Trend Micro Security™ (for Mac) 2.1
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/jp/solution/000207383

法人向け製品のサポートについて

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

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

著作権について

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

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan

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

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2022 Trend Micro Incorporated. All rights reserved.

TSEM38924/200214_JP (2022/01)

目次

はじめに

はじめに 11
Trend Micro Security (for Mac) ドキュメント 12
対象読者 12
ドキュメントの表記規則 13

第 1 章：製品の概要

はじめに 16
本リリースの新機能 16
主な機能 16
Trend Micro Security (for Mac) サーバ 17
Trend Micro Security (for Mac) エージェント 18
用語 19

第 2 章：サーバのインストール

サーバのインストール要件 22
アップデート元 22
Trend Micro Security (for Mac) サーバのインストール 23
製品の初回アクティベート 26
サーバでのインストール後のタスクの実行 27
Trend Micro Security (for Mac) サーバのアンインストール 28

第 3 章：使用開始

Web コンソール 32
    Web コンソールを開く 32
セキュリティの概要 33

エージェントツリー 34
エージェントツリーの一般的なタスク 35
エージェントツリー固有のタスク 36
グループ 37
グループの追加 38
グループまたはエージェントの削除 38
グループの名前変更 39
エージェントの移動 39
ウィジェット 40
[接続ステータス] ウィジェット 40
[アップデートステータス] ウィジェット 41
[検出ステータス] ウィジェット 42
Trend Micro Smart Protection 42
スマートフィードバック 44

第 4 章：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要件 48
セキュリティエージェントのインストールファイルとセットアップファイル 48
1 つのエンドポイントへのインストール 49
セキュリティエージェントのインストール後のタスク 55
セキュリティエージェントのアンインストール 56

第 5 章：最新の保護状態の維持

コンポーネント 60
アップデートの概要 61
サーバアップデート 62
サーバアップデート元の設定 63
サーバアップデート用のプロキシ設定の指定 64
サーバのアップデート方法 65
エージェントのアップデート 66
エージェントのアップデートの設定 68
[概要] 画面からのエージェントアップデートの起動 70

[エージェント管理] 画面からのエージェントアップデートの起動 70

第 6 章：セキュリティリスクからのエンドポイントの保護

セキュリティリスクについて 74
ウイルスと不正プログラム 74
スパイウェアとグレーウェア 76

検索の種類 77
リアルタイム検索 77
手動検索 79
予約検索 80
検索開始 81

すべての検索の種類に共通の設定 82
検索条件 82
検出時の処理 85
検索除外 86
検索のキャッシュ設定 90

セキュリティリスク通知とログ 92
管理者通知設定の指定 92
管理者向けのセキュリティリスクの通知の設定 93
管理者向けのアウトブレーク通知の設定 94
セキュリティリスクログの表示 95

第 7 章：Web ベースの脅威からのエンドポイントの保護

Web からの脅威 102

Web レピュテーション 102

Web レピュテーションの設定 103

承認済み URL リストの設定 106

Web レピュテーションログの表示 106

第 8 章：サーバおよびエージェントの管理

サーバおよびエージェントのアップグレード 110
サーバのアップグレード 110
エージェントのアップグレード 113

ログの管理 114
ライセンスの管理 114
サーバデータベースのバックアップ 116
サーバデータベースの復元 116
エージェント/サーバ間の通信の設定 117
セキュリティエージェントのアイコン 119

第 9 章：サポート情報

トラブルシューティング 124
Web コンソールへのアクセス 124
サーバのアンインストール 126
エージェントのインストール 127
エージェントの一般的なエラー 128
テクニカルサポート 128
トラブルシューティングのリソース 129
製品サポート情報 129
トレンドマイクロへのウイルス解析依頼 130
その他のリソース 132

付録 A：Trend Micro Security (for Mac) での IPv6 サポート

Trend Micro Security (for Mac) サーバおよびエージェントの IPv6 サポート 134
Trend Micro Security (for Mac) サーバの IPv6 要件 134
Trend Micro Security (for Mac) エージェントの IPv6 要件 134
IPv6 シングルスタックサーバの制限事項 135
IPv6 シングルスタックエージェントの制限事項 135
IPv6 アドレスの設定 136
IP アドレスが表示される画面 137

索引

索引 139

はじめに

Trend Micro Security (for Mac) 管理者ガイドへようこそ。このドキュメントでは、Trend Micro Security (for Mac) サーバとエージェントのインストール、使用開始の手順、およびサーバとエージェントの管理について説明します。

Trend Micro Security (for Mac) ドキュメント

Trend Micro Security (for Mac) に付属するドキュメントは以下のとおりです。

ドキュメント	説明
管理者ガイド	Trend Micro Security (for Mac) サーバとエージェントのインストール、使用開始の手順、およびサーバとエージェントの管理について説明する PDF ドキュメントです。
ヘルプ	操作手順、使用にあたってのアドバイス、および目的別の作業手順を提供する HTML ファイルです。
Readme	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。他のドキュメントには記載されていない可能性のある最新の製品情報を提供します。
製品 Q&A	問題解決およびトラブルシューティング情報のオンラインデータベース。製品の既知の問題に関する最新の情報を得ることができます。製品 Q&A にアクセスするには、次の Web サイトをご覧ください。 https://success.trendmicro.com/jp/technical-support

製品ドキュメントは弊社の「最新版ダウンロード」サイトから入手することも可能です。

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

対象読者

Trend Micro Security (for Mac) 付属のドキュメントは、次のユーザを対象としています。

- Trend Micro Security (for Mac) 管理者: サーバおよびエージェントのインストールと管理を含む Trend Micro Security (for Mac) 管理の責任者。ネットワーキングおよびサーバ管理についての高度な知識を持つユーザであることが想定されています。

- エンドユーザ: 使用しているエンドポイントに Trend Micro Security (for Mac) エージェントがインストールされているユーザ。コンピュータ初心者から上級ユーザまでを対象としています。

ドキュメントの表記規則

情報を簡単に特定して理解できるようにするため、Trend Micro Security (for Mac) 付属のドキュメントでは次の表記規則を使用しています。

表 1. ドキュメントの表記規則

表記規則	説明
注意	設定上の注意事項または推奨事項について説明します。
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について説明します。
警告!	ネットワーク上のエンドポイントが損傷を受ける可能性のある操作について警告します。

第 1 章

製品の概要

この章では、Trend Micro™ Security (for Mac)™ と、その機能の概要について説明します。

はじめに

Trend Micro™ Security (for Mac)™ は、セキュリティリスク、複合型の脅威、およびプラットフォームに依存しない Web ベースの攻撃に対して最新のエンドポイント保護機能を提供します。

Trend Micro Security (for Mac) サーバは、ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) のトレンドマイクロ製品と統合されたプラグインプログラムで、プラグインマネージャフレームワークを介してインストールされます。Trend Micro Security (for Mac) サーバは、エンドポイントにエージェントを配信します。

本リリースの新機能

Trend Micro Security (for Mac) には、次の新機能と機能強化が含まれています。

機能/強化点	詳細
プラットフォームのサポート	セキュリティエージェントは、macOS™ 12 (Monterey) のエンドポイントにインストールできるようになりました。

主な機能

Trend Micro Security (for Mac) には、次の機能や利点があります。

表 1-1. 主な機能

機能	利点
セキュリティリスクからの保護	Trend Micro Security (for Mac) は、ファイルを検索し、検出されたセキュリティリスクに応じた処理を実行することでセキュリティリスクからコンピュータを保護します。短期間に大量のセキュリティリスクが検出された場合は大規模感染の兆候があります。Trend Micro Security (for Mac)からの大規模感染の通知により、管理者は感染したエンドポイントを修復したり、安全が確保されるまでそれらを隔離したりするなど、迅速な対応が可能となります。

機能	利点
Web レピュテーション	Web レピュテーションテクノロジは、不正な Web サイトや危険と考えられる Web サイトをネットワークレベルでブロックし、企業ネットワークの内外にあるエンドポイントを保護します。Web レピュテーションにより感染経路は遮断され、不正コードのダウンロードが阻止されます。 ウイルスバスター ビジネスセキュリティを Smart Protection Server または Trend Micro Smart Protection Network と統合することにより、Web サイトとページの信頼性を検証します。
一元管理	Web ベースの管理コンソールは、ネットワーク上のすべてのセキュリティエージェントへの透過的なアクセスを管理者に提供します。Web コンソールにより、すべてのセキュリティエージェントへのセキュリティポリシー、パターンファイル、およびソフトウェアアップデートの自動配信が一元管理されます。管理者は、リモート管理や、エージェントまたはエージェントグループごとの設定を行うことができます。

Trend Micro Security (for Mac) サーバ

Trend Micro Security (for Mac) サーバは、すべてのエージェントの設定、セキュリティリスクのログ、およびアップデートを行う中央リポジトリです。

Trend Micro Security (for Mac) サーバは、次の 2 つの重要な機能を実行します。

- Trend Micro Security (for Mac) エージェントの監視および管理
- エージェントに必要なコンポーネントのダウンロード。Trend Micro Security (for Mac) サーバの初期設定では、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がダウンロードされ、エージェントに配信されます。

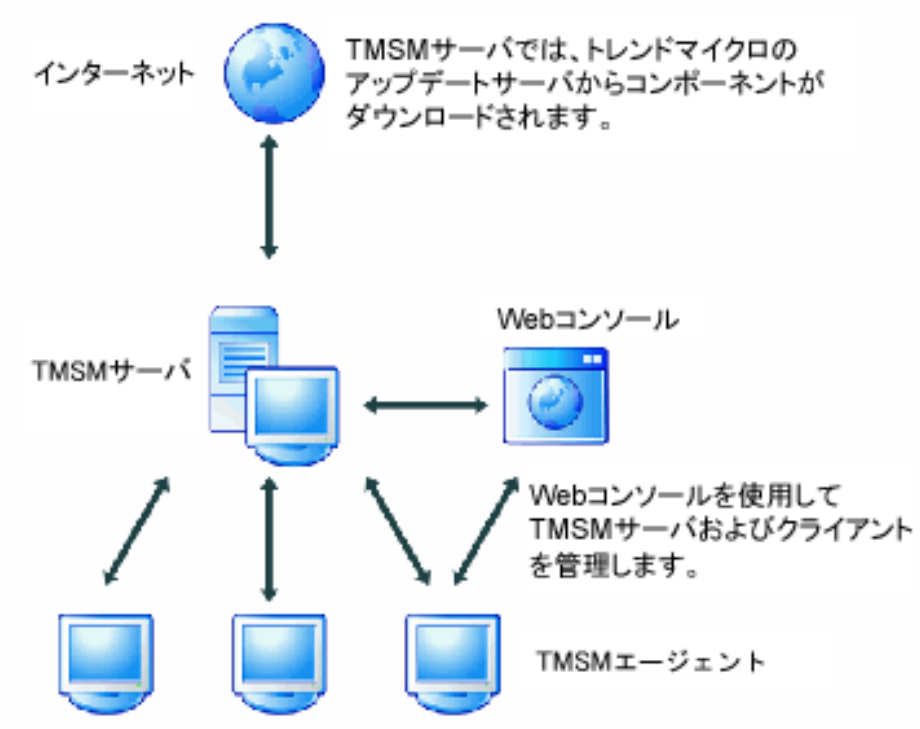


図 1-1. Trend Micro Security (for Mac) サーバが機能するしくみ

Trend Micro Security (for Mac) では、サーバとエージェント間でリアルタイムの双方向通信が実現されます。エージェントは、ネットワーク上のほぼどこからでもアクセス可能なブラウザベースの Web コンソールで管理されます。サーバは、ActiveMQ プロトコルを使用してエージェントと通信します。

Trend Micro Security (for Mac) エージェント

それぞれのエンドポイントに Trend Micro Security (for Mac) エージェントをインストールすることによって、セキュリティリスクからエンドポイントを保護します。エージェントでは、次の 3 つの検索の種類が提供されます。

- リアルタイム検索
- 予約検索
- 手動検索

エージェントは、インストール元の上位 Trend Micro Security (for Mac) サーバにステータスを報告します。エージェントは、イベントおよびステータス情報をリアルタイムでサーバに送信します。エージェントは、ActiveMQ プロトコルを使用してサーバと通信します。

用語

次の表は、Trend Micro Security (for Mac) 付属のドキュメントで使用されている用語を示しています。

用語	説明
エージェントまたはセキュリティエージェント	エンドポイントにインストールされる Trend Micro Security (for Mac) のセキュリティエージェントプログラム
エンドポイント	セキュリティエージェントがインストールされたコンピュータ
エージェントユーザ (またはユーザ)	エンドポイントでセキュリティエージェントを管理しているユーザ
サーバ	Trend Micro Security (for Mac) のサーバプログラム
サーバコンピュータ	Trend Micro Security (for Mac) サーバがインストールされたコンピュータ
管理者 (または Trend Micro Security (for Mac) の管理者)	Trend Micro Security (for Mac) サーバを管理している人
コンソール	Trend Micro Security (for Mac) サーバおよびセキュリティエージェントの設定を指定および管理するためのユーザインタフェース サーバプログラムのコンソールは「Web コンソール」と呼ばれ、セキュリティエージェントプログラムのコンソールは「エージェントコンソール」と呼ばれます。

用語	説明
セキュリティリスク	ウイルス、不正プログラム、スパイウェア、グレーウェア、および Web からの脅威の総称
製品サービス	Microsoft 管理コンソール (MMC) から管理される Trend Micro Security (for Mac) サービス
コンポーネント	セキュリティリスクの検索、検出、および処理を実行するもの
エージェントのインストールフォルダ	セキュリティエージェントのファイルが含まれるエンドポイント上のフォルダ /ライブラリ/Application Support/TrendMicro
サーバのインストールフォルダ	Trend Micro Security (for Mac) のサーバファイルが含まれるサーバコンピュータ上のフォルダ。Trend Micro Security (for Mac) サーバをインストールすると、同じウイルスバスター ビジネスセキュリティサーバディレクトリにこのフォルダが作成されます。 ウイルスバスター ビジネスセキュリティサーバのインストール時の初期設定では、サーバのインストールフォルダは次のいずれかの場所に設定されます。 • C:¥Program Files¥Trend Micro¥Security Server¥Addon¥TMSM • C:¥Program Files (x86)¥Trend Micro¥Security Server¥Addon¥TMSM
デュアルスタック	IPv4 アドレスと IPv6 アドレスの両方のアドレスを持つエンティティ。次に例を示します。 • デュアルスタックエンドポイントとは、IPv4 と IPv6 の両方のアドレスを持つエンドポイントです。 • デュアルスタックエージェントとは、デュアルスタックエンドポイントにインストールされたエージェントです。 • デュアルスタックプロキシサーバ (DeleGate など) は、IPv4 と IPv6 のアドレスを変換できます。
IPv4 シングルスタック	IPv4 アドレスのみを持つエンティティ
IPv6 シングルスタック	IPv6 アドレスのみを持つエンティティ

第 2 章

サーバのインストール

この章では、Trend Micro Security (for Mac) サーバのシステム要件とインストール手順について説明します。

サーバのインストール要件

サーバのインストール要件のリストについては、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

注意

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

アップデート元

Trend Micro Security (for Mac) サーバをインストールする前に、ウイルスバスター ビジネスセキュリティ Web コンソールで [アップデート] > [サーバ] > [アップデート元] に移動して、プラグインマネージャのアップデート元を確認します。アップデート元は、次のいずれかになります。

表 2-1. 使用可能なアップデート元

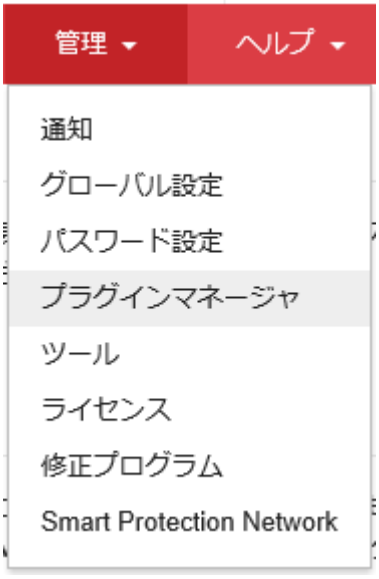
選択したアップデート元	説明および指示
トレンドマイクロのアップデートサーバ	初期設定のアップデート元は、トレンドマイクロのアップデートサーバです。このサーバに接続するにはインターネット接続が必要です。 サーバコンピュータがプロキシサーバを介してインターネットに接続している場合は、そのプロキシ設定を使用してインターネット接続を確立できることを確認してください。

選択したアップデート元	説明および指示
その他のアップデート元	複数のアップデート元を指定している場合: • サーバコンピュータがリスト上の 1 番目のアップデート元に接続できることを確認してください。1 番目のアップデート元に接続できない場合、サーバコンピュータは別のアップデート元への接続を試行しません。 • 1 番目のアップデート元に、プラグインマネージャの最新バージョンのコンポーネントリスト (OSCE_AOS_COMP_LIST.xml) および Trend Micro Security (for Mac) インストールパッケージが含まれていることを確認します。 アップデート元の設定についてサポートが必要な場合は、サポートセンターまでお問い合わせください。
現在のファイルのコピーを含むイントラネットの場所	アップデート元がイントラネットの場合: • サーバコンピュータとアップデート元との接続が機能することを確認してください。 • アップデート元に、プラグインマネージャの最新バージョンのコンポーネントリスト (OSCE_AOS_COMP_LIST.xml) および Trend Micro Security (for Mac) インストールパッケージが含まれていることを確認します。 イントラネットのアップデート元の設定についてサポートが必要な場合は、サポートセンターまでお問い合わせください。

Trend Micro Security (for Mac) サーバのインストール

手順

1. ウイルスバスター ビジネスセキュリティ Web コンソールを開いて、メインメニューの [管理] > [プラグイン] をクリックします。

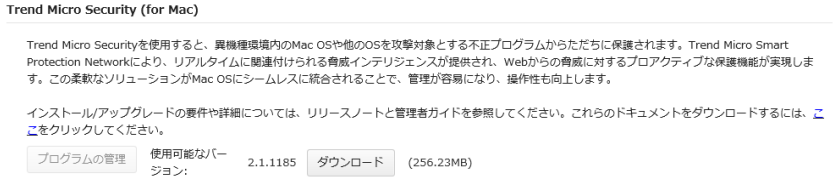


2. [Trend Micro Security (for Mac)] セクションに移動して、[ダウンロード] をクリックします。

   ダウンロードするファイルのサイズが [ダウンロード] ボタンの横に表示されます。

   プラグインマネージャにより、パッケージが <ウイルスバスター 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¥Download¥Product にダウンロードされます。

   <ウイルスバスター 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。



3. ダウンロードの進行状況を確認します。

ダウンロード中は、この画面以外にも移動できます。

パッケージのダウンロード中に問題が発生した場合は、ウイルスバスター ビジネスセキュリティ Web コンソールでサーバアップデートログを確認してください。メインメニューで、[レポート] > [ログクエリ] をクリックします。

4. Trend Micro Security (for Mac) をただちにインストールするには、[インストール] をクリックします。後でインストールする場合は、次の手順を実行します。

   a. [後でインストール] をクリックします。

   b. [プラグインマネージャ] 画面を開きます。

   c. [Trend Micro Security (for Mac)] セクションに移動して、[インストール] をクリックします。

5. 使用許諾契約を読み、同意できる場合は [同意する] をクリックして条件に同意します。

   インストールが開始します。

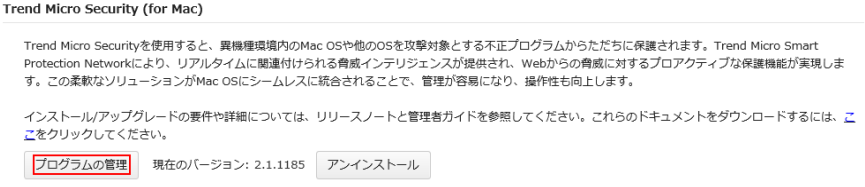
6. インストールの進行状況を確認します。インストール後に、[プラグインマネージャ] 画面が再ロードされます。

製品の初回アクティベート

手順

1. ウイルスバスター ビジネスセキュリティ Web コンソールを開いて、メインメニューの [管理] > [プラグイン] をクリックします。

2. [Trend Micro Security (for Mac)] セクションに移動して、[プログラムの管理] をクリックします。



3. 製品のアクティベーションコードを入力して、[保存] をクリックします。アクティベーションコードでは大文字と小文字が区別されます。

アクティベーションコードをお持ちでない場合は、リンクをクリックして、トレンドマイクロの登録用 Web サイトにアクセスしてください。登録を完了すると、トレンドマイクロからアクティベーションコードが記載されたメールが届きます。これで、アクティベーションを続行できます。

体験版のライセンスをアクティベートした場合は、ライセンスの有効期限が切れる前に製品版にアップグレードしてください。

サーバでのインストール後のタスクの実行

手順

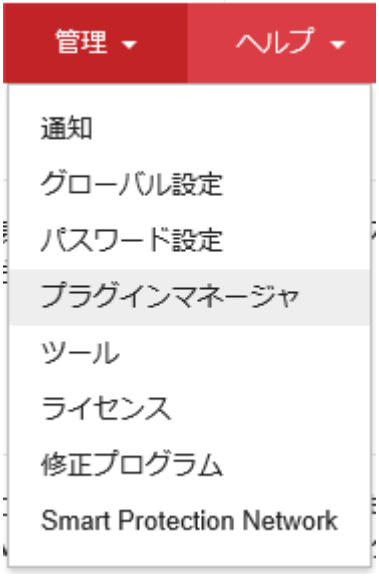
1. Microsoft 管理コンソールに次のサービスが表示されていることを確認します。
   - ActiveMQ for Trend Micro Security (for Mac)
   - Trend Micro Security (for Mac)
2. Windows タスクマネージャで次のプロセスが実行中であることを確認します。TMSMMainService.exe
3. レジストリエディタに次のレジストリキーが存在することを確認します。`HKEY_LOCAL_MACHINE¥Software¥TrendMicro¥OfficeScan¥service¥AoS¥OSCE_ADDON_TMSM`

4. Trend Micro Security (for Mac) サーバのファイルが <サーバのインストールフォルダ> に配置されていることを確認します。

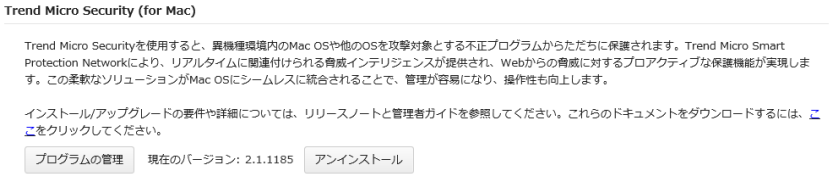
Trend Micro Security (for Mac) サーバのアンインストール

手順

1. ウイルスバスター ビジネスセキュリティ Web コンソールを開いて、メインメニューの [管理] > [プラグイン] をクリックします。



2. [Trend Micro Security (for Mac)] セクションに移動して、[アンインストール] をクリックします。



3. アンインストールの進行状況を確認します。アンインストール中は、この画面以外にも移動できます。アンインストールが完了したら、Trend Micro Security (for Mac) サーバは再度インストール可能になります。

注意

アンインストールパッケージによって Trend Micro Security (for Mac) が使用する Java Runtime Environment (JRE) が削除されることはありません。JRE が他のアプリケーションによって使用されていない場合は、JRE を削除できます。

第 3 章

使用開始

この章では、Trend Micro Security (for Mac) の使用を開始するための手順と、初期設定について説明します。

Web コンソール

Web コンソールは、Trend Micro Security (for Mac) エージェントを監視し、エージェントに配信される設定を指定するためのユーザインタフェースです。コンソールには一連の初期設定と値が搭載されており、セキュリティ要件と仕様に基づき設定を行うことができます。

Web コンソールを使って、以下を実行できます。

- エンドポイントにインストールされたエージェントの管理
- 同時設定と同時管理を目的とした、エージェントの論理グループへの編成
- 検索設定を指定した、単一または複数エンドポイントでの検索の開始
- セキュリティリスクに関する通知の設定と、エージェントから送信されたログの表示
- 大規模感染の基準と通知の設定

Web コンソールを開く

始める前に

ネットワーク上の、次の要件を満たす任意のエンドポイントから Web コンソールを開きます。

- 解像度 800x600、256 色以上をサポートするモニタ
- サポートされる Web ブラウザ:
  - ウイルスバスター ビジネスセキュリティ 10.0 の場合
    - Microsoft Internet Explorer 9 以降のバージョン
    - Microsoft Edge
    - Firefox
    - Chrome

- ウイルスバスター ビジネスセキュリティ 9.5 の場合
  - Microsoft Internet Explorer 7

手順

1. Web ブラウザで、ウイルスバスター ビジネスセキュリティサーバの URL を入力します。
2. パスワードを入力して、ウイルスバスター ビジネスセキュリティ Web コンソールにログオンします。
3. メインメニューで、[管理] > [プラグイン] をクリックします。
4. [Trend Micro Security (for Mac)] セクションに移動して、[プログラムの管理] をクリックします。

セキュリティの概要

Trend Micro Security (for Mac)の Web コンソールを開くかメインメニューで [概要] をクリックすると、[概要] 画面が表示されます。

ヒント

画面表示を定期的に更新して、最新情報を入手してください。

エージェント

[エージェント] セクションには、次の情報が表示されます。

- Trend Micro Security (for Mac)サーバとすべてのエージェントとの接続状況。リンクをクリックすると、エージェント設定を指定できるエージェントツリーが表示されます。
- 検出されたセキュリティリスクおよび Web からの脅威の数
- セキュリティリスクおよび Web からの脅威が検出されたエンドポイントの数。数字をクリックすると、セキュリティリスクや Web からの脅威

が検出されたエンドポイントの一覧を表示するエージェントツリーが開きます。エージェントツリーで、次のタスクを実行してください。

- 1 つ以上のエージェントを選択し、[ログ] > [セキュリティリスクログ] をクリックして、ログ基準を指定します。表示された画面の [結果] 列で、セキュリティリスクに対する検出時の処理が正常に実行されたかどうかを確認します。

  検索結果の一覧については、96 ページの「検索結果」を参照してください。

- 1 つ以上のエージェントを選択し、[ログ] > [Web レピュテーションログ] をクリックして、ログ基準を指定します。表示された画面で、ブロックされた Web サイトの一覧を確認します。ブロックしない Web サイトは、承認済み URL の一覧に追加できます。

  詳細については、106 ページの「承認済み URL リストの設定」を参照してください。

アップデートステータス

[アップデートステータス] の表には、Trend Micro Security (for Mac)コンポーネントと、エンドポイントをセキュリティリスクから保護するエージェントプログラムに関する情報が含まれます。

この表には次のタスクが含まれます。

- 最新でないコンポーネントがある場合は、速やかにアップデートします。

  詳細については、70 ページの「[概要] 画面からのエージェントアップデートの起動」を参照してください。

- サーバをアップグレードした直後は、エージェントを最新のプログラムバージョンまたはビルドにアップグレードします。

  エージェントのアップグレード手順については、110 ページの「サーバおよびエージェントのアップグレード」を参照してください。

エージェントツリー

Trend Micro Security (for Mac) エージェントツリーには、サーバが現在管理しているすべてのエージェントが表示されます。すべてのエージェントはい

ずれかのグループに属しています。エージェントツリーの上にあるメニュー項目を使用すると、同じ設定を特定のグループに属しているすべてのエージェントに対して同時に指定、管理、および適用できます。

エージェントツリーの一般的なタスク

エージェントツリーで実行できる一般的なタスクは次のとおりです。

手順

- すべてのグループおよびエージェントを選択するには、ルートアイコン ( ) をクリックします。ルートアイコンを選択してからエージェントツリーの上にあるタスクを選択すると、設定画面が表示されます。この画面では、次の一般的なオプションを選択できます。
  - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェントに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。
  - 今後追加されるグループにのみ適用: 今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。
- 連続する複数のグループやエージェントを選択するには、選択範囲の最初のグループまたはエージェントをクリックし、<Shift> キーを押しながら最後のグループまたはエージェントをクリックします。
- 連続していない複数のグループまたはエージェントを選択するには、<Ctrl> キーを押しながら目的のグループまたはエージェントをクリックします。
- 管理対象エージェントを検索するには、[エンドポイントの検索] ボックスにエージェントの完全な名前または名前の一部を入力します。一致するエージェント名のリストがエージェントツリーに表示されます。

注意

特定のエージェントを検索する際は、IPv6 アドレスまたは IPv4 アドレスを指定できません。

- 列情報に基づいてエージェントを並べ替えるには、列名をクリックします。
- エージェントツリーの下にエージェントの総数が表示されます。
- エージェントのリストとそのステータスをエージェントツリーから.csv 形式でエクスポートするには、[エクスポート] ボタン ( ) をクリックします。

エージェントツリー固有のタスク

エージェントツリーの上部には、次のタスクを実行できるメニュー項目が表示されます。

メニューボタン	タスク
タスク	• エージェントのコンポーネントをアップデートします。 詳細については、66 ページの「エージェントのアップデート」を参照してください。 • エンドポイントで検索開始を実行します。 詳細については、81 ページの「検索開始」を参照してください。

メニューボタン	タスク

設定	• 検索設定を指定します。
	  • 79 ページの「手動検索」
	  • 77 ページの「リアルタイム検索」
	  • 80 ページの「予約検索」
	  • 86 ページの「検索除外」
	  • 90 ページの「検索のキャッシュ設定」
	• Web レピュテーション設定を指定します。
	詳細については、103 ページの「Web レピュテーションの設定」を参照してください。
	• アップデート設定を指定します。
	詳細については、68 ページの「エージェントのアップデートの設定」を参照してください。

ログ	ログが表示されます。 • 95 ページの「セキュリティリスクログの表示」 • 106 ページの「Web レピュテーションログの表示」
エージェントツリー管理	Trend Micro Security (for Mac) グループを管理します。 詳細については、37 ページの「グループ」を参照してください。

グループ

Trend Micro Security (for Mac) のグループは、同じ設定を共有し、同じタスクを実行する一連のエージェントです。エージェントをグループに編成すると、同じ設定を特定のグループに属しているすべてのエージェントに対して同時に指定、管理、および適用できます。

管理を簡素化するために、部門または実行する機能に基づいてエージェントをグループ分けします。感染のリスクが高いエージェントを 1 つのグループに集めて、これらすべてのエージェントに対してさらに安全な設定を適用することもできます。グループの追加または名前変更、別のグループへのエー

ジェントの移動、またはエージェントの完全な削除を実行できます。エージェントツリーから削除されたエージェントは、エンドポイントから自動的にアンインストールされるわけではありません。エージェントでは、コンポーネントのアップデートなどサーバ依存タスクを引き続き実行できます。ただし、サーバではそのエージェントが認識されなくなるため、設定や通知がエージェントに送信されなくなります。

エージェントがエンドポイントからアンインストールされた場合は、エージェントツリーからは自動的に削除されず、接続状態は「オフライン」になります。エージェントツリーからエージェントを手動で削除してください。

グループの追加

手順

1. [エージェント管理] に移動します。
2. [エージェントツリー管理] > [グループの追加] をクリックします。
3. 追加するグループの名前を入力します。
4. [追加] をクリックします。

   新しいグループがエージェントツリーに表示されます。

グループまたはエージェントの削除

始める前に

グループを削除する前に、そのグループに属しているエージェントがないかどうかを確認し、ある場合はそれらのエージェントを別のグループに移動します。

エージェントの移動方法の詳細については、39 ページの「エージェントの移動」を参照してください。

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、特定のグループまたはエージェントを選択します。
3. [エージェントツリー管理] > [グループ/エージェントの削除] をクリックします。
4. [OK] をクリックして削除を確認します。

グループの名前変更

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、名前を変更するグループを選択します。
3. [エージェントツリー管理] > [グループの名前変更] をクリックします。
4. グループの新しい名前を入力します。
5. [名前の変更] をクリックします。

   新しいグループ名がエージェントツリーに表示されます。

エージェントの移動

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、グループに属している 1 つまたは複数のエージェントを選択します。
3. [エージェントツリー管理] > [エージェントの移動] をクリックします。

4. エージェントの移動先となるグループを選択します。
5. 対象のエージェントに新しいグループの設定を適用するかどうかを指定します。

ヒント

エージェントツリー内でエージェントをドラッグアンドドロップして別のグループに移動することもできます。

6. [移動] をクリックします。

ウィジェット

ウイルスバスター ビジネスセキュリティのダッシュボードで Trend Micro Security (for Mac) のウィジェットを管理します。ウィジェットは、Trend Micro Security (for Mac) のアクティベーション後に利用できます。

ウィジェットを表示するには、ウイルスバスター ビジネスセキュリティのバージョンが 9.5 以降で、プラグインマネージャのバージョンが 1.5 以降であることを確認してください。

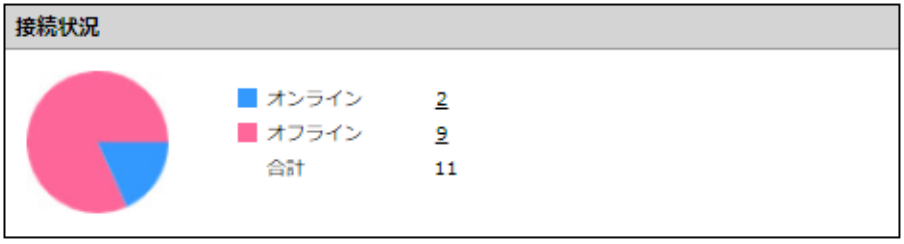
ウィジェットの使用の詳細については、ウイルスバスター ビジネスセキュリティのドキュメントを参照してください。

[接続ステータス] ウィジェット

[接続ステータス] ウィジェットには、エージェントの Trend Micro Security (for Mac) サーバとの接続状況が表示されます。

特定のステータスのエージェント数が 1 以上の場合、その数をクリックすると、Trend Micro Security (for Mac) エージェントツリー内のエージェントを

表示できます。これらのエージェントでタスクを開始したり、エージェントの設定を変更できます。



[アップデートステータス] ウィジェット

[アップデートステータス] ウィジェットには、エンドポイントをセキュリティリスクから保護するコンポーネントとプログラムが表示されます。

アップデートステータス (オンラインエージェント: 1)				
コンポーネント	現在のバージョン	最新	旧版	アップデート率
ウイルスパターンファイル	15.749.80	1	0	100.00%
スパイウェア監視パターンファイル	2.267.00	1	0	100.00%
ウイルス検索エンジン 32-bit	11.000.1006	0	1	0.00%
ウイルス検索エンジン 64-bit	11.000.1006	0	1	0.00%
プログラム	現在のバージョン	最新	旧版	アップデート率
Trend Micro Securityエージェント	3.6.1100	1	0	100.00%

このウィジェットには、次の情報が表示されます。

- 各コンポーネントの現在のバージョン。
- コンポーネントが古いままのエージェントの数 ([旧版] 列)。アップデートの必要なエージェントがある場合、数のリンクをクリックするとアップデートが開始されます。
- エージェントプログラムで数のリンクをクリックすると、アップグレードされていないエージェントが表示されます。

注意

このリンクをクリックすると Trend Micro Security (for Mac) サーバのコンソールが開き、追加のタスクを実行できます。

[検出ステータス] ウィジェット

[検出ステータス] ウィジェットには、セキュリティリスクと Web からの脅威の数が表示されます。

検出ステータス		
種類	検出数	感染したコンピュータ
セキュリティリスク	14	6
Webからの脅威	6	2

感染エンドポイントの数が 1 以上の場合、その数をクリックすると、Trend Micro Security (for Mac) エージェントツリー内のエージェントを表示できます。これらのエージェントでタスクを開始したり、エージェントの設定を変更できます。

Trend Micro Smart Protection

Trend Micro Smart Protection は、Web からの脅威やセキュリティリスクからユーザを保護する、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インフラストラクチャです。これは、軽量エージェントを使用し、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や Web 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することで、ローカルソリューションおよびホステッドソリューションの機能を強化して、企業ネットワーク内、自宅、または外出先にいるユーザを保護します。ネットワークにアクセスする製品、サービス、およびユーザが増えるにつれて、お客さまのセキュリティ保護は自動的に更新および強化され、ユーザに対する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。

クラウド上のレピュテーション、検索、および相関分析テクノロジを組み込むことにより、Trend Micro Smart Protection ソリューションではこれまでの

ようにパターンファイルをダウンロードする必要がなくなり、またデスクトップのアップデートに伴う遅延も解消されます。

Smart Protection サービス

Smart Protection サービスには、次のコンポーネントが含まれます。

- Web レピュテーションサービス: Web レピュテーションサービスにより、これまでトレンドマイクロのみでホストされていた URL レピュテーションデータをローカルの Smart Protection ソースにホストできるようになります。両方のテクノロジによって、パターンファイルのアップデート時や URL の有効性チェック時に消費される帯域幅が削減されます。

  詳細については、102 ページの「Web レピュテーション」を参照してください。

- スマートフィードバック: 新しい脅威に予防的に対応するため、トレンドマイクロでは世界中のトレンドマイクロ製品から匿名で送信される情報を収集し続けています。

  詳細については、44 ページの「スマートフィードバック」を参照してください。

Smart Protection ソース

Web レピュテーションサービスは、Smart Protection ソース、つまり Trend Micro Smart Protection Network と Smart Protection Server を介して配信されます。

Trend Micro Smart Protection Network はグローバルに展開されたインターネットベースのインフラストラクチャであり、企業ネットワークにアクセスできないユーザを対象としています。

Smart Protection Server は、ローカルの企業ネットワークにアクセスするユーザを対象としています。Smart Protection サービスをローカルサーバで企業ネットワークに対してローカライズし、効率を最適化します。

外部セキュリティエージェントの Smart Protection ソース

外部エージェント (Trend Micro Security (for Mac) サーバとの接続を維持できないセキュリティエージェント) は、Smart Protection Network に Web レ

ピュテーションクエリを送信します。クエリを正常に送信するにはインターネット接続が必要です。

[Web レピュテーションサービス] 画面に移動して、外部エージェントの Web レピュテーションポリシーを有効にします。詳細な手順については、103 ページの「Web レピュテーションの設定」を参照してください。

内部セキュリティエージェントの Smart Protection ソース

内部エージェント (Trend Micro Security (for Mac) サーバとの接続を維持しているセキュリティエージェント) は、Smart Protection Server または Smart Protection Network にクエリを送信できます。

ソース	詳細
Smart Protection Server	プライバシー上の問題があり、Web レピュテーションクエリを企業ネットワーク内に制限したい場合は、ソースに Smart Protection Server を設定します。
Trend Micro Smart Protection Network	設定の必要なリソースがなく、Smart Protection Server を維持するには、ソースに Trend Micro Smart Protection Network を設定します。

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、トレンドマイクロ製品と、弊社が所有する 24 時間体制の脅威に関する研究センターおよびテクノロジとの間に、継続的な両方向の情報交換を実現します。個々の顧客の定期的なレピュテーションチェックで検出された新しい脅威により、トレンドマイクロのすべての脅威データベースが自動的に更新され、それ以降に顧客に特定の脅威が発生するのを防ぐことができます。

トレンドマイクロでは、顧客とパートナーの大規模なグローバルネットワークを通じ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り、最新の脅威に対して自動的なリアルタイムの保護を実現し、「相互の連携が強化された」セキュリティを提供します。これは、地域住民がコミュニティを主体的に保護する自警団のように機能します。特定の情報の内容ではなく、情報源のレピュテーションに基づいて脅威情報が収集されるため、顧客の個人情報やビジネス情報のプライバシーは常に保護されます。

トレンドマイクロに送信される情報の例:

- ファイルのチェックサム
- アクセスされた Web サイト
- サイズとパスを含むファイルの情報
- 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中止できます。

ヒント

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への参加は必要はありません。参加は任意であり、いつでも中止できます。トレンドマイクロでは、トレンドマイクロのすべてのお客様により効果的な保護を提供できるように、スマートフィードバックへの参加をお勧めしています。

Smart Protection Network の詳細については、次のページを参照してください。

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

第 4 章

エージェントのインストール

この章では、Trend Micro Security (for Mac) エージェントのインストール要件と手順について説明します。

エージェントをアップグレードする方法の詳細については、110 ページの「サーバおよびエージェントのアップグレード」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

エージェントのインストール要件のリストについては、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

注意

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

セキュリティエージェントのインストールファイルとセットアップファイル

セキュリティエージェントをインストールするには、エンドポイントでインストールパッケージ (`tmsminstall.zip`) を起動します。

注意

セキュリティエージェントをアップグレードするには、110 ページの「サーバおよびエージェントのアップグレード」を参照してください。

Trend Micro Security (for Mac) サーバから必要なエージェントインストールパッケージを取得して、エンドポイントにコピーします。

パッケージを取得する方法は 2 とおりあります。

- Trend Micro Security (for Mac) Web コンソールで、[管理] > [エージェントセットアップファイル] に進み、[エージェントインストールファイル] の下にあるリンクをクリックします。

注意

この画面には、エージェントのアンインストールパッケージへのリンクも表示されています。これらのパッケージを使用してエンドポイントからエージェントプログラムを削除します。削除するエージェントプログラムのバージョンに応じてパッケージを選択します。

Trend Micro Security (for Mac) エージェントのアンインストールについては、48 ページの「セキュリティエージェントのインストールファイルとセットアップファイル」を参照してください。

- <サーバのインストールフォルダ>¥TMSM_HTML¥ClientInstall に移動します。

1 つのエンドポイントへのインストール

1 つ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するプロセスは、その他の一般的な Mac ソフトウェアのインストールプロセスとほぼ同様です。

インストール中に、iCoreService への接続の許可を求めるメッセージがユーザに表示される場合があります。これは、サーバへのエージェントの登録に使用されます。このメッセージが表示された場合は接続を許可するようにユーザに指示してください。

手順

1. 対象のエンドポイントに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を確認して、インストールされている場合はアンインストールします。
2. エージェントインストールパッケージ (tmsminstall.zip) を取得します。

   パッケージを取得する方法については、48 ページの「セキュリティエージェントのインストールファイルとセットアップファイル」を参照してください。
3. エンドポイントに tmsminstall.zip をコピーし、アーカイブユーティリティなどの Mac 標準のアーカイブツールを使用して起動します。

警告!

Mac 標準以外のアーカイブツールで起動すると、tmsminstall.zip 内のファイルが破損する場合があります。

ターミナルから tmsminstall.zip を起動するには、次のコマンドを使用します。

```
ditto -xk <tmsminstall.zip ファイルのパス> <インストール先フォルダ>
```

次に例を示します。

```
ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/Desktop
```

tmsminstall.zip を起動すると、新規フォルダ tmsminstall が作成されます。

4. tmsminstall フォルダを開き、tmsminstall.pkg を起動します。
5. インストールの続行を求めるメッセージが表示されたら、[続ける] をクリックします。

6. [はじめに] 画面で、[続ける] をクリックして次に進みます。

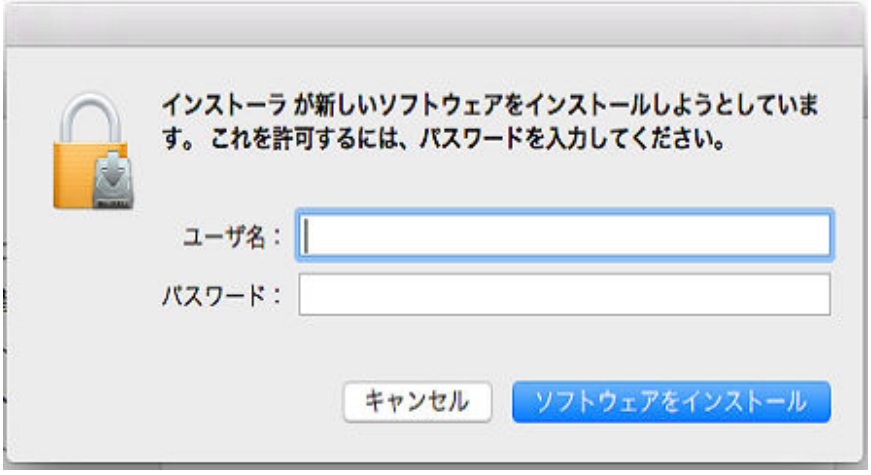
7. 留意事項を読み、[続ける] をクリックします。

8. [インストールの種類] 画面で、[インストール] をクリックします。

9. [名前] と [パスワード] を入力して、インストールプロセスを開始します。

注意

対象のエンドポイントに対する管理者権限があるアカウントの名前とパスワードを指定します。



10. インストールが正常に実行されたら、[閉じる] をクリックしてインストールプロセスを完了します。

エージェントは、エージェントインストールパッケージを取得したサーバに自動的に登録されます。また、エージェントは初めてアップデートされます。

次に進む前に

エージェントのインストール後のタスクを実行します。詳細については、55 ページの「セキュリティエージェントのインストール後のタスク」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後のタスク

手順

1. 以下を確認します。
   - Trend Micro Security (for Mac) エージェントのアイコン ( ) がエンドポイントのメニューバーに表示されていること。
   - セキュリティエージェントのファイルが <エージェントのインストールフォルダ> に配置されていること。
   - Web コンソールのエージェントツリーにエージェントが表示されていること。エージェントツリーにアクセスするには、メインメニューの [エージェント管理] をクリックします。
2. セキュリティエージェントコンソールで [アップデート] をクリックし、コンポーネントをアップデートします。セキュリティエージェントが、Trend Micro Security (for Mac) サーバからコンポーネントをダウンロードします。詳細については、66 ページの「エージェントのアップデート」を参照してください。

エージェントからサーバに接続できない場合、エージェントはトレンドマイクロのアップデートサーバから直接ダウンロードを実行します。アップデートサーバに接続するには、インターネット接続が必要です。

3. エンドポイントで手動検索を開始します。

次に進む前に

インストール後にエージェントで問題が発生した場合は、エージェントをアンインストールしてから再インストールしてみてください。

セキュリティエージェントのアンインストール

セキュリティエージェントプログラムのアンインストールは、そのプログラムで問題が発生した場合にのみ実行します。エンドポイントがセキュリティリスクから保護されるように、すぐにエージェントプログラムを再インストールしてください。

手順

1. Trend Micro Security (for Mac) サーバからセキュリティエージェントアンインストールパッケージ (`tmsmuninstall.zip`) を取得します。Trend Micro Security (for Mac) Web コンソールで、[管理] > [エージェントセットアップファイル] に進み、[エージェントアンインストールファイル] の下にあるリンクをクリックします。
2. エンドポイントにパッケージをコピーして起動します。
3. [名前] と [パスワード] を入力して、アンインストールプロセスを開始します。

   注意

   対象のエンドポイントに対する管理者権限があるアカウントの名前とパスワードを指定します。

4. アンインストールが正常に実行されたら、[閉じる] をクリックしてアンインストールプロセスを完了します。

次に進む前に

サーバからセキュリティエージェントの登録を解除します。

1. Web コンソールで、[エージェント管理] をクリックして、アンインストールされたセキュリティエージェントを選択します。
2. [エージェントツリー管理] > [グループ/エージェントの削除] をクリックします。

第 5 章

最新の保護状態の維持

この章では、Trend Micro Security (for Mac) 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。

コンポーネント

Trend Micro Security (for Mac) では、最新のセキュリティリスクからエンドポイントを保護するために、さまざまなコンポーネントを使用しています。これらのコンポーネントを最新状態に保つには、手動アップデートまたは予約アップデートを実行します。

Trend Micro Security (for Mac) エージェントでは、コンポーネントだけでなく、アップデートされた設定ファイルを Trend Micro Security (for Mac) サーバから受け取ります。エージェントでは、新しい設定を適用するために設定ファイルが必要です。Web コンソールで Trend Micro Security (for Mac) の設定を変更するたびに、設定ファイルが変更されます。

ウイルスパターンファイル

Trend Micro Security (for Mac) が最新のウイルス、不正プログラム、および複合型脅威の攻撃を識別するための情報を含みます。トレンドマイクロは週に数回、または有害なウイルスや不正プログラムが発見されるたびに、新しいウイルスパターンファイルを作成し、公開しています。

スパイウェア監視パターンファイル

スパイウェア監視パターンファイルには、Trend Micro Security (for Mac) がスパイウェアおよびグレーウェアを特定するのに役立つ情報が含まれています。

ウイルス検索エンジン

トレンドマイクロ製品の中枢です。もともとは、ファイルベースのコンピュータウイルスの対策として開発されました。現在の検索エンジンはより洗練され、不正プログラムやスパイウェアなどの多種多様なセキュリティリスクを検出します。また、調査用に開発、使用される管理ウイルスも検出できます。

検索エンジンのアップデート

パターンファイルにセキュリティリスクに関する最新情報を格納することによって、セキュリティ対策の状態を最新に維持しながら、検索エンジンのアップデート数を最小限にとどめています。それにもかかわらず、定期的に新しい検索エンジンのバージョンが使用可能になります。トレンドマイクロは、次の状況で新しいエンジンを公開します。

- ソフトウェアへの新しい検索および検出テクノロジの導入
- 検索エンジンで処理できない、潜在的に有害な新しいセキュリティリスクの発見
- 検索パフォーマンスの向上
- ファイル形式、スクリプト言語、エンコード、または圧縮形式の追加

エージェントプログラム

Trend Micro Security (for Mac) エージェントプログラムは、セキュリティリスクからの実際の保護を提供します。

アップデートの概要

コンポーネントのアップデートはすべて、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、Trend Micro Security (for Mac) サーバによって最新のコンポーネントがダウンロードされます。

トレンドマイクロのアップデートサーバ以外のアップデート元からアップデートするように Trend Micro Security (for Mac) サーバを設定できます。これを行うには、ユーザ指定のアップデート元を設定する必要があります。アップデート元の設定についてサポートが必要な場合は、サポートセンターまでお問い合わせください。

次の表は、Trend Micro Security (for Mac) サーバおよびエージェントに対するコンポーネントアップデートのさまざまなオプションを示しています。

表 5-1. サーバとエージェントのアップデートオプション

アップデートオプション	説明
トレンドマイクロのアップデートサーバ Trend Micro Security (for Mac) サーバ エージェント	Trend Micro Security (for Mac) サーバは、トレンドマイクロのアップデートサーバ (またはユーザ指定のアップデート元が設定されている場合は別のアップデート元) から最新のコンポーネントを受信して、エージェントに配信します。
トレンドマイクロのアップデートサーバ エージェント	Trend Micro Security (for Mac) エージェントは、Trend Micro Security (for Mac) サーバに接続できない場合、直接トレンドマイクロの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ます。

サーバアップデート

Trend Micro Security (for Mac) サーバは、次の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。

- ウイルスパターンファイル
- スパイウェア監視パターンファイル
- ウイルス検索エンジン

Web コンソールの [概要] 画面で最新バージョンのコンポーネントを参照して、コンポーネントがアップデートされているエージェントの数と、古いままのエージェントの数を確認します。

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、アップデートを正常にダウンロードするように正しいプロキシ設定を使用してください。

サーバアップデート元の設定

トレンドマイクロのアップデートサーバまたは他のアップデート元からコンポーネントをダウンロードするように Trend Micro Security (for Mac) サーバを設定します。

注意

サーバに IPv6 アドレスのみが割り当てられている場合は、サーバアップデートにおける IPv6 の制限事項について、135 ページの「IPv6 シングルスタックサーバの制限事項」を参照してください。

利用可能なアップデートがサーバでダウンロードされると、コンポーネントをアップデートするようにサーバからエージェントへ通知が自動的に送信されます。コンポーネントのアップデートが重要な場合は、[エージェント管理] > [タスク] > [アップデート] に移動して、エージェントにすぐに通知が送信されるようにサーバを設定します。

手順

1. [サーバアップデート] > [アップデート元] に移動します。
2. コンポーネントのアップデートのダウンロード元になる場所を選択します。
   - トレンドマイクロのアップデートサーバを選択する場合:
     - Trend Micro Security (for Mac) サーバからインターネットに接続できることを確認します。
     - プロキシサーバを使用している場合は、プロキシ設定を使用してインターネット接続が可能かどうかをテストしてください。

       詳細については、64 ページの「サーバアップデート用のプロキシ設定の指定」を参照してください。

- ユーザ指定のアップデート元を選択する場合:
  - 適切な環境を設定して、このアップデート元のリソースをアップデートしてください。
  - サーバコンピュータとこのアップデート元との接続が機能することも確認してください。アップデート元の設定についてサポートが必要な場合は、サポートセンターまでお問い合わせください。

3. [保存] をクリックします。

サーバアップデート用のプロキシ設定の指定

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ダウンロードするときにプロキシ設定を使用するように Trend Micro Security (for Mac) サーバを設定します。

注意

サーバに IPv6 アドレスのみが割り当てられている場合は、プロキシ設定における IPv6 の制限事項について、135 ページの「IPv6 シングルスタックサーバの制限事項」を参照してください。

手順

1. [管理] > [外部プロキシ設定] に移動します。
2. プロキシサーバの使用を有効にするチェックボックスをオンにします。
3. プロキシサーバの名前または IPv4/IPv6 アドレス、およびポート番号を指定します。
4. プロキシサーバに認証が必要な場合、所定のフィールドにユーザ名とパスワードを入力します。
5. [保存] をクリックします。

サーバのアップデート方法

Trend Micro Security (for Mac) サーバのコンポーネントのアップデートは、手動で行うか、またはアップデートスケジュールを設定することによって行います。

- 手動アップデート:重要なアップデートがある場合には、手動アップデートを実行することによりサーバでただちにアップデートを取得できます。詳細については、66 ページの「サーバの手動アップデート」を参照してください。
- 予約アップデート:Trend Micro Security (for Mac) サーバは、予約された日時にアップデート元に接続して、最新のコンポーネントを取得します。詳細については、65 ページの「サーバのアップデートの予約」を参照してください。

サーバでアップデートが完了すると、アップデートするようにサーバからエージェントへ通知がすぐに送信されます。

サーバのアップデートの予約

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を自動的にダウンロードするように、Trend Micro Security (for Mac) サーバを設定します。予約アップデートを使用することは、セキュリティリスクからの保護を常に最新に維持する簡単かつ効率的な方法です。

サーバでアップデートが完了すると、アップデートするようにサーバからエージェントへ通知が送信されます。

手順

1. [サーバアップデート] > [予約アップデート] に移動します。
2. アップデート対象コンポーネントを選択します。
3. アップデートスケジュールを指定します。

   毎日、毎週、毎月のアップデートの場合、Trend Micro Security (for Mac) がアップデートを実行する期間を時間単位で指定します。Trend Micro Security (for Mac) は、この期間の任意の時間にアップデートを実行します。

毎月のアップデートでは、29 日、30 日、31 日を選択した場合、これらの日付がない月では、Trend Micro Security (for Mac) によってその月の最終日にアップデートが実行されます。

4. [保存] をクリックします。

サーバの手動アップデート

サーバをインストールまたはアップグレードした後、および大規模感染が発生したときには、Trend Micro Security (for Mac) サーバでコンポーネントを手動でアップデートします。

手順

1. [サーバアップデート] > [手動アップデート] に移動します。
2. アップデート対象コンポーネントを選択します。
3. [アップデート] をクリックします。

   サーバがアップデートされたコンポーネントをダウンロードします。

   サーバでアップデートが完了すると、アップデートするようにサーバからエージェントへ通知がすぐに送信されます。

エージェントのアップデート

最新のセキュリティリスクに対するエージェントの保護状態を維持するには、エージェントのコンポーネントを定期的にアップデートします。コンポーネントが著しく古い場合や、大規模感染が発生したときにもエージェントをアップデートしてください。エージェントが Trend Micro Security (for Mac)サーバまたはトレンドマイクロのアップデートサーバから長期間アップデートを実行できないでいると、エージェントのコンポーネントは著しく古くなります。

エージェントのアップデート方法

エージェントをアップデートする方法はいくつかあります。

アップデート方法	説明
管理者が開始する手動アップデート	次の Web コンソール画面からアップデートを開始します。 • [エージェント管理] 画面。 詳細については、70 ページの「[エージェント管理] 画面からのエージェントアップデートの起動」を参照してください。 • [概要] 画面。 詳細については、70 ページの「[概要] 画面からのエージェントアップデートの起動」を参照してください。
自動アップデート	• サーバでアップデートが完了すると、アップデートするようにサーバからエージェントへ通知がすぐに送信されます。 • アップデートは、設定したスケジュールに従って実行できます。1 つまたは複数のエージェントおよびドメインに、またはサーバが管理するすべてのエージェントに適用されるスケジュールを設定できます。 詳細については、68 ページの「エージェントのアップデートの設定」を参照してください。
ユーザが開始する手動アップデート	ユーザがエンドポイントからアップデートを開始します。

エージェントのアップデート元

初期設定では、エージェントは Trend Micro Security (for Mac)サーバからコンポーネントをダウンロードします。Trend Micro Security (for Mac)エージェントは、Trend Micro Security (for Mac)サーバからアップデートする際、コンポーネントだけでなくアップデート済みの設定ファイルも受け取ります。エージェントでは、新しい設定を適用するために設定ファイルが必要です。Web コンソールで Trend Micro Security (for Mac)の設定を変更するたびに、設定ファイルが変更されます。

エージェントをアップデートする前に、Trend Micro Security (for Mac)サーバに最新のコンポーネントがあるかどうかを確認してください。

Trend Micro Security (for Mac) サーバのアップデート方法については、62 ページの「サーバアップデート」を参照してください。

Trend Micro Security (for Mac)サーバを使用できない場合は、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するように、1 つ、複数、またはすべてのエージェントを設定します。

詳細については、68 ページの「エージェントのアップデートの設定」を参照してください。

注意

エージェントに IPv6 アドレスのみが割り当てられている場合は、エージェントのアップデートにおける IPv6 の制限事項について、135 ページの「IPv6 シングルスタックエージェントの制限事項」を参照してください。

エージェントのアップデートにおける注意事項と留意事項

- Trend Micro Security (for Mac)エージェントでは、アップデートの実行時にプロキシ設定を使用できます。プロキシ設定は、エージェントコンソールで設定されます。
- アップデートの実行中、エンドポイントのメニューバー上の Trend Micro Security (for Mac)アイコンによって、製品がアップデートされていることが示されます。エージェントプログラムのアップグレードが利用可能な場合、エージェントではアップデートが実行されてから、最新プログラムバージョンまたはビルドへのアップグレードが実行されます。アップデートが完了するまで、ユーザはコンソールからいずれのタスクも実行することはできません。
- [概要] 画面にアクセスして、すべてのエージェントがアップデートされたかどうかを確認します。

エージェントのアップデートの設定

エージェントのアップデートの詳細については、66 ページの「エージェントのアップデート」を参照してください。

手順

1. [エージェント管理] に移動します。

2. エージェントツリーで、ルートアイコン
(

) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。

3. [設定] > [アップデート設定] の順にクリックします。

4. トレンドマイクロのアップデートサーバからのアップデートのダウンロードをエージェントに許可するチェックボックスをオンにします。

注意

エージェントに IPv6 アドレスのみが割り当てられている場合は、エージェントのアップデートにおける IPv6 の制限事項について、135 ページの「IPv6 シングルスタックエージェントの制限事項」 を参照してください。

---

5. 予約アップデートを設定するには、次の手順を実行します。

   a. [予約アップデートを有効にする] を選択します。

   b. スケジュールを設定します。

   c. [毎日] または [毎週] を選択する場合は、アップデートの時刻と Trend Micro Security (for Mac) サーバがエージェントにコンポーネントのアップデートを通知する時間を指定します。たとえば、開始時刻が午後 12 時で、時間が 2 時間の場合、サーバはすべてのオンラインエージェントに対して午後 12 時から午後 2 時までランダムに、コンポーネントをアップデートするよう通知します。この設定では、すべてのオンラインエージェントが指定された開始時刻に同時にサーバに接続することを防ぐため、サーバに向かうトラフィックの量が著しく減少します。

6. エージェントツリーでグループまたはエージェントを選択している場合は、[保存] をクリックすると設定がそのグループまたはエージェントに適用されます。ルートアイコン
(

) を選択した場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用:すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェン

トに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。

- 今後追加されるグループにのみ適用: 今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。

[概要] 画面からのエージェントアップデートの起動

その他のエージェントのアップデート方法については、66 ページの「エージェントのアップデート」を参照してください。

手順

1. 上部のメニューで [概要] をクリックします。
2. [アップデートステータス] セクションに移動して、[旧版] 列の下にあるリンクをクリックします。

   エージェントツリーが表示され、アップデートが必要なエージェントがすべて示されます。
3. アップデートするエージェントを選択します。
4. [タスク] > [アップデート] の順にクリックします。

   通知を受信しているエージェントがアップデートを開始します。エンドポイントでは、メニューバーの Trend Micro Security (for Mac) アイコンによって、製品がアップデート中であることが示されます。アップデートが完了するまで、ユーザはコンソールからいずれのタスクも実行することはできません。

[エージェント管理] 画面からのエージェントアップデートの起動

その他のエージェントのアップデート方法については、66 ページの「エージェントのアップデート」を参照してください。

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン
   (

) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [タスク] > [アップデート] の順にクリックします。

   通知を受信しているエージェントがアップデートを開始します。エンドポイントでは、メニューバーの Trend Micro Security (for Mac) アイコンによって、製品がアップデート中であることが示されます。アップデートが完了するまで、ユーザはコンソールからいずれのタスクも実行することはできません。

第 6 章

セキュリティリスクからのエンドポイントの保護

この章では、ファイルベースの検索を使用して、エンドポイントをセキュリティリスクから保護する方法について説明します。

セキュリティリスクについて

セキュリティリスクには、ウイルス、不正プログラム、スパイウェア、およびグレーウェアがあります。Trend Micro Security (for Mac) は、ファイルを検索し、検出されたセキュリティリスクに応じた処理を実行することでセキュリティリスクからコンピュータを保護します。短期間に大量の数のセキュリティリスクが検出された場合は大規模感染の兆候を示しています。Trend Micro Security (for Mac) は、大規模感染予防ポリシーを実行して、感染したエンドポイントが完全に危険な状態でなくなるまで隔離することによって大規模感染を抑制します。通知やログはセキュリティリスクの監視に役立ち、即座に処理が必要な場合の警告となります。

ウイルスと不正プログラム

いまや無数のウイルス/不正プログラムが存在し、毎日作成されています。今日、ウイルス/不正プログラムは企業のネットワークやメールシステム、Web サイトの脆弱性などに対し、非常に大きなダメージを与えています。

Trend Micro Security (for Mac) は、次の種類のウイルス/不正プログラムからエンドポイントを保護します。

ウイルス/不正プログラムの種類	説明
ジョークプログラム	ジョークプログラムはウイルスのようなプログラムで、エンドポイントの画面上にいたずらな表現を表示したりします。
トロイの木馬プログラム	トロイの木馬は実行形式のプログラムで、複製を作ることはありませんが、エンドポイントに常駐して不正な動作をします。たとえば、ポートを開いてハッカーを侵入させたりします。このプログラムは、エンドポイントへアクセスするためにトロイポートを使用することがよくあります。エンドポイントからウイルスを取り除くはずのアプリケーションが、実際にはエンドポイントにウイルスを導き入れるアプリケーションであったというのがトロイの木馬の例です。

ウイルス/不正プログラムの種類	説明
ウイルス	ウイルスは、複製するプログラムです。ウイルスは、複製のために自分自身を他のプログラムファイルに添付し、ホストプログラムの実行時に常に実行されるようにします。 • システム領域感染型ウイルス: パーティションやディスクの起動セクタに感染するウイルスです。 • Java 不正コード: Java で記述されているか、または Java に埋め込まれている、OS に依存しないウイルスコードです。 • マクロウイルス: アプリケーションマクロとしてコード化され、多くの場合ドキュメントに含まれているウイルスです。 • VB スクリプト、Java スクリプト、HTML ウイルス: Web ページに内在し、ブラウザを通じてダウンロードされるウイルスです。 • ワーム: コンピュータワームは自己完結型のプログラム (複数の場合あり) で、自体の一部または全部をコピーすることで機能を他のエンドポイントシステムに拡散します。多くの場合メールが利用されます。
テストウイルス	テストウイルスは不活性のファイルで、ウイルス検索ソフトにより検出されます。EICAR テストスクリプトのようにウイルス対策ソフトが適切に検索するかどうかテストするのに使います。
パッカー	パッカーは、圧縮され、暗号化された Windows 実行可能プログラムまたは Linux™実行可能プログラムで、トロイの木馬などがあります。実行ファイルの圧縮は、ウイルス対策製品による検出を難しくします。
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性質を示す不審なファイルは、このウイルス/不正プログラムの種類に分類されます。潜在的なウイルス/不正プログラムの詳細については、トレンドマイクロのオンラインウイルスデータベースの次のページを参照してください。 https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/
その他	「その他」に該当するのは、いずれのウイルス/不正プログラムの種類にも分類されないウイルス/不正プログラムです。

スパイウェアとグレーウェア

スパイウェアおよびグレーウェアとは、ネットワーク上のエンドポイントのパフォーマンスに悪影響を与える可能性があるアプリケーションやファイルのうち、ウイルスや不正プログラムに分類されないものを指します。スパイウェアおよびグレーウェアは、企業に対して、セキュリティ、機密保持、および法的責任における深刻なリスクをもたらします。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、エンドポイ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。

Trend Micro Security (for Mac) は、次の種類のスパイウェア/グレーウェアからエンドポイントを保護します。

スパイウェア/グレーウェアの種類	説明
スパイウェア	スパイウェアは、アカウントユーザ名、パスワード、クレジットカード番号などのデータ、およびその他の機密情報を収集し、第三者に送信します。
アドウェア	アドウェアは、広告を表示したり、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、今後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。
ダイヤラー	ダイヤラーは、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エンドポイントからモデム経由でダイヤルするよう強制します。多くの場合、この電話番号は通話時間に応じて課金される有料サービスや国際電話番号であり、企業に多額の費用が課せられる可能性があります。
ハッキングツール	ハッキングツールは、ハッカーがエンドポイントに入るのを助けます。
リモートアクセスツール	リモートアクセスツールは、ハッカーがリモートアクセスしてエンドポイントをコントロールするのを助けます。
パスワードクラックアプリケーション	この種類のアプリケーションは、ユーザ名およびパスワードを解読するために使用します。
その他	「その他」に該当するのは、いずれのスパイウェア/グレーウェアの種類にも分類されない潜在的に不正なプログラムです。

検索の種類

Trend Micro Security (for Mac) では、エンドポイントをセキュリティリスクから保護するために、次の検索の種類を提供しています。

検索の種類	説明
リアルタイム検索	エンドポイント上のファイルを受信、開く、ダウンロード、コピー、および変更したときに自動的に検索されます。 77 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	ユーザが要求したファイル (またはファイルのセット) を検索する手動の検索です。 79 ページの「手動検索」を参照してください。
予約検索	管理者が設定したスケジュールに従って、エンドポイント上のファイルが自動的に検索されます。 80 ページの「予約検索」を参照してください。
検索開始	1 つ以上の対象エンドポイント上にあるファイルを検索する、管理者が開始する検索です。 81 ページの「検索開始」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、継続的に実行される検索です。リアルタイム検索では、ファイルの受信時、開かれたとき、ダウンロード時、コピー時、または変更時に毎回、ファイルにセキュリティリスクが存在するかどうかが検索されます。Trend Micro Security (for Mac) でセキュリティリスクが検出されなかった場合、ファイルは元の場所に残され、ユーザはそのファイルに引き続きアクセスできます。Trend Micro Security (for Mac) がセキュリティリスクを検出した場合は通知メッセージが表示され、感染ファイルの名前と該当するセキュリティリスクが示されます。

リアルタイム検索の設定を、1 つ以上のエージェントおよびグループに設定および適用するか、またはサーバが管理するすべてのエージェントに設定および適用します。

リアルタイム検索の設定

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [設定] > [リアルタイム検索設定] をクリックします。
4. 次の検索基準を設定します。
   - 82 ページの「ファイルに対するユーザのアクティビティ」
   - 83 ページの「検索設定」
5. [処理] タブをクリックし、Trend Micro Security (for Mac) でセキュリティリスクが検出されたときに実行する処理を設定します。

   検索時の処理の詳細は、85 ページの「検出時の処理」を参照してください。
6. エージェントツリーでグループまたはエージェントを選択している場合は、[保存] をクリックすると設定がそのグループまたはエージェントに適用されます。ルートアイコン ( ) を選択した場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用:すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェントに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。
   - 今後追加されるグループにのみ適用: 今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。

手動検索

手動検索はオンデマンドの検索であり、ユーザがエージェントコンソールで検索を実行するとただちに開始されます。検索にかかる時間は、検索するファイル数やエンドポイントのハードウェアリソースによって異なります。

手動検索の設定を、1 つ以上のエージェントおよびグループに設定および適用するか、またはサーバが管理するすべてのエージェントに設定および適用します。

手動検索の設定

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [設定] > [手動検索設定] をクリックします。
4. 次の検索基準を設定します。
   - 83 ページの「検索設定」
   - 84 ページの「CPU 使用率」
5. [処理] タブをクリックし、Trend Micro Security (for Mac) でセキュリティリスクが検出されたときに実行する処理を設定します。

   検索時の処理の詳細は、85 ページの「検出時の処理」を参照してください。
6. エージェントツリーでグループまたはエージェントを選択している場合は、[保存] をクリックすると設定がそのグループまたはエージェントに適用されます。ルートアイコン ( ) を選択した場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用:すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェン

トに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。

- 今後追加されるグループにのみ適用: 今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。

予約検索

予約検索は指定された日時に自動的に実行されます。エージェントで予約検索を使用して検索ルーチンを自動化し、検索の管理効率を向上します。

予約検索の設定を、1 つ以上のエージェントおよびグループに設定および適用するか、またはサーバが管理するすべてのエージェントに設定および適用します。

予約検索の設定

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [設定] > [予約検索設定] をクリックします。
4. チェックボックスをオンにして、予約検索を有効にします。
5. 次の検索基準を設定します。
   - 84 ページの「スケジュール」
   - 83 ページの「検索対象」
   - 83 ページの「検索設定」

- 84 ページの「CPU 使用率」

6. [処理] タブをクリックし、Trend Micro Security (for Mac) でセキュリティリスクが検出されたときに実行する処理を設定します。

   検索時の処理の詳細は、85 ページの「検出時の処理」を参照してください。

7. エージェントツリーでグループまたはエージェントを選択している場合は、[保存] をクリックすると設定がそのグループまたはエージェントに適用されます。ルートアイコン ( ) を選択した場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用:すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェントに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。
   - 今後追加されるグループにのみ適用: 今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。

検索開始

検索開始は、Trend Micro Security (for Mac) の管理者によって Web コンソールを通してリモートで開始され、1 つ以上のエンドポイントに対して実行できます。

感染の疑いがあるエンドポイントで検索開始を開始します。

検索開始の実行

始める前に

実際のスケジュールを除く予約検索のすべての設定が、検索開始の実行時に使用されます。検索開始を実行する前に設定を指定するには、80 ページの「予約検索の設定」の手順に従ってください。

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [タスク] > [検索開始] をクリックします。

すべての検索の種類に共通の設定

検索の種類ごとに、検索条件、検索除外、および検索時の処理の 3 つの設定を行います。これらの設定を 1 つ以上のエージェントおよびグループに配信するか、またはサーバが管理するすべてのエージェントに配信します。

検索条件

ファイルの種類や拡張子などのファイル属性を使用して、特定の検索の種類で検索するファイルを指定します。また、検索をトリガする条件を指定します。たとえば、ファイルがエンドポイントにダウンロードされるたびに検索するよう、リアルタイム検索を設定します。

ファイルに対するユーザのアクティビティ

リアルタイム検索を実行するファイルに対するアクティビティを指定します。次のオプションから選択します。

- 作成中/変更中のファイルを検索:エンドポイントに (ファイルのダウンロード後などに) 取り込まれた新しいファイル、または変更中のファイルを検索します。
- 読み込み中のファイルを検索: ファイルを開くときに検索します。
- 次のファイルを検索: 作成された/変更された/読み込まれたファイル

たとえば、3 番目のオプションを選択した場合、エンドポイントにダウンロードされた新しいファイルが検索され、セキュリティリスクが検出されない場

合には現在の場所に残されます。この残されたファイルは、ユーザがそのファイルを開いたとき、およびユーザがそのファイルを変更した場合は変更内容が保存される前に、検索されます。

検索対象

次のオプションから選択します。

- 検索可能なすべてのファイル:すべてのファイルを検索します。
- トレンドマイクロの推奨設定で検索されたファイルタイプ: 不正コードが含まれている可能性のあるファイルのみを検索します。これには無害な拡張子名で偽装されたファイルも含まれます。
- フルパスのファイル名またはフォルダ名:指定されたファイルまたは特定のフォルダ内のファイルのみを検索します。

  1. ファイルのフルパスまたはディレクトリパスを入力して、[追加] をクリックします。
     - ファイルのフルパスの例:`/Users/username/temp.zip`
     - ディレクトリパスの例:`/Users/username`
  2. ディレクトリパスまたはファイルのフルパスを削除するには、パスを選択して [削除] をクリックします。

検索設定

Trend Micro Security (for Mac) は、圧縮ファイル内の個々のファイルを検索できます。Trend Micro Security (for Mac) では、次の圧縮の種類がサポートされています。

拡張子	種類
.zip	Pkzip によって作成されるアーカイブ
.rar	RAR によって作成されるアーカイブ
.tar	Tar によって作成されるアーカイブ

拡張子	種類
.arj	ARJ 圧縮アーカイブ
.hqx	BINHEX
.gz、.gzip	Gnu ZIP
.Z	LZW/圧縮 16 ビット
.bin	MacBinary
.cab	Microsoft キャビネットファイル
Microsoft 圧縮/MSCOMP	
.eml、mht	MIME
.td0	Teledisk 形式
.bz2	Unix BZ2 Bzip 圧縮ファイル
.uu	UUEncode
.ace	WinAce

CPU 使用率

Trend Micro Security (for Mac) は、あるファイルを検索した後、次のファイルを検索する前に一時停止することができます。この設定は、手動検索、予約検索、および ScanNow で使用されます。

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
- 低:ファイル検索の間隔をあける

スケジュール

予約検索を実行する頻度 (毎日、毎週、毎月) や時刻を設定します。

毎月の予約検索では、29 日、30 日、31 日を選択した場合、これらの日付がない月では、Trend Micro Security (for Mac) によってその月の最終日に予約検索が実行されます。

検出時の処理

特定の検索の種類でセキュリティリスクを検出したときに Trend Micro Security (for Mac) が実行する処理を指定します。

Trend Micro Security (for Mac) による検出時の処理は、セキュリティリスクを検出した検索の種類によって異なります。たとえば、Trend Micro Security (for Mac) で手動検索 (検索の種類) によってセキュリティリスクが検出された場合は、感染ファイルが駆除 (処理) されます。

Trend Micro Security (for Mac) がセキュリティリスクに対して実行可能な処理は次のとおりです。

ウイルス検出時の処理	詳細
削除	Trend Micro Security (for Mac) は感染ファイルをエンドポイントから削除します。
隔離	Trend Micro Security (for Mac) は、感染ファイルの名前を変更し、そのファイルをエンドポイントの隔離ディレクトリ (<エージェントのインストールフォルダ>/common/lib/vsapi/quarantine) に移動します。 隔離ディレクトリに移動した隔離ファイルに対して、Trend Micro Security (for Mac) は、ユーザ指定の処理に基づいて、さらに別の処理を実行できます。Trend Micro Security (for Mac) が隔離ファイルに対して実行できる処理には、削除、駆除、復元があります。ファイルの復元とは、処理を何も実行せずにファイルを元の場所に戻すことです。ユーザは、実際には無害な場合にファイルを復元できます。ファイルの駆除とは、隔離ファイルからセキュリティリスクを削除して、駆除が正常に実行された場合にそのファイルを元の場所に戻すことです。

ウイルス検出時の処理	詳細
駆除	Trend Micro Security (for Mac) は、感染ファイルからセキュリティリスクを削除したうえで、ユーザにファイルへのアクセスを許可します。 ファイルを駆除できない場合は、Trend Micro Security (for Mac) は 2 次処理として、隔離、削除、放置のいずれかを実行します。2 次処理を設定するには、[エージェント管理] > [設定] > {検索の種類} に移動し、[処理] タブをクリックします。
放置	Trend Micro Security (for Mac) は、感染ファイルに対する処理を実行しませんが、検出したセキュリティリスクをログに記録します。ファイルは元の場所に残ります。 Trend Micro Security (for Mac) は、誤検出を減らすために、潜在的なウイルス/不正プログラムの種類に感染したファイルに対して常に「放置」を実行します。その後の解析で潜在的なウイルス/不正プログラムが実際にセキュリティリスクであることが確認されると、新しいパターンファイルがリリースされ、Trend Micro Security (for Mac) で適切な検出時処理を実行できるようになります。実際には無害であることが確認されると、その潜在的なウイルス/不正プログラムは以降は検出されません。 たとえば、「123.pdf」というファイルで「x_probable_virus」が検出された場合、Trend Micro Security (for Mac) は検出時に処理を実行しません。「x_probable_virus」がトロイの木馬プログラムであることが確認されると、新しいウイルスパターンファイルがリリースされます。新しいパターンファイルがロードされると、Trend Micro Security (for Mac) は「x_probable_virus」をトロイの木馬プログラムとして検出するようになり、トロイの木馬プログラムに対する処理が「削除」の場合、「123.pdf」は削除されます。

検索除外

検索除外を設定すると、検索のパフォーマンスを向上させ、既知の無害なファイルの検索をスキップできるようになります。特定の種類の検索を実行するときに、Trend Micro Security (for Mac) は検索除外リストをチェックして、検索から除外するエンドポイント内のファイルを決定します。

検索除外リスト	詳細
ファイル	Trend Micro Security (for Mac) では、次に該当するファイルは検索しません。 • 検索除外リストに指定したディレクトリパスの下にあるファイル • 検索除外リストに指定したファイルのフルパス (ディレクトリパスとファイル名) に一致するファイル
ファイル拡張子	Trend Micro Security (for Mac) は、ファイルの拡張子がこの除外リストに含まれているいずれかのファイル拡張子に一致する場合、そのファイルを検索しません。

検索除外リスト設定

検索除外リストの詳細については、「86 ページの「検索除外」」を参照してください。

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [設定] > [検索除外の設定] の順にクリックします。
4. チェックボックスをオンにして検索除外を有効にします。
5. [検索除外リスト (ファイル)] を設定するには
   a. ファイルのフルパスまたはディレクトリパスを入力し、[追加] をクリックします。

      注意:

      • ファイル名のみを入力することはできません。
      • 最大 64 のパスを指定できます。次の表の例を参照してください。

パス	詳細	例

ファイルのフルパス	エンドポイント上の特定のファイルを除外します。	• 例 1:
		`/file.log`
		• 例 2:
		`/System/file.log`

ディレクトリパス	特定のフォルダおよびそのサブフォルダにあるすべてのファイルを除外します。	• 例 1:
		`/System/`
		検索から除外されるファイルの例:
		• `/System/file.log`
		• `/System/Library/file.log`
		検索されるファイルの例:
		• `/Applications/file.log`
		• 例 2:
		`/System/Library`
		検索から除外されるファイルの例:
		• `/System/Library/file.log`
		• `/System/Library/Filters/file.log`
		検索されるファイルの例:
		• `/System/file.log`

- フォルダ名の代わりにアスタリスクワイルドカード (*) を使用します。

  次の表の例を参照してください。

パス	ワイルドカードの使用例
ファイルのフルパス	`/Users/Mac/*/file.log` 検索から除外されるファイルの例: • /Users/Mac/Desktop/file.log • /Users/Mac/Movies/file.log 検索されるファイルの例: • /Users/file.log • /Users/Mac/file.log

ディレクトリパス	• 例 1:
	`/Users/Mac/*`
	検索から除外されるファイルの例:
	• /Users/Mac/doc.html
	• /Users/Mac/Documents/doc.html
	• /Users/Mac/Documents/Pics/pic.jpg
	検索されるファイルの例:
	• /Users/doc.html
	• 例 2:
	`/*/Components`
	検索から除外されるファイルの例:
	• /Users/Components/file.log
	• /System/Components/file.log
	検索されるファイルの例:
	• /file.log
	• /Users/file.log
	• /System/Files/file.log

- フォルダ名の部分一致はサポートされていません。たとえば、`/Users/*user/temp` と入力して、「end_user」や「new_user」な

ど、フォルダ名の末尾が「user」であるフォルダ内のファイルを除外することはできません。

b. パスを削除するには、そのパスを選択して [削除] をクリックします。

6. [検索除外リスト (ファイル拡張子)] を設定するには

a. ファイル拡張子をピリオドなしで入力し、[追加] をクリックします。たとえば、`pdf` と入力します。最大 64 のファイル拡張子を指定できます。

b. ファイル拡張子を削除するには、そのファイル拡張子を選択して [削除] をクリックします。

7. エージェントツリーでグループまたはエージェントを選択している場合は、[保存] をクリックすると設定がそのグループまたはエージェントに適用されます。ルートアイコン ( ) を選択した場合は、次のオプションのいずれかを選択します。

- すべてのエージェントに適用:すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェントに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。
- 今後追加されるグループにのみ適用:今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。

検索のキャッシュ設定

検索を実行するたびに、エージェントは変更されたファイルのキャッシュをチェックし、前回のエージェントの起動以降にファイルが変更されたかどうかを確認します。

- ファイルが変更されている場合、エージェントはそのファイルを検索し、検索されたファイルのキャッシュに追加します。
- ファイルが変更されていない場合、エージェントは、そのファイルが検索されたファイルのキャッシュに存在するかどうかを確認します。

- 検索されたファイルのキャッシュに存在する場合、ファイルの検索は省略されます。
- ファイルが検索されたファイルのキャッシュに存在しない場合、エージェントは承認済みファイルのキャッシュを確認します。

注意

承認済みファイルのキャッシュには、Trend Micro Security (for Mac) が信頼できるとみなしたファイルが含まれます。信頼できるファイルとは、一連のバージョンのパターンファイルで検索され、毎回安全であると宣言されたファイル、もしくは長期間未変更のままの安全なファイルです。

  - 承認済みファイルのキャッシュに存在する場合、ファイルの検索は省略されます。
  - ファイルが承認済みファイルのキャッシュに存在しない場合、エージェントはファイルを検索し、それを検索されたファイルのキャッシュに追加します。

検索エンジンまたはパターンファイルが更新されるたびに、キャッシュのすべてまたは一部が消去されます。

検索が頻繁に実行され、多数のファイルがキャッシュに含まれる場合は、検索時間が大幅に短縮されます。

検索の実行頻度が低い場合は、キャッシュ機能を無効にすることをお勧めします。

検索のキャッシュ設定

手動検索キャッシュの詳細については、90 ページの「検索のキャッシュ設定」を参照してください。

手順

1. [エージェント管理] に移動します。

2. エージェントツリーで、ルートアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [設定] > [検索のキャッシュ設定] をクリックします。
4. [手動検索のキャッシュを有効にする] を選択します。
5. エージェントツリーでグループまたはエージェントを選択している場合は、[保存] をクリックすると設定がそのグループまたはエージェントに適用されます。ルートアイコン ( ) を選択した場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用:すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェントに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。
   - 今後追加されるグループにのみ適用:今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。

セキュリティリスク通知とログ

Trend Micro Security (for Mac) には、検出されたセキュリティリスクや発生した大規模感染に関する情報を、管理者と他の Trend Micro Security (for Mac) の管理者に知らせるために、一連の初期設定の通知メッセージが用意されています。

Trend Micro Security (for Mac) では、セキュリティリスクの検出時にログが生成されます。

管理者通知設定の指定

Trend Micro Security (for Mac) の管理者は、セキュリティリスクが検出された場合や大規模感染が発生した場合に、メールで通知を受信できます。

手順

1. [通知] > [一般設定] に移動します。
2. [SMTP サーバ] に、IPv4/IPv6 アドレスまたはエンドポイント名を入力します。
3. 1～65535 の値でポート番号を入力します。
4. [送信元] に送信者のメールアドレスを入力します。
5. [保存] をクリックします。

管理者向けのセキュリティリスクの通知の設定

Trend Micro Security (for Mac) においてセキュリティリスクを検知するか、セキュリティリスクに対する処理が失敗し、管理者の介在を必要とする場合に、通知メッセージを送信するように設定します。

通知はメールで受信できます。Trend Micro Security (for Mac) がメールで通知を正常に送信できるように、管理者通知設定を指定します。詳細については、92 ページの「管理者通知設定の指定」を参照してください。

手順

1. [通知] > [標準通知] に移動します。
2. [条件] タブで、セキュリティリスクが検出されるたびに通知を送信するか、またはセキュリティリスクの処理が失敗した場合にのみ通知を送信するかを指定します。
3. [保存] をクリックします。
4. [メール] タブで、次の操作を行います。
   a. 通知を有効にして、メールで送信されるようにします。
   b. メールの受信者、および初期設定の件名をそのまま使用するか、変更するかを指定します。

      [メッセージ] でデータを表現するには、トークン変数を使用します。

変数	説明
%v	セキュリティリスク名
%s	セキュリティリスクが検出されたエンドポイント
%m	エンドポイントが属しているエージェントツリーグループ
%p	セキュリティリスクの場所
%y	検出の日時

5. [保存] をクリックします。

管理者向けのアウトブレーク通知の設定

大規模感染をセキュリティリスクの検出数と検出期間によって定義します。大規模感染基準を定義したら、管理者とその他の Trend Micro Security (for Mac) の管理者に対して大規模感染について通知するように Trend Micro Security (for Mac) を設定し、早期に対応できるようにします。

通知はメールで受信できます。Trend Micro Security (for Mac) がメールで通知を正常に送信できるように、管理者通知設定を指定します。詳細については、92 ページの「管理者通知設定の指定」を参照してください。

手順

1. [通知] > [アウトブレーク通知] に移動します。
2. [条件] タブで、次の値を指定します。
   - セキュリティリスクの固有ソースの数
   - 検出数
   - 検出期間

ヒント
この画面では初期設定値を使用することを推奨します。

検出数を超えると、Trend Micro Security (for Mac) によって大規模感染が宣言され、通知メッセージが送信されます。たとえば、検出数を 100 と指定すると、Trend Micro Security (for Mac) は、101 番目のセキュリティリスクを検出した後に通知を送信します。

3. [保存] をクリックします。
4. [メール] タブで、次の操作を行います。
   a. 通知を有効にして、メールで送信されるようにします。
   b. メールの受信者、および初期設定の件名をそのまま使用するか、変更するかを指定します。

      [メッセージ] でデータを表現するには、トークン変数を使用します。

変数	説明
%CV	検出されたセキュリティリスクの総数
%CC	セキュリティリスクを含むエンドポイントの総数

5. メールに含める追加情報を選択します。エージェント/グループ名、セキュリティリスク名、パスと感染ファイル、検出日時、および検索結果を含めることができます。
6. [保存] をクリックします。

セキュリティリスクログの表示

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン
   (

) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。

3. [ログ] > [セキュリティリスクログ] をクリックします。
4. ログの基準を指定して [ログを表示] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。
   - セキュリティリスク検出の日時
   - セキュリティリスクが含まれるエンドポイント
   - セキュリティリスク名
   - セキュリティリスクの感染源
   - セキュリティリスクを検出した検索の種類
   - 検出時の処理が正常に実行されたかどうかを示す検索結果。検索結果の詳細については、96 ページの「検索結果」を参照してください。
   - プラットフォーム
6. ログを CSV ファイルに保存するには、[エクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

注意

多数のログをエクスポートする場合は、エクスポートタスクが終了するまで待ちます。エクスポートタスクが終了する前にページを閉じると、.csv ファイルが生成されません。

次に進む前に

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログ削除スケジュールを設定します。ログの管理方法の詳細については、114 ページの「ログの管理」を参照してください。

検索結果

ウイルス/不正プログラムのログには次の検索結果が表示されます。

- 削除
  - 1 次処理は削除で、感染ファイルが削除されました。
  - 1 次処理は駆除ですが、駆除は失敗しました。2 次処理は削除で、感染ファイルが削除されました。
- 隔離
  - 1 次処理は隔離で、感染ファイルが隔離されました。
  - 1 次処理は駆除ですが、駆除は失敗しました。2 次処理は隔離で、感染ファイルが隔離されました。
- 駆除

  感染ファイルが駆除されました。
- 放置
  - 1 次処理は放置です。Trend Micro Security (for Mac) は、感染ファイルに何も処理を実行しませんでした。
  - 1 次処理は駆除ですが、駆除は失敗しました。2 次処理は放置のため、Trend Micro Security (for Mac) は感染ファイルに何も処理を実行しませんでした。
- ファイルのウイルスを駆除、またはファイルを隔離できません。

  駆除が 1 次処理で、隔離が 2 次処理ですが、両方の処理が失敗しました。

  解決策: 以下の「ファイルを隔離できません。」を参照してください。
- ファイルのウイルスを駆除、またはファイルを削除できません。

  駆除が 1 次処理で、削除が 2 次処理ですが、両方の処理が失敗しました。

  解決策: 以下の「ファイルを削除できません。」を参照してください。
- ファイルを隔離できません。

  感染ファイルは、別のアプリケーションによりロックされているか、実行中か、または CD 内にあります。使用しているアプリケーションがファイルを解放した後かそのファイルが実行された後に、Trend Micro Security (for Mac) はそのファイルを隔離します。

解決策:

CD 内に感染したファイルがある場合、そのウイルスがネットワーク上の他のエンドポイントに感染する可能性があるので、その CD は使用しないことを検討してください。

- ファイルを削除できません。

  感染ファイルは、別のアプリケーションによりロックされているか、実行中か、または CD 内にあります。使用しているアプリケーションがファイルを解放した後かそのファイルが実行された後に、Trend Micro Security (for Mac) はそのファイルを削除します。

  解決策:

  CD 内に感染したファイルがある場合、そのウイルスがネットワーク上の他のエンドポイントに感染する可能性があるので、その CD は使用しないことを検討してください。

- ファイルのウイルスを駆除できません。

  このファイルのウイルスは駆除できない可能性があります。解決策と詳細については、98 ページの「駆除できないファイル」を参照してください。

駆除できないファイル

ウイルス検索エンジンは、以下のファイルを駆除できません。

駆除できないファイル	説明と解決策
ワームに感染したファイル	コンピュータワームは自己完結型のプログラム (複数の場合あり) で、自体の一部または全部をコピーすることで機能を他のエンドポイントシステムに拡散します。通常、ネットワーク接続またはメールの添付ファイルを通じて伝播されます。ワームは、自己完結型のプログラムであるため駆除できません。 解決策: トレンドマイクロはワームを削除することを推奨します。
書き込み保護された感染ファイル	解決策: 書き込み保護を解除して、セキュリティエージェントがファイルを駆除できるようにします。

駆除できないファイル	説明と解決策
パスワードで保護されたファイル	パスワードで保護されたファイルまたは圧縮ファイルが含まれます。 解決策: パスワード保護を解除して、セキュリティエージェントがこれらのファイルを駆除できるようにします。
バックアップファイル	RB0～RB9 の拡張子が付いたファイルは、感染したファイルのバックアップコピーです。セキュリティエージェントでは、駆除プロセス中にウイルス/不正プログラムによってファイルが破損した場合、感染ファイルのバックアップを作成します。 解決策: セキュリティエージェントが感染ファイルを正常に駆除した場合は、バックアップコピーを保持する必要はありません。エンドポイントが正常に動作すれば、バックアップファイルを削除できます。

第 7 章

Web ベースの脅威からのエンドポイントの保護

この章では、Web ベースの脅威について、および Trend Micro Security (for Mac) を使用して Web ベースの脅威からネットワークとエンドポイントを保護する方法について説明します。

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、感染したエンドポイント上ではなく 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。

かつてのハッカー、ウイルス作成者、スパムメール送信者、スパイウェア作成者は、昨今ではサイバー犯罪者と呼ばれています。このような犯罪者は Web からの脅威を 2 つの目的のために利用します。第一の目的は、営利目的のために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、感染したエンドポイントは、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として利用される場合もあります。さらに、この脅威により Web 上の商取引での信用を喪失し、インターネット上のビジネスの前提となる信頼関係が崩壊してしまう危険性もあります。第二の目的は、ユーザの CPU の処理能力を奪って金儲け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クリック型課金によるスパムメールの送信や支払いの強要などがあります。

Web レピュテーション

Web レピュテーションテクノロジは、Web サイトの経過期間、場所の変更の履歴、および不正プログラムの動作分析により発見される疑わしい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採点することで、Web ドメインの信頼性を追跡します。これにより継続的にサイトを検索し、感染した Web サイトにユーザがアクセスするのを防ぎます。

エージェントは、Smart Protection ソースにクエリを送信して、ユーザがアクセスしようとしている Web サイトのレピュテーションを確認します。Web サイトのレピュテーションは、エンドポイントに適用される特定の Web レピュテーションポリシーに関連付けられています。使用しているポリシーに応じて、Web サイトへのアクセスがブロックまたは許可されます。

注意

この機能は、2014 年 4 月時点でリリースされている最新の Safari™、Mozilla™ Firefox™、Google Chrome™ブラウザをサポートします。

Web レピュテーションの設定

Web レピュテーション設定には、Trend Micro Security (for Mac)が Web サイトへのアクセスをブロックするか許可するかを指定するポリシーが含まれます。Trend Micro Security (for Mac)は、使用する適切なポリシーを決定するために、エージェントの位置をチェックします。エージェントが Trend Micro Security (for Mac)サーバに接続できる場合、そのエージェントの位置は「内部」になります。サーバに接続できない場合、エージェントの場所は「外部」です。

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [設定] > [Web レピュテーション設定] の順にクリックします。
4. 外部エージェントのポリシーを設定するには
   a. [外部エージェント] タブをクリックします。
   b. [Web レピュテーションポリシーを有効にする] を選択します。

      ポリシーが有効になると、外部エージェントは Web レピュテーションクエリを Trend Micro Smart Protection Network に送信します。

      注意

      セキュリティエージェントに IPv6 アドレスのみが割り当てられている場合は、Web レピュテーションクエリにおける IPv6 の制限事項について、135 ページの「IPv6 シングルスタックエージェントの制限事項」を参照してください。

c. 使用可能な Web レピュテーションのセキュリティレベルから [高]、[中]、または [低] を選択します。

注意

Trend Micro Security (for Mac)は、セキュリティレベルに従って URL へのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを [低] に設定した場合、Trend Micro Security (for Mac)は Web からの脅威であるとわかっている URL だけをブロックします。セキュリティレベルを高くするほど、Web 脅威の検出率は高くなりますが、誤検出の可能性も高くなります。

d. Web レピュテーションのフィードバックを送信するには、表示されている URL をクリックします。トレンドマイクロの Web レピュテーションクエリシステムがブラウザウィンドウに表示されます。

5. 内部エージェントのポリシーを設定するには

a. [内部エージェント] タブをクリックします。

b. [Web レピュテーションポリシーを有効にする] を選択します。

ポリシーが有効になると、内部エージェントは Web レピュテーションクエリを以下のいずれかかの場所に送信します。

- [Smart Protection Server にクエリを送信する] オプションが有効な場合は、Smart Protection Server。
- [Smart Protection Server にクエリを送信する] オプションが無効な場合は、Trend Micro Smart Protection Network。

注意

セキュリティエージェントに IPv6 アドレスのみが割り当てられている場合は、Web レピュテーションクエリにおける IPv6 の制限事項について、135 ページの「IPv6 シングルスタックエージェントの制限事項」を参照してください。

c. 使用可能な Web レピュテーションのセキュリティレベルから [高]、[中]、または [低] を選択します。

注意

Trend Micro Security (for Mac)は、セキュリティレベルに従って URL へのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを [低] に設定した場合、Trend Micro Security (for Mac)は Web からの脅威であるとわかっている URL だけをブロックします。セキュリティレベルを高くするほど、Web 脅威の検出率は高くなりますが、誤検出の可能性も高くなります。

エージェントは、セキュリティレベルに関係なく、未テストの Web サイトをブロックしません。

d. Web レピュテーションのフィードバックを送信するには、表示されている URL をクリックします。トレンドマイクロの Web レピュテーションクエリシステムがブラウザウィンドウに表示されます。

e. エージェントに、Web レピュテーションログのサーバへの送信を許可するかどうかを選択します。Trend Micro Security (for Mac)によってブロックされた URL を解析し、アクセスしても安全だと考えられる URL を適切に処理する場合には、エージェントによるログの送信を許可します。

6. エージェントツリーでグループまたはエージェントを選択している場合は、[保存] をクリックすると設定がそのグループまたはエージェントに適用されます。ルートアイコン ( ) を選択した場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用:すべての既存のエージェント、および既存または今後追加されるグループに加えられる新しいエージェントに、設定を適用します。今後追加されるグループとは、設定を指定した時点で作成されていないグループのことです。
   - 今後追加されるグループにのみ適用: 今後追加されるグループに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のグループに加えられる新しいエージェントには設定を適用しません。

承認済み URL リストの設定

承認済み URL により、Web レピュテーションポリシーが回避されます。これらの URL は、Web レピュテーションポリシーでブロックするよう設定しても、Trend Micro Security (for Mac) ではブロックされません。安全であることが判明している URL を承認済み URL リストに追加します。

手順

1. [管理] > [Web レピュテーションの承認済み URL リスト] に移動します。
2. テキストボックスに URL を指定します。ワイルドカード文字 (*) は URL の任意の位置に追加できます。

   例:

   - `www.trendmicro.com/*`は、www.trendmicro.com ドメインにあるすべてのページを指定します。
   - `*.trendmicro.com/*`は、trendmicro.com のいずれかのサブドメインのすべてのページを指定します。

   IP アドレスを含む URL を入力できます。URL に IPv6 アドレスが含まれる場合は、アドレスを角括弧で囲みます。
3. [追加] をクリックします。
4. エントリを削除するには、承認済み URL の横にあるアイコンをクリックします。
5. [保存] をクリックします。

Web レピュテーションログの表示

始める前に

サーバに Web レピュテーションログを送信するように、内部エージェントを設定します。Trend Micro Security (for Mac) によってブロックされた URL

を解析し、アクセスしても安全だと考えられる URL を適切に処理する場合には、この設定を実行します。

手順

1. [エージェント管理] に移動します。
2. エージェントツリーで、ルートアイコン
   (

) をクリックしてすべてのエージェントを含めるか、特定のグループまたはエージェントを選択します。
3. [ログ] > [Web レピュテーションログ] をクリックします。
4. ログの基準を指定して [ログを表示] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。
   - Trend Micro Security (for Mac) が URL をブロックした日時
   - ユーザが URL へのアクセスに使用したエンドポイント
   - ブロックされた URL
   - URL の危険度
   - ブロックされた URL に関する詳細情報を提供する Trend Micro Web Reputation Query システムへのリンク
6. ログを CSV ファイルに保存するには、[エクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

   注意

   多数のログをエクスポートする場合は、エクスポートタスクが終了するまで待ちます。エクスポートタスクが終了する前にページを閉じると、.csv ファイルが生成されません。

次に進む前に

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログ削除スケジュールを設定します。

ログの管理方法の詳細については、114 ページの「ログの管理」を参照してください。

第 8 章

サーバおよびエージェントの管理

この章では、Trend Micro Security (for Mac) サーバおよびエージェントの管理と追加の設定について説明します。

サーバおよびエージェントのアップグレード

プラグインマネージャのコンソールには、Trend Micro Security (for Mac) の新しいビルドまたはバージョンが表示されます。

新しいビルドまたはバージョンが利用可能になった場合は、すぐにサーバとエージェントをアップグレードします。

アップグレードする前に、サーバおよびエージェントに 22 ページの「サーバのインストール要件」および 48 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」で説明されているリソースがあることを確認してください。

サーバのアップグレード

始める前に

トレンドマイクロでは、アップグレードで問題が発生した場合に復元できるように、サーバのプログラムファイルとデータベースをバックアップすることをお勧めします。

- プログラムファイル
  - 初期設定のパス:

    ```
    C:¥Program Files¥Trend Micro¥Security Server¥Addon¥TMSM
    ```

    または

    ```
    C:¥Program Files (x86)¥Trend Micro¥Security Server¥Addon¥TMSM
    ```

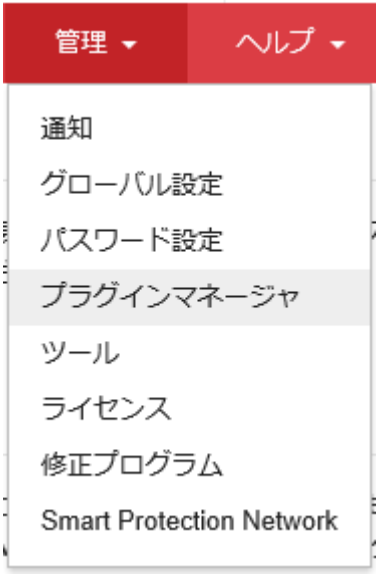
  - バックアップするファイル:
    - ..¥apache-activemq¥conf¥activemq.xml
    - ..¥apache-activemq¥conf¥broker.pem
    - ..¥apache-activemq¥conf¥broker.ks
    - ..¥apache-activemq¥bin¥win32¥wrapper.conf
    - ..¥apache-activemq¥bin¥win64¥wrapper.conf

- ..¥ServerInfo.plist

- データベースファイル。116 ページの「サーバデータベースのバックアップ」を参照してください。

手順

1. ウイルスバスター ビジネスセキュリティの Web コンソールを開いて、メインメニューの [オプション設定] > [プラグイン] をクリックします。

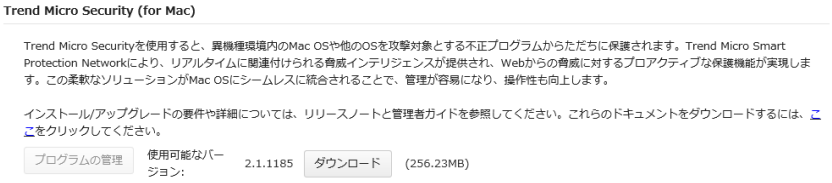


2. [Trend Micro Security (for Mac)] セクションに移動して、[ダウンロード] をクリックします。

   ダウンロードするファイルのサイズが [ダウンロード] ボタンの横に表示されます。

   プラグインマネージャにより、パッケージが <ウイルスバスター 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¥Download¥Product にダウンロードされます。

<ウイルスバスター 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。



3. ダウンロードの進行状況を確認します。

   ダウンロード中は、この画面以外にも移動できます。

   パッケージのダウンロード中に問題が発生した場合は、ウイルスバスター ビジネスセキュリティの Web コンソールでサーバアップデートログを確認してください。メインメニューで、[レポート] > [ログクエリ] をクリックします。

4. Trend Micro Security (for Mac) をただちにアップグレードするには、[今すぐアップグレード] をクリックします。後でアップグレードする場合は、次の手順を実行します。

   a. [後でアップグレード] をクリックします。

   b. [プラグインマネージャ] 画面を開きます。

   c. [Trend Micro Security (for Mac)] セクションに移動して、[アップグレード] をクリックします。

5. アップグレードの進行状況を確認します。アップグレード後に、[プラグインマネージャ] 画面が再ロードされます。

エージェントのアップグレード

手順

1. 次のいずれかの手順を実行します。

   - 手動アップデートを実行します。コンポーネントの一覧で [ビジネスセキュリティクライアント] を選択していることを確認してください。
   - エージェントツリーで、アップグレードするエージェントを選択し、[タスク] > [アップデート] をクリックします。
   - 予約アップデートが有効な場合は、[ビジネスセキュリティクライアント] が選択されていることを確認します。
   - エージェントコンソールから [アップデート] をクリックするようユーザに指示します。

   通知を受信するセキュリティエージェントがアップグレードを開始します。エンドポイントでは、メニューバー上の Trend Micro Security (for Mac) アイコンによって、製品がアップデートされていることが示されます。アップグレードが完了するまで、ユーザはコンソールからいずれのタスクも実行することはできません。

2. アップグレードのステータスを確認します。

   a. メインメニューで [概要] をクリックし、[エージェント] セクションに移動します。

   b. [旧版] 列の下にあるリンクをクリックします。エージェントツリーが表示され、アップグレードされていないセキュリティエージェントがすべて示されます。

   c. アップグレードされていないセキュリティエージェントをアップグレードするには、[タスク] > [アップデート] をクリックします。

ログの管理

Trend Micro Security (for Mac) では、セキュリティリスクの検出とブロックされた URL に関する包括的なログが保持されます。これらのログを使用して、組織の保護ポリシーを評価し、感染や攻撃のリスクが高いエージェントを特定します。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、Web コンソールで手動でログを削除するか、またはログの削除スケジュールを設定します。

手順

1. [管理] > [ログ管理] に移動します。
2. [ログの自動削除を有効にする] を選択します。
3. すべてのログを削除するか、特定の日数より古いログのみを削除するかを選択します。
4. ログを削除する頻度と時刻を指定します。
5. [保存] をクリックします。

ライセンスの管理

ウイルスバスター ビジネスセキュリティサーバの以前のバージョンでは、Trend Micro Security (for Mac) とは別のライセンスが使用されていました。ウイルスバスター ビジネスセキュリティ 9 以降のウイルスバスター ビジネスセキュリティサーバと Trend Micro Security (for Mac) では同じライセンスが使用されます。Trend Micro Security (for Mac) は、照会されるとウイルスバスター ビジネスセキュリティサーバのライセンスを自動的に取得します。

製品ライセンスのステータスによって、ユーザが利用できる機能が決まります。詳細は次の表を参照してください。

ライセンスの種類とステータス	機能			
	リアルタイム検索	手動検索/予約検索	Web レピュテーション	パターンファイル更新
製品版、アクティベーション完了	有効	有効	有効	有効
体験版、アクティベーション完了	有効	有効	有効	有効
製品版、サポート契約終了	有効	有効	無効	無効
体験版、サポート契約終了	無効	無効	無効	無効
アクティベーション未完了	無効	無効	無効	無効

注意

サーバに IPv6 アドレスのみが割り当てられている場合は、ライセンスのアップデートにおける IPv6 の制限事項について、135 ページの「IPv6 シングルスタックサーバの制限事項」を参照してください。

手順

1. [管理] > [製品ライセンス] に移動します。
2. ライセンス情報を表示します。最新のライセンス情報を取得するには、[ステータスをオンラインで確認] をクリックします。

   ライセンス情報のセクションには次の詳細が表示されます。

   - ステータス: [アクティベーション完了] または [サポート契約終了] のいずれかが表示されます。
   - バージョン: [製品版] または [体験版] バージョンのいずれかが表示されます。体験版を使用している場合は、いつでも製品版にアップグレードできます。アップグレードの手順については、[製品のライセンスアップグレードについて] をクリックしてください。

- ライセンス有効期限: ライセンスの有効期限日。
- アクティベーションコード: ライセンスのアクティベーションに使用するコード。

サーバデータベースのバックアップ

手順

1. Microsoft 管理コンソールから次のサービスを停止します。
   - ActiveMQ for Trend Micro Security
   - Trend Micro Security for (Mac)
2. SQL Server Management Studio を開きます (例: Windows の [スタート] メニュー > [すべてのプログラム] > [Microsoft SQL Server {バージョン}] > [SQL Server Management Studio])。
3. `db_TMSM` を検索し、SQL Server Management Studio の [バックアップ] 機能を使用してデータベースファイルをバックアップします。

   詳細については、SQL Server Management Studio のドキュメントを参照してください。
4. 停止中のサービスを開始します。

サーバデータベースの復元

始める前に

バックアップ時に作成されたデータベースファイルのバックアップを用意します。詳細については、116 ページの「サーバデータベースのバックアップ」を参照してください。

手順

1. Microsoft 管理コンソールから次のサービスを停止します。
   - ActiveMQ for Trend Micro Security
   - Trend Micro Security for (Mac)
2. SQL Server Management Studio を開きます (例: Windows の [スタート] メニュー > [すべてのプログラム] > [Microsoft SQL Server {バージョン}] > [SQL Server Management Studio])。
3. `db_TMSM` を検索し、SQL Server Management Studio の [デタッチ] オプションを使用して現在のデータベースファイルをデタッチします。

   詳細については、SQL Server Management Studio のドキュメントを参照してください。
4. データベースファイルのバックアップをアタッチするには、[アタッチ] オプションを使用します。
5. 停止中のサービスを開始します。

エージェント/サーバ間の通信の設定

セキュリティエージェントでは、それらのエージェントを管理するサーバが、サーバの名前または IPv4/IPv6 アドレスによって識別されます。Trend Micro Security (for Mac) サーバのインストール時に、インストーラによってサーバコンピュータの IP アドレスが識別され、[エージェント/サーバ間の通信] 画面に表示されます。

サーバはセキュリティエージェントと待機ポートを通じて通信します。初期設定ではポート番号は 61617 です。

注意

- このポート番号を変更する場合は、他のアプリケーションとの競合やエージェント/サーバ間の通信に関する問題が発生しないように、そのポートが現在使用されていないことを確認してください。
- ファイアウォールアプリケーションがサーバコンピュータで使用されている場合は、待機ポートを通じてエージェント/サーバ間の通信がファイアウォールによってブロックされないようにします。たとえば、エンドポイントでウイルスバスター 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有効になっている場合は、待機ポートでトラフィックの送受信を許可する除外設定をポリシーに追加してください。
- サーバにプロキシサーバ経由で接続するようにセキュリティエージェントを設定できます。ただし、プロキシサーバは通常、企業ネットワーク内のエージェント/サーバ間の通信には必要ありません。
- 既存のサーバ名および IPv4/IPv6 アドレスすべてをアップデートまたは置換するか、待機ポートまたはプロキシ設定を変更する計画がある場合は、セキュリティエージェントをインストールする前に行ってください。trend_client_program_plural をインストールした後に変更を行うと、セキュリティエージェントからサーバへの接続が切断されます。接続を再確立するには、セキュリティエージェントを再インストールするしか方法はありません。

手順

1. [管理] > [エージェント/サーバ間の通信] に移動します。
2. [サーバ名と待機ポート] で、サーバの名前または IPv4/IPv6 アドレス、および待機ポートを入力します。

   注意

   [サーバ名/IP アドレス] に複数のエントリがある場合、セキュリティエージェントはランダムにエントリを選択します。すべてのエントリでエージェント/サーバ間の通信を確立できることを確認してください。

3. [プロキシ設定] で、セキュリティエージェントからサーバにプロキシサーバ経由で接続するかどうかを選択します。
   a. プロキシサーバプロトコルを選択します。

b. プロキシサーバの名前または IPv4/IPv6 アドレス、およびポート番号を入力します。

c. プロキシサーバに認証が必要な場合、所定のフィールドにユーザ名とパスワードを入力します。

4. [保存] をクリックします。

5. 設定を適用するために Trend Micro Security (for Mac) のサービスを再起動するよう求められたら、次の手順を実行します。

a. <サーバのインストールフォルダ> に移動します。

b. `restart_TMSM.bat` をダブルクリックします。

c. すべてのサービスが再起動されるまで待ちます。

セキュリティエージェントのアイコン

エンドポイントのタスクトレイおよびメインコンソールに表示されるアイコンは、セキュリティエージェントのステータスと実行中のタスクを示しています。

トレイアイコン	メニューアイコン	説明
		エージェントは稼働中で、上位サーバに接続しています。
		製品ライセンスはアクティベートされています。
		エージェントは稼働中ですが、上位サーバから接続を切断しています。
		利用できる新しいコンポーネントバージョンがあります。速やかにエージェントをアップデートします。
		コンピュータを再起動して解決する必要があるセキュリティ脅威がエージェントによって検出されました。
		エージェントはセキュリティリスクを検索中で、上位サーバに接続しています。
		エージェントは、上位サーバからコンポーネントをアップデートしています。

トレイアイコン	メニューアイコン	説明
		コンポーネントアップデートのインストールを完了するためには、エージェントを再起動する必要があります。
		エージェントは上位サーバに登録されていますが、製品ライセンスがアクティベートされていません。ライセンスがアクティベートされていない場合、エージェント機能の一部を使用できません。 詳細については、114 ページの「ライセンスの管理」を参照してください。
		エージェントは上位サーバに登録されていません。製品ライセンスは、アクティベートされている場合とアクティベートされていない場合の両方の可能性があります。 エージェントが上位サーバに登録されてない場合は、次のようになります。
		製品ライセンス (製品版または体験版) はアクティベートされていますが、期限が切れています。ライセンスの期限が切れている場合、エージェント機能の一部を使用できません。
		サポートされていないプラットフォームにエージェントがインストールされました。
		エージェントが正常に機能していません。エージェントを最新リリースにアップグレードするか、テクニカルサポートに問い合わせてください。
		エージェントが検索を完了したか、セキュリティ脅威を検出しました。

第 9 章

サポート情報

この章では、発生する可能性のある問題のトラブルシューティングと、サポートへの連絡方法について説明します。

トラブルシューティング

Web コンソールへのアクセス

問題:

Web コンソールにアクセスできません。

手順

1. エンドポイントが、Trend Micro Security (for Mac) サーバのインストールおよび実行に必要な要件を満たしていることを確認します。

   詳細については、22 ページの「サーバのインストール要件」を参照してください。

2. 次のサービスが起動されていることを確認します。

   - ActiveMQ for Trend Micro Security (for Mac)
   - トレンドマイクロ プラグインマネージャ
   - SQL Server (TMSM)
   - Trend Micro Security (for Mac)

3. デバッグログを収集します。ログで検索を実行するときは、「error」や「fail」をキーワードとして使用します。

   - インストールログ: `C:¥TMSM*.log`
   - 一般的なデバッグログ: <サーバのインストールフォルダ>`\debug.log`
   - ウイルスバスター ビジネスセキュリティのデバッグログ: `C:¥Program Files¥Trend Micro¥Security Server¥PCCSRV¥Log¥ofcdebug.log`

     a. ファイルが存在しない場合は、デバッグログを有効にします。ウイルスバスター ビジネスセキュリティ Web コンソールのバナーで、「Trend Micro」の「M」をクリックして、デバッグログ設定を指定し、[保存] をクリックします。

b. Web コンソールへのアクセスに関する問題の発生に至ったプロセスを再現します。

c. デバッグログを取得します。

4. HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥TrendMicro¥TMSM に移動して、Trend Micro Security (for Mac) のレジストリキーを確認します。

5. データベースファイルとレジストリキーを確認します。

   a. C:¥Program Files¥Microsoft SQL Server¥MSSQL.x¥MSSQL¥Data¥または C:¥Program Files(x86)¥Microsoft SQL Server ¥MSSQL.x¥MSSQL¥Data¥に、次のファイルが存在することを確認します。

      - db_TMSM.mdf
      - db_TMSM_log.LDF

   b. Microsoft SQL Server のレジストリキーに、Trend Micro Security (for Mac) のデータベースのインスタンスが存在することを確認します。

      - HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Microsoft SQL Server¥TMSM
      - HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Microsoft SQL Server¥ TMSM¥ MSSQLServer¥CurrentVersion

6. 次の項目をトレンドマイクロに送信してください。

   - レジストリファイル

     a. HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Microsoft SQL server¥TMSM に移動します。

     b. [ファイル] > [エクスポート] をクリックして、レジストリキーを .reg ファイルに保存します。

   - サーバコンピュータに関する情報

     - OS とバージョン
     - ハードディスク空き容量

- RAM 空き容量
- 侵入防御ファイアウォールなどその他のプラグインプログラムがインストールされているかどうか。

7. Trend Micro Security (for Mac) サービスを再起動します。
   a. <サーバのインストールフォルダ> に移動します。
   b. `restart_TMSM.bat` をダブルクリックします。
   c. すべてのサービスが再起動されるまで待ちます。
8. Trend Micro Security (for Mac) サービスは常に実行されている必要があります。このサービスが実行されていないと、ActiveMQ サービスに関する問題が発生する可能性があります。
   a. `C:¥Program Files¥Trend Micro¥Security Server¥Addon¥TMSM ¥apache-activemq¥data¥*.*`の ActiveMQ データのバックアップを作成します。
   b. ActiveMQ データを削除します。
   c. `restart_TMSM.bat` をダブルクリックして、Trend Micro Security (for Mac) サービスを再起動します。
   d. Web コンソールに再度アクセスしてみて、アクセスの問題が解決されているかどうかを確認します。

サーバのアンインストール

問題:

次のメッセージが表示されます。

プラグインプログラムをアンインストールできません。プラグインプログラムのアンインストールコマンドがレジストリキーにありません。

手順

1. レジストリエディタを開いて、HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥OfficeScan¥service¥AoS¥OSCE_Addon_Service_CompList_Version に移動します。
2. 値を 1.0.1000 にリセットします。
3. プラグインプログラムのレジストリキーを削除します (例: HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥OfficeScan¥service¥AoS¥OSCE_ADDON_xxxx)。
4. トレンドマイクロ プラグインマネージャサービスを再起動します。
5. プラグインプログラムをダウンロードしてインストールしてから、アンインストールします。

エージェントのインストール

問題:

インストールに失敗しました。インストールパッケージ (tmsminstall.zip) が Mac 標準以外のアーカイブツール、またはコマンドラインツールで「unzip」などのサポートされていないコマンドを使用して起動されたため、解凍されたフォルダ (tmsminstall) が破損しました。

手順

1. 解凍されたフォルダ (tmsminstall) を削除します。
2. アーカイブユーティリティなどの Mac 標準のアーカイブツールを使用してインストールパッケージを再度起動します。

   次のコマンドを使用して、コマンドラインからパッケージを起動することもできます。

   - ditto -xk <tmsminstall.zip ファイルのパス> <インストール先フォルダ>

     次に例を示します。

```
ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/
Desktop
```

エージェントの一般的なエラー

問題:

セキュリティエージェントでエラーまたは問題が発生しました。

手順

1. <エージェントのインストールフォルダ>/Tools を開き、Trend Micro デバッグマネージャを起動します。
2. ツールの画面に表示される指示に従って正常にデータを収集します。

警告!

ユーザがツールをエンドポイントの別の場所に移動した場合、ツールは動作しません。ツールが移動された場合は、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、インストールします。

ツールが別の場所にコピーされた場合は、コピーされたツールを削除して、元の場所からツールを実行します。

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。

- 129 ページの「トラブルシューティングのリソース」
- 129 ページの「製品サポート情報」
- 130 ページの「トレンドマイクロへのウイルス解析依頼」
- 132 ページの「その他のリソース」

トラブルシューティングのリソース

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

サポートポータルの利用

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

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

脅威データベース

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

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

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

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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

注意

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

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/ 駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

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

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

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

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

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

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

メールレピュテーションについて

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

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

Web レピュテーションについて

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

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

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

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

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

注意

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

脅威解析・サポートセンター TrendLabs (トレンドラボ)

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

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

付録 A

Trend Micro Security (for Mac) での IPv6 サポート

この付録では、IPv6 アドレスをサポートする環境に Trend Micro Security (for Mac) を導入する場合に必要な内容について説明します。この付録には、Trend Micro Security (for Mac) での IPv6 サポートに関する情報が含まれています。

IPv6 の概念、および IPv6 アドレスをサポートするネットワークの設定に関連するタスクに詳しいユーザを対象としています。

Trend Micro Security (for Mac) サーバおよびエージェントの IPv6 サポート

Trend Micro Security (for Mac) の IPv6 サポートはバージョン 2.0 から開始されました。以前のバージョンの Trend Micro Security (for Mac) は、IPv6 アドレスをサポートしていません。IPv6 のサポートは、IPv6 要件を満たす Trend Micro Security (for Mac) サーバおよび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。

Trend Micro Security (for Mac) サーバの IPv6 要件

Trend Micro Security (for Mac) サーバは、IPv6 をサポートするウイルスバスター ビジネスセキュリティサーババージョンと一緒にインストールする必要があります。

ウイルスバスター ビジネスセキュリティでの IPv6 サポートは、バージョン 8.0 から開始されました。Trend Micro Security (for Mac) と互換性のある以前のバージョンのウイルスバスター ビジネスセキュリティ (22 ページの「サーバのインストール要件」を参照) では、IPv6 アドレスがサポートされていません。

IPv6 サポートの詳細については、ウイルスバスター ビジネスセキュリティ 9.5 以降のドキュメントを参照してください。

Trend Micro Security (for Mac) エージェントの IPv6 要件

Trend Micro Security (for Mac) エージェントでサポートされるすべての Mac OS X バージョンでは、IPv6 もサポートされます。

接続先の一部のエンティティでは IPv4 アドレス指定しかサポートされないため、エージェントに IPv4 と IPv6 の両方のアドレスを割り当てることをお勧めします。

IPv6 シングルスタックサーバの制限事項

次の表は、Trend Micro Security (for Mac) サーバに IPv6 アドレスのみが割り当てられている場合の制限事項を示しています。

表 A-1. IPv6 シングルスタックサーバの制限事項

項目	制限事項
エージェント管理	IPv6 シングルスタックサーバでは IPv4 シングルスタックエージェントを管理できません。
アップデートと一元管理	IPv6 シングルスタックサーバは、次のような IPv4 シングルスタックのアップデート元からアップデートしたり、IPv4 シングルスタックの一元管理製品にレポートを送信したりすることはできません。 ・ トレンドマイクロのアップデートサーバ ・ 任意の IPv4 シングルスタックのカスタムアップデート元
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では、トレンドマイクロのオンライン登録サーバに接続して製品を登録したり、ライセンスを取得したり、ライセンスをアクティベート/更新したりすることはできません。
プロキシ接続	IPv6 シングルスタックサーバは、IPv4 シングルスタックプロキシサーバ経由で接続することはできません。

これらの制限事項のほとんどは、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克服できます。Trend Micro Security (for Mac) サーバと、その接続先またはサービスの提供先となるエンティティとの間にプロキシサーバを配置します。

IPv6 シングルスタックエージェントの制限事項

次の表は、エージェントに IPv6 アドレスのみが割り当てられている場合の制限事項を示しています。

表 A-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
上位サーバ	IPv6 シングルスタックエージェントを IPv4 シングルスタックサーバで管理することはできません。
アップデート	IPv6 シングルスタックエージェントを、次のような IPv4 シングルスタックのアップデート元からアップデートすることはできません。 • 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 Trend Micro Security (for Mac) サーバ
Web レピュテーションクエリ	IPv6 シングルスタックエージェントは、Web レピュテーションクエリを Trend Micro Smart Protection Network に送信できません。
プロキシ接続	IPv6 シングルスタックエージェントは、IPv4 シングルスタックプロキシサーバ経由で接続することはできません。
エージェント配信	Apple Remote Desktop は、エージェントを IPv6 シングルスタックエンドポイントに配信できません。こうしたエンドポイントは常にオフラインと表示されるためです。

これらの制限事項のほとんどは、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克服できます。エージェントと接続先のエンティティとの間にプロキシサーバを配置してください。

IPv6 アドレスの設定

Web コンソールを使用すると、IPv6 アドレスまたは IPv6 アドレスの範囲を設定できます。設定上のガイドラインは次のとおりです。

- Trend Micro Security (for Mac) では標準の IPv6 アドレス表記を使用できます。

  次に例を示します。

  ```
  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
```

- 次のようにリンクローカルな IPv6 アドレスを使用することもできます。

```
fe80::210:5aff:feaa:20a2
```

> **警告!**
> リンクローカルな IPv6 アドレスを指定する際には注意してください。Trend Micro Security (for Mac) ではリンクローカルな IPv6 アドレスを使用できますが、状況によっては正しく機能しない場合があります。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にあり、リンクローカルな IPv6 アドレスで識別されている場合、エージェント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 に含まれる場合は、アドレスを角括弧で囲みます。
- IPv6 アドレス範囲では、通常プレフィックスおよびプレフィックスの長さが必要になります。

IP アドレスが表示される画面

エージェントツリーでは、[IPv6 アドレス] 列の下にエージェントの IPv6 アドレスが表示されます。

索引

アルファベット

CPU 使用率, 84
IPv6 のサポート, 134
    制限事項, 135
Smart Protection
    Web レピュテーションサービス, 43
Web からの脅威, 102
Web コンソール, 32
    概要, 32
Web レピュテーション, 102
Web レピュテーションサービス, 43

あ

ウィジェット, 40–42
ウイルス/不正プログラムの検索
    結果, 96
エージェント/サーバ間の通信, 117
エージェントツリー, 35
    一般的なタスク, 35

か

検索条件
    CPU 使用率, 84
    検索対象ファイル, 83
    スケジュール, 84
    ファイルに対するユーザのアクティビティ, 82
検索の種類, 77
コンポーネント, 41

さ

スマートフィードバック, 43

た

トレンドマイクロの推奨設定, 83

は

パフォーマンス制御, 84
プログラム, 41