-8. デバイスコントロールの権限

権限	デバイス上のファイル	受信ファイル
フルアクセス	許可される操作: コピー、移動、開く、保存、削除、実行	許可される操作: 保存、移動、コピー ファイルをデバイスに保存、移動、およびコピーできます。
アクセス権なし	禁止される操作: すべての操作 ユーザはデバイスとそれに含まれるファイルを表示できます (たとえば、Windows Explorer から)。	禁止される操作: 保存、移動、コピー
読み取り	許可される操作: コピー、開く 禁止される操作: 保存、移動、削除、実行	禁止される操作: 保存、移動、コピー
変更	許可される操作: コピー、移動、開く、保存、削除 禁止される操作: 実行	許可される操作: 保存、移動、コピー
読み取りおよび実行	許可される操作: コピー、開く、実行 禁止される操作: 保存、移動、削除	禁止される操作: 保存、移動、コピー

- 除外設定: 特定のデバイスに対して読み取りアクセス権がないユーザでも、除外リストに含まれるファイルまたはプログラムについてはすべて、実行および開く操作が許可されます。

  ただし、USB 自動実行防止を有効にしている場合は、除外リストに含まれるファイルであっても、実行することはできません。

  除外リストにエントリを追加するには、パスまたはデジタル署名も含めてファイル名を入力し、[除外リストに追加する] をクリックします。

6. [保存] をクリックします。

ユーザツール

- 迷惑メール対策ツールバー: Microsoft Outlook でスパムメールをフィルタして、統計値を示し、特定の設定を変更することができます。
- ケース診断ツール: トレンドマイクロケース診断ツール (CDT) は、問題の発生時に顧客の製品から必要なデバッグ情報を収集します。このツールは製品のデバッグステータスのオン/オフを自動的に切り替え、問題のカテゴリに応じて必要なファイルを収集します。トレンドマイクロはこの情報を使用して、製品に関連した問題をトラブルシューティングします。

  このツールはセキュリティエージェントのコンソール 上から確認できます。
- クライアント/サーバ通信ツール:クライアント/サーバ通信の問題解決に使用します。

  このツールはセキュリティエージェントのコンソール 上から確認できます。

ユーザツールを設定する

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [ユーザツール] をクリックします。

   新しい画面が表示されます。
5. 必要に応じて次の項目をアップデートします。
   - 迷惑メール対策ツールバー: Microsoft Outlook でスパムメールをフィルタします。

6. [保存] をクリックします。

エージェントの権限

エージェントの権限を付与すると、ユーザはクライアント上のセキュリティエージェントの設定を変更できます。

ヒント

組織全体に統制されたセキュリティポリシーを適用するには、ユーザには限定的な権限のみ与えることをお勧めします。これによって、ユーザが検索設定を変更したり、セキュリティエージェントをアンロードしたりするのを防ぐことができます。

エージェントの権限を設定する

手順

1. [デバイス] に移動します。
2. デスクトップまたはサーバグループを 選択します。
3. [ポリシーの設定] をクリックします。

   [ポリシーの設定: <グループ名>] 画面が表示されます。
4. [エージェントの権限] をクリックします。
5. 必要に応じて次の項目を設定します。

セクション	権限
ウイルス/スパイウェア対策	• リアルタイム検索の設定 • 手動検索の設定 • 予約検索の設定 • 予約検索のスキップ
ファイアウォール	ファイアウォール設定

セクション	権限
Web レピュテーション - 閲覧を続ける	コンピュータを再起動するまで特定の不正 URL の閲覧を続けることをユーザに許可するリンクを表示します。警告は引き続き他の不正 URL に表示されます。
URL フィルタ - 閲覧を続ける	コンピュータを再起動するまで特定の制限付き URL の閲覧を続けることをユーザに許可するリンクを表示します。警告は引き続き他の制限付き URL に表示されます。
挙動監視	挙動監視タブを表示し、ユーザによるリストのカスタマイズを許可します。
信頼済みプログラム	信頼済みプログラムの一覧の変更をユーザに許可します。
プロキシ設定	プロキシの設定をユーザに許可します。 注意 この機能を無効にすると、プロキシ設定が初期設定にリセットされます。

セクション	権限
アップデート権限	• 手動アップデートの実行を許可 • トレンドマイクロのアップデートサーバを 2 次アップデート元として使用 • 自動でのビルドのバージョンアップ、HotFix、Critical Patch、Patch、Service Pack を無効にする **注意** HotFix、Patch、Critical Patch、Service Pack を大量のエージェントに同時に配布すると、ネットワークトラフィックが著しく増加することがあります。配布の日時をずらせるように、複数のグループでこのオプションを有効にすることを検討してください。 このオプションを有効にすると、エージェントの自動ビルドバージョンアップが無効になりますが、自動バージョンアップ (たとえば、バージョン 7.x から現行バージョンにバージョンアップ) は無効になりません。自動バージョンアップを無効にするには、セキュリティサーバインストールパッケージを実行し、バージョンアップを遅らせるオプションを選択します。
ビジネスセキュリティエージェントセルフプロテクション	ユーザまたは他のプロセスがトレンドマイクロのプログラムファイル、レジストリ、プロセスを変更するのを防ぎます。

6. [保存] をクリックします。

第 6 章

検索の管理

本章では、セキュリティエージェントで検索を実行して、ネットワークとエージェントを脅威から保護する方法について説明します。

検索について

検索時にトレンドマイクロの検索エンジンは、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。各脅威には一意の「シグネチャ」、つまり他のコードと区別できる特性を表す文字列が含まれているので、このコードの実行機能を持たない断片がパターンファイルに取り込まれます。検索エンジンは、各検索対象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。

検索エンジンは、脅威を含むファイルを検出すると、駆除、隔離などの処理を実行します。これらの処理は、検索作業の設定時にカスタマイズできます。

ビジネスセキュリティ には、3 種類の検索があります。検索の種類によって目的と用途は異なりますが、設定の方法はほぼ同様です。

- リアルタイム検索。詳細については、120 ページの「リアルタイム検索」を参照してください。
- 手動検索。詳細については、121 ページの「手動検索」を参照してください。
- 予約検索。詳細については、123 ページの「予約検索」を参照してください。

セキュリティエージェントでは、検索の実行時に 2 つの検索方法のいずれかを使用することができます。

- スマートスキャン
- 従来型スキャン

詳細については、83 ページの「検索方法」を参照してください。

リアルタイム検索

リアルタイム検索は、セキュリティエージェントで、ファイルが開かれたり、ダウンロード、コピー、または変更されたりするたびに、ファイルを検索し脅威が含まれていないかどうかを確認します。リアルタイム検索の設定方法の詳細については、87 ページの「セキュリティエージェントのリアルタイム検索の設定」を参照してください。

手動検索

手動検索とは、必要に応じて実行する検索です。

手動検索では、セキュリティエージェントコンピュータ上のファイルから脅威を検出し、処理します。

検索に要する時間は、クライアントのハードウェアリソースと 検索するファイル数によって異なります。進行中の手動検索は、Web コンソールからリモートで実行された場合はビジネスセキュリティサーバの 管理者が、クライアントで直接実行された場合はユーザが停止できます。

ヒント

トレンドマイクロでは、大規模感染の発生後に手動検索を実行することをお勧めします。

注意

[検索] > [手動検索] 画面では、アグレッシブ検索を実行することはできません。

手動検索を実行する

この手順では、ビジネスセキュリティサーバの 管理者が、Web コンソールからセキュリティエージェント の手動検索を実行する方法について説明します。

注意

手動検索は、Windows タスクバーのセキュリティエージェントのアイコンを 右クリックして [手動検索] をクリックすることで、クライアントからも 直接実行できます。

手順

1. [検索] > [手動検索] に移動します。
2. 手動検索を実行する前に、設定を適用するグループを選択し、必要な手動検索の設定を行います。

手順と注意	推奨検索設定
セキュリティエージェントの検索設定をカスタマイズするには、デスクトップまたはサーバグループをクリックします。 124 ページの「セキュリティエージェントの検索対象と処理」を参照してください。 **注意** セキュリティエージェントの検索設定は、ユーザがクライアントから直接手動検索を実行する場合にも使用されます。ただし、ユーザに自分の検索設定を指定できる権限を付与している場合は、そのユーザの指定した設定が検索で使用されます。	検索対象 • すべての検索可能ファイル –検索可能なファイルをすべて検索に含めます。検索不能なファイルとは、パスワードで保護されたファイル、暗号化されたファイル、またはユーザ定義の検索制限を超えるファイルです。 • 圧縮ファイルを検索する最大レイヤ数: 1:圧縮ファイルの 1 階層までのファイルを検索します。初期設定のサーバグループでは「オフ」、デスクトップグループでは「オン」がそれぞれの初期設定になります。 検索除外 • トレンドマイクロ製品がインストールされているディレクトリを検索から除外する 詳細設定 • スパイウェアの承認済みリストの変更 (スパイウェア対策用)

3. 検索するグループのチェックボックスをオンにします。
4. [検索実行] をクリックします。

   ビジネスセキュリティサーバからエージェントに 対して、手動検索を実行するよう通知が送信されます。表示される [検索通知の結果] 画面に、通知を受信および受信しなかったエージェントの数が示されます。
5. 進行中の検索を停止するには、[検索停止] をクリックします。

   ビジネスセキュリティサーバからエージェントに 対して、手動検索を停止するよう別の通知が送信されます。表示される [検索通知停止の結果] 画面に、通知を受信および受信しなかったエージェントの数が示されます。検索の実行中にオフラインになった場合やネットワークが一時的に

切断された場合は、セキュリティエージェントが通知を受信できないことがあります。

予約検索

予約検索は設定した時刻と頻度で検索を実行します。

ヒント

ユーザやネットワークが破綻する危険性を最小限に抑制するために、予約検索はオフピーク時間に実行してください。

予約検索を設定する

自動アップデートと同じ時刻に検索を予約することはお勧めできません。これにより、予約検索が予定よりも早く停止してしまう可能性があります。同様に予約検索の実行中に手動検索を開始すると、予約検索が停止してしまいます。ただし、それ以降は予約に従って再度実行されます。

手順

1. [検索] > [予約検索] の順に移動します。
2. [スケジュール] タブをクリックします。
   a. 検索頻度 (毎日、週 1 回、または月 1 回) と開始時刻を設定します。各グループでは、独自の予約を指定できます。

      注意

      月 1 回の設定の場合、選択した日付が無い月は予約検索は実行されません。

   b. (オプション) [予約検索の完了後、クライアントをシャットダウンする] を選択します。
   c. [保存] をクリックします。
3. [設定] タブをクリックして、設定を適用するグループを選択し、必要な予約検索の設定を行います。

手順と注意	推奨検索設定
セキュリティエージェントの検索設定をカスタマイズするには、デスクトップまたはサーバグループをクリックします。124 ページの「セキュリティエージェントの検索対象と処理」を参照してください。 注意 ユーザに自分の検索設定を指定できる権限を付与している場合は、そのユーザの指定した設定が検索で使用されます。	検索対象 • すべての検索可能ファイル —検索可能なファイルをすべて検索に含めます。検索不能なファイルとは、パスワードで保護されたファイル、暗号化されたファイル、またはユーザ定義の検索制限を超えるファイルです。 • 圧縮ファイルを検索する最大レイヤ数: 2:圧縮ファイルの 2 階層までのファイルを検索します。
	検索除外 • トレンドマイクロ製品がインストールされているディレクトリを検索から除外する
	詳細設定 • スパイウェアの承認済みリストの変更 (スパイウェア対策用)

4. 予約検索の設定を適用するグループのチェックボックスをオンにします。

   注意
   予約検索を無効にするには、グループのチェックボックスをオフにします。

5. [保存] をクリックします。

セキュリティエージェントの検索対象と処理

検索のタイプ (手動検索、予約検索、およびリアルタイム検索) ごとに、次の設定をします。

検索するファイル

検索方法を選択します。

- すべての検索可能ファイル:検索可能なファイルをすべて検索に含めます。検索不能なファイルとは、パスワードで保護されたファイル、暗号化されたファイル、またはユーザ定義の検索制限を超えるファイルです。

  注意

  検索可能なファイルをすべて検索する場合、長い時間とリソースが必要になります。

- トレンドマイクロの推奨設定で検索されるファイルタイプ: 実際のファイルタイプに基づいてファイルを検索します。254 ページの「トレンドマイクロの推奨設定」を参照してください。
- 検索対象の拡張子の選択: 拡張子を基準にして検索対象ファイルを手動で指定します。複数のエントリがある場合には、カンマ (,) で区切ります。

検索条件を選択します。(リアルタイム検索のみ)

- 読み取り: コンテンツを読み取られたファイルを検索します。ファイルは、開かれたとき、実行されたとき、コピーされたとき、または移動されたときに読み取られます。
- 書き込み: コンテンツが書き込まれている最中のファイルを検索します。ファイルのコンテンツは、ファイルの変更、保存、ダウンロード、または別の場所からのコピーの際に書き込まれます。
- 読み取りまたは書き込み

除外設定

次の設定を指定可能です。

- 除外の有効化または無効化
- 検索からのトレンドマイクロ製品ディレクトリの除外
- 検索からのその他のディレクトリの除外

  指定したディレクトリパスのサブディレクトリもすべて 検索対象外となります。

- ファイル名、またはファイル名と完全パスの検索からの除外
- ファイル拡張子の除外

  ファイルの拡張子に「*」などのワイルドカード文字は使用できません。

詳細設定

検索の種類	オプション
リアルタイム検索	POP3 メッセージを検索する: 初期設定の場合、メール検索では、ポート 110 を介して送信され、受信ボックスと迷惑メールフォルダにある新着メッセージのみを検索できます。セキュア POP3 (SSL-POP3) はサポートされていません。 • Microsoft Outlook 2007、2010、または 2013 • Mozilla Thunderbird 1.5 以上 メール検索では、IMAP メッセージのセキュリティリスクは検出できません。
リアルタイム検索	システムのシャットダウン時にフロッピーディスクを検索する
リアルタイム検索	IntelliTrap を有効にする: IntelliTrap により、圧縮ファイルに含まれるボットなどの不正コードが検出されます。254 ページの「IntelliTrap」を参照してください。
リアルタイム検索	メモリで検出された不正プログラムの変種/亜種を隔離する: リアルタイム検索と挙動監視が有効化され、このオプションが選択されている場合、実行中のプロセスのメモリで圧縮された不正プログラムが検索されます。挙動監視が検出した圧縮された不正プログラムは隔離されます。
リアルタイム検索、手動検索、予約検索	圧縮ファイルを検索する最大レイヤ数: ファイルを圧縮するたびに、階層が 1 つ増えます。感染したファイルを複数の階層に圧縮した場合、指定した階層まで検索します。階層が増えると、より多くの時間とリソースが必要になります。
リアルタイム検索、手動検索、予約検索	スパイウェアの承認済みリストの変更:エージェントのコンソールからは設定できません。

検索の種類	オプション
手動検索、予約検索	CPU 使用率:セキュリティエージェントでは、1 つのファイルの検索後、次のファイルの検索を開始する前に一時停止することができます (一時停止した後、CPU 使用率が指定された数値まで下がるのを待って再開します)。 次のオプションから選択します。 • 高: 間隔をあけず連続してファイルを検索する • 中: CPU 使用率が 50%を超えるとファイル検索を一時中断し、50%以下のときは一時中断しない • 低: CPU 使用率が 20%を超えるとファイル検索を一時中断し、20%以下のときは一時中断しない
手動検索、予約検索	高度なクリーンナップの実行 (FakeAV):セキュリティエージェントは、偽セキュリティソフトウェア (FakeAV とも呼ばれます) による処理を停止します。エージェントは、詳細なクリーンナップルールを使用して、FakeAV の挙動を示すアプリケーションを予防的に検出および停止します。

スパイウェア/グレーウェアの除外リスト

特定のアプリケーションは、インストールされたシステムに損害を与える可能性があるという理由でなく、クライアントやネットワークを不正プログラムやハッカーからの攻撃にさらす可能性があるという理由で、スパイウェアと分類されます。

ビジネスセキュリティ には、潜在的に危険なアプリケーションのリストがあります。初期設定でそうしたアプリケーションがクライアントで 実行されないようにします。

クライアントがスパイウェアに分類されたアプリケーションを実行する必要がある場合は、アプリケーション名をスパイウェア/グレーウェアの除外リストに追加する必要があります。

ウイルス検出時の処理

ウイルス/不正プログラムに対してセキュリティエージェントが実行できる処理は次のとおりです。

表 6-1. ウイルス/不正プログラム検索の処理

処理	説明
削除	感染ファイルを削除します。
隔離	感染ファイルの名前を変更し、クライアントの一時隔離ディレクトリに移動します。 セキュリティエージェントは、次に、隔離されたファイルを指定された隔離ディレクトリ (初期設定ではビジネスセキュリティサーバにあります) に送信します。 セキュリティエージェントは、このディレクトリに送信される隔離ファイルを暗号化します。 隔離されたファイルのいずれかを復元する必要がある場合は、VSEncrypt ツールを使用します。
駆除	感染ファイルを駆除します。駆除されるまでそのファイルへのフルアクセスは許可されません。 駆除不可能な場合、セキュリティエージェントは 2 次処理として 隔離、削除、拡張子変更、または放置のいずれかを実行します。 注意 一部のファイルは駆除できません。詳細については、261 ページの「駆除できないファイル」を参照してください。
拡張子変更	感染ファイルの拡張子を「vir」に変更します。ユーザは拡張子変更されたファイルを開くことはできませんが、特定のアプリケーションと関連付ければ開くことは可能です。 拡張子変更された感染ファイルを開くと、ウイルス/不正プログラムが実行されるおそれがあります。
放置 (ログのみ)	手動検索および予約検索のみで実行できます。セキュリティエージェントでは、リアルタイム検索の間にこの検索処理を使用できません。これは、感染ファイルを開こうとしたり実行しようとする操作を検出したときに何も実行しなければ、ウイルス/不正プログラムが実行されるのを許容することになるためです。その他の検索処理はすべて、リアルタイム検索の間に使用できます。

処理	説明
アクセス拒否	リアルタイム検索の間にのみ実行できます。セキュリティエージェントで、感染ファイルを開こうとしたり実行しようとする操作を検出した場合、ただちに操作がブロックされます。 ユーザは感染ファイルを手動で削除できます。

セキュリティエージェントが実行する検索処理は、スパイウェア/グレーウェアを検出した検索の種類に応じて異なります。ウイルスや不正プログラムの種類ごとに特定の処理を設定できますが、スパイウェア/グレーウェアのすべての種類に対して設定できる処理は 1 つのみです。たとえば、手動検索 (検索の種類) によって特定の種類のスパイウェア/グレーウェアが検出された場合、影響を受けるシステムリソースが駆除 (処理) されます。

スパイウェア/グレーウェアに対してセキュリティエージェントが実行できる処理は次のとおりです。

表 6-2. スパイウェア/グレーウェア検索処理

処理	説明
駆除	プロセスの終了、またはレジストリ、ファイル、Cookie、ショートカットの削除。
放置 (ログのみ)	検出されたスパイウェア/グレーウェアのコンポーネントに対して何の処理も実行せずに、スパイウェア/グレーウェアの検出をログに記録します。この処理は、手動検索および予約検索のみで実行できます。リアルタイム検索では、この処理は「アクセス拒否」となります。 セキュリティエージェントは、検出されたスパイウェア/グレーウェアが除外リストに含まれている場合、いかなる処理も実行しません。
アクセス拒否	検出されたスパイウェア/グレーウェアのコンポーネントへのアクセス (コピー、開く) を拒否します。この処理は、リアルタイム検索の間にのみ実行できます。手動検索および予約検索の際、この処理は「放置」となります。

トレンドマイクロの推奨処理

ウイルス/不正プログラムの種類ごとに、異なる検索処理が必要になります。検索処理のカスタマイズには、ウイルス/不正プログラムに関する知識が必要であり、時間と手間のかかる作業になる可能性があります。トレンドマイクロの推奨処理を使用して、この問題に対応することが可能です。

トレンドマイクロの推奨処理とは、ウイルス/不正プログラムに事前に割り当てられている一連の検索処理です。検索処理について詳しくない場合や、ウイルス/不正プログラムに適した検索処理の判断が難しい場合は、トレンドマイクロの推奨処理をお勧めします。

トレンドマイクロの推奨処理を使用する利点は、次のとおりです。

- 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検索処理が使用されます。検出時の処理を設定する手間が省けます。
- ウイルス作成者は、ウイルス/不正プログラムによる攻撃手段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、最新の脅威やウイルス/不正プログラムの最新の攻撃手段に対応して保護できるように更新されます。

次の表はトレンドマイクロの推奨処理が、各種のウイルスや不正プログラムを処理する方法を示しています。

表 6-3. ウイルス/不正プログラムに適用されるトレンドマイクロの推奨処理

ウイルス/不正プログラム	リアルタイム検索		手動検索/予約検索	
	1 次処理	2 次処理	1 次処理	2 次処理
ジョークプログラム	隔離	削除	隔離	削除
ワーム/トロイの木馬	隔離	削除	隔離	削除
パッカー	隔離	該当なし	隔離	該当なし
不正プログラムの疑い	放置 (ログのみ)	該当なし	放置(ログのみ)またはユーザ設定の処理	該当なし
ウイルス	駆除	隔離	駆除	隔離
テストウイルス	アクセス拒否	該当なし	該当なし	該当なし
その他の不正プログラム	駆除	隔離	駆除	隔離

注意

- 一部のファイルは駆除できません。詳細については、261 ページの「駆除できないファイル」を参照してください。
- トレンドマイクロの推奨処理は、スパイウェア/グレーウェア検索には使用できません。
- これらの設定のデフォルト値は、新しいパターンファイルが使用可能になると変更される場合があります。

詳細設定

検索の種類	オプション
リアルタイム検索、予約検索	ウイルス/スパイウェアの検出時にデスクトップまたはサーバに警告メッセージを表示する
リアルタイム検索、予約検索	潜在的なウイルス/スパイウェアの検出時にデスクトップまたはサーバに警告メッセージを表示する
手動検索、リアルタイム検索、予約検索	潜在的なウイルス/不正プログラムの検出時にクリーンナップを実行する: トレンドマイクロの推奨処理を選択し、潜在的なウイルス/不正プログラムの処理をカスタマイズした場合にのみ選択可能になります。

第 7 章

アップデートの管理

本章では、ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) のコンポーネントとアップデート手順について説明します。

アップデートの概要

すべてのコンポーネントのアップデートは、トレンドマイクロのアップデートサーバから取得されます。アップデートが利用可能な場合、アップデートされたコンポーネントがビジネスセキュリティサーバにダウンロードされ、次にそれらはセキュリティエージェントに配信されます。

1 台のビジネスセキュリティサーバが 多数のセキュリティエージェントを 管理している場合、アップデートを実行すると大量のサーバコンピュータリソースが使用され、サーバの安定性とパフォーマンスに影響する可能性があります。この問題に対処するため、ビジネスセキュリティ はアップデートエージェント機能を備えています。この機能により、特定のセキュリティエージェントで、他のセキュリティエージェントにアップデートを 配信するタスクを共有できます。

次の表に、ビジネスセキュリティサーバとエージェントのコンポーネントのアップデートオプションと 、それらを使用する際の推奨事項を示しています。

表 7-1. アップデートオプション

アップデート順序	説明	推奨事項
1. アップデートサーバまたはその他のアップデート元 2. ビジネスセキュリティサーバ 3. エージェント	ビジネスセキュリティサーバは、アップデートサーバまたはその他のアップデート元からアップデートされたコンポーネントを受信し、次にそれをセキュリティエージェントに直接配信します。	ビジネスセキュリティサーバとエージェント間に低帯域幅の部分がない場合に、この方法を使用してください。

アップデート順序	説明	推奨事項
1. アップデートサーバまたはその他のアップデート元 2. ビジネスセキュリティサーバ 3. アップデートエージェント、アップデートエージェントのないセキュリティエージェント 4. その他すべてのセキュリティエージェント	ビジネスセキュリティサーバは、アップデートサーバ (またはその他のアップデート元) から最新のコンポーネントを受信して、それらを直接次に配信します。 • アップデートエージェント • アップデートエージェントのないセキュリティエージェント その後、アップデートエージェントはコンポーネントを対応するセキュリティエージェントに配信します。これらのセキュリティエージェントがアップデートできない場合、ビジネスセキュリティサーバから直接アップデートします。	ビジネスセキュリティサーバとセキュリティエージェント間に低帯域幅の部分がある場合、この方法を使用するとネットワークのトラフィック負荷を分散させることができます。
1. アップデートサーバ 2. セキュリティエージェント	どのアップデート元からもアップデートできないセキュリティエージェントは、アップデートサーバから直接アップデートします。	この方法は最後の手段としてのみ提供されています。この方法を使用するには、次の設定を行う必要があります。 [アップデート権限] の下にある [トレンドマイクロのアップデートサーバを 2 次アップデート元として使用] を有効にします。

アップデート可能なコンポーネント

ビジネスセキュリティ では、各種コンポーネントを使用して最新の脅威からエージェントを保護します。手動または自動アップデートを実行して、これらのコンポーネントを常に最新の状態にしてください。

コンポーネントのリストは次のいずれかの方法で確認できます。

- [アップデート] > [手動アップデート] に移動します。

- [最新ステータス] に移動し、[エージェントのステータス] ウィジェットで [コンポーネントステータスの確認] をクリックします。

次の表に、ビジネスセキュリティサーバにより、アップデートサーバからダウンロードされるコンポーネントのリストを示します。

表 7-2. ウイルス対策とスマートスキャン

コンポーネント	配信先	説明
ウイルスパターンファイル	従来型スキャンを使用するセキュリティエージェント	ウイルスパターンファイルには、最新のウイルス/不正プログラムおよび複合型脅威の攻撃をセキュリティエージェントが識別するための情報が格納されています。トレンドマイクロでは、週に数回、新バージョンのウイルスパターンファイルを作成し、リリースしているほか、特に破壊力のあるウイルス/不正プログラムの検出に伴い、随時、新バージョンのパターンファイルをリリースしています。
IntelliTrap パターンファイル	セキュリティエージェント	IntelliTrap パターンファイルは、実行ファイルとして圧縮されたリアルタイム圧縮ファイルを検出します。 詳細については、254 ページの「IntelliTrap」を参照してください。
IntelliTrap 除外パターンファイル	セキュリティエージェント	IntelliTrap 除外パターンファイルには、「承認済み」圧縮ファイルのリストが含まれます。
ウイルス検索エンジン (32/64 ビット)	セキュリティエージェント	検索エンジンはウイルスおよび不正プログラムを検出するコンポーネントです。検索エンジンは高度な機能を備え、さまざまな種類のウイルスおよび不正プログラムを検出できます。 このエンジンとパターンファイルでは、すべてのファイルのすべてのバイトを検索するのではなく、連携することによって以下の特定を行います。 • ウイルスコードの手がかりとなる特性 • ウイルスが存在するファイル内の正確な位置

コンポーネント	配信先	説明
スマートスキャンパターンファイル	セキュリティエージェントに配信されません。このパターンファイルはビジネスセキュリティサーバ内に維持され、セキュリティエージェントから受信した検索クエリに応答するときに使用されます。	スマートスキャンモードでは、セキュリティエージェントは 2 つの軽量型のパターンファイルを使用します。これらのパターンファイルは連携して、従来の不正プログラム対策およびウイルス対策パターンファイルにより提供されるものと同等の保護を提供します。 パターン定義の大部分はスマートスキャンパターンファイルに含まれています。スマートスキャンエージェントパターンファイルには、スマートスキャンパターンファイルに含まれないその他のすべてのパターン定義が含まれます。 セキュリティエージェントは、スマートスキャンエージェントパターンファイルを使用してセキュリティ上の脅威を検索します。検索時にファイルのリスクを特定できない場合、セキュリティエージェントは、ビジネスセキュリティサーバ上でホストされるサービスであるスキャンサーバに検索クエリを送信して、リスクを検証します。スキャンサーバは、スマートスキャンパターンファイルを使用してリスクを検証します。セキュリティエージェントは、検索のパフォーマンスを向上するために、スキャンサーバにより提供される検索クエリの結果を「キャッシュ」します。
スマートスキャンエージェントパターンファイル	スマートスキャンを使用するセキュリティエージェント	
ダメージクリーンナップテンプレート	セキュリティエージェント	ダメージクリーンナップテンプレートは、ダメージクリーンナップエンジンでトロイの木馬ファイルとプロセスを特定し、削除するために使用されます。
ダメージクリーンナップエンジン (32 ビット/64 ビット)	セキュリティエージェント	ダメージクリーンナップエンジンはトロイの木馬およびトロイの木馬プロセスを検索して、除去します。

コンポーネント	配信先	説明
メモリ検査パターンファイル	セキュリティエージェント	このテクノロジは、ポリモーフィック (ミューテーション) 型ウイルスの強化されたウイルス検索を提供し、ファイル実行をエミュレートすることによりウイルスパターンファイルベースの検索を増強します。その後、不正な目的を示す証拠がないか、制御された環境で結果が分析されます。システムのパフォーマンスにはほとんど影響を及ぼしません。
CI エンジン (32/64 ビット)	セキュリティエージェント	CI エンジンは、あまり普及していないファイルで実行されるプロセスを監視し、動作の特性を抽出します。抽出された情報は、CI クエリハンドラによって、分析のために機械学習型検索エンジンに送信されます。
CI パターンファイル	セキュリティエージェント	CI パターンファイルには、既知のいずれの脅威にも関連しない「承認済み」の動作のリストが含まれます。
CI クエリハンドラ (32/64 ビット)	セキュリティエージェント	CI クエリハンドラは、CI エンジンで特定された動作を処理し、機械学習型検索エンジンにレポートを送信します。
高度な脅威検索エンジン (32/64 ビット)	セキュリティエージェント	高度な脅威検索エンジンは、あまり普及していないファイルからファイル特性を抽出し、その情報を機械学習型検索エンジンに送信します。
高度な脅威相関パターンファイル	セキュリティエージェント	高度な脅威相関パターンファイルには、既知のいずれの脅威にも関連しないファイル特性のリストが含まれます。
起動時クリーンナップドライバ (32/64 ビット)	セキュリティエージェント	起動時クリーンナップドライバは、オペレーティングシステムのドライバ群より先にロードされ、ブート型ルートキットを検出、遮断します。セキュリティエージェントのロード後、起動時クリーンナップドライバはダメージクリーンナップサービスを呼び出して、ルートキットをクリーンナップします。

表 7-3. スパイウェア対策

コンポーネント	配信先	説明
スパイウェア/グレーウェア検索エンジン v.6 (32/64 ビット)	セキュリティエージェント	スパイウェア検索エンジンは、スパイウェア/グレーウェアの検索を実行し、これらに適したスマートスキャンを実行します。
スパイウェア/グレーウェアパターンファイル v.6	セキュリティエージェント	スパイウェアパターンファイルは、ファイル/プログラム、メモリ内のモジュール、Windows レジストリおよび URL ショートカット内のスパイウェア/グレーウェアを特定します。
スパイウェア/グレーウェアパターンファイル	セキュリティエージェント	

表 7-4. ネットワークウイルス

コンポーネント	配信先	説明
ファイアウォールパターンファイル	セキュリティエージェント	ウイルスパターンファイルと同様、ファイアウォールパターンファイルは、エージェントで、ウイルスシグネチャ (ネットワークウイルスの存在を示すビットやバイトの一意のパターン) の識別に使用されます。

表 7-5. 挙動監視およびデバイスコントロール

コンポーネント	配信先	説明
挙動監視検出パターンファイル (32 ビット/64 ビット)	セキュリティエージェント	不審な脅威の挙動の検出に使用するルールが含まれるパターンファイルです。
挙動監視コアドライバ (32 ビット/64 ビット)	セキュリティエージェント	このカーネルモードドライバは、システムイベントを監視して、ポリシー施行のための挙動監視コアサービスに渡します。
挙動監視コアサービス (32 ビット/64 ビット)	セキュリティエージェント	このユーザモードサービスには、次の機能があります。 • ルートキット検出の提供 • 外部デバイスへのアクセス規制 • ファイル、レジストリキー、およびサービスの保護

コンポーネント	配信先	説明
挙動監視設定パターンファイル	セキュリティエージェント	挙動監視ドライバではこのパターンファイルを使用して通常のシステムイベントを識別し、それらをポリシー施行から除外します。
ダメージリカバリパターンファイル	セキュリティエージェント	ダメージリカバリパターンファイルには、不審な脅威の挙動監視に使用されるポリシーが含まれています。
デジタル署名パターンファイル	セキュリティエージェント	このパターンファイルには、システムイベントを管理するプログラムが安全かどうかを特定するために挙動監視コアサービスで使用される、有効なデジタル署名のリストが含まれます。
ポリシー施行パターンファイル	セキュリティエージェント	挙動監視コアサービスでは、このパターンファイルのポリシーに照らしてシステムイベントがチェックされます。
メモリ検索実行パターンファイル (32 ビット/64 ビット)	セキュリティエージェント	挙動監視コアサービスは、メモリ上で実行される不審プログラムをこのパターンファイルを使用して検出します。
プログラム検査監視パターンファイル	セキュリティエージェント	プログラム検査監視パターンファイルは、挙動監視に使用される検査ポイントを監視し、保存します。
脅威追跡パターンファイル (32 ビット/64 ビット)	セキュリティエージェント	脅威追跡パターンファイルは、ファイルレスマルウェアの攻撃を特定します。

表 7-6. ブラウザ脆弱性対策

コンポーネント	配信先	説明
ブラウザ脆弱性対策パターンファイル	セキュリティエージェント	このパターンファイルは、最新の Web ブラウザ脆弱性を識別し、脆弱性により Web ブラウザが悪用されることを防ぎます。
スクリプトアナライザ共通パターンファイル	セキュリティエージェント	このパターンファイルは、Web ページ内のスクリプトを分析し、不正なスクリプトを特定します。

表 7-7. スパムメール (迷惑メール) 対策

コンポーネント	配信先	説明
スパムメール対策パターンファイル	セキュリティエージェント	スパムメールを識別します。
スパムメール検索エンジン (Windows、32/64 ビット)	セキュリティエージェント	スパムメールを検出します。

表 7-8. 機械学習型検索

コンポーネント	配信先	説明
機械学習型検索ローカルモデル(ファイル検出)	セキュリティエージェント	機械学習型検索ローカルモデル (ファイル検出) は、エンドポイントがインターネットに接続されていない場合に、実行可能ファイルの脅威を特定します。

HotFix、Patch、および Service Pack

製品の正式リリース後、トレンドマイクロでは、問題への対処、製品のパフォーマンスの強化、または新機能の追加のために次のものを開発しています。

- 254 ページの「Critical Patch」
- 254 ページの「HotFix」
- 257 ページの「Patch」
- 260 ページの「Service Pack」

下記のトレンドマイクロの Web サイトで、新しい Critical Patch、Patch、または Service Pack のリリースに関する情報を確認してください。

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

すべてのリリースには、インストール、配信、および設定に必要な情報が記載された Readme ファイルが含まれています。Readme ファイルをよくお読みのうえ、インストールしてください。

ビジネスセキュリティサーバのアップデート

自動アップデート

ビジネスセキュリティサーバは、次のタイミングで自動的にアップデートを実行します。

- インストール直後
- ビジネスセキュリティサーバのサービス 起動時
- 自動アップデート (初期設定では 1 時間ごと)

手動アップデート

アップデートが必要な場合は、Web コンソールから手動アップデートを実行できます。

サーバのアップデートに関する注意事項とヒント

- アップデート後、ビジネスセキュリティサーバはコンポーネントアップデートをエージェントに自動的に配信します。エージェントに配信されるコンポーネントの詳細については、135 ページの「アップデート可能なコンポーネント」を参照してください。
- IPv6 シングルスタックのビジネスセキュリティサーバは 、次のタスクを実行できません。
  - トレンドマイクロのアップデートサーバまたは IPv4 シングルスタックのその他のアップデート元から直接アップデートを入手すること
  - IPv4 シングルスタックのエージェントへアップデートを 直接配信すること

  同様に、IPv4 シングルスタックのビジネスセキュリティサーバは 、IPv6 シングルスタックのカスタムアップデート 元から直接アップデートを取得したり、IPv6 シングルスタックのエージェントにアップデートを 直接配信することはできません。

  このような状況で、ビジネスセキュリティサーバがアップデートを 取得および配信できるようにするには、DeleGate などの IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

- プロキシサーバを使用してインターネットに接続する場合は、最新コンポーネントを正常にダウンロードできるように [管理] > [グローバル設定] > [プロキシ] タブでプロキシを適切に設定する必要があります。

コンポーネントの複製

トレンドマイクロでは、クライアントの保護を最新の状態に保つために、パターンファイルを定期的にリリースします。パターンファイルは定期的にアップデートされるため、ビジネスセキュリティサーバでは、パターンファイルのダウンロードを迅速化するためのコンポーネントの複製というメカニズムを使用します。

最新バージョンのパターンファイル全体がトレンドマイクロのアップデートサーバからダウンロード可能である場合、差分パターンファイルもダウンロードすることができます。差分パターンファイルは、パターンファイル全体の一部で、以前のバージョンと最新バージョン間の変更部分を表します。たとえば、最新バージョンが 175 である場合、差分パターンファイル v_173.175 には、バージョン 173 には存在しなかったバージョン 175 のシグネチャが含まれます (パターンファイルの番号はリリースごとに 2 ずつ増加するため、バージョン 173 はパターンファイル全体の前のバージョンです)。差分パターンファイル v_171.175 には、バージョン 171 には存在しなかったバージョン 175 のシグネチャが含まれます。

最新のパターンファイルをダウンロードする際に生成されるネットワークトラフィックを減らすために、ビジネスセキュリティサーバはコンポーネントの複製を実行します。これは、サーバで差分パターンファイルのみをダウンロードする場合に使用されるコンポーネントのアップデート方法です。コンポーネントの複製を利用するには、ビジネスセキュリティサーバが定期的にアップデートされている必要があります。そうでないと、サーバはパターンファイル全体をダウンロードするよう強制されます。

コンポーネントの複製は次のコンポーネントに適用されます。

- ウイルスパターンファイル
- スマートスキャンエージェントパターンファイル
- ダメージクリーンナップテンプレート
- IntelliTrap 除外パターンファイル
- スパイウェアパターンファイル

ビジネスセキュリティサーバのアップデート元を設定する

始める前に

初期設定では、ビジネスセキュリティサーバはトレンドマイクロのアップデートサーバからアップデートを取得します。ビジネスセキュリティサーバがアップデートサーバに直接到達できない場合は、その他のアップデート元を指定します。

- アップデート元がトレンドマイクロのアップデートサーバの 場合は、インターネットへの接続を確認します。プロキシサーバを使用している場合は、インターネット接続に必要なプロキシ設定を行ってください。詳細については、185 ページの「インターネットプロキシを設定する」を参照してください。
- アップデート元がその他のアップデート元 である場合は、そのアップデート元の環境を設定します。また、ビジネスセキュリティサーバとこのアップデート元との間の接続が機能していることを確認します。
- IPv6 シングルスタックのビジネスセキュリティサーバは 、トレンドマイクロのアップデートサーバまたは IPv4 シングルスタックのカスタムアップデート元から直接アップデートできません。同様に、IPv4 シングルスタックのビジネスセキュリティサーバは、IPv6 シングルスタックのカスタムアップデート元から直接アップデートできません。このような場合にビジネスセキュリティサーバでアップデート 元に接続できるようにするには、IP アドレスを変換可能なデュアルスタックプロキシサーバ (DeleGate など) が必要です。

手順

1. [アップデート] > [アップデート元] に移動します。
2. [サーバ] タブで、アップデート元を選択します。
   - トレンドマイクロのアップデートサーバ
   - 現在のファイルのコピーを含むイントラネットの場所 –アップデート元への UNC パス (`\\Web\ActiveUpdate` など) を入力します。また、ビジネスセキュリティサーバがこのアップデート 元への接続に使用するログオン情報 (ユーザ名とパスワード) も指定します。

- その他のアップデート元 –このアップデート元への URL を入力します。ビジネスセキュリティサーバから、アップデート元の Web サイトへアクセスできることを確認します。

3. [保存] をクリックします。

ビジネスセキュリティサーバを手動でアップデートする

セキュリティサーバのインストールまたはアップグレード 後、および大規模感染が発生した場合は必ず、サーバ上のコンポーネントを手動でアップデートします。

手順

1. 次のいずれかの手順で手動アップデートに移動します。
   - [アップデート] > [手動アップデート] に移動します。
   - [最新ステータス] に移動し、[エージェントのステータス] ウィジェットで [コンポーネントステータスの確認] をクリックします。

   [手動アップデート] 画面が表示されます。
2. アップデートするコンポーネントを 選択します。

   コンポーネントの詳細については、135 ページの「アップデート可能なコンポーネント」を参照してください。
3. [今すぐアップデート] をクリックします。

   新しい画面が表示され、アップデート状況が表示されます。アップデートが正常に終了すると、ビジネスセキュリティサーバは 最新のコンポーネントをエージェントに自動的に配信します。

ビジネスセキュリティサーバの自動アップデートを設定する

定期的にアップデート元をチェックして、利用可能なアップデートがあれば自動的にダウンロードするように、ビジネスセキュリティサーバを 設定します。自動アップデートは、脅威からの保護機能を常に最新の状態に保つための簡単で効果的な方法です。

ウイルスパターンファイル、検索エンジンおよびその他のコンポーネントは定期的にアップデートされます。エージェントのコンポーネントを常に最新

にするために、コンポーネントのアップデートは 1 日に 1 回 (大規模感染の発生時はそれよりも頻繁に) 行うことをお勧めします。

重要

検索と更新を同時に実行するようにスケジュールしないでください。自動アップデートと同じ時刻にスケジュールすると、予約検索が途中で中断される可能性があります。

手順

1. [アップデート] > [自動アップデート] に移動します。
2. アップデートするコンポーネントを選択します。

   コンポーネントの詳細については、135 ページの「アップデート可能なコンポーネント」を参照してください。
3. [スケジュール] タブをクリックして、アップデートスケジュールを指定します。
   - [従来型スキャンによるアップデート] には、スマートスキャンパターンファイルおよびスマートスキャンエージェントパターンファイル以外のすべてのコンポーネントが含まれます。毎日、毎週、または毎月のアップデートの場合、[開始時刻] リストボックスで、予約アップデートを実行する時刻について、範囲 (時間単位) を指定します。ビジネスセキュリティサーバは、この範囲の任意の時刻にアップデートを実行します。

     注意

     毎月の自動アップデートの場合 (非推奨)、選択した日付が無い月は自動アップデートは実行されません。
   - [スマートスキャンによるアップデート] には、スマートスキャンパターンファイルおよびスマートスキャンエージェントパターンファイルのみが含まれます。スマートスキャンを使用するエージェントがない場合、この項目は無視してください。

4. [保存] をクリックします。

コンポーネントをロールバックする

ロールバックとは、ウイルスパターンファイル、スマートスキャンエージェントパターンファイル、およびウイルス検索エンジンを前のバージョンに戻すことを指します。これらのコンポーネントが適切に機能しない場合、それらを前のバージョンにロールバックします。ビジネスセキュリティサーバには、現在と前のバージョンのウイルス検索エンジン、および最新の三世代分のウイルスパターンファイルとスマートスキャンエージェントパターンファイルが保持されています。

注意

ロールバックできるのは上記のコンポーネントのみです。

ビジネスセキュリティは、32 ビットプラットフォームと 64 ビットプラットフォームを実行するエージェントではそれぞれ異なる検索エンジンを使用します。これらの検索エンジンは個別にロールバックする必要があります。ロールバック手順はすべての種類の検索エンジンで同一です。

手順

1. [アップデート] > [ロールバック] に移動します。
2. 特定のコンポーネントについて [同期] をクリックすると、エージェントのコンポーネントのバージョンをサーバ上のコンポーネントのバージョンと同期するようにエージェントに通知されます。
3. 特定のコンポーネントについて [ロールバック] をクリックすると、ビジネスセキュリティサーバとエージェントの 両方のコンポーネントがロールバックされます。

セキュリティエージェントのアップデート

自動アップデート

セキュリティエージェントのコンポーネントアップデートは 、以下のタイミングで実施されます。

- エージェントのインストール直後
- ビジネスセキュリティサーバのアップデート 完了後
- アップデートエージェントのアップデート 完了後
- 自動アップデート (間隔は変更できません)
  - オフィス内のセキュリティエージェントでは 8 時間ごと
  - オフィス外のセキュリティエージェントでは 2 時間ごと

手動アップデートを実行する

セキュリティエージェントは、ビジネスセキュリティサーバから自動的にアップデートを受信します。

オフィスネットワークにしばらく接続していなかった場合や、セキュリティ上の脅威に対する最新の保護機能を緊急に必要とする場合 (大規模感染の発生時など)、手動でアップデートすることができます。

プロキシサーバを使用してインターネットに接続する場合は、プロキシ設定が正しいことを確認する必要があります。

手順

1. メインコンソールを開き、[アップデート] をクリックします。

   注意

   手動アップデートは、Windows タスクバーのセキュリティエージェントのアイコンを右クリックして [今すぐアップデート] をクリックすることで直接実行できます。

2. アップデートが完了したら、[閉じる] をクリックします。

エージェントのアップデートに関する注意事項とヒント

- セキュリティエージェントは、ビジネスセキュリティサーバ、アップデートエージェント、またはトレンドマイクロのアップデートサーバからアップデートされます。

アップデートプロセスの詳細については、134 ページの「アップデートの概要」を参照してください。

- IPv6 シングルスタックのエージェントは、IPv4 シングルスタックのビジネスセキュリティサーバ/アップデートエージェントおよびトレンドマイクロのアップデートサーバから直接アップデートを取得できません。

  同様に、IPv4 シングルスタックのエージェントは、IPv6 シングルスタックのビジネスセキュリティサーバ/アップデートエージェントから直接アップデートを取得できません。

  このような状況でエージェントがアップデートを取得できるようにするには、DeleGate などの IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

- エージェントでアップデートされるコンポーネントの詳細については、135 ページの「アップデート可能なコンポーネント」を参照してください。

- アップデート時、エージェントはコンポーネントの他に、アップデートされた設定ファイルをビジネスセキュリティサーバから受信します。エージェントに新しい設定を適用するには、設定ファイルが必要です。Web コンソールからエージェントの設定を変更するたびに、設定ファイルの内容が変更されます。

アップデートエージェント

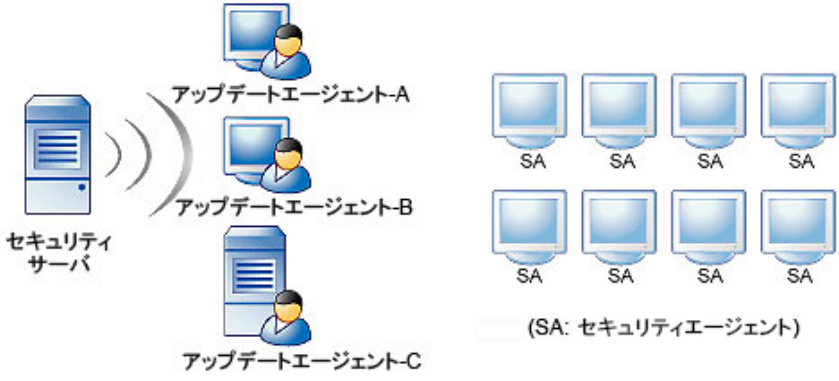
アップデートエージェントは、ビジネスセキュリティサーバやアップデートサーバから最新のコンポーネントを受信して、他のセキュリティエージェントに配信できるセキュリティエージェントです。

クライアントとビジネスセキュリティサーバ 間のネットワークセクションで「帯域幅が狭い」または「トラフィックが大きい」と認識された場合、セキュリティエージェントがアップデートエージェントとして 機能するように指定できます。アップデートエージェントを使用すると、コンポーネントのアップデート時にすべてのセキュリティエージェントがビジネスセキュリティサーバにアクセスする必要がなくなるため、ネットワーク帯域幅の消費量が減少します。ネットワークが場所によってセグメント化され、セグメント間のネットワークリンクのトラフィック負荷が大きいことが多い場合は、セグメ

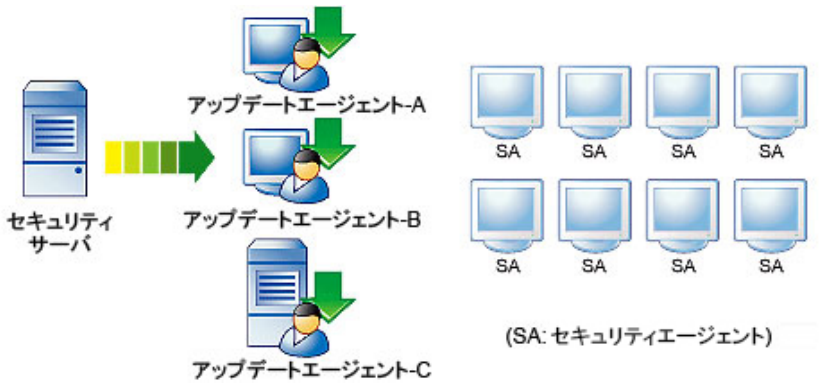
ントごとに 1 つ以上のセキュリティエージェントをアップデートエージェントとして機能させることをお勧めします。

アップデートエージェントのアップデートプロセスの 説明を次に示します。

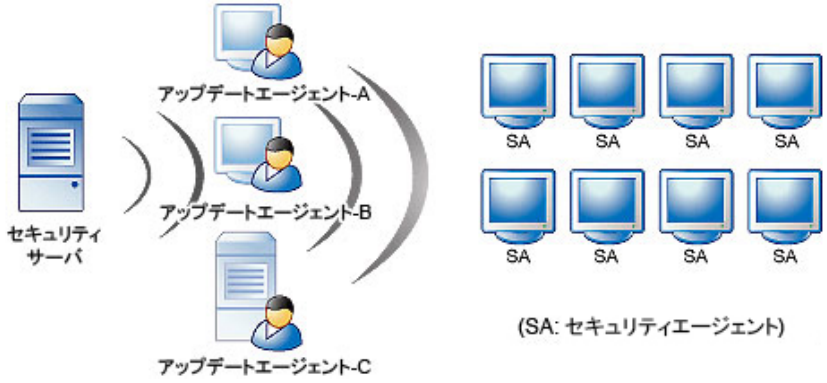
1. ビジネスセキュリティサーバはアップデートエージェントに 新しいアップデートが利用可能になったことを通知します。



2. アップデートエージェントは最新のコンポーネントをビジネスセキュリティサーバからダウンロードします。



3. 次に、ビジネスセキュリティサーバはセキュリティエージェントに 最新のコンポーネントが利用可能になったことを通知します。

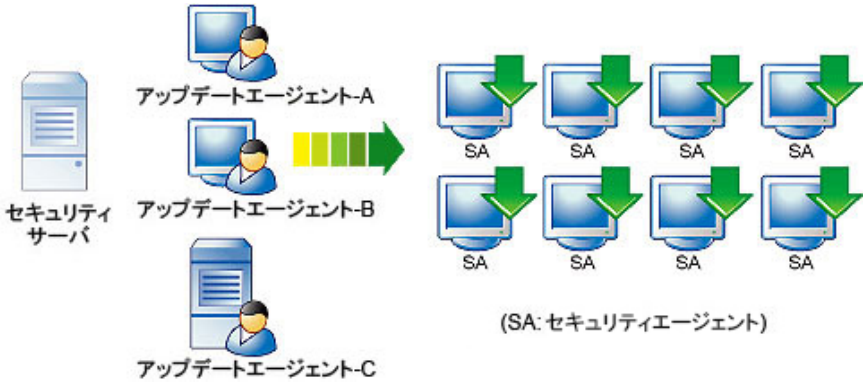


4. 各セキュリティエージェントは、ビジネスセキュリティサーバで 設定したアップデート先をもとに、適切なアップデート元を判定します。初期設定の場合、Web コンソール上でその他のアップデート元として追加された順序によって決定されます。各セキュリティエージェントは、アップデート元を特定するまで、最初のエントリから 1 つずつチェックします。

アップデートエージェントオーダテーブル

IPアドレス範囲	アップデート エージェント
10.1.1.1-10.1.1.10	UA-A
10.2.1.1-10.2.1.10	UA-B
10.3.1.1-10.3.1.10	UA-C

5. 特定するとセキュリティエージェントは、割り当てられたアップデートエージェントから最新のコンポーネントをダウンロードします。何らかの理由で割り当てられたアップデートエージェントを 使用できない場合、セキュリティエージェントは、ビジネスセキュリティサーバから 最新のコンポーネントのダウンロードを試行します。



アップデートエージェントを設定する

手順

1. [アップデート] > [アップデート元] に移動します。
2. [アップデートエージェント] タブをクリックします。
3. 次のタスクを実行します。

タスク	手順
セキュリティエージェントをアップデートエージェントとして割り当て	a. [アップデートエージェントの割り当て] で、[追加] をクリックします。 新しい画面が表示されます。 b. リストボックスから、アップデートエージェントとして機能させる 1 つ以上のエージェントを選択します。 c. [保存] をクリックします。 画面が閉じます。 d. [アップデートエージェントの割り当て] に戻り、アップデートエージェントが他のアップデートエージェントではなく、必ずビジネスセキュリティサーバから最新コンポーネントをダウンロードするようにするには、[常にビジネスセキュリティからアップデートをダウンロードする] をオンにします。

タスク	手順
セキュリティエージェントをアップデートエージェントからアップデートするように設定	a. [その他のアップデート元] で、[セキュリティエージェントおよびアップデートエージェントのその他のアップデート元を有効にする] をオンにします。 **注意** このオプションをオフにすると、セキュリティエージェントがアップデートエージェントからアップデートされなくなり、アップデート元をビジネスセキュリティサーバに効率的に切り替えることができます。 b. [追加] をクリックします。 新しい画面が表示されます。 c. アップデートエージェントからアップデートするセキュリティエージェントの IP アドレスを入力します。 • IPv4 のアドレス範囲を入力します。 単一のセキュリティエージェントを指定するには、[開始値] と [終了値] の両方にそのセキュリティエージェントの IP アドレスを入力します。 • IPv6 の場合、IP プレフィックスとプレフィックス長を入力します。 d. ドロップダウンリストからアップデートエージェントを選択します。 ドロップダウンリストが使用できない場合は、アップデートエージェントが設定されていません。 e. [保存] をクリックします。 画面が閉じます。 f. 必要に応じて追加の IP 範囲を定義します。複数の IP 範囲を定義した場合、[並べ替え] オプションを使用して IP 範囲の優先度を設定できます。ビジネスセキュリティサーバからセキュリティエージェントに対してアップデートが利用できることが通知されると、セキュリティエージェントは IP アドレスの範囲のリストを検索して該当するアップデート元を識別します。セキュリティエージェントは、該当す

タスク	手順
	るアップデート元が見つかるまで、リストの先頭から順に検索します。 ヒント フェイルオーバー対策として、同じ IP 範囲に対して複数のアップデートエージェントを定義できます。そうすると、セキュリティエージェントがあるアップデートエージェントからアップデートできない場合に、別のアップデートエージェントからアップデートを試行するようになります。これを実行するには、同じ IP 範囲で少なくとも 2 つのエントリを作成し、各エントリを異なるアップデートエージェントに割り当てます。
アップデートエージェントの削除	アップデートエージェントを削除するには、[アップデートエージェントの割り当て] に移動し、削除するアップデートエージェントのコンピュータ名に対応するチェックボックスをオンにして、[削除] をクリックします。 指定したアップデート元が削除されたセキュリティエージェントは、アップデート元がビジネスセキュリティサーバへ切り替わります。別のアップデートエージェントを指定することも可能です。
アップデートエージェントからのセキュリティエージェントの割り当て解除	ある IP 範囲に属するセキュリティエージェントがアップデートエージェントからアップデートしないようにするには、[その他のアップデート元] に移動し、そのセキュリティエージェントの IP アドレス範囲に対応するチェックボックスをオンにし、[削除] をクリックします。

4. [保存] をクリックします。

第 8 章

最新ステータスの利用

最新ステータス

ビジネスセキュリティは、セキュリティエージェントの管理に役立つ視覚的なクイックリファレンスとして機能するウィジェットを提供します。

ビジネスセキュリティ Web コンソールを開くか、メインメニューの [最新ステータス] をクリックすると、[最新ステータス] 画面が表示されます。

表 8-1. [最新ステータス] ウィジェット

ウィジェット	説明
アクションセンター	管理者に問題解決のための措置を求めるイベントが表示されます。
セキュリティリスクの検出数	ネットワーク上のエンドポイントの概要を提供します。特定の時間内に検出された脅威の数やネットワークに影響を与えた脅威の種類が表示されます。
ランサムウェアの概要	このウィジェットでは、指定時間内に発生したあらゆるランサムウェア攻撃の概要が提供されます。
エージェントのステータス	このウィジェットでは、ネットワーク上のセキュリティエージェントの接続とアップデート状況の概要が提供されます。

[最新ステータス] 画面に表示される情報の更新間隔は、セクションごとに異なります。画面の情報を手動で更新するには、[表示更新] ボタンをクリックします。

アクションセンター

管理者に問題解決のための措置を求めるイベントが表示されます。

一部のイベントにはトレンドマイクロ推奨処理ボタンが表示されます。ボタンをクリックし、問題解決をお試しください。あるいは、イベントをクリックし、詳細をご確認ください。

表 8-2. アクションセンターイベント

イベント	推奨
ウイルス対策 - 解決されていない脅威	次のソリューションにて、対処方法をご確認ください。 http://tmqa.jp/biz10_action_fail

イベント	推奨
ウイルス対策 - エンドポイントでのリアルタイム検索無効	ネットワーク上にあり、保護対象とするすべてのデバイスでリアルタイム検索を有効にしてください。
スパイウェア対策 - デバイスの再起動が必要な検出	デバイスを再起動し、もう一度お試しください。
ライセンスイベント	[管理] > [ライセンス] に移動してライセンスのステータスを確認してください。
リソース不足 - 残りディスク容量が%threshold%未満	不要なファイルを削除して、ディスクの空き容量を確保してください。 詳細については、225 ページの「ディスク容量を節約する」を参照してください。
Smart Protection サービス - サービスは使用できません	ビジネスセキュリティコンソールでスマートスキャンサーバのステータスを確認し、サーバが正常に動作していることを確認してください。
更新 - パターンファイルリリースから 1 時間後のアップデート率が%threshold%未満	セキュリティエージェントのインターネット接続を確認し、セキュリティエージェントを再度更新してください。
更新 - ビジネスセキュリティサーバコンポーネントが%threshold%日以上アップデートされていない	コンポーネントの自動アップデートがビジネスセキュリティサーバで有効になっていること、およびビジネスセキュリティサーバがインターネットに接続できることを確認してください。
更新 - スマートスキャンパターンファイルが%threshold%時間以上アップデートされていない	スマートスキャンパターンファイルの自動アップデートがビジネスセキュリティサーバで有効になっていること、およびビジネスセキュリティサーバがインターネットに接続できることを確認してください。

ウイルス対策:解決されていない脅威

この情報は、アクションセンターで [ウイルス対策 - 解決されていない脅威: %N%] イベントをクリックすると表示されます。リアルタイム検索、手動検索、予約検索を実行すると、ビジネスセキュリティによりこのログ情報が生成または更新されます。

- [アクションセンターから消去する] をクリックすると、[最新ステータス] 画面にリダイレクトされ、アクションセンターから通知イベントが削除されます。この画面でイベントに関連付けられているログはログクエリで引き続き利用できます。
- [エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	前回ウイルスや不正プログラムを駆除または削除しようとして失敗した日時
デバイス名	影響を受けたデバイスの名前
ウイルス/不正プログラム名	検出されたウイルスまたは不正プログラムの名前 リンクをクリックすると、トレンドマイクロの脅威データベースが表示されます。そこでは、この脅威による攻撃を手動で駆除する手順など、脅威の詳細情報を調べることができます。
ファイル名	ウイルスまたは不正プログラムによって改変されたファイルの名前
パス	感染したファイルの場所
検索の種類	ウイルスまたは不正プログラムの検出に使用した検索の種類
処理	ウイルス/不正プログラム検出に対してビジネスセキュリティが実行した処理

ウイルス対策: エンドポイントでのリアルタイム検索無効

この情報は、アクションセンターで [ウイルス対策 - エンドポイントでのリアルタイム検索無効: %N%] イベントをクリックすると確認できます。

- [リアルタイム検索を有効にする] をクリックすると、すべてのデバイスで検索が有効になります。
- [エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
デバイス名	リアルタイム検索が無効になっているデバイスの名前
グループ名	デバイスが属するグループの名前

スパイウェア対策:デバイスの再起動が必要な検出

このログ情報は、アクションセンターで [スパイウェア対策 - デバイスの再起動が必要な検出: %N%] イベントをクリックすると表示されます。

- [アクションセンターから消去する] をクリックすると、[最新ステータス] 画面にリダイレクトされ、アクションセンターから通知イベントが削除されます。この画面でイベントに関連付けられているログはログクエリで引き続き利用できます。
- [エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントがスパイウェアまたはグレーウェア検出の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	影響を受けたデバイスの名前
スパイウェア/グレーウェア名	検出されたスパイウェアまたはグレーウェアの名前 リンクをクリックすると、トレンドマイクロの脅威データベースが表示されます。そこでは、この脅威による攻撃を手動で駆除する手順など、脅威の詳細情報を調べることができます。
検索の種類	スパイウェアまたはグレーウェアの検出に使用した検索の種類

リソース不足 - 残りディスク容量

この情報は、アクションセンターで [リソース不足 - 残りディスク容量が%threshold%未満] イベントをクリックすると確認できます。

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
サーバ名	ディスク容量が不足しているサーバの名前
グループ名	サーバが属しているグループの名前

更新 - アップデートが必要なエージェント

この情報は、アクションセンターで [更新 - パターンファイルリリースから 1 時間後のアップデート率が%threshold%未満] イベントをクリックすると確認できます。この画面には、エンジンまたはパターンファイルのアップデートが必要なセキュリティエージェントのリストが表示されます。

- [今すぐアップデート] をクリックすると、アップデートが必要なセキュリティエージェントに最新のコンポーネントにアップデートするように通知されます。
- [コンポーネントステータスの確認] をクリックすると、[手動アップデート] 画面が開きます。
- [エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
デバイス名	コンポーネントのアップデートが必要なデバイスの名前
グループ名	デバイスが属するグループの名前
検索方法	• スマートスキャン • 従来型スキャン

セキュリティリスクの検出数

ネットワーク上のエンドポイントの概要を提供します。特定の時間内に検出された脅威の数やネットワークに影響を与えた脅威の種類が表示されます。

-  または  をクリックして、表示を切り替えます。

- [既知の脅威]、[未知の脅威]、または [ポリシー違反] タブをクリックして、特定の脅威の検出情報を表示します。

表示	説明
グラフ ()	• グラフの下部にある脅威の種類名をクリックすると、グラフの検出情報の表示/非表示が切り替わります。 • 特定の日のノードにカーソルを合わせると、表示されている脅威の種類の検出合計数が表示されます。ノードをクリックすると、一覧で強調表示されている脅威の種類のログ画面にリダイレクトされます。
表 ()	• 検出数をクリックすると、検出詳細の一覧が表示されるログ画面が開きます。

セキュリティリスク検出: ウイルス/不正プログラム

この情報は、[セキュリティリスクの検出数] ウィジェットの [既知の脅威] タブで次のリンクをクリックすると表示されます。

- リスト表示のウイルス/不正プログラム検出数
- グラフ表示のウイルス/不正プログラムノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントがウイルス/不正プログラム検出の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	影響を受けたデバイスの名前
ウイルス/不正プログラム名	検出されたウイルスまたは不正プログラムの名前 リンクをクリックすると、トレンドマイクロの脅威データベースが表示されます。そこでは、この脅威による攻撃を手動で駆除する手順など、脅威の詳細情報を調べることができます。

列	説明
ファイル名	ウイルスまたは不正プログラムによって改変されたファイルの名前
パス	感染したファイルの場所
検索の種類	ウイルスまたは不正プログラムの検出に使用した検索の種類
処理	ウイルス/不正プログラム検出に対してビジネスセキュリティが実行した処理

セキュリティリスク検出: スパイウェア/グレーウェア

この情報は、[セキュリティリスクの検出数] ウィジェットの [既知の脅威] タブで次のリンクをクリックすると表示されます。

- リスト表示のスパイウェア/グレーウェア検出数
- グラフ表示のスパイウェア/グレーウェアノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントがスパイウェアまたはグレーウェア検出の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	影響を受けたデバイスの名前 名前をクリックすると、そのデバイスで検出された個々のスパイウェアまたはグレーウェアのリストが表示されます。
スパイウェア/グレーウェア名	検出されたスパイウェアまたはグレーウェアの名前
検索の種類	スパイウェアまたはグレーウェアの検出に使用した検索の種類

列	説明
処理	スパイウェアまたはグレーウェア検出に対してビジネスセキュリティが実行した処理

セキュリティリスク検出: Web レピュテーション

この情報は、[セキュリティリスクの検出数] ウィジェットの [既知の脅威] タブで次のリンクをクリックすると表示されます。

- リスト表示の Web レピュテーション検出数
- グラフ表示の Web レピュテーションノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントが URL 違反の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	禁止 URL にアクセスを試みているデバイスの名前
URL	禁止 URL
危険度	感染しやすさおよびダメージを受ける可能性に基づいて、TrendLabs が割り当てた危険度。

セキュリティリスク検出: ネットワークウイルス

この情報は、[セキュリティリスクの検出数] ウィジェットの [既知の脅威] タブで次のリンクをクリックすると表示されます。

- リスト表示のネットワークウイルス検出数
- グラフ表示のネットワークウイルスノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントがネットワークウイルス検出の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	影響を受けたデバイスの名前
攻撃元 IP アドレス	攻撃元の IP アドレス
攻撃先 IP アドレス	攻撃先の IP アドレス
パケット方向	パケットの方向
ネットワークウイルス名	検出されたネットワークウイルスの名前
件数	ネットワークウイルスの検出数 (検出するたびにカウント)

セキュリティリスク検出: 挙動監視

この情報は、[セキュリティリスクの検出数] ウィジェットの [未知の脅威] タブで次のリンクをクリックすると表示されます。

- リスト表示の挙動監視の検出数
- グラフ表示の挙動監視ノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントが挙動監視違反の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	ポリシー違反を検出したデバイスの名前
セキュリティ上の脅威	セキュリティ上の脅威の種類
プログラム	操作の実行元プログラム
イベントの種類	関連するシステムイベント

列	説明
検索対象	操作の実行対象
操作	ユーザが実行し、違反を引き起こした操作
結果	挙動監視違反に対して実行した処理

セキュリティリスク検出: 機械学習型検索

この情報は、[セキュリティリスクの検出数] ウィジェットの [未知の脅威] タブで次のリンクをクリックすると表示されます。

- リスト表示の機械学習型検索での検出数
- グラフ表示の機械学習型検索ノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
 / 	アイコンをクリックして、表の行の下に表示されるログの詳細を展開したり閉じたりできます。
日時	セキュリティエージェントからビジネスセキュリティに検出情報が報告された日時
デバイス名	影響を受けたデバイスの名前
グループ名	デバイスが属するグループの名前
未知の脅威	潜在的な脅威の名前
脅威の可能性	どの脅威の種類にある程度一致してるか

列	説明
ファイル名	ファイルオブジェクトの名前またはプロセスを実行したプログラムの名前 重要 この検出で報告されるファイル名は、他のエンドポイントで検出されたファイル名と異なることがあります。機械学習型検索では、検出された項目をファイル名ではなくファイルハッシュ値に基づいて関連付けます。
パス	ファイルオブジェクトのパスまたはプロセスを実行したプログラムのパス
感染経路	脅威の感染経路
処理	検出された項目に対してビジネスセキュリティで実行された処理

セキュリティリスク検出: 機械学習型検索の詳細

この情報は、[セキュリティリスク検出: 機械学習型検索] ログ画面の最初の列でいずれかの

アイコンをクリックすると確認できます。

ログの詳細は 2 つのタブで構成されます。

- 未知の脅威: 機械学習型検索の分析結果が表示されます。
- ファイル名: この検出ログのファイルのプロパティおよび証明書情報に関する全般的な詳細が表示されます。

ヒント

[除外リストに追加する] をクリックすると、検出されたファイルのファイルハッシュ値をグローバルな機械学習型検索除外リストにすばやく追加できます。除外リストのすべての項目については [グローバル設定] 画面に表示されます。

詳細については、195 ページの「除外リストの設定」を参照してください。

次の表に、[未知の脅威] タブに表示される情報を示します。

表 8-3. [未知の脅威] タブの詳細

項目	説明
脅威の可能性	どの脅威の種類にある程度一致してるか
潜在的脅威の種類	ファイルに含まれる脅威を機械学習型検索で他の既知の脅威と比較した結果、最も可能性が高いと分析された脅威の種類
脅威 ID	検出された脅威の種類との関連が疑われるファイル/プロセスで使用されている API 関数のリスト 重要 API 関数は、脅威の種類を特定するための要素の 1 つにすぎません。機械学習型検索では、脅威の可能性と潜在的な脅威の種類を特定するために、他にもさまざまなファイル特性や分析手法を使用します。
検出の種類	脅威が検出されたオブジェクトの種類 「(ファイル」または「プロセス」)
類似する既知の脅威	検出された脅威にファイル/プロセスの特性が似ている既知の脅威の種類のリスト

セキュリティリスク検出: URL フィルタ

この情報は、[セキュリティリスクの検出数] ウィジェットの [ポリシー違反] タブで次のリンクをクリックすると表示されます。

- リスト表示の URL フィルタ検出数
- グラフ表示の URL フィルタノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントが URL 違反の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	禁止 URL にアクセスを試みているデバイスの名前
URL	禁止 URL

セキュリティリスク検出: デバイスコントロール

この情報は、[セキュリティリスクの検出数] ウィジェットの [ポリシー違反] タブで次のリンクをクリックすると表示されます。

- リスト表示のデバイスコントロール検出数
- グラフ表示のデバイスコントロールノード

[エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントがデバイスコントロール違反の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	ポリシー違反を検出したデバイスの名前
種類	ストレージデバイスの種類
権限	ストレージデバイスに対して設定されている権限
プログラム	操作の実行元プログラム
対象	操作の実行対象

列	説明
操作	実行された処理

ランサムウェアの概要

このウィジェットでは、指定時間内に発生したあらゆるランサムウェア攻撃の概要が提供されます。

既定ビューには、ランサムウェア検出の概要が表示されます。また、感染経路に基づいて攻撃が分類されます。

- 既定のビューのランサムウェア検出数をクリックすると、[ランサムウェアの概要] ログ画面が開きます。この画面には、ランサムウェア検出の詳細が表示されます。
- ドロップダウンリストを使用して、表示を切り替えます。

 をクリックすると、検出情報がチャートに表示されます。

- 特定の日のノードにカーソルを合わせると、表示されている検出カテゴリの検出合計数が表示されます。ノードをクリックすると、[ランサムウェアの概要] ログ画面にリダイレクトされます。この画面には、その特定の日のランサムウェア検出詳細が表示されます。

ランサムウェアの概要ログ

この情報は、グラフでノードをクリックするか、[ランサムウェアの概要] ウィジェットで検出数をクリックすると確認できます。

- [感染経路] および [期間] のリストを使用して表示内容を調整できます。
- [エクスポート] をクリックすると、イベントログが CSV ファイル形式で保存されます。

列	説明
日時	セキュリティエージェントがランサムウェア検出の状況をビジネスセキュリティサーバにアップデートした日時

列	説明
セキュリティ上の脅威	ランサムウェアの種類 • ウイルス/不正プログラム名: 既知のランサムウェアファイルが検出されたときにその名前が表示されます。 • 不正なファイル暗号化: ビジネスセキュリティで不審プログラムによるファイルの暗号化が検出されたときに表示されます。 • <URL>: ビジネスセキュリティでランサムウェアに関連する既知の URL が検出されたときに表示されます。
ソース	脅威を検出した検索の種類
ファイルのパス/URL	• ランサムウェアのファイルパス • ランサムウェアに感染した URL
処理	ランサムウェア検出に対してビジネスセキュリティが実行した処理
デバイス名	影響を受けたデバイスの名前
感染経路	ランサムウェアの感染経路
詳細	[表示] をクリックするとログの詳細が表示されます。

ランサムウェア: 挙動監視ログの詳細

この情報は、[ランサムウェアの概要] ログ画面の [詳細] 列の [表示] リンクをクリックすると表示されます。

行	説明
日時	セキュリティエージェントが挙動監視違反の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	ポリシー違反を検出したデバイスの名前
セキュリティ上の脅威	セキュリティ上の脅威の種類
プログラム	操作の実行元プログラム

行	説明
イベントの種類	関連するシステムイベント
検索対象	操作の実行対象
操作	ユーザが実行し、違反を引き起こした操作
結果	挙動監視違反に対して実行した処理

ランサムウェア:URL フィルタログの詳細

この情報は、[ランサムウェアの概要] ログ画面の [詳細] 列の [表示] リンクをクリックすると表示されます。

行	説明
日時	セキュリティエージェントが URL 違反の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	禁止 URL にアクセスを試みているデバイスの名前
URL	禁止 URL
URL カテゴリ	禁止 URL のカテゴリ
処理	URL 違反に対してビジネスセキュリティが実行した処理

ランサムウェア:ウイルスログの詳細

この情報は、[ランサムウェアの概要] ログ画面の [詳細] 列の [表示] リンクをクリックすると表示されます。

行	説明
日時	セキュリティエージェントがランサムウェア検出の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	影響を受けたデバイスの名前

行	説明
ウイルス/不正プログラム名	検出されたランサムウェアの名前 リンクをクリックすると、トレンドマイクロの脅威データベースが表示されます。そこでは、この脅威による攻撃を手動で駆除する手順など、脅威の詳細情報を調べることができます。
ファイル名	ランサムウェアによって破損したファイルの名前
パス	感染したファイルの場所
感染経路	ランサムウェアがデバイスにアクセスした手段
検索の種類	ランサムウェアの検出に使用した検索の種類
処理	ランサムウェア検出に対してビジネスセキュリティが実行した処理

ランサムウェア:Web レピュテーションログの詳細

この情報は、[ランサムウェアの概要] ログ画面の [詳細] 列の [表示] リンクをクリックすると表示されます。

行	説明
日時	セキュリティエージェントが URL 違反の状況をビジネスセキュリティサーバにアップデートした日時
デバイス名	禁止 URL にアクセスを試みているデバイスの名前
URL	禁止 URL
危険度	感染しやすさおよびダメージを受ける可能性に基づいて、TrendLabs が割り当てた危険度。
処理	URL 違反に対してビジネスセキュリティが実行した処理

エージェントのステータス

このウィジェットでは、ネットワーク上のセキュリティエージェントの接続とアップデート状況の概要が提供されます。

- ステータスの横の件数をクリックすると [デバイス] 画面にリダイレクトされ、そのステータスのデバイスの詳細が一覧表示されます。
- [デバイスの追加] をクリックすると [デバイスの追加] 画面にリダイレクトされ、追加のデバイスにセキュリティエージェントをインストールできます。

  詳細については、23 ページのエージェントのインストールを参照してください。
- [コンポーネントステータスの確認] をクリックすると、[手動アップデート] 画面にリダイレクトされ、最新のコンポーネントの情報を確認できます。

  詳細については、135 ページの「アップデート可能なコンポーネント」を参照してください。

第 9 章

通知の管理

本章では、さまざまな通知オプションの使用方法について説明します。

通知の使用

管理者が長い時間をかけてビジネスセキュリティを監視しなくても大規模感染に関する警告を事前にメールで受け取れるようにするには、ネットワークで異常なイベントが発生したときにサーバから通知を送信するように設定します。

初期設定では、[通知] 画面に一覧表示されるすべてのイベントが選択されており、これらのイベントが発生すると、サーバから管理者に通知が送信されます。

表 9-1. 「要確認」の通知

イベントの種類	説明
脅威イベント	
ウイルス対策 - 解決されていない脅威	ウイルス/不正プログラムの脅威に対する処理に失敗したときに発生します。 次の検索処理は検出数に含まれません: 潜在的なセキュリティリスクを放置しました
ウイルス対策 - エンドポイントでのリアルタイム検索無効	エンドポイントでリアルタイム検索が無効になっているときに発生します。
スパイウェア対策 - デバイスの再起動が必要な検出	エンドポイントでスパイウェア/グレーウェアが検出され、脅威を完全に取り除くために再起動が必要なときに発生します。
システムイベント	
更新 - アップデートが必要なエージェント	セキュリティエージェントが最新の状態でなく、コンポーネントのアップデートが必要なときに発生します。
更新 - アップデートが必要なスマートスキャンパターンファイル	スマートスキャンパターンファイルが最新の状態でなく、パターンファイルのアップデートが必要なときに発生します。
更新 - アップデートが必要なビジネスセキュリティサーバコンポーネント	ビジネスセキュリティサーバが最新の状態でなく、コンポーネントのアップデートが必要な場合に発生します。

イベントの種類	説明
Smart Protection サービス - サービスは使用できません	スマートスキャン用に設定されているセキュリティエージェントが Smart Protection サービスに接続できないか、サービスが利用できないときに発生します。
リソース不足 - 残りディスク容量	一部のサーバの残りディスク容量が指定した割合を下回ったときに発生します。
ライセンスイベント	
ライセンス - 有効期限切れ	ライセンスの有効期限が終了したときに発生します。
ライセンス - 有効期限が残り 60 日未満	ライセンスの有効期限が近づいているときに発生します。

表 9-2. 「警告」の通知

イベントの種類	説明
脅威イベント	
ウイルス対策 - エンドポイントでのウイルス検出数が次の条件を超えた時:	指定した期間内に指定した数を超えるウイルス/不正プログラムの脅威がエンドポイントで検出されたときに発生します。
スパイウェア対策 - スパイウェア/グレーウェア検出数が次の条件を超えた時:	指定した期間内に指定した数を超えるスパイウェア/グレーウェアの脅威がエンドポイントで検出されたときに発生します。
ウイルス対策 - 受信した総メッセージ数に対するスパムメールの割合が次の条件を超えた時:	受信した総メッセージ数に対するスパムメールの割合が指定した値を超えたときに発生します。
Web レピュテーション - URL 違反数が次の条件を超えた時:	指定した期間内に指定した数を超える URL 違反が検出されたときに発生します。
URL フィルタ - URL 違反数が次の条件を超えた時:	指定した期間内に指定した数を超える URL 違反が検出されたときに発生します。
機械学習型検索 - 未知の脅威の検出数がしきい値を次の条件を超えた時:	指定した期間内に指定した数を超える未知の脅威が検出されたときに発生します。

イベントの種類	説明
挙動監視 - 挙動監視違反数が次の条件を超えた時:	指定した期間内に指定した数を超える挙動監視違反が検出されたときに発生します。
ネットワークウイルス - ネットワークウイルス検出数が次の条件を超えた時:	指定した期間内に指定した数を超えるネットワークウイルスが検出されたときに発生します。
デバイスコントロール - デバイスコントロール違反数が次の条件を超えた時:	指定した期間内に指定した数を超えるデバイスコントロール違反が検出されたときに発生します。

通知イベントを設定する

ビジネスセキュリティ には、次の 3 とおりの通知方法があります。

- SNMP 通知
- Windows イベントログ
- メール通知

手順

1. [管理] > [通知]に移動します。
2. SNMP 通知を受け取るには、[SNMP 通知] で設定します。

   簡易ネットワーク管理プロトコル (SNMP) は、ネットワーク管理に使用されるプロトコルです。SNMP トラップ内のデータを表示するには、Management Information Base ブラウザを使用します。

   a. [SNMP 通知の有効化] を選択します。

   b. SNMP トラップの IP アドレスを指定します。

   c. SNMP コミュニティを指定します。
3. Windows イベントログによる通知を受け取るには、[ログ] で [Windows のイベントログによる通知を有効にする] 選択します。
4. メール通知を受け取るには、送信者と受信者を指定します。

ヒント

複数のエントリはセミコロン (;) で区切ります。

5. [要確認] タブまたは [警告] タブをクリックします。
6. [種類] 列で、通知を受け取るイベントの種類に対応するチェックボックスをオンにします。
7. [警告しきい値] 列で、通知を送信する基準となる期間および検出数または違反数を適宜指定します。
8. 各イベント通知の件名やメッセージ本文をカスタマイズするには、[種類] 列で通知のリンクをクリックします。

   通知のカスタマイズの詳細については、179 ページの「トークン変数」を参照してください。
9. [保存] をクリックします。

トークン変数

トークン変数を使用して、イベント通知の件名行とメッセージ本文をカスタマイズします。

次のトークンは、デスクトップやサーバで検出された脅威イベントを表します。

トークン	説明	警告の種類
%COUNT	検出数を挿入します。	警告イベント:すべて
$CSM_SERVERNAME	ビジネスセキュリティサーバの名前を挿入します。	すべて
%DATE	ライセンスの残りの日数を挿入します。	ライセンス - 有効期限切れ ライセンス - 有効期限が残り 60 日未満

トークン	説明	警告の種類
%DATE_TIME	イベントの日時を挿入します。	ウイルス対策 - 解決されていない脅威 ウイルス対策 - エンドポイントでのリアルタイム検索無効 スパイウェア対策 - デバイスの再起動が必要な検出 更新 - アップデートが必要なエージェント 更新 - アップデートが必要なビジネスセキュリティサーバコンポーネント Smart Protection サービス - サービスは使用できません リソース不足 - 残りディスク容量
%DEVICE_COUNT	影響を受けたデバイスの数を挿入します。	ウイルス対策 - 解決されていない脅威 ウイルス対策 - エンドポイントでのリアルタイム検索無効 スパイウェア対策 - デバイスの再起動が必要な検出 更新 - アップデートが必要なエージェント リソース不足 - 残りディスク容量 次を除くすべての警告イベント: ウイルス対策 - 受信した総メッセージ数に対するスパムメールの割合が次の条件を超えた時:

トークン	説明	警告の種類
%FROM	イベントの開始日時を挿入します。	次を除くすべての警告イベント: ウイルス対策 - 受信した総メッセージ数に対するスパムメールの割合が次の条件を超えた時:
%NUMBER	イベント数を表示します。	ウイルス対策 - 解決されていない脅威 ウイルス対策 - エンドポイントでのリアルタイム検索無効 スパイウェア対策 - デバイスの再起動が必要な検出 次を除くすべての警告イベント: ウイルス対策 - 受信した総メッセージ数に対するスパムメールの割合が次の条件を超えた時:
%THRESHOLD%	イベントのしきい値を挿入します。	更新 - アップデートが必要なエージェント 更新 - アップデートが必要なスマートスキャンパターンファイル 更新 - アップデートが必要なビジネスセキュリティサーバコンポーネント Smart Protection サービス - サービスは使用できません リソース不足 - 残りディスク容量 警告イベント:すべて

トークン	説明	警告の種類
%TO	イベントの終了日時を挿入します。	次を除くすべての警告イベント: ウイルス対策 - 受信した総メッセージ数に対するスパムメールの割合が次の条件を超えた時:

```
件名: [ビジネスセキュリティサーバ – <$CSM_SERVERNAME>] [要確認]
ウイルス対策 – 解決されていない脅威: %NUMBER
メッセージ: ウイルスバスター ビジネスセキュリティ通知
* ウイルス対策 – 解決されていない脅威: %NUMBER
* レポート日時: %DATE_TIME
* 影響を受けたデバイス: %DEVICE_COUNT
* 推奨される処理:
  次のソリューションにて、対処方法をご確認ください。
  http://tmqa.jp/biz10_action_fail
```

```
件名: [ビジネスセキュリティサーバ – サーバ A] [要確認]
ウイルス対策 – 解決されていない脅威: 5
メッセージ: ウイルスバスター ビジネスセキュリティ通知
* ウイルス対策 – 解決されていない脅威: 5
* レポート日時: February 14, 2018 年 2 月 14 日
* 影響を受けたデバイス: 2
* 推奨される処理:
  次のソリューションにて、対処方法をご確認ください。
  http://tmqa.jp/biz10_action_fail
```

第 10 章

グローバル設定の管理

本章では、エージェントのグローバル設定と、セキュリティサーバのシステム設定について説明します。

グローバル設定

Web コンソールから、ビジネスセキュリティサーバおよびセキュリティエージェントのグローバル設定を指定できます。

タブ	説明
プロキシ	ネットワークでプロキシサーバを使用してインターネットに接続している場合、次のサービスに関してプロキシサーバの設定を指定します。 • コンポーネントのアップデートおよびライセンス通知 • Web レピュテーション、挙動監視、およびスマートスキャン 詳細については、185 ページの「インターネットプロキシを設定する」を参照してください。
SMTP	SMTP サーバ設定は、ビジネスセキュリティサーバによって生成されるすべての通知とレポートに適用されます。 詳細については、186 ページの「SMTP サーバを設定する」を参照してください。
デスクトップ/サーバ	セキュリティ設定は、すべてのセキュリティエージェントに適用されます。 詳細については、187 ページの「デスクトップ/サーバの設定」を参照してください。
システム	オフラインのエージェントの自動削除、エージェントの接続ステータスの確認、および隔離フォルダの保守について設定できます。 詳細については、191 ページの「システム設定を行う」を参照してください。
除外設定	Web レピュテーション、URL フィルタ、および機械学習型検索のそれぞれで定義したポリシーの設定よりも優先する除外リストを設定できます。 詳細については、195 ページの「除外リストの設定」を参照してください。

インターネットプロキシを設定する

ビジネスセキュリティサーバおよびエージェントがプロキシサーバを 使用してインターネットに接続している場合、次の機能およびトレンドマイクロのサービスを利用するためにプロキシサーバの設定を指定します。

- ビジネスセキュリティサーバ ― コンポーネントのアップデートおよびライセンスの管理
- セキュリティエージェント ― Web レピュテーション、URL フィルタ、挙動監視、スマートフィードバック、およびスマートスキャン

手順

1. [管理] > [グローバル設定] に移動します。
2. [プロキシ] タブで、必要に応じて次のものをアップデートします。
    - ビジネスセキュリティサーバのプロキシ
        - アップデートおよびライセンス 通知にプロキシサーバを使用する
        - SOCKS 4/5 を使用する
        - アドレス: IPv4/IPv6 アドレスまたはホスト名
        - ポート番号
        - プロキシサーバ認証
            - ユーザ名
            - パスワード
    - セキュリティエージェントのプロキシ
        - アップデートプロキシで指定した資格情報の使用

注意

セキュリティエージェントは、Internet Explorer のプロキシサーバとポート番号を使用してインターネットに接続します。クライアント上の Internet Explorer とビジネスセキュリティサーバが同じ資格情報を共有している場合にのみ、このオプションを使用してください。

- ユーザ名
- パスワード

3. [保存] をクリックします。

SMTP サーバを設定する

SMTP サーバ設定は、ビジネスセキュリティによって生成されるすべての通知とレポートに適用されます。

手順

1. [管理] > [グローバル設定] に移動します。
2. [SMTP] タブをクリックして、必要に応じて次のものをアップデートします。
   - SMTP サーバ:SMTP サーバの IPv4/IPv6 アドレスまたは名前を入力します。
   - ポート番号
   - SMTP サーバ認証を有効にする
     - ユーザ名
     - パスワード
3. 設定が正しいことを確認するために、[テストメールの送信] をクリックします。送信が失敗した場合は、設定を変更するか、SMTP サーバのステータスを確認してください。

4. [保存] をクリックします。

デスクトップ/サーバの設定

デスクトップ/サーバのオプションは、ビジネスセキュリティ のグローバル設定から設定できます。この設定よりも、個々のグループの設定が優先されます。グループの特定のオプションが未設定の場合は、デスクトップ/サーバのオプションが使用されます。たとえば、あるグループに対して承認済み URL が 1 つも定義されていない場合は、この画面で設定されたすべての承認済み URL がそのグループに適用されます。

手順

1. [管理] > [グローバル設定] に移動します。
2. [デスクトップ/サーバ] タブをクリックし、必要に応じて次の項目をアップデートします。

設定	説明
ロケーション認識	ロケーション認識を使用すると、管理者は、クライアントがどのようにネットワークに接続されているかに応じて、セキュリティ設定を制御できます。 ロケーション認識は、オフィス内とオフィス外の接続設定を制御します。 セキュリティエージェントは、Web コンソールに設定されたゲートウェイ情報に基づいてクライアントの場所を特定し、ユーザがアクセスできる Web サイトを制御します。ユーザの場所に応じて制限内容が異なります。 • ロケーション認識を有効にする:ここでの設定が、ファイアウォール、Web レピュテーションのオフィス内/オフィス外接続設定、および自動アップデートの頻度に影響するようになります。 • ゲートウェイの情報:このリストに登録されているクライアントおよび接続は、ネットワークにリモートで接続するときに (VPN を使用) ロケーション認識が有効化されていれば、内部接続設定を使用します。 • ゲートウェイ IP アドレス

設定	説明
	• MAC アドレス:MAC アドレスを追加すると、指定のデバイスのみが接続できるようになるため、セキュリティが大幅に強化されます。 エントリを削除するには、対応する削除アイコン (x) をクリックします。
管理者への問い合わせ	管理者への問い合わせでは、セキュリティエージェントに関して、管理者への問い合わせ先がユーザに通知されます。必要に応じて次の項目をアップデートします。 • 管理者への問い合わせのラベル • 管理者への問い合わせのメールアドレス • 追加情報:ユーザがラベルの上にマウスを配置すると表示されます。
一般検索	• スマートスキャンサービスを無効にする:すべてのセキュリティエージェントが従来型スキャンモードに切り替えられます。スマートスキャンは、ここで再度有効にされるまで使用できません。特定のセキュリティエージェントグループのみを切り替えるには、[デバイス] > {グループ} > [ポリシーの設定] > [検索方法] に移動します。 注意 セキュリティエージェントの検索方法の切り替えに関するガイドラインについては、85 ページの「検索方法を設定する」を参照してください。 • 遅延検索を有効にする:この機能を有効にすると、ファイルをコピーする際の検索処理のタイミングが遅延します。パフォーマンスは向上しますが、セキュリティリスクをもたらす可能性があります。 警告! 遅延検索を有効にすると、セキュリティ上のリスクが生じることがあります。 • シャドウコピーセクションの除外: シャドウコピーまたはボリュームスナップショットのサービスによって、指定のボリューム上のファイルまたはフォルダのバックアップ

設定	説明
	コピーまたはスナップショットが手動または自動で作成されます。 • ビジネスセキュリティのデータベースフォルダを除外する: このオプションがオンの場合、ビジネスセキュリティサーバにインストールされているエージェントは、リアルタイム検索の実行時に限って、自身のデータベースを検索しません。 初期設定では、ビジネスセキュリティのデータベースは検索対象外です。検索時に発生する可能性があるデータベースの破損を回避するために、このチェックボックスはそのままオンにしておくようお勧めします。 • Microsoft ドメインコントローラフォルダを除外する: このオプションがオンの場合は、ドメインコントローラにインストールされているエージェントが検索を実行するときに、ドメインコントローラのフォルダは検索対象外となります。このフォルダには、ユーザ情報、ユーザ名、パスワードなどの重要な情報が保存されています。
ウイルス検索	• 圧縮ファイルの検索制限: 検索対象の圧縮ファイルにおける、解凍後のファイルサイズおよび圧縮ファイル内のファイル数の最大値を指定します。 • 圧縮ファイルのウイルス駆除: 圧縮ファイル内の感染ファイルに対して駆除が試行されます。 • OLE オブジェクトを {} 階層まで検索: ここで指定した数の OLE 階層が検索対象となります。OLE は、1 つのアプリケーションでオブジェクトを作成し、別のアプリケーションでそのオブジェクトをリンクしたり埋め込んだりするために使用されます。たとえば、.xls ファイルを.doc ファイルの中に埋め込むことができます。 • 手動検索をクライアントのショートカットメニューに追加: [セキュリティエージェント上の脅威の検索] リンクを右クリックメニューに追加します。このオプションをオンにすると、ユーザはデスクトップ上または Windows エクスプローラ内のファイルまたはフォルダを右クリックしてそのファイルまたはフォルダの手動検索を実行できるようになります。
スパイウェア検索	• Cookie の検索: セキュリティエージェントは Cookie を検索します。

設定	説明
	• Cookie 検出をスパイウェアログに追加: 検出されたスパイウェア Cookie をスパイウェアログに追加します。
ファイアウォール	[ファイアウォールを無効にしてドライバをアンインストールする] チェックボックスをオンにすると、ビジネスセキュリティエージェントのファイアウォールがアンインストールされ、ファイアウォール関連のドライバが削除されます。 注意 ファイアウォールを無効にした場合、ファイアウォールを再び有効にするまで関連する設定は使用できません。
HTTPS Web 評価	この機能を有効にすると、Chrome、Firefox および Microsoft Edge で、Web レピュテーションおよび URL フィルタの設定と照合して HTTPS の URL が確認されます。 注意 この機能はブラウザのアドオンを必要としません。 Internet Explorer の場合は、Web レピュテーションと URL フィルタリングを有効にする際に設定したブラウザアドオンを使用して、HTTPS URL を確認します。
警告	{} 日間経過してもウイルスパターンファイルがアップデートされない場合、Windows タスクバーに警告アイコンを表示:指定の日数が経過してもパターンファイルがアップデートされていないときに、クライアントの画面に警告アイコンを表示します。
セキュリティエージェントのアンインストール	• パスワード入力無しでのセキュリティエージェントのアンインストールを許可する • セキュリティエージェントのアンインストール時にパスワード入力を要求する
セキュリティエージェントのロック解除と終了	• クライアントユーザによるパスワードを使用しないコンピュータ上のセキュリティエージェントの終了とロック解除を許可する

設定	説明
	• クライアントユーザにセキュリティエージェントを終了してロック解除するためのパスワードの入力を要求する **注意** セキュリティエージェントをロック解除すると、ユーザは、[デバイス] > {グループ} > [ポリシーの設定] > [エージェントの権限] に指定された設定をすべて変更できるようになります。
優先される IP アドレス	この設定は、デュアルスタックビジネスセキュリティサーバでのみ使用可能で、デュアルスタックエージェントによってのみ適用されます。 エージェントは、インストールまたはアップグレード後に、IP アドレスを使用してビジネスセキュリティサーバに登録されます。 次のオプションから選択します。 • 最初に IPv4、次に IPv6: エージェントは IPv4 アドレスを最初に使用します。IPv4 アドレスを使用して登録できない場合、エージェントは IPv6 アドレスを使用します。どちらの IP アドレスを使用しても登録できない場合は、優先度の高い方の IP アドレスを使用して再試行します。 • 最初に IPv6、次に IPv4: エージェントは IPv6 アドレスを最初に使用します。IPv6 アドレスを使用して登録できない場合、エージェントは IPv4 アドレスを使用します。どちらの IP アドレスを使用しても登録できない場合は、優先度の高い方の IP アドレスを使用して再試行します。

3. [保存] をクリックします。

システム設定を行う

[グローバル設定] 画面の [システム] セクションには、オフラインのエージェントの自動削除、エージェントの接続ステータスの確認、および隔離フォルダの保守に関するオプションがあります。

手順

1. [管理] > [グローバル設定] に移動します。
2. [システム] タブをクリックして、必要に応じて次のものをアップデートします。

設定	説明
オフラインセキュリティエージェントの削除	セキュリティエージェントをクライアントから削除するためにアンインストールプログラムを実行すると、ビジネスセキュリティサーバへの通知が自動的に送信されます。ビジネスセキュリティサーバがこの通知を受け取ると、クライアントが存在しなくなったことを示すために、セキュリティ設定のグループツリーからクライアントのアイコンが削除されます。 ただし、セキュリティエージェントが別の方法 (ハードディスクの再フォーマット、クライアントファイルの手動削除など) で削除された場合は、削除されたことをビジネスセキュリティサーバが認識しないため、セキュリティエージェントのステータスはオフラインと表示されます。ユーザがエージェントを長期間終了または無効化した場合も、サーバにはセキュリティエージェントがオフライン状態として表示されます。 セキュリティ設定のグループツリーにアクティブなクライアントだけを表示するには、オフラインのセキュリティエージェントをセキュリティ設定のグループツリーから自動的に削除するようにビジネスセキュリティサーバを設定します。 • セキュリティエージェント自動削除を有効にする –ビジネスセキュリティサーバにアクセスしていない期間が指定の日数に達したクライアントを自動的に削除します。 • {} 日以上アクセスのないセキュリティエージェントを自動削除する –許容されるクライアントのオフライン日数を指定します。この日数に達すると、クライアントは Web コンソールから削除されます。

設定	説明

エージェントの接続状態の確認	ビジネスセキュリティでは、クライアントの接続ステータスはセキュリティ設定のグループツリーの「オンライン/オフライン」項目に表示されます。ただし、何らかの条件によって、セキュリティ設定のグループツリーで表示されているステータスと、エージェントの接続状態が異なる場合があります。たとえば、クライアントのネットワークケーブルが誤って抜かれた場合、エージェントはオフラインであることをビジネスセキュリティサーバに通知できません。このため、セキュリティ設定のグループツリーではこのエージェントはオンラインとして表示されます。
	
	エージェントとサーバの接続状態は手動で確認するか、確認のスケジュールを Web コンソールで設定できます。
	
	  注意
	接続状態の確認では、特定のグループまたはエージェントの選択はできません。ビジネスセキュリティサーバに登録されたすべてのエージェントとの 接続状態が確認されます。
	
	• 接続状態を定期的に確認する:エージェントとサーバの接続状態の確認をスケジュールに従って自動的に実行します。
	  • 毎時間
	  • 毎日
	  • 毎週
	  • 開始時刻 —確認を開始する時刻です。
	• 接続状態を確認 —接続状態の確認をすぐに開始します。

設定	説明
隔離フォルダ設定	初期設定では、セキュリティエージェントは隔離された感染ファイルをビジネスセキュリティサーバの次のディレクトリに送信します。 <ビジネスセキュリティサーバのインストールフォルダ >¥PCCSRV¥Virus ディレクトリを変更する必要がある場合は (ディスク容量が足りない場合など)、[隔離ディレクトリ設定] フィールドに「D:¥Quarantined Files」などの絶対パスを入力します。この場合、[デバイス] > {グループ} > [ポリシーの設定] > [隔離] で同じ変更を適用するようにしてください。そうしないと、エージェントは<ビジネスセキュリティサーバのインストールフォルダ >¥PCCSRV¥Virus にファイルを送信し続けます。 また、次の管理設定も実行してください。 • 隔離フォルダの容量:隔離フォルダのサイズを MB 単位で指定します。 • 隔離ファイルの最大サイズ —隔離フォルダに保存される 1 ファイルあたりの最大サイズを MB 単位で指定します。 • すべての隔離ファイルを削除 —隔離フォルダ内のファイルをすべて削除します。フォルダに空き領域がないときは、新しいファイルがアップロードされても、そのファイルは保存されません。 エージェントからビジネスセキュリティサーバに隔離されたファイルを送信しないようにするには、[デバイス] > {グループ} > [ポリシーの設定] > [隔離] で新しいディレクトリを設定し、すべての管理設定を無視します。手順については、96 ページの「隔離ディレクトリ」を参照してください。

設定	説明
セキュリティエージェントのインストール	セキュリティエージェントのインストールディレクトリ — セットアップで各セキュリティエージェントがインストールされる場所です。インストール時に、セキュリティエージェントのインストールディレクトリを入力するよう指示されます。 必要に応じて、絶対パスを入力してディレクトリを変更します。今後インストールするエージェントのみがこのディレクトリにインストールされます。既存のエージェントは現在のディレクトリに保持されます。 次の変数のいずれかを使用して、インストールパスを設定します。 • `$BOOTDISK` —起動ディスクドライブ • `$WINDIR` —Windows のインストール先フォルダ • `$ProgramFiles` —プログラムフォルダ

3. [保存] をクリックします。

除外リストの設定

手順

1. [管理] > [グローバル設定] に移動します。
2. [除外設定] タブをクリックして、必要に応じて次のものを設定します。

セクション	説明
Web レピュテーションおよび URL フィルタ	• 承認済み URL リスト: Web レピュテーションおよび URL フィルタの検証から除外される Web サイト (およびそれらのサブドメイン) です。 注意 承認済みリストは、ブロックするリストより優先されます。URL が除外リストのエントリと一致する場合、それがブロックするリストに含まれる場合でも、エージェントは常にその URL へのアクセスを許可します。 特定のグループに対する承認済み/ブロックする URL を設定すると、そのグループに対してはグローバル設定の除外設定は適用されません。 • ブロックする URL リスト: URL フィルタの検証で常にブロックされる Web サイト (およびそれらのサブドメイン) です。 • プロセス除外リスト: Web レピュテーションおよび URL フィルタの検証から除外されるプロセスです。組織が信頼できると見なした重要なプロセスを入力してください。 ヒント プロセス除外リストを更新し、最新リストがサーバからエージェントに配信されると、クライアントコンピュータ上の (ポート 80、81、または 8080 を介した) すべてのアクティブな HTTP 接続が数秒間切断されます。プロセス除外リストの更新はオフピーク時間帯に実行することを検討してください。 • IP 除外リスト:Web レピュテーションおよび URL フィルタの検証から除外される IP アドレス

セクション	説明
	(192.168.10.1 など) です。組織が信頼できると見なした重要な IP アドレスを入力してください。 • Web レピュテーションおよび URL フィルタのログをビジネスセキュリティサーバに送信する
機械学習型検索除外リスト	このリストに追加したファイルは、セキュリティエージェントでも不正ファイルとして検出されなくなります。検索対象から除外するファイルの SHA-1 ハッシュ値を入力します。必要に応じて、除外理由やハッシュ値に関連付けられたファイル名をメモとして指定することができます。

3. [保存] をクリックします。

第 11 章

ログとレポートの使用

本章では、ログとレポートを使用してシステムを監視しウイルス対策を分析する方法について説明します。

ログ

ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) では、ウイルス/不正プログラムおよびスパイウェア/グレーウェアの検出、イベント、およびアップデートに関する包括的なログが保存されます。これらのログは、組織のウイルス対策ポリシーの査定や、感染リスクの高いクライアントの特定、およびアップデートが正常に配信されたかどうかの確認に使用します。

注意

CSV ログファイルを表示するには、Microsoft Excel などの表計算ソフトなどを使用してください。

ビジネスセキュリティ では、次の種類のログが管理されます。

- Web コンソールイベントログ
- デスクトップ/サーバイベントログ

表 11-1. ログの種類と内容

種類 (ログエントリの生成元)	ログの内容 (内容を取得するログの種類)
Web コンソールイベント	• 手動検索 (Web コンソールから起動) • アップデート (ビジネスセキュリティサーバのアップデート) • コンソールイベント

種類 (ログエントリの生成元)	ログの内容 (内容を取得するログの種類)

デスクトップ/サーバ	• ウイルス/不正プログラムログ
	  • 手動検索
	  • リアルタイム検索
	  • 予約検索
	• スパイウェア/グレーウェアログ
	  • 手動検索
	  • リアルタイム検索
	  • 予約検索
	• 機械学習型検索ログ
	• Web レピュテーションログ
	• URL フィルタログ
	• 挙動監視ログ
	• アップデートログ
	• ネットワークウイルスログ
	• イベントログ
	• デバイスコントロールログ
	• アップデート配信ログ
	• ランサムウェア関連ログ
	  • ウイルス対策/不正プログラム対策
	  • 挙動監視
	  • Web レピュテーション
	  • URL フィルタ
	  • 機械学習型検索

ログクエリの使用

ログクエリは、ログデータベースから情報を収集するときに実行します。クエリの設定と実行には、[ログクエリ] 画面を使用します。結果は、.CSV ファイルにエクスポートするか、印刷できます。

手順

1. [レポート] > [ログクエリ] に移動します。
2. 必要に応じて次のオプションをアップデートします。
   - レポート生成期間
     - プルダウンメニューから選択
     - 表示期間を指定 –クエリを特定の期間に限定する場合に指定します。
   - 種類 –各ログの種類の内容については、200 ページの「ログ」を参照してください。
     - Web コンソールイベント
     - デスクトップ/サーバイベント
   - ログの内容 –選択できるオプションは、ログの [種類] によって異なります。
3. [ログの表示] をクリックします。
4. ログを CSV 形式で保存するには、[エクスポート] をクリックします。CSV ファイルを表示するには、表計算ソフトウェアを使用してください。

レポート

1 回限りのレポートを手動で生成することも、予約レポートを生成するようにビジネスセキュリティサーバを 設定することもできます。

レポートは、印刷することも、管理者またはその他の個人にメールで送信することもできます。

レポートに表示されるデータは、レポートが生成された時点でのビジネスセキュリティサーバに 蓄積されたログ数が反映されたものです。ログ数は、新

しいログが追加されたり、既存のログが削除されると変わります。[レポート] > [管理] で、手動でログを削除したり、ログの削除予定を設定することができます。

1 回限りのレポートを使用する

手順

1. [レポート] > [1 回限りのレポート] の順に移動します。
2. 次のタスクを実行します。

タスク	手順
レポートの生成	a. [追加] をクリックします。 新しい画面が表示されます。 b. 次の設定をします。 • レポート名 • レポート生成期間:日付を限定してレポートを作成します。 • レポートの内容:すべての脅威を選択するには、[すべて選択] チェックボックスをオンにします。脅威を 1 つずつ選択するには、対応するチェックボックスをオンにします。プラス (+) アイコンをクリックすると内容が展開されます。 • レポートの送信先 • 受信者:受信者のメールアドレスを入力し、セミコロン (;) でそれらを区切ります。 • 形式:PDF または HTML レポートへのリンクを選択します。[PDF] を選択すると、PDF がメールに添付されます。 c. [追加] をクリックします。

タスク	手順
レポートの表示	[レポート名] 列でレポートへのリンクをクリックします。最初のリンクは PDF レポートを開き、2 番目のリンクは HTML レポートを開きます。 レポートに表示されるデータは、レポートが生成された時点でのビジネスセキュリティサーバに蓄積されたログ数が反映されたものです。ログ数は、新しいログが追加されたり、既存のログが削除されると変わります。[レポート] > [管理] で、手動でログを削除したり、ログの削除予定を設定することができます。 レポートの内容の詳細については、208 ページの「レポートについて」を参照してください。
レポートの削除	a. レポートのリンクを含む行を選択します。 b. [削除] をクリックします。 注意 レポートを自動的に削除するには、[レポート] > [管理] > [レポート] タブに移動して、ビジネスセキュリティが保持する 1 回限りのレポートの最大数を設定します。初期設定の 1 回限りのレポート数は 10 です。その数を超過すると、ビジネスセキュリティサーバではレポートが保持期間の長いものから削除されます。

予約レポートを使用する

手順

1. [レポート] > [予約レポート] の順に移動します。
2. 次のタスクを実行します。

タスク	手順
予約レポートのテンプレートの作成	a. [追加] をクリックします。 新しい画面が表示されます。 b. 次の設定をします。 • レポートテンプレート名 • 生成スケジュール: 毎日、毎週、または毎月、およびレポートを生成する時刻 月次レポートの場合、31、30、29 日を選択したときに、その日数よりも少ない月にはレポートは生成されません。 • レポートの内容:すべての脅威を選択するには、[すべて選択] チェックボックスをオンにします。脅威を 1 つずつ選択するには、対応するチェックボックスをオンにします。プラス (+) アイコンをクリックすると内容が展開されます。 • レポートの送信先 • 受信者:受信者のメールアドレスを入力し、セミコロン (;) でそれらを区切ります。 • 形式:PDF または HTML レポートへのリンクを選択します。[PDF] を選択すると、PDF がメールに添付されます。 c. [追加] をクリックします。

タスク	手順
予約レポートの表示	a. 予約レポートの生成元のテンプレートを含んだ行で、[レポート履歴] をクリックします。 新しい画面が表示されます。 b. [表示] 列でレポートへのリンクをクリックします。最初のリンクは PDF レポートを開き、2 番目のリンクは HTML レポートを開きます。 レポートに表示されるデータは、レポートが生成された時点でのビジネスセキュリティサーバに蓄積されたログ数が反映されたものです。ログ数は、新しいログが追加されたり、既存のログが削除されると変わります。[レポート] > [管理] で、手動でログを削除したり、ログの削除予定を設定することができます。 レポートの内容の詳細については、208 ページの「レポートについて」を参照してください。
テンプレートの管理タスク	
テンプレートの設定の編集	テンプレートをクリックして、表示された新しい画面で設定を編集します。 変更の保存後に生成されたレポートで新しい設定が使用されます。
テンプレートの有効化/無効化	[有効] 列のアイコンをクリックします。 予約レポートの生成を一時的に停止する場合はテンプレートを無効にし、再度レポートが必要なときに有効にします。

タスク	手順
テンプレートの削除	テンプレートを選択して、[削除] をクリックします。 テンプレートを削除しても、そのテンプレートから生成された予約レポートは削除されませんが、Web コンソールからレポートへのリンクは使用できなくなります。レポートには、ビジネスセキュリティサーバコンピュータから直接アクセスできます。レポートは、手動でコンピュータから削除するか、ビジネスセキュリティサーバが [レポート] > [管理] > [レポート] タブで設定された予約レポートの自動削除設定に従って自動的に削除した場合にのみ削除されます。 テンプレートを自動的に削除するには、[レポート] > [管理] > [レポート] タブに移動して、ビジネスセキュリティが保持するテンプレートの最大数を設定します。初期設定のテンプレート数は 10 です。その数を超過すると、ビジネスセキュリティサーバではテンプレートが保持期間の長いものから削除されます。
レポートの管理タスク	
予約レポートへのリンクの送信	メールで予約レポートへのリンクを送信します (PDF 形式)。受信者は、メールメッセージ内のリンクをクリックすると、PDF ファイルへアクセスできます。受信者がビジネスセキュリティサーバコンピュータへ接続できることを確認してください。接続できない場合、ファイルは表示されません。 注意 メールでは PDF ファイルへのリンクのみが提供されます。実際の PDF ファイルは添付されません。 a. 予約レポートの生成元のテンプレートを含んだ行で、[レポート履歴] をクリックします。 新しい画面が表示されます。 b. レポートを選択して、[送信] をクリックします。 初期設定のメールクライアントが開き、レポートへのリンクを含んだ新規メールが表示されます。

タスク	手順
予約レポートの削除	a. 予約レポートの生成元のテンプレートを含んだ行で、[レポート履歴] をクリックします。 新しい画面が表示されます。 b. レポートを選択して、[削除] をクリックします。 注意 レポートを自動的に削除するには、[レポート] > [管理] > [レポート] タブに移動して、ビジネスセキュリティが保持するテンプレートごとの予約レポートの最大数を設定します。初期設定の予約レポート数は 10 です。その数を超過すると、ビジネスセキュリティサーバではレポートが保持期間の長いものから削除されます。

レポートについて

ビジネスセキュリティのレポートには、以下に示す情報が表示されます。表示される情報は、選択されたオプションによって異なることがあります。

表 11-2. レポートの内容

レポート項目	説明
ウイルス対策	デスクトップ/サーバのウイルス概要 ウイルスレポートには、検索エンジンによって検出されて処理が実行されたウイルス/不正プログラムの数と種類に関する詳細情報が表示されます。また、検出数の多いウイルス/不正プログラムの名前の一覧も表示されます。ウイルス/不正プログラムの名前をクリックすると、新しい Web ブラウザページが開いてトレンドマイクロのウイルス情報ページが表示され、そのウイルス/不正プログラムの詳細情報を読むことができます。

レポート項目	説明
	ウイルスが検出されたデスクトップ/サーバの上位 5 件 ウイルス/不正プログラムの検出を報告しているデスクトップまたはサーバの上位 5 件が表示されます。同じクライアントでウイルス/不正プログラムが頻繁に検出される場合は、高いセキュリティリスクがあることを示している可能性があり、詳細の調査が必要です。
スパイウェア対策	デスクトップ/サーバのスパイウェア/グレーウェア概要 スパイウェア/グレーウェアレポートには、クライアントで検出されたスパイウェア/グレーウェアの詳細情報 (検出数やビジネスセキュリティによって実行された処理など) が表示されます。このレポートには、スパイウェア検索時に実行された各処理の比率を表す円グラフも表示されます。
	スパイウェアが検出されたデスクトップ/サーバの上位 5 件 検出されたスパイウェア/グレーウェアの上位 5 件、およびスパイウェア/グレーウェア検出数の多いデスクトップ/サーバの上位 5 件もレポートに表示されます。検出されたスパイウェア/グレーウェアの詳細情報を参照するには、スパイウェア/グレーウェアの名前をクリックします。新しい Web ブラウザページが開き、トレンドマイクロ Web サイトに掲載されているそのスパイウェア/グレーウェアの関連情報が表示されます。
機械学習型検索	機械学習型検索ポリシー違反のあったプログラムの上位 5 件
	機械学習型検索ポリシー違反のあったコンピュータの上位 10 件
Web レピュテーション	Web レピュテーションポリシー違反のあったコンピュータの上位 10 件
URL フィルタ	違反した URL カテゴリポリシーの上位 5 件 最も頻繁にアクセスされたポリシー違反 Web サイトカテゴリのリストです。
	URL カテゴリポリシー違反のあったコンピュータの上位 10 件
挙動監視	挙動監視ポリシー違反のあったプログラムの上位 5 件
	挙動監視ポリシー違反のあったコンピュータの上位 10 件

レポート項目	説明
デバイスコントロール	デバイスコントロールポリシー違反のあったコンピュータの上位 10 件
ネットワークウイルス	検出されたネットワークウイルスの上位 10 件 ファイアウォールドライバによって検出されたネットワークウイルスの中で頻度の多い上位 10 件のリストです。 ウイルスの名前をクリックすると、新しい Web ブラウザページが開いてトレンドマイクロのウイルス情報ページが表示され、そのウイルスの詳細情報を読むことができます。
	攻撃されたコンピュータ上位 10 件 ネットワーク上のクライアントのうち、報告されたウイルスの検出数が多かった上位 10 件のリストです。

レポートとログの管理タスクを実行する

手順

1. [レポート] > [管理] に移動します。
2. 次のタスクを実行します。

タスク	手順
レポートとテンプレートの最大数の設定	1 回限りのレポート、予約レポート (テンプレートごと)、およびビジネスセキュリティサーバで使用可能なテンプレートの数を制限できます。その数を超過すると、ビジネスセキュリティサーバではレポートまたはテンプレートが保持期間の長いものから削除されます。 a. [レポート] タブをクリックします。 b. 保持する 1 回限りのレポート、予約レポート、およびレポートテンプレートの最大数を入力します。
ログの自動削除の設定	a. [ログの自動削除] タブをクリックします。 b. ログの種類を選択し、ログの最長保持期間を指定します。この期間を超えるログは削除されます。

タスク	手順
ログの手動削除	a. [ログの手動削除] タブをクリックします。 b. ログの各種類について、最長保持期間を入力します。この期間を超えるログは削除されます。すべてのログを削除するには、「0」を入力します。 c. [削除] をクリックします。

3. [保存] をクリックします。

第 12 章

管理タスクの実行

本章では、製品ライセンスの表示、プラグインマネージャの操作、ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) サーバのアンインストールなどの管理タスクの実行方法について説明します。

Web コンソールのパスワードを変更する

Web コンソールのパスワードには、複雑なパスワードを使用することをお勧めします。複雑なパスワードとは、1 つ以上の大文字 (A〜Z)、1 つ以上の小文字 (a〜z)、1 つ以上の数字 (0〜9)、および 1 つ以上の特殊記号または句読点 (!@#$%^&,.:;?) を含む 8 文字以上のパスワードです。このパスワードには、ユーザのログイン名と同じものではなく、パスワードそのものにログイン名が含まれていないことも要求されます。また、ユーザの姓名や生年月日など、ユーザを簡単に特定できるような項目を含めることもできません。

手順

1. [管理] > [パスワード設定] に移動します。
2. 指示に従って下記の項目を入力します。
   - 現在のパスワード
   - 新しいパスワード
   - パスワードの確認: 確認のために、新しいパスワードをもう一度入力します。
3. [保存] をクリックします。

プラグインマネージャを使用する

プラグインマネージャは、ビジネスセキュリティサーバとエージェントの 両方のプログラムが利用可能になった場合に、ただちにプログラムを Web コンソールに表示するための機能です。これらのプログラムのインストールと管理は Web コンソールから実行できます。たとえば、クライアント用プラグインプログラムをエージェントにインストールできます。[管理] > [プラグインマネージャ] から、プラグインマネージャをダウンロードしてインストールします。インストールが完了すると、利用可能なプラグインプログラムの確認ができるようになります。詳細については、プラグインマネージャおよびプラグインプログラムのドキュメントを参照してください。

製品ライセンスを管理する

[ライセンス] 画面では、サポート契約の更新、アップグレード、および詳細情報の表示を実行できます。

[ライセンス] 画面には、ライセンスの詳細情報が表示されます。インストール時に選択したオプションによって、ライセンスは製品版または体験版のいずれかになります。どちらの場合でも、サポート契約を結ぶことができます。サポート契約の期間が終了すると、ネットワーク上のクライアントは非常に限られた方法でしか保護されません。[ライセンス] 画面でサポート契約の期限を確認し、失効前にサポート契約を更新してください。

注意

トレンドマイクロ製品の各種コンポーネントに対するライセンスは、地域によって異なります。インストール完了後、ご使用のレジストレーションキー/アクティベーションコードで利用可能なコンポーネントの概要を参照できます。ライセンスされているコンポーネントについて確認するには、トレンドマイクロの営業部または販売代理店にお問い合わせください。

ライセンスの更新

製品版のビジネスセキュリティ に更新またはアップグレードするには、サポート契約を購入する必要があります。製品版にはアクティベーションコードが必要です。

製品ライセンスを更新する方法は 2 つあります。

- Web コンソールの [最新ステータス] 画面に移動して、表示される指示に従います。この指示は、ライセンスの有効期限が終了する前の 60 日間と、終了した後の 30 日間表示されます。
- 更新手続きの詳細について、トレンドマイクロの営業部または販売代理店に問い合わせます。

  販売代理店では、ビジネスセキュリティサーバ 上のファイルに連絡先情報を保存しておくことができます。次の場所でファイルを確認してください。

  ```
  {ビジネスセキュリティサーバのインストールフォルダ }¥PCCSRV¥Private
  ¥contact_info.ini
  ```

注意

{ビジネスセキュリティサーバのインストールフォルダ }は通常、C:¥Program Files¥Trend Micro¥Security Server です。

いずれかの方法で手続きを終えると、トレンドマイクロ担当者が、Trend Micro Product Registration を使用して登録情報をアップデートします。

ビジネスセキュリティサーバが 製品登録サーバへポーリングして、新しい有効期限を直接製品登録サーバから受信します。ライセンスを更新するときに、新しいアクティベーションコードを手入力する必要はありません。

新しいライセンスをアクティベートする

ライセンスの種類によってビジネスセキュリティ のアクティベーションコードは異なります。

表 12-1. ライセンスの種類とアクティベーションコード

ライセンスの種類	アクティベーションコード
製品版のビジネスセキュリティ	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

注意

アクティベーションコードをお持ちでない場合は、弊社営業担当者にお問い合わせください。

http://tmqa.jp/biz10_buy

ライセンスの種類を変更する場合は、[ライセンス] 画面を使用して新しいアクティベーションコードを入力してください。

1. [管理] > [ライセンス] に移動します。
2. [新規入力]をクリックします。
3. 新しい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。

修正プログラムの適用設定をする

ビジネスセキュリティ に自動的に修正プログラムを適用するように設定します。

手順

1. [管理] > [修正プログラム] に移動します。

   [設定] タブが表示されます。

2. [修正プログラム適用の設定] で、[修正プログラムのダウンロードを有効にする] を選択します。

3. 新しい修正プログラムが利用可能になったときに実行する処理を指定します。

   - ダウンロード: 設定したスケジュールに従って、修正プログラムをダウンロードフォルダに自動的にダウンロードします。
   - ダウンロードして適用: 設定したスケジュールに従って、修正プログラムを自動的にダウンロードして適用します。

4. 処理を実行するスケジュールを指定します。

   注意

   適用が完了してビジネスセキュリティサーバが再起動されるまでに、少し時間がかかることがあります。修正プログラムの適用は、影響が最も少ない時間に実行するようにしてください。

5. [保存] をクリックします。

修正プログラムの通知設定を設定する

修正プログラムが公開された際に、管理者および指定したユーザへ通知するようにウイルスバスター ビジネスセキュリティを設定します。新しい修正プログラムが利用可能になると、管理者および指定したユーザはセキュリティエージェントのポップアップ、またはメールで通知を受け取ります。

- セキュリティエージェント — OS の通知領域付近に通知が表示されます。

- メール

手順

1. [管理] > [修正プログラム] に移動します。
2. [通知] をクリックします。
3. セキュリティエージェントからポップアップ通知を受け取るには、[セキュリティエージェント通知] で設定します。
   a. [追加] をクリックします。
   b. リストからセキュリティエージェントを選択します。

      ヒント
      隣接する複数のセキュリティエージェントを選択するには、選択範囲内の最初のエージェントをクリックして、<Shift> キーを押しながら選択範囲内の最後のエージェントをクリックします。隣接していないセキュリティエージェントの範囲を選択するには、選択範囲内の最初のセキュリティエージェントをクリックして、<Ctrl> キーを押しながら選択するセキュリティエージェントをクリックします。

   c. [保存] をクリックします。
4. 修正プログラムに関する通知をメールで受け取るには、[メール通知] で受信者を指定します。

   注意
   メール通知を受け取るには、[管理] > [グローバル設定] の [SMTP] タブで設定を行う必要があります。

5. [保存] をクリックします。

スマートフィードバックプログラムに参加する

スマートフィードバックの詳細については、4 ページの「スマートフィードバック」を参照してください。

手順

1. [管理] > [Smart Protection Network] に移動します。
2. [トレンドマイクロスマートフィードバックを 有効にする] をクリックします。
3. クライアントコンピュータ 上にあるファイルの潜在的なセキュリティ 上の脅威に関する情報を送信するには、[不審なプログラムファイルのフィードバックを有効にする] チェックボックスをオンにします。

   注意

   スマートフィードバックに送信されるファイルにはユーザデータは含まれず、脅威の解析の目的のみに送信されます。

4. 所属の組織をトレンドマイクロで判別するのを容易にするために、[業種] で種類を選択します。
5. [保存] をクリックします。

エージェントのインタフェース言語を変更する

初期設定では、エージェントのインタフェースで 使用される言語は、クライアントの OS 上で設定されている地域に対応します。エージェントのインタフェース 言語は変更できます。

プログラム設定の保存と復元

ビジネスセキュリティサーバをロールバックできるように、ビジネスセキュリティサーバデータベースと重要な設定ファイルのコピーを保存できます。以前の設定の復元が必要になるのは、問題が発生したためにビジネスセキュリティサーバを再インストールする場合や、直前の設定に戻す必要が生じた場合です。

手順

1. ビジネスセキュリティサーバの「Trend Micro Security Server Master Service」を停止します。
2. 以下のファイルおよびフォルダを、別の場所に手動でコピーします。

警告!

この作業にバックアップ用のツールやアプリケーションを使用しないでください。

<ビジネスセキュリティサーバのインストールパス >¥PCCSRV

- ofcscan.ini ―グローバル設定を含んでいます。
- ous.ini ―ウイルス対策コンポーネントインストールのアップデート元のテーブルを含んでいます。
- Private フォルダ ―ファイアウォールおよびアップデート元の設定を含んでいます。
- Pccnt¥Common¥OfcPfw.dat ―ファイアウォールの設定を含んでいます。
- Download¥OfcPfw.dat ―ファイアウォールインストール設定を含んでいます。
- Log フォルダ ―システムイベントおよび接続状態の確認ログを含んでいます。
- Virus フォルダ ―ビジネスセキュリティによって感染ファイルが隔離されるフォルダです。

- HTTPDB フォルダ ―ビジネスセキュリティデータベースを 含んでいます。

3. ビジネスセキュリティサーバをアンインストールします 。222 ページの「ビジネスセキュリティサーバをアンインストールする 」を参照してください。
4. 新規インストールを実行します。『ビジネスセキュリティ インストールガイド』を参照してください。
5. セットアッププログラムが完了したら、復元先コンピュータ上の「Trend Micro Security Server Master Service」を停止します。
6. バックアップファイルに記載されているウイルスパターンファイルのバージョンを更新します。
   a. 再インストール後のサーバから現在のウイルスパターンファイルのバージョンを確認します。

      <ビジネスセキュリティサーバのインストールパス >¥PCCSRV¥Private ¥component.ini.[6101]

      ComponentName==ウイルスパターンファイル

      Version=xxxxxx 0 0

   b. バックアップファイル内のウイルスパターンファイルのバージョンをアップデートします。

      ¥Private¥component.ini

      注意

      ビジネスセキュリティサーバのインストール 先を変更している場合、バックアップファイルの ofcscan.ini と¥private ¥ofcserver.ini のパス情報を更新する必要があります。
7. 作成したバックアップを使用して、ビジネスセキュリティ データベースと対象コンピュータ上の PCCSRV フォルダ内の関連ファイルと関連フォルダを上書きします。
8. Trend Micro Security Server Master Service を再起動します。

ビジネスセキュリティサーバをアンインストールする

ビジネスセキュリティサーバをアンインストールすると 、スキャンサーバもアンインストールされます。

ビジネスセキュリティ では、ビジネスセキュリティサーバを 安全にコンピュータから削除するためのアンインストールプログラムが 用意されています。ビジネスセキュリティサーバを 削除する前に、すべてのクライアントからエージェントを削除してください。

ビジネスセキュリティサーバをアンインストールしても 、エージェントはアンインストールされません。ビジネスセキュリティサーバをアンインストールする前に、すべてのエージェントをアンインストールするか 他のビジネスセキュリティサーバに移動する必要があります。58 ページの「エージェントを削除する」を参照してください。

手順

1. サーバのインストールに使用したコンピュータで [スタート] > [コントロール パネル] > [プログラムの追加と削除] または [プログラムと機能] の順にクリックします。
2. ビジネスセキュリティ を選択して [変更と削除] または [アンインストール] をクリックします。

   確認画面が表示されます。
3. [次へ] をクリックします。

   サーバのアンインストールプログラムから 、管理者パスワードを入力するよう求められます。
4. テキストボックスに管理者パスワードを入力し、[次へ] をクリックします。

   サーバファイルの削除が開始されます。ビジネスセキュリティサーバのアンインストールが完了すると、確認メッセージが表示されます。
5. [OK] をクリックしてアンインストールプログラムを 終了します。

第 13 章

管理ツールの使用

本章では、管理ツール、クライアントツール、およびアドインを使用する方法について説明します。

ツールの種類

ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) には、サーバの設定やクライアントの管理など、さまざまな操作を簡単に実行できるようにするためのツールがあります。

注意

管理ツールおよびクライアントツールは Web コンソールから起動できません。アドインは Web コンソールからダウンロードできます。

ツールの使用方法については、次の関連するセクションを参照してください。

これらのツールは、次の 3 種類に分類されます。

- 管理ツール
  - ログオンスクリプトウィザード (SetupUsr.exe) — セキュリティエージェントのインストールを自動化します。33 ページの「ログオンスクリプトウィザードによるインストール」を参照してください。
  - 脆弱性検索ツール (TMVS.exe) — ネットワーク上の保護されていないコンピュータを特定します。43 ページの「脆弱性検索ツールを使用したインストール」を参照してください。
  - Trend Micro Disk Cleaner — 不要なビジネスセキュリティのバックアップファイル、ログファイル、および使用していないパターンファイルを削除します。225 ページの「ディスク容量を節約する」を参照してください。
  - スキャンサーバ (検索サーバ) データベース移動ツール — スキャンサーバのデータベースを安全に別のディスクドライブに移動します。228 ページの「スキャンサーバデータベースを移動する」を参照してください。
- クライアントツール
  - Client Packager (ClnPack.exe) — セキュリティエージェントとコンポーネントを含む自己解凍ファイルを作成します。35 ページの「Client Packager を使用したインストール」を参照してください。

- 感染ファイル暗号化処理の復元ツール (VSEncode.exe) — ビジネスセキュリティにより暗号化された感染ファイルを開きます。228 ページの「感染ファイル暗号化処理の復元」を参照してください。
- セキュリティエージェント ID の再生成ツール (regenid.exe) — ReGenID ユーティリティは、セキュリティエージェントが複製されたコンピュータか仮想マシンかに応じて、セキュリティエージェントの ClientID を再生成するために使用します。230 ページの「ReGenID ツールを使用する」を参照してください。

- アドイン — 管理者がサポートされる Windows OS のコンソールで、最新のセキュリティ情報とシステム情報を表示できるようにします。これらは [最新ステータス] 画面に表示されるのと同様の高いレベルの情報です。231 ページの「SBS アドインと EBS アドインを管理する」を参照してください。

注意

旧バージョンのビジネスセキュリティに付属するツールの中には、このバージョンでは利用できないものがあります。これらのツールが必要な場合は、サポート担当者にお問い合わせください。

ディスク容量を節約する

Disk Cleaner を実行して、ビジネスセキュリティサーバとクライアントのディスク容量を節約します。

ビジネスセキュリティサーバで Disk Cleaner を実行する

始める前に

Disk Cleaner ツール (TMDiskCleaner.exe) は、次のディレクトリで、使用していないバックアップ、ログ、およびパターンファイルを識別して削除し、空きディスク容量を増やします。

- {セキュリティエージェント}¥AU_Data¥AU_Temp¥*
- {セキュリティエージェント}¥Reserve
- {ビジネスセキュリティサーバ}¥PCCSRV¥TEMP¥* (隠しファイルを除きます)

- {ビジネスセキュリティサーバ}¥PCCSRV¥Web¥Service¥AU_Data¥AU_Temp¥*
- {ビジネスセキュリティサーバ}¥PCCSRV¥wss¥*.log
- {ビジネスセキュリティサーバ}¥PCCSRV¥wss¥AU_Data¥AU_Temp¥*
- {ビジネスセキュリティサーバ}¥PCCSRV¥Backup¥*
- {ビジネスセキュリティサーバ}¥PCCSRV¥Virus¥* (2 週間以上経過した隔離済みファイルを削除します。ただし NOTVIRUS ファイルは除きます)
- {ビジネスセキュリティサーバ}¥PCCSRV¥ssaptpn.xxx (最新のパターンファイルのみを保持します)
- {ビジネスセキュリティサーバ}¥PCCSRV¥lpt$vpn.xxx (最新の 3 つパターンファイルのみを保持します)
- {ビジネスセキュリティサーバ}¥PCCSRV¥icrc$oth.xxx (最新の 3 つパターンファイルのみを保持します)
- {ビジネスセキュリティサーバ}¥DBBackup¥* (最新の 2 つのサブフォルダのみを保持します)

手順

1. ビジネスセキュリティサーバで、次のディレクトリに移動します。

   {サーバのインストールフォルダ}¥PCCSRV¥Admin¥Utility¥

2. TMDiskCleaner.exe をダブルクリックします。

   Trend Micro Worry-Free Business Security Disk Cleaner が表示されます。

   注意

   ファイルは復元できません。

3. [Delete Files] をクリックして、使用していないバックアップ、ログ、およびパターンファイルの検索と削除を実行します。

コマンドラインインタフェースを使用してビジネスセキュリティサーバで Disk Cleaner を実行する

手順

1. ビジネスセキュリティサーバで、コマンドプロンプトウィンドウを開きます。
2. コマンドプロンプトで次のコマンドを実行します。

   ```
   TMDiskCleaner.exe [/hide] [/log] [/allowundo]
   ```

   - `/hide`:ツールをバックグラウンドプロセスとして実行します。
   - `/log`:処理のログを DiskClean.log として現在のフォルダに保存します。

     注意

     `/log` は、`/hide` の使用時のみ使用可能になります。

   - `/allowundo`:ファイルをごみ箱に移動します。完全な削除は行いません。
3. Disk Cleaner ツールを頻繁に実行するには、Windows のスケジュールタスクを使用して新しいタスクを設定します。詳細については、Windows のドキュメントを参照してください。

クライアントのディスク容量を節約する

クライアントのディスク容量を節約するには、セキュリティエージェントがインストールされているデスクトップ/サーバ上で次の操作を行います。

- 隔離ファイルを削除します。
- ログファイルを削除します。
- Windows のディスククリーンナップユーティリティを 実行します。

スキャンサーバデータベースを移動する

スキャンサーバがインストールされているディスクドライブのディスク 容量が不十分な場合、Scan Server Database Mover ツールを使用してスキャンサーバデータベースを他のディスクドライブに安全に移動できます。

ビジネスセキュリティサーバコンピュータに 複数のディスクドライブがあり、新しいディスクドライブに 3 GB 以上の使用可能ディスク領域があることを確認してください。マップ済みのドライブは使用できません。データベースを手動で移動したり、他のツールを使用して移動したりしないでください。

手順

1. ビジネスセキュリティサーバコンピュータで、<ビジネスセキュリティサーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility に移動します。
2. ScanServerDBMover.exe を起動します。
3. [変更] をクリックします。
4. [参照] をクリックして、他のディスクドライブの 移動先ディレクトリを参照します。
5. [OK] をクリックし、データベースが移動されたら [完了] をクリックします。

感染ファイル暗号化処理の復元

感染ファイルが開かれないようにするために、ビジネスセキュリティ では、次の時点でファイルが暗号化されます。

- ファイルを隔離する前
- 駆除を実行する前のファイルをバックアップするとき

ビジネスセキュリティ では、ファイルから情報を取得する必要がある場合に、そのファイルを復号し、復元できるツールが提供されています。ビジネスセキュリティ では、次のファイルを復号および復元できます。

表 13-1. ビジネスセキュリティで復号および復元可能なファイル

ファイル	説明
クライアントで隔離されたファイル	このファイルは次のディレクトリにあります。 • <セキュリティエージェントのインストールフォルダ >¥SUSPECT¥Backup または<セキュリティエージェントのインストールフォルダ >¥quarantine このファイルは、指定された隔離ディレクトリ (通常はビジネスセキュリティサーバのディレクトリ) にアップロードされます。
指定された隔離ディレクトリの隔離されたファイル	初期設定では、このディレクトリはビジネスセキュリティサーバコンピュータに配置されます (<ビジネスセキュリティサーバのインストールフォルダ >¥PCCSRV¥Virus)。このディレクトリを変更するには、[管理] > [グローバル設定] > [システム] タブの [隔離フォルダ設定] に移動します。
バックアップされた暗号化ファイル	このファイルは、エージェントで駆除可能な、感染ファイルのバックアップです。これらのファイルは次のフォルダにあります。 • <セキュリティエージェントのインストールフォルダ >¥Backup これらのファイルを復元するには、ユーザがクライアントの隔離ディレクトリに移動する必要があります。

警告!

感染したファイルを復元すると、他のファイルやクライアントにウイルス /不正プログラムの感染が拡大するおそれがあります。ファイルを復元する前に、感染したクライアントを分離し、このクライアントの重要なファイルをバックアップ場所に移動してください。

セキュリティエージェントでファイルを復号および復元する

手順

1. コマンドプロンプトを開き、<セキュリティエージェントのインストールフォルダ> に移動します。

2. 次のように入力して VSEncode.exe を実行します。

   ```
   VSEncode.exe /u
   ```

   このパラメータは、<セキュリティエージェントのインストールフォルダ>¥SUSPECT¥Backup にあるファイルのリストを表示する画面を開きます。

   管理者は [スパイウェア/グレーウェア] タブで、スパイウェア/グレーウェアに分類されたファイルを復元できます。画面には、<セキュリティエージェントのインストールフォルダ>¥BackupAS にあるファイルのリストが表示されます。

3. 復元するファイルを選択して、[復元] をクリックします。

   注意
   このツールで一度に復元できるファイルは 1 つのみです。

4. 開いた画面で、ファイルを復元するフォルダを指定します。

5. [OK] をクリックします。

   注意
   エージェントでファイルが再度検索され、ファイルを復元したすぐ後に感染しているとして処理される場合があります。このファイルが検索されることを防ぐため、検索除外リストに追加してください。

   124 ページの「セキュリティエージェントの 検索対象と処理」を参照してください。

   ファイルが復元され、指定したフォルダに保存されます。

6. [閉じる] をクリックします。

ReGenID ツールを使用する

セキュリティエージェントのインストールにはそれぞれ、固有のグローバル一意識別子 (GUID) を与える必要があり、これによりビジネスセキュリティサーバはエージェントを個別に識別できます。GUID の重複は、多くの場合、クライアントの複製や、仮想化コンピュータによって発生します。

複数のエージェントが同じ GUID をレポートする場合は、ReGenID ツールを実行して、各クライアントに一意の GUID を生成してください。

手順

1. ビジネスセキュリティサーバで、次のディレクトリに移動します。<サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility
2. セキュリティエージェントがインストールされたクライアントの 一時フォルダに WFBS_WIN_All_ReGenID.exe をコピーします。

   例: C:¥temp
3. WFBS_WIN_All_ReGenID.exe をダブルクリックして画面上の指示に従います。

   セキュリティエージェントが停止し、クライアント GUID が削除されます。
4. セキュリティエージェントを再起動します。

   セキュリティエージェントで、新しいクライアント GUID が生成されます。

SBS アドインと EBS アドインを管理する

ビジネスセキュリティでは、管理者が次の Windows OS のコンソールで、最新のセキュリティとエージェントのステータス情報を表示できるアドインを用意しています。

- Windows Small Business Server (SBS) 2008
- Windows Essential Business (EBS) Server 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

SBS アドインと EBS アドインを手動でインストールする

サポートされている OS を実行しているエンドポイントにビジネスセキュリティサーバをインストールするときは、SBS または EBS アドインが自動的に

インストールされます。サポートされている OS を実行している別のエンドポイントでアドインを使用するには、アドインを手動でインストールする必要があります。

手順

1. ビジネスセキュリティサーバの Web コンソールにログオンします。
2. [管理] > [ツール]に移動します。
3. [アドイン] をクリックします。
4. 対応する [ダウンロード] リンクをクリックしてインストーラを取得します。
5. インストーラを対象エンドポイントにコピーして起動します。

SBS アドインまたは EBS アドインの使用

手順

1. SBS または EBS のコンソールを開きます。
2. [セキュリティ] タブで、[ウイルスバスター ビジネスセキュリティ] をクリックします。ステータス情報が表示されます。

付録 A

セキュリティエージェントのアイコン

本章では、エージェント上に表示されるさまざまなセキュリティエージェントのアイコンについて説明します。

セキュリティエージェントのステータスを確認する

次の画像はセキュリティエージェントのコンソールです。

次の表は、セキュリティエージェントコンソールのメインユーザインタフェースに表示されるアイコンとその意味を示しています。

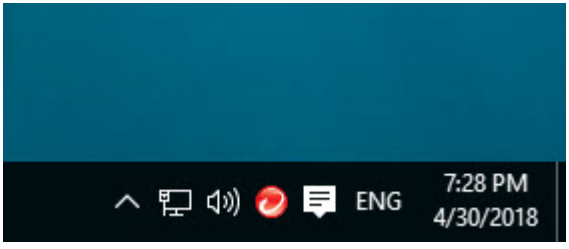
表 A-1. セキュリティエージェントコンソールのメインユーザインタフェースのアイコン

アイコン	ステータス	説明と処理
	保護が有効— 保護された状態であり、ソフトウェアは最新です	ソフトウェアは最新であり適切に実行されています。処理は必要ありません。
	コンピュータの再起動 — コンピュータを再起動してセキュリティ上の脅威の解決を完了してください	脅威によっては処理を完了するためにコンピュータの再起動が必要になる場合があります。 コンピュータを再起動してこれらの脅威の解決を完了してください。
	危険な状態— 管理者にお問い合わせください	リアルタイム検索が無効になっているか、それとは別の理由で危険な状態になっています。 リアルタイム検索を有効にします。有効にしても問題が解決しない場合は、サポート担当者にお問い合わせください。
	今すぐアップデート— アップデートを (数値) 日間受信していません (従来型スキャンの場合)	ウイルスパターンファイルが 3 日間以上アップデートされていません。 セキュリティエージェントをすぐにアップデートしてください。
	スマートスキャン使用不可— インターネット接続を確認してください	セキュリティエージェントが、スキャンサーバに 15 分以上アクセスしていません。 最新のパターンファイルで検索するために、ネットワークに接続していることを確認してください。

アイコン	ステータス	説明と処理
	コンピュータの再起動 – コンピュータを再起動してアップデートのインストールを完了してください	コンポーネントのアップデート処理を完了するためにコンピュータの再起動が必要になる場合があります。コンピュータを再起動してアップデートを完了してください。
	プログラムのアップデート –セキュリティエージェントプログラムをアップデートしています	アップデートが進行中です。完了するまでネットワークから切断しないでください。

Windows のタスクバーでセキュリティエージェントアイコンを確認する

次のセキュリティエージェントアイコンが Windows タスクバーに表示されます:

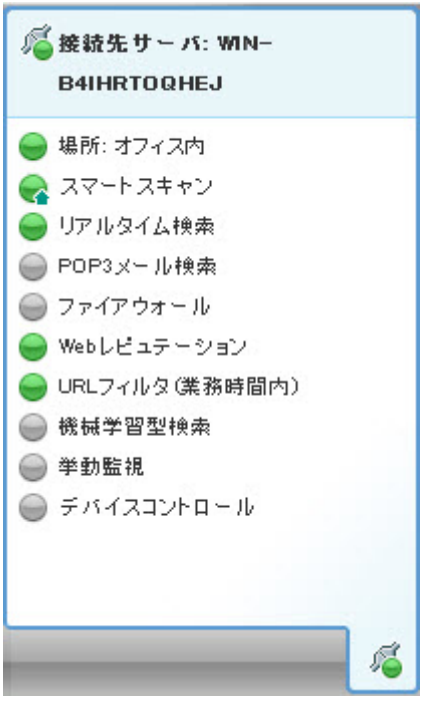


アイコン	意味
	ステータスは正常です。
	(アニメーションで表示) 手動検索または予約検索を実行中です。セキュリティエージェントは従来型スキャンまたはスマートスキャンを使用しています。
	セキュリティエージェントはアップデートを実行中です。

アイコン	意味
	処理が必要です。 • リアルタイム検索が無効です • 不正プログラムを駆除するために再起動が必要です • エンジンがアップデートされたため再起動が必要です • ランサムウェアによって暗号化されたファイルを復元するため再起動が必要です • アップデートが必要です  注意 セキュリティエージェントのメインコンソールを開いて、必要な処理を確認してください。

コンソールのフライオーバーにアクセスする

セキュリティエージェント コンソールの右下にある小さなアイコン上にマウスポインタを重ねると、セキュリティエージェント コンソールのフライオーバーが開きます。



次の表は、コンソールのフライオーバーアイコンとその 意味を示しています。

表 A-2. コンソールのフライオーバーアイコン

機能	アイコン	意味
接続		ビジネスセキュリティサーバに接続されています。
		ビジネスセキュリティサーバには接続されていませんが、リアルタイム検索は引き続き実行されています。パターンファイルが最新でない可能性があります。Windows タスクバーでエージェントアイコンを右クリックし、[今すぐアップデート] をクリックします。

機能	アイコン	意味
場所		オフィス内 (内部ネットワーク)
		オフィス外 (外部ネットワーク)
リアルタイム検索		オン
		オフ
POP3 メール検索		オン
		オフ
スマートスキャン		グローバルスマートスキャンサーバに接続されています。
		スキャンサーバまたはグローバルスマートスキャンサーバに接続できません。
		スマートスキャンが無効です。従来型スキャンを使用しています。
• ファイアウォール • Web レピュテーション • URL フィルタ • 挙動監視 • デバイスコントロール • 機械学習型検索		オン
		オフ

付録 B

ビジネスセキュリティの IPv6 のサポート

本付録は、ビジネスセキュリティを IPv6 アドレス指定をサポートする環境にインストールするユーザにお読みいただく必要があります。本付録では、ビジネスセキュリティでの IPv6 のサポートに関する情報をのみを提供します。

IPv6 の概念、および IPv6 アドレス指定をサポートするネットワークの設定作業に詳しいユーザを対象読者としています。

ビジネスセキュリティの IPv6 のサポート

ビジネスセキュリティでは、バージョン 9.0 以降、IPv6 がサポートされています。それより前のビジネスセキュリティでは、IPv6 アドレス指定はサポートされません。IPv6 のサポートは、IPv6 の要件を満たすビジネスセキュリティサーバ、セキュリティエージェントのインストールまたはアップグレード後に自動的に有効になります。

ビジネスセキュリティサーバの IPv6 の要件

ビジネスセキュリティサーバの IPv6 の要件は次のとおりです。

- IPv4 エージェントと IPv6 エージェントを管理する場合は、サーバに IPv4 アドレスと IPv6 アドレスの両方を指定して、サーバをホスト名で識別する必要があります。サーバが IPv4 アドレスで識別されている場合、IPv6 シングルスタックエージェントはサーバに 接続できません。IPv4 シングルスタッククライアントが IPv6 アドレスで識別されているサーバに接続する場合にも、同様の問題が発生します。
- サーバが IPv6 エージェントのみを管理する場合は、IPv6 アドレスを使用することが最低要件となります。サーバはホスト名または IPv6 アドレスで識別できます。サーバがホスト名で識別されている場合は、完全修飾ドメイン名 (FQDN) を使用することをお勧めします。これは、IPv6 シングルスタック環境では、WINS サーバがホスト名を対応する IPv6 アドレスに変換できないためです。
- `ping` や `nslookup` コマンドなどを使用して、ホストマシンの IPv6 または IPv4 アドレスを取得できることを確認します。
- ビジネスセキュリティサーバを IPv6 シングルスタックコンピュータにインストールする場合は、IPv4 アドレスと IPv6 アドレスを変換できる DeleGate などのデュアルスタックプロキシサーバを 設定します。プロキシサーバをビジネスセキュリティサーバとインターネットの 間に設置して、トレンドマイクロがホストするサービス (たとえばアップデートサーバ、オンライン登録 Web サイト、Trend Micro Smart Protection Network など) にサーバが正常に接続できるようにします。

IPv6 シングルスタックサーバの制限事項

次の表は、IPv6 アドレスのみ指定されているビジネスセキュリティサーバの制限事項を示しています。

表 B-1. IPv6 シングルスタックサーバの制限事項

項目	制限事項
エージェントの管理	IPv6 シングルスタックサーバでは、次を実行できません。 • IPv4 シングルスタッククライアントへのエージェントのインストール • IPv4 シングルスタックのエージェントの管理
アップデートおよび集中管理	IPv6 シングルスタックサーバは、IPv4 シングルスタックの次のアップデート元からはアップデートできません。 • トレンドマイクロのアップデートサーバ • IPv4 シングルスタックのその他のアップデート元
製品登録、アクティベーション、および更新	IPv6 シングルスタックサーバは、トレンドマイクロのオンライン登録サーバに接続できないので、製品の登録、ライセンスの取得、およびライセンスのアクティベートや更新はできません。
プロキシ接続	IPv6 シングルスタックサーバは、IPv4 シングルスタックのプロキシサーバを介して接続できません。
プラグインソリューション	IPv6 シングルスタックサーバにはプラグインマネージャがありますが、次の場所にプラグインソリューションをインストールすることはできません。 • IPv4 シングルスタックエージェントまたは IPv4 シングルスタックホスト (直接接続できないため) • IPv6 シングルスタックエージェントまたは IPv6 シングルスタックホスト (IPv6 をサポートするプラグインソリューションがないため)

これらの制限事項の多くは、IPv4 アドレスと IPv6 アドレスを変換できる DeleGate などのデュアルスタックプロキシサーバを 設定することで回避できます。プロキシサーバは、ビジネスセキュリティサーバと 、接続先またはサービスの提供先との間に設置します。

IPv6 シングルスタックエージェントの制限事項

次の表は、IPv6 アドレスのみ指定されているセキュリティエージェント の制限事項を示しています。

表 B-2. IPv6 シングルスタックエージェントの制限事項

項目	制限事項
上位ビジネスセキュリティサーバ	IPv6 シングルスタックエージェントは、IPv4 シングルスタックのビジネスセキュリティサーバでは管理できません。
アップデート	IPv6 シングルスタックエージェントは、IPv4 シングルスタックの次のアップデート元からはアップデートできません。 • トレンドマイクロのアップデートサーバ • IPv4 シングルスタックのビジネスセキュリティサーバ • IPv4 シングルスタックのアップデートエージェント • IPv4 シングルスタックのその他のアップデート元
検索クエリおよびスマートフィードバック	IPv6 シングルスタックのセキュリティエージェントは Trend Micro Smart Protection Network にクエリを送信できないので、スマートフィードバックは使用できません。
プラグインソリューション	IPv6 をサポートするプラグインソリューションがないため、IPv6 シングルスタックエージェントにはプラグインソリューションをインストールできません。
プロキシ接続	IPv6 シングルスタックセキュリティエージェントは、IPv4 シングルスタックのプロキシサーバを介して接続できません。

これらの制限事項の多くは、IPv4 アドレスと IPv6 アドレスを変換できる DeleGate などのデュアルスタックプロキシサーバを 設定することで回避できます。プロキシサーバは、セキュリティエージェント と接続先との間に設置します。

IPv6 アドレスを設定する

Web コンソールを使用して、IPv6 アドレスまたは IPv6 のアドレス範囲を設定できます。設定のガイドラインを次にいくつか示します。

- ビジネスセキュリティ では、標準の IPv6 アドレス表記がサポートされます。

  例を以下に示します。

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- ビジネスセキュリティでは、次の例に示すようなリンクローカルの IPv6 アドレスもサポートされます。

```
fe80::210:5aff:feaa:20a2
```

警告!

ビジネスセキュリティではリンクローカルの IPv6 アドレスがサポートされますが、状況によっては予期したとおりに動作しない場合もあるため、リンクローカルの IPv6 アドレスを指定する際には注意が必要です。たとえば、アップデート元が別のネットワークセグメント上にあり、それがリンクローカルの IPv6 アドレスで識別される場合、セキュリティエージェントではそのアップデート元からアップデートできません。

- IPv6 アドレスが URL の一部である場合は、アドレスを角カッコ ([]) で囲みます。
- IPv6 のアドレス範囲では、通常、プレフィックス長を入力する必要があります。サーバで IP アドレスのクエリを実行する必要のある設定では、サーバが大量の IP アドレスについてクエリを実行する際に発生する可能性のあるパフォーマンス上の問題を回避するため、プレフィックス長の制限が適用されます。たとえば、外部サーバ管理機能の場合、プレフィックスの長さは 112 (65,536 個の IP アドレス) から 128 (2 個の IP アドレス) でなければなりません。
- IPv6 アドレスまたはアドレス範囲に関する設定には、セキュリティエージェントに配信されても無視されるものがあります。たとえば、Trend Micro Smart Protection ソースリストを設定しており、IPv6 アドレスで識別された Smart Protection Server がリストに含まれている場合、IPv4 セキュリティエージェントはそのサーバを無視して、他の Trend Micro Smart Protection ソースに接続します。

IP アドレスを表示する画面

ここでは、Web コンソールでの IP アドレスの表示場所を示します。

- セキュリティ設定のグループツリー

  IPv6 シングルスタックエージェントの IPv6 アドレスは、セキュリティ設定のグループツリーの [IP アドレス] 列に表示されます。デュアルスタックエージェントでは、サーバへの登録に IPv6 アドレスを使用した場合、IPv6 アドレスが表示されます。

  注意

  デュアルスタックエージェントがサーバへの 登録に使用する IP アドレスは、[管理] > [グローバル設定] > [デスクトップ/サーバ] タブの [優先される IP アドレス] で設定できます。

  エージェントの設定をファイルにエクスポートすると、エクスポートされたファイルにも IPv6 アドレスが表示されます。

- ログ

  ログにデュアルスタックおよび IPv6 シングルスタックエージェントの IPv6 アドレスが表示されます。

付録 C

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/dcx/s/?language=ja

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/dcx/s/threat?language=ja

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。

付録 D

製品の用語と概念

この付録の各項目は、トレンドマイクロ製品とテクノロジに関する詳細情報を示しています。

Critical Patch

Critical Patch とは、セキュリティ上の問題に対応するもので、すべてのお客さまに対して配信されます。Critical Patch にはセットアッププログラムが含まれます。

HotFix

HotFix とは、お客さま固有の問題に対する修正プログラムです。HotFix は、お客さま固有の問題に対応するものであるため、すべてのお客さまに配布されるものではありません。

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、検索するファイルを特定する方法です。実行可能ファイル (.exe など) では、ファイルの種類はファイルの内容に基づいて判断されます。その他のファイルの種類 (.txt など) は、ファイルのヘッダに基づいて判断されます。

トレンドマイクロの推奨設定には、次の利点があります。

- パフォーマンスの最適化: トレンドマイクロの推奨設定は、最小限のシステムリソースを使用するため、エージェントのアプリケーションには影響しません。
- 検索時間の短縮: 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するため、感染の危険性があるファイルだけが検索されます。そのため、すべてのファイルを検索する場合に比べ、検索時間が大幅に短縮されます。

IntelliTrap

IntelliTrap は、トレンドマイクロ独自のヒューリスティックテクノロジであり、リアルタイム圧縮と、パッカーなどの他の不正プログラムの性質を組み合わせた脅威を検出するのに使用されます。このテクノロジは、ウイルス、不正プログラム、ワーム、トロイの木馬、バックドア、およびボットの検出に使用できます。ウイルス作成者は、通常、さまざまなファイル圧縮スキームを使用して、ウイルスや不正プログラムのフィルタを回避しようとします。IntelliTrap は、ルールとパターンファイルを使用したリアルタイムの検索エンジン技術です。16 種類の一般的な圧縮タイプのいずれかを使用した、最大

17 層の圧縮ファイルに存在する既知のウイルス/不正プログラムを検出し、削除します。

注意

IntelliTrap は、ウイルス検索と同じ検索エンジンを使用します。そのため、IntelliTrap のファイルの扱いおよび検索ルールは、管理者がウイルス検索で定義したものと同じです。

エージェントでは、ボットやその他の不正プログラムの検出が IntelliTrap ログに記録されます。レポートに記録するため、IntelliTrap ログの内容をエクスポートできます。

IntelliTrap は、ボットやその他の不正プログラムを検索する際に、次のコンポーネントを使用します。

- ウイルス検索エンジン
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル

侵入検知システム (IDS)

侵入検知システム (IDS) を使用すると、エンドポイントへの攻撃の手がかりとなるネットワークパケットのパターンを特定できます。

侵入検知システム (IDS) を使用すると、次の既知の侵入を防止できます。

侵入	説明
過大フラグメント (Too Big Fragment)	ハッカーが対象エンドポイントに対して特大サイズの TCP/UDP パケットを送りつけるという DoS (サービス拒否) 攻撃です。これによって、エンドポイントのバッファがオーバーフローするため、エンドポイントがフリーズしたり、再起動したりする可能性があります。

侵入	説明
Ping of Death	ハッカーが対象エンドポイントに対して特大サイズの ICMP/ICMPv6 パケットを送りつけるという DoS (サービス拒否) 攻撃です。これによって、エンドポイントのバッファがオーバーフローになり、エンドポイントがフリーズしたり、再起動したりする可能性があります。
重複 ARP (Conflicted ARP)	ハッカーが対象エンドポイントに、同じ IP アドレスを送信元および送信先アドレスとして指定して、アドレス解決プロトコル (ARP) 要求を送信する攻撃です。侵入対象エンドポイントは自身に ARP 応答 (自身の MAC アドレス) を送信し続けるため、フリーズやクラッシュを招くことになります。
SYN フラッド (Syn Flood)	プログラムから複数の TCP 同期 (SYN) パケットがエンドポイントに送信される、DoS (サービス拒否) 攻撃です。これによって、エンドポイントが同期確認 (SYN/ACK) 応答を送信し続けることになります。そのため、エンドポイントのメモリを著しく消費し、最終的にエンドポイントがクラッシュする可能性があります。
オーバーラッピングフラグメント (Overlapping Fragment Attack)	ティアドロップ攻撃と似ており、オーバーラッピング TCP フラグメントをエンドポイントに送りつける DoS (サービス拒否) 攻撃です。これによって、最初の TCP フラグメントのヘッダ情報が上書きされ、ファイアウォールを通過してしまう場合があります。ファイアウォールはそれ以降の不正コードを含むフラグメントの通過を許可し、フラグメントが侵入対象エンドポイントに到達します。
ティアドロップ (Teardrop)	オーバーラッピングフラグメント攻撃と似ており、IP フラグメントを使用した DoS (サービス拒否) 攻撃です。2 つ目以降の IP フラグメントのオフセット値が混乱することにより、受信側のエンドポイントの OS がフラグメントを組み立て直そうとしたときに、クラッシュする可能性があります。
タイニーフラグメント攻撃 (Tiny Fragment Attack)	小さいサイズの TCP フラグメントが一番目の TCP パケットヘッダー情報を次のフラグメントに押し込む攻撃です。これによって、トラフィックをフィルタリングするルータが、不正なデータが含まれている可能性のある後続のフラグメントを見過ごしてしまう場合があります。
フラグメント化 IGMP (Fragmented IGMP)	フラグメント化 IGMP パケットを送信する DoS (サービス拒否) 攻撃で、対象エンドポイントでは、それらの IGMP パケットを適切に処理することができません。これによって、エンドポイントがフリーズしたり、処理速度が低下したりする可能性があります。

侵入	説明
Land 攻撃 (LAND Attack)	エンドポイントに、送信元と送信先を同じアドレスに指定して IP 同期 (SYN) パケットを送信する攻撃で、エンドポイントは同期確認 (SYN/ACK) 応答を自身に送信することになります。これによって、エンドポイントがフリーズしたり、処理速度が低下したりする可能性があります。

Patch

Patch とは、HotFix と Critical Patch が 1 つにまとめられたもので、複数の問題を解決します。トレンドマイクロは、定期的に Patch を公開しています。Windows 版の Patch にはセットアッププログラムが含まれますが、Windows 版以外の Patch には通常、セットアップスクリプトが用意されています。

検索除外リスト

セキュリティエージェントの検索除外リスト

初期設定で検索から除外されるトレンドマイクロ製品の一覧を以下に示します。

表 D-1. セキュリティエージェントの検索除外リスト

製品名	インストールパスの場所

InterScan eManager 3.5x	`HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥InterScan eManager¥CurrentVersion`
	
	`ProgramDirectory=`

InterScan eManager (InterScan for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	`HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange eManager¥CurrentVersion`
	
	`ProgramDirectory=`

InterScan for Lotus Notes eManager NT	`HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Lotus Notes¥CurrentVersion`
	
	`AppDir=`
	
	`DataDir=`
	
	`IniDir=`

製品名	インストールパスの場所
Interscan Web Security Suite	HKEY_LOCAL_MACHINE¥Software¥TrendMicro¥Interscan Web Security Suite Program Directory= C:¥Program Files¥Trend Micro¥IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥InterScan WebProtect¥CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥ InterScan FTP VirusWall¥CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥ InterScan Web VirusWall¥CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥ InterScan E-Mail VirusWall¥CurrentVersion ProgramDirectory={Installation Drive}:¥INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥ InterScan NSAPI Plug-In¥CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥ InterScan E-Mail VirusWall ¥CurrentVersion ProgramDirectory=
IM Security (IMS)	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥IM Security ¥CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

製品名	インストールパスの場所
InterScan for Microsoft Exchange	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥ScanOption¥Advance QuarantineFolder= HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥IMCScan¥ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥IMCScan¥ScanOption¥Advance QuarantineFolder=

製品名	インストールパスの場所
InterScan for Microsoft Exchange	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥ManualScan¥ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥QuarantineManager QMDir= HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥CurrentVersion¥HomeDir から exclusion.txt ファイルのパスを取得します。

Service Pack

Service Pack とは、HotFix と Patch が統合され、大幅な機能拡張が含まれている修正プログラムで、製品のバージョンアップに相当します。Windows 版および Windows 版以外の Service Pack のどちらにも、セットアッププログラムとセットアップスクリプトが含まれます。

トロイの木馬に脆弱なポート

トロイの木馬に脆弱なポートとは、一般にトロイの木馬プログラムがクライアントへの接続に使用するポートのことです。大規模感染が発生した場合、ビジネスセキュリティではトロイの木馬プログラムが使用する可能性がある次の番号のポートがブロックされます。

表 D-2. トロイの木馬に脆弱なポート

ポート番号	トロイの木馬プログラム	ポート番号	トロイの木馬プログラム
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy

ポート番号	トロイの木馬プログラム	ポート番号	トロイの木馬プログラム
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

駆除できないファイル

ウイルス検索エンジンでは、次のファイルを駆除できません。

表 D-3. 駆除できないファイルの解決策

駆除できないファイル	説明と解決策
トロイの木馬に感染したファイル	トロイの木馬は、メッセージの表示、ファイルの消去、ディスクのフォーマットなど、予期しない、または許可されていない一般に不正な処理を実行するプログラムです。トロイの木馬はファイルに感染しないため駆除は必要はありません。 解決策: ダメージクリーンナップエンジンとダメージクリーンナップテンプレートを使用してトロイの木馬を削除します。
ワームに感染したファイル	ワームは、ワーム自体またはその一部の動作可能なコピーを他のクライアントシステムに拡散できる自己完結型プログラムまたはプログラムのセットです。伝播には通常、ネットワーク接続やメールの添付ファイルが利用されます。ワームはファイルが自己完結型プログラムであるため駆除できません。 解決策:トレンドマイクロではワームを削除することをお勧めします。
書き込み保護された感染ファイル	解決策:ファイルを駆除できるよう書き込み保護を解除します。
パスワード保護されたファイル	パスワード保護されたファイルには、パスワード保護された圧縮ファイルや Microsoft Office ファイルが含まれます。 解決策:ファイルを駆除できるようパスワード保護を解除します。
バックアップファイル	RB0～RB9 のような拡張子を持つファイルは感染ファイルのバックアップコピーです。駆除処理中にウイルス/不正プログラムによってファイルが破壊された場合に備えて、駆除処理では感染ファイルのバックアップを作成します。 解決策:正常に駆除された場合、感染ファイルのバックアップコピーを残しておく必要はありません。クライアントが通常どおり機能している場合は、バックアップファイルを削除してもかまいません。
ごみ箱の感染ファイル	システムが稼働中のため、ごみ箱から感染ファイルを削除できない場合があります。 解決策: 1. クライアントを MS-DOS モードで再起動します。 2. コマンドプロンプトを開きます。

駆除できないファイル	説明と解決策

	3. 次を入力してファイルを削除します。
	`cd \`
	`cd recycled`
	`del *.* /S`
	最後のコマンドでごみ箱内のすべてのファイルが削除されます。

Windows の一時フォルダまたは Internet Explorer の一時フォルダ内の感染ファイル	クライアントが使用しているため、Windows の一時フォルダまたは Internet Explorer の一時フォルダ内の感染ファイルを駆除できない場合があります。駆除するファイルが Windows の動作に必要な一時ファイルである場合もあります。
	解決策:
	1. クライアントを MS-DOS モードで再起動します。
	2. 感染ファイルが Windows の一時フォルダにある場合:
	a. コマンドプロンプトを開き、Windows の一時フォルダに移動します (初期設定では `C:¥Windows¥Temp` にあります)。
	b. 次を入力してファイルを削除します。
	`cd temp`
	`attrib -h`
	`del *.* /S`
	最後のコマンドで Windows の一時フォルダ内のすべてのファイルが削除されます。
	c. クライアントを通常モードで再起動します。
	3. 感染ファイルが Internet Explorer の一時フォルダにある場合:
	a. コマンドプロンプトを開き、Internet Explorer の一時フォルダに移動します (初期設定では `C:¥Users¥<ユーザ名>¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files` にあります)。
	b. 次を入力してファイルを削除します。
	`cd tempor~1`

駆除できないファイル	説明と解決策

	`attrib -h`
	`del *.* /S`
	最後のコマンドで Internet Explorer の一時フォルダ内のすべてのファイルが削除されます。
	c. クライアントを通常モードで再起動します。

サポートされていない圧縮形式で圧縮されたファイル	解決策:ファイルを解凍します。
現在実行中のロックされたファイル	解決策:ファイルのロックを解除するか、実行が終了するまで待ちます。
破損しているファイル	解決策:ファイルを削除します。

索引

アルファベット

あ

か

さ

た