Trend Micro Apex One™

Patch 14

管理者ガイド

for MAC

※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、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Trend Micro Service One、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro

P/N: APEM149881/231220_JP (2024/1)

プライバシーと個人データの収集に関する規定

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

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

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

重要

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

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

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

目次

はじめに

はじめに 1
Apex One (Mac) ドキュメント 2
対象読者 2
ドキュメントの表記規則 3
用語 3

第 1 章：製品の概要

はじめに 2
本リリースの新機能 2
主な機能 2
Apex One (Mac) サーバ 4
Apex One (Mac) セキュリティエージェント 5

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 8
アップデート元 10
Apex One (Mac) サーバのインストール 11
製品の初回アクティベート 12
サーバでのインストール後のタスクの実行 13
Apex One (Mac) サーバのアンインストール 14

第 3 章：使用開始

使用開始 16
Web コンソール 16
Web コンソールを開く 17
セキュリティの概要 17

エージェントツリー 19
エージェントツリーの一般的なタスク 19
エージェントツリー固有のタスク 20
グループ 22
グループの追加 23
グループまたはセキュリティエージェントの削除 23
グループの名前変更 24
セキュリティエージェントの移動 24
エージェントを別のグループに移動する 24
セキュリティエージェントを別のサーバに移動する .. 25
ウィジェット 26
エージェントの接続状況 (Mac) ウィジェット 26
表として表示される [エージェントの接続状況 (Mac)] ウィジェット 27
円グラフとして表示される [エージェントの接続状況 (Mac)] ウィジェット 28
エージェントのアップデート (Mac) ウィジェット 29
セキュリティリスクの検出 (Mac) ウィジェット 29
Trend Micro Smart Protection 30
スマートフィードバック 33

第 4 章：セキュリティエージェントのインストール

エージェントのインストール要件 36
エージェントのインストール方法と設定ファイル 37
1 つのエンドポイントへのインストール 39
エージェントのインストール後のタスク 46
エージェントのアンインストール 52

第 5 章：最新の保護状態の維持

コンポーネント 56
アップデートの概要 57
サーバアップデート 58
サーバアップデート元の設定 59

サーバアップデート用のプロキシ設定の指定 60
サーバのアップデート方法 61
サーバのアップデートの予約 61
サーバの手動アップデート 62
エージェントのアップデート 62
エージェントの自動アップデート設定 65
エージェントのアップデートの設定 66
[概要] 画面からのエージェントアップデートの起動 67
[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 68

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 70
ウイルスと不正プログラム 70
スパイウェアとグレーウェア 72
検索方法の種類 73
初期設定の検索方法 73
検索方法の比較 73
検索方法の変更 74
スマートスキャンから従来型スキャンへの切り替え 75
従来型スキャンからスマートスキャンへの切り替え 76
検索の種類 79
リアルタイム検索 80
リアルタイム検索の設定 80
リアルタイム検索: [対象] タブ 81
リアルタイム検索: [処理] タブ 82
手動検索 83
手動検索の設定 83
手動検索: [対象] タブ 84
手動検索: [処理] タブ 86
予約検索 86
予約検索の設定 87
予約検索: [対象] タブ 88
予約検索: [処理] タブ 89
検索開始 92
検索開始の実行 92

サポートされる圧縮ファイルの種類 92
検出時の処理 93
検索除外 95
検索除外リスト設定 96
検索のキャッシュ設定 99
検索のキャッシュ設定 100
信頼済みプログラムリスト 101
信頼済みプログラムリストの設定 102
検索ログの表示 103
セキュリティリスク通知とログ 104
管理者通知設定の指定 104
管理者向けのセキュリティリスクの通知の設定 105
管理者向けのアウトブレーク通知の設定 106
セキュリティリスクログの表示 107
検索結果 108
駆除できないファイル 110
セキュリティリスクの検出数のリセット 111

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 114
Web レピュテーション 114
Web レピュテーションの設定 115
承認済み URL リストと URL ブロックリストの設定 118
Web レピュテーションログの表示 119

第 8 章：デバイスコントロールの使用

デバイスコントロール 122
ストレージデバイスに対する権限 122
デバイスコントロールの設定 123
デバイスリストツール 125
デバイスリストツールの実行 125

セキュリティエージェント向けのデバイスコントロール通知の設定 126
デバイスコントロールログの表示 127

第 9 章：サーバおよびセキュリティエージェントの管理

権限とその他の設定 130
エージェントセルフプロテクションの設定 130
ソフトウェア安全性評価サービスの有効化 131
機械学習型検索の有効化 132
サーバおよびセキュリティエージェントのアップグレード ... 133
サーバのアップグレード 133
セキュリティエージェントのアップグレード 135
ログの管理 136
ライセンスの管理 136
サーバデータベースのバックアップ 138
サーバデータベースの復元 139
本リリースでの Apex Central および Control Manager の統合 139
キーパフォーマンスインジケータウィジェット 140
サーバ接続設定 140
キーパフォーマンスインジケータの設定 141
ウィジェットの設定 142
エージェント/サーバ間の通信の設定 143
オフラインセキュリティエージェント 145
オフラインセキュリティエージェントの自動削除 145
エージェントのアイコン 146

第 10 章：サポート情報

トラブルシューティング 150
Web コンソールへのアクセス 150
サーバのアンインストール 152

エージェントのインストール 153
エージェント/サーバ間の通信 154
エージェントの一般的なエラー 155

テクニカルサポート 156

トラブルシューティングのリソース 156
サポートポータルの利用 156
脅威データベース 156
製品サポート情報 157
サポートサービスについて 157
トレンドマイクロへのウイルス解析依頼 158
メールレピュテーションについて 158
ファイルレピュテーションについて 158
Web レピュテーションについて 159
その他のリソース 159
最新版ダウンロード 159

付録 A：Apex One (Mac) での IPv6 サポート

Apex One (Mac) サーバおよびセキュリティエージェントの IPv6 サポート 162

Apex One (Mac) セキュリティエージェントの IPv6 要件 162

IPv6 シングルスタックサーバの制限事項 162

IPv6 シングルスタックエージェントの制限事項 163

IPv6 アドレスの設定 164

IP アドレスが表示される画面 165

索引

索引 167

はじめに

はじめに

Apex One (Mac) 管理者ガイドへようこそ。このドキュメントでは、Apex One (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。

Apex One (Mac) ドキュメント

Apex One (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	Apex One (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/dcx/s/?language=ja

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

Apex One (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。

- Apex One (Mac) 管理者: サーバおよびセキュリティエージェントのインストールと管理を含む Apex One (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 Apex One (Mac) 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。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、Apex One (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。

用語

次の表は、Apex One (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 Apex One (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	Apex One (Mac) のサーバプログラム
サーバコンピュータ	Apex One (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 Apex One (Mac) の管理者)	Apex One (Mac) サーバを管理している人

用語	説明
コンソール	Apex One (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。
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 Apex One (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 `/Library/Application Support/TrendMicro`
サーバのインストールフォルダ	Apex One (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。Apex One (Mac) サーバをインストールすると、同じ Apex One サーバディレクトリにこのフォルダが作成されます。 Apex One 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¥OfficeScan¥Addon¥TMSM` • `C:¥Program Files¥Trend Micro¥Apex One¥Addon¥TMSM` • `C:¥Program Files (x86)¥Trend Micro¥OfficeScan¥Addon¥TMSM` • `C:¥Program Files (x86)¥Trend Micro¥Apex One¥Addon¥TMSM`

用語	説明
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 1 章

製品の概要

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

はじめに

Trend Micro Apex One™ (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。

Apex One (Mac) サーバは、Apex One やウイルスバスター ビジネスセキュリティなど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。Apex One (Mac) サーバは、エンドポイントにセキュリティエージェントを配信します。

本リリースの新機能

Apex One (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	説明
Trend Vision One の通信の強化	Trend Vision One との通信が強化され、より効果的に Apex One (Mac)からの情報のアップデートができるようになりました。

主な機能

Apex One (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
スマートスキャン	Apex One (Mac)は、スマートスキャンを使用して検索プロセスの効率を高めます。このテクノロジでは、これまでローカルエンドポイントに格納されていた大量のシグネチャが、Smart Protection ソースにオフロードされます。これにより、増加し続けるシグネチャのアップデートがエンドポイントとネットワークに与える負荷が軽減されます。 スマートスキャンと、セキュリティエージェントへのスマートスキャンの配信方法の詳細については、73 ページの「検索方法の種類」を参照してください。

機能	利点
ダメージクリーンナップサービス	ダメージクリーンナップサービスは、完全に自動化されたプロセスを介して、ファイルベースのコンピュータウイルス、ネットワークウイルス、およびウイルスやワームの残骸 (トロイの木馬、ウイルスファイル) を駆除します。トロイの木馬がもたらす脅威や迷惑行為に対処するために、ダメージクリーンナップサービスでは次の処理が実行されます。 • 活動中のトロイの木馬を検出および削除 • トロイの木馬が作成したプロセスを中止 • トロイの木馬が変更したシステムファイルを修復 • トロイの木馬により作成されたファイルとアプリケーションを削除 ダメージクリーンナップサービスはバックグラウンドで自動的に実行されるため、設定は必要ありません。ユーザがその実行を認識することもありません。ただし、Apex One (Mac) は、エンドポイントを再起動してトロイの木馬の削除プロセスを完了するようにユーザに通知することがあります。
セキュリティリスクからの保護	Apex One (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。Apex One (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。
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。 Apex One 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。

機能	利点
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。

Apex One (Mac) サーバ

Apex One (Mac) サーバは、すべてのセキュリティ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。

サーバは、次の 2 つの重要な機能を実行します。

- セキュリティエージェントの監視および管理
- セキュリティエージェントに必要なコンポーネントのダウンロード。Apex One (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、セキュリティエージェントに配信されます。

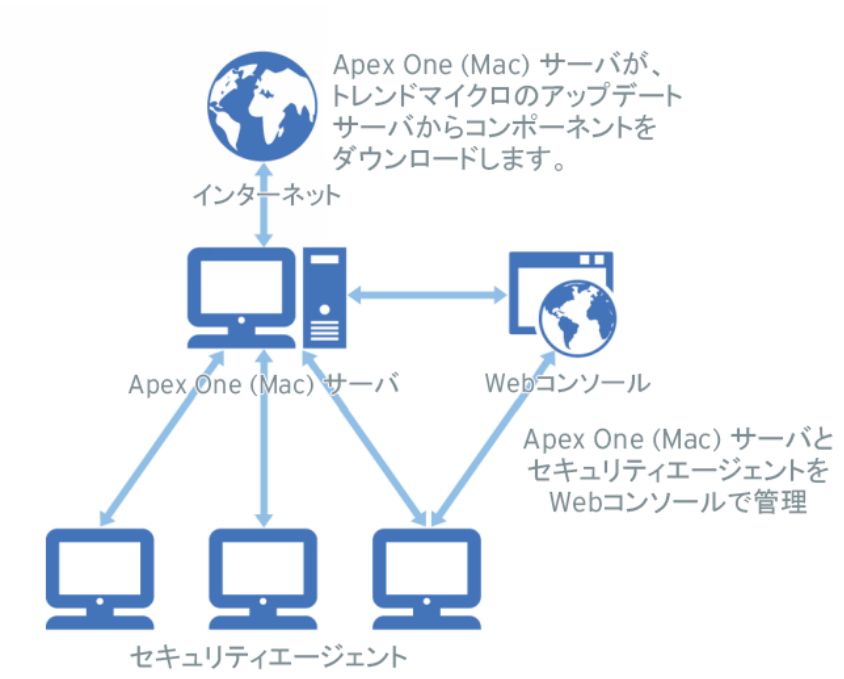


図 1-1. Apex One (Mac) サーバが機能するしくみ

Apex One (Mac) では、サーバとセキュリティ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。セキュリティエージェントは、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™を使用してセキュリティエージェントと通信します。

Apex One (Mac) セキュリティエージェント

それぞれのエンドポイントに Apex One (Mac) セキュリティ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。セキュリティエージェントでは、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

セキュリティエージェントは、インストール元の上位 Apex One (Mac) サーバにステータスを報告します。セキュリティエージェントは、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。セキュリティエージェントは、ActiveMQ プロトコルを使用してサーバと通信します。

第 2 章

サーバのインストール

この章では、Apex One (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

重要

Apex One (Mac) Patch 2 以降をインストールするか、または Apex One (Mac) Patch 2 以降を適用する前に、Microsoft インターネットインフォメーションサービス (IIS) の証明書の有効期限が切れていないことを確認してください。

詳細については https://success.trendmicro.com/dcx/s/solution/000283035?language=ja を確認してください。

サーバのインストール要件は、次のとおりです。

表 2-1. サーバのインストール要件

リソース	要件
Apex One サーバ	2019 以降
ウイルスバスター コーポレートエディション サーバ	XG 以降
プラグインマネージャ	2.0 以降
RAM	1GB 以上 (2GB を推奨)

リソース	要件

ハードディスク空き容量	• システムドライブ (通常、C:ドライブ) にウイルスバスター Corp.サーバがインストールされている場合: 7GB 以上
	• システムドライブ (通常、C:ドライブ) に Apex One サーバがインストールされている場合: 5GB 以上
	• システムドライブにウイルスバスター Corp.または Apex One サーバがインストールされていない場合:
	  • ウイルスバスター Corp.サーバがインストールされているドライブに 7GB 以上。Apex One (Mac) サーバはこのドライブにインストールされます。
	  • Apex One サーバがインストールされているドライブに 5GB 以上。Apex One (Mac) サーバはこのドライブにインストールされます。
	  • システムドライブに 7GB 以上。Apex One (Mac) サーバで使用される他社製のプログラムはこのドライブにインストールされます。

その他	• Microsoft™ .NET Framework 3.5 および 4.6.1
	• Microsoft Windows Installer 3.1 以上
	• 次の他社製プログラムは、存在しない場合は自動的にインストールされます。
	  • Microsoft SQL Server 2008 R2 Express、2016 Express、または 2016 SP1 Express
	  • Apache™ ActiveMQ 5.15.4
	  • Microsoft Visual C++ 2017 再頒布可能版
	
	注意
	• ウイルスバスター Corp.サーバに Apex One (Mac)をインストールする場合は、Java ランタイム環境 (JRE) をインストールする必要があります。
	• 最適なパフォーマンスを実現するには、JRE 1.8 以上をインストールしてください。Windows x86 用および x64 用の JRE はどちらもサポートされます。

アップデート元

Apex One (Mac) サーバをインストールする前に、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.) または Apex One の 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 2-2. 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。
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 Apex One (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。

選択したアップデート元	説明および指示
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 Apex One (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。

Apex One (Mac) サーバのインストール

重要

Apex One (Mac) Patch 2 以降をインストールするか、または Apex One (Mac) Patch 2 以降を適用する前に、Microsoft インターネットインフォメーションサービス (IIS) の証明書の有効期限が切れていないことを確認してください。

詳細については、https://success.trendmicro.com/dcx/s/solution/000283035?language=ja を参照してください。

手順

1. 次の操作は、ドメインコントローラの役割が設定されたサーバに Apex One (Mac) をインストールする場合にのみ実行してください。
   a. `<サーバのインストールフォルダ>¥PCCSRV¥Admin¥Utility¥SQL` フォルダに移動します。
   b. テキストエディタを使用して `InstallCfgFile.ini` ファイルを開きます。
   c. `SQLSVCACCOUNT` 値の設定を、`NT AUTHORITY\NETWORK SERVICE` から `NT AUTHORITY\SYSTEM` に変更します。
   d. ファイルを保存します。

2. Apex One またはウイルスバスター Corp. Web コンソールを開いて、メインメニューの [プラグイン] をクリックします。
3. [Apex One (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 `<サーバのインストールフォルダ>¥PCCSRV¥Download` にダウンロードされます。

   `<サーバのインストールフォルダ>` は通常、`C:¥Program Files¥Trend Micro¥OfficeScan` または `C:¥Program Files¥Trend Micro¥Apex One` です。
4. 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、Apex One またはウイルスバスター Corp.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、[ログ] > [サーバアップデート] をクリックします。
5. ダウンロード処理が完了した後、[インストール] をクリックして Apex One (Mac) をインストールします。
6. 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。
7. 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. Apex One またはウイルスバスター Corp. Web コンソールを開いて、メインメニューの [プラグイン] をクリックします。

2. [Apex One (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、[オンラインで登録] 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、トレンドマイクロよりアクティベーションコードが記載されたメールが送信されてきます。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。
4. ライセンスの詳細画面が表示されたら、[起動] をクリックして Web コンソールを開きます。
5. [起動] をクリックして、Web コンソールを開きます。

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 Apex One (Mac)
   - Apex One (Mac) Main Service
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. Apex One (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。

Apex One (Mac) サーバのアンインストール

手順

1. Apex One またはウイルスバスター Corp. Web コンソールを開いて、メインメニューの [プラグイン] をクリックします。
2. [Apex One (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、Apex One (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 Apex One (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、Apex One (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。

使用開始

ここでは、Apex One (Mac) をできるだけ速やかに稼働させるために必要な作業の概要について説明します。

手順

1. エージェント/サーバ間の通信設定を指定します。

   詳細については、143 ページの「エージェント/サーバ間の通信の設定」を参照してください。

2. Trend Micro Apex One (Mac) サーバをインストールしたコンピュータでファイアウォールが使用されている場合は、エージェント/サーバ間の通信トラフィックが待機ポートでブロックされていないことを確認します。

   コンピュータで Apex One 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。

3. Apex One (Mac)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します。

   詳細については、35 ページのセキュリティエージェントのインストールを参照してください。

Web コンソール

Web コンソールは、セキュリティエージェントを監視し、セキュリティ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セキュリティエージェントの管理
- 同時設定と同時管理を目的とした、セキュリティ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、セキュリティ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 1024x768、256 色以上をサポートするモニタ
- Web ブラウザ: Apex One に準ずる。

手順

1. Web ブラウザで、Apex One サーバまたはウイルスバスター Corp.サーバの URL を入力します。
2. ユーザ名とパスワードを入力して、Apex One サーバまたはウイルスバスター Corp.サーバにログオンします。
3. メインメニューで、[プラグイン] をクリックします。
4. [Apex One (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

Apex One (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。

- すべてのセキュリティエージェントと Apex One (Mac) サーバとの接続状態。リンクをクリックすると、セキュリティ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 つ以上のセキュリティ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、108 ページの「検索結果」を参照してください。
  - 1 つ以上のセキュリティ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、118 ページの「承認済み URL リストと URL ブロックリストの設定」を参照してください。

検出ステータス

[検出ステータス] の表には、セキュリティリスクと Web からの脅威の検出の総数、および感染したエンドポイントの数が表示されます。

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、Apex One (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セキュリティ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、67 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、セキュリティ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、133 ページの「サーバおよびセキュリティ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

Apex One (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セキュリティエージェントが表示されます。すべてのセキュリティ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セキュリティ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] ボックスにエンドポイ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。
- 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 (エクスポート) 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、62 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、92 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	• 検索方法を指定します。
	詳細については、73 ページの「検索方法の種類」を参照してください。
	• 検索設定を指定します。
	  • 83 ページの「手動検索」
	  • 80 ページの「リアルタイム検索」
	  • 86 ページの「予約検索」
	  • 95 ページの「検索除外」
	  • 99 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、115 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。
	• エージェントセルフプロテクションを設定します。
	詳細については、130 ページの「エージェントセルフプロテクションの設定」を参照してください。
	• デバイスコントロール設定を指定します。
	詳細については、123 ページの「デバイスコントロールの設定」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、66 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。
	• 信頼済みプログラムリストを設定します。
	詳細については、102 ページの「信頼済みプログラムリストの設定」を参照してください。
	• 機械学習型検索を設定します。
	詳細については、132 ページの「機械学習型検索の有効化」を参照してください。

メニューボタン	タスク
ログ	ログを表示して統計をリセットします。 • 107 ページの「セキュリティリスクログの表示」 • 119 ページの「Web レピュテーションログの表示」 • 103 ページの「検索ログの表示」 • 127 ページの「デバイスコントロールログの表示」 • 111 ページの「セキュリティリスクの検出数のリセット」
エージェントツリー管理	Apex One (Mac) グループを管理します。 詳細については、22 ページの「グループ」を参照してください。

グループ

Apex One (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、別のサーバ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。

グループまたはセキュリティ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セキュリティ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セキュリティ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、24 ページの「エージェントを別のグループに移動する」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セキュリティ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。

セキュリティエージェントの移動

セキュリティエージェントを別のエージェントグループまたは Apex One (Mac) サーバに移動できます。

エージェントを別のグループに移動する

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、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. [選択したエージェントを別のグループに移動する] を選択します。
5. ドロップダウンリストからグループを選択します。
6. 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。

7. [移動] をクリックします。

セキュリティエージェントを別のサーバに移動する

注意

- セキュリティエージェントは、同じバージョンかそれ以降のバージョンの別の Trend Micro Apex One (Mac) サーバにのみ移動できます。
- セキュリティエージェントをオンプレミスの Trend Micro Apex One (Mac)サーバから Server as a Service (SaaS) サーバに (またはその逆に) 移動する場合は、Trend Micro Apex One (Mac)セキュリティエージェントが待機ポートを介してサーバと通信できること、およびセキュリティエージェントエンドポイントと同じポートを使用するアプリケーションがないことを確認してください。

  次の表は待機ポートを示しています。

  表 3-1. エージェント/サーバ間の通信ポート

サーバの種類	待機ポート
オンプレミス	• セキュリティエージェントバージョン 3.5.3xxx 以上: 4343 • セキュリティエージェントバージョン 3.5.2xxx 以前: 61617
SaaS	443

  詳細については、143 ページの「エージェント/サーバ間の通信の設定」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、1 つ以上のセキュリティ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. 選択したエージェントを別のサーバに移動する を選択します。
5. サーバの名前またはアドレス、および HTTPS ポート番号を入力します。
6. [オフラインのエージェントを強制的に移動する] を選択して、オフラインのセキュリティエージェントを指定のサーバに移動します。

注意

7 日が経過してもオフラインのセキュリティエージェントがオンラインにならない場合、セキュリティエージェントは元のサーバにと留まり、指定のサーバには移動されません。

7. [移動] をクリックします。

ウィジェット

Apex One (Mac) ウィジェットは Apex One のダッシュボードで管理します。ウィジェットは、Apex One (Mac) のアクティベーション後に利用できます。

ウィジェットの使用の詳細については、Apex One のドキュメントを参照してください。

エージェントの接続状況 (Mac) ウィジェット

[エージェントの接続状況 (Mac)] ウィジェットは、エージェントの Apex One (Mac) サーバとの接続状況を表示します。データは表および円グラフで表示されます。表示アイコン ( ) をクリックして、表と円グラフを切り替えることができます。

表として表示される [エージェントの接続状況 (Mac)] ウィジェット

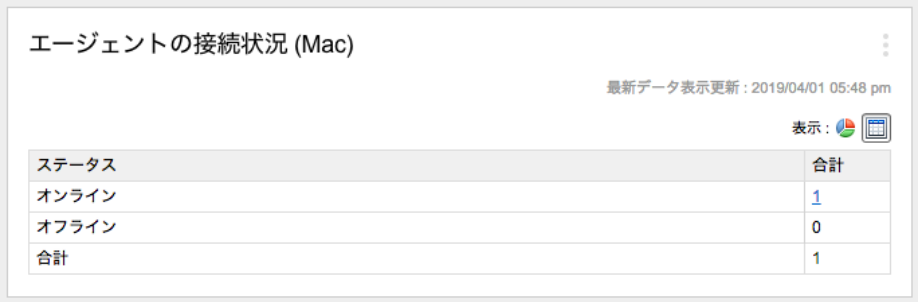


図 3-1. 表を表示する [エージェントの接続状況 (Mac)] ウィジェット

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、Apex One (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。

円グラフとして表示される [エージェントの接続状況 (Mac)] ウィジェット

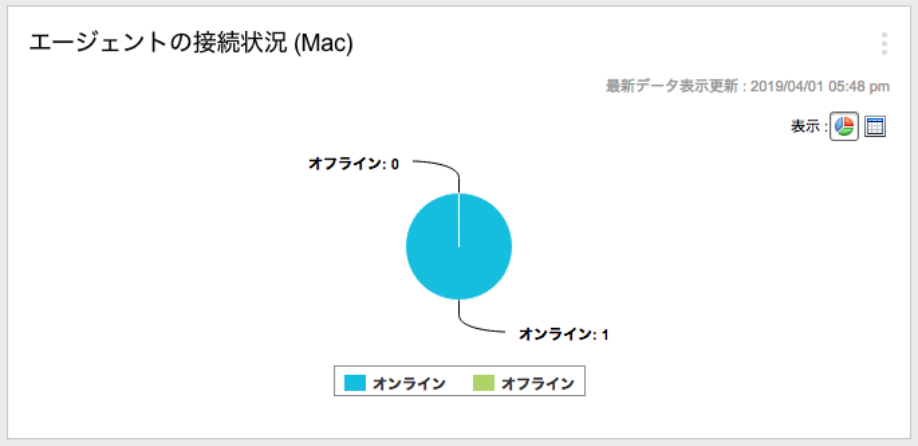


図 3-2. 円グラフを表示する [エージェントの接続状況 (Mac)] ウィジェット

円グラフには各ステータスのエージェント数が表示されますが、Apex One (Mac) エージェントツリーへのリンクは表示されません。ステータスをクリックすると、その部分を円グラフの残りの部分から切り離したり、再度結合したりできます。

エージェントのアップデート (Mac) ウィジェット

エージェントのアップデート (Mac) 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: 0、スマートスキャン: 2、従来型スキャン: 0)

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	15.903.80	0	0	0%
スパイウェア監視パターンファイル	2.295.00	0	0	0%
ウイルス検索エンジン (64ビット)	11.000.1006	0	0	0%
ダメージクリーンナップエンジン (64ビット)	1.500.1031	2	0	100%
高度な脅威検索エンジン (64ビット)	12.000.1009	2	0	100%
スマートスキャンエージェントパターンファイル	15.905.00	0	2	0%
ダメージクリーンナップテンプレート	0.011.11	2	0	100%
Macヒューリスティックパターンファイル	1.496.00	1	1	50%
プログラム	現在のバージョン	最新	旧版	アップデート率
Apex One (Mac) セキュリティエージェント	3.5.2204	2	0	100%

図 3-3. [エージェントのアップデート (Mac)] ウィジェット

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 Apex One (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。

セキュリティリスクの検出 (Mac) ウィジェット

[セキュリティリスクの検出 (Mac)] 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。

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、Apex One (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。このソリューションでは、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レピュテーション、Web レピュテーション、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。

- 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は、これまでエージェントエンドポイントに格納されていた大量の不正プログラム対策署名を、Smart Protection ソースにオフロードします。
- 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、114 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送信される情報を収集し続けています。

  詳細については、33 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

ファイルレピュテーションサービスおよび 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 (Apex One (Mac) サーバまたはウイルスバスター Corp.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、115 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 (Apex One (Mac) サーバまたはウイルスバスター Corp.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、クエリを Smart Protection Server または Smart Protection Network のいずれかに送信できます。

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。

内部セキュリティエージェントのソースとしての Smart Protection Server

このオプションでは、Apex One (Mac) セキュリティエージェントは、Apex One またはウイルスバスター Corp.セキュリティエージェント用に設定されている Smart Protection Server にクエリを送信します。

注意

Apex One (Mac) サーバがウイルスバスター Corp.とともにインストールされている場合は、ウイルスバスター Corp.を Apex One 2019 以降にアップグレードしてください。

使用しているウイルスバスター Corp.のバージョンが XG 以降の場合は、次のガイドラインに従って、セキュリティエージェントから Smart Protection Server にクエリを送信できるようにしてください。

1. まだ Smart Protection 環境を設定していない場合は、ここで設定します。環境の設定手順とガイドラインについては、ウイルスバスター Corp.のドキュメントを参照してください。
2. ウイルスバスター Corp.サーバの Web コンソールで、[Web レピュテーション設定] 画面に移動し、[Smart Protection Server にクエリを送信する] オプションを有効にします。詳細な手順については、115 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。

重要

このオプションが Apex Central または Control Manager のポリシー管理で有効化されていて、ウイルスバスター Corp.とともにインストールされている Apex One (Mac)サーバに配信されている場合、設定は反映されず、オプションは無効なままになります。

3. Smart Protection Server が使用可能であることを確認します。すべての Smart Protection Server が使用できない場合、エージェントは Trend Micro Smart Protection Network にクエリを送信せず、エンドポイントは攻撃されやすい状態のままとなります。
4. Smart Protection Server を定期的に更新して、保護を最新の状態に維持してください。

内部エージェントのソースとしての Trend Micro Smart Protection Network

クエリを Trend Micro Smart Protection Network に送信するにはインターネット接続が必要です。

Trend Micro Smart Protection Network を内部エージェントのソースに設定するには、[Web レピュテーションサービス] 画面に移動して、内部エージェントの Web レピュテーションポリシーを有効にします。オプション [Smart Protection Server にクエリを送信する] が選択されていないことを確認してください。詳細な手順については、115 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。

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
- 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

セキュリティエージェントのインストール

この章では、Apex One (Mac) セキュリティ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。

セキュリティ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、133 ページの「サーバおよびセキュリティエージェントのアップグレード」を参照してください。

エージェントのインストール要件

エージェントのインストール要件は、次のとおりです。

表 4-1. エージェントのインストール要件

リソース	要件
OS	• macOS™ Sonoma 14 • macOS™ Ventura 13 • macOS™ Monterey 12 • macOS™ Big Sur 11 • macOS™ Catalina 10.15

ハードウェア	• プロセッサ:
	  • Intel® Core
	  • Apple®シリコン
	• RAM: 2GB 以上
	• ハードディスク空き容量: 512MB 以上

リソース	要件

サーバ/エージェント間通信	• SSL ポート (Endpoint Sensor 機能で使用。Apex One サーバに設定されているものと同じ SSL ポート番号。)
	• 待機ポート:
	  • セキュリティエージェントバージョン 3.5.3xxx 以上: 4343
	  重要
	  Apex One サーバに設定されているものと同じ待機ポートを使用してください。
	  待機ポートをアップデートする予定がある場合には、セキュリティエージェントをインストールする前にアップデートを実施してください。セキュリティエージェント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。
	  詳細については、143 ページの「エージェント/サーバ間の通信の設定」を参照してください。
	  • セキュリティエージェントバージョン 3.5.2xxx 以前: 61617

その他	• *.trendmicro.com へのアクセス • インターネット接続用のプロキシサーバの設定 (必要な場合)

エージェントのインストール方法と設定ファイル

セキュリティエージェントは、次のいずれかの方法でインストールできます。

- エンドポイントでインストールパッケージ (`tmsminstall.zip`) を起動して 1 台のエンドポイントにインストールする方法
- セキュリティエージェントが含まれる OS イメージを配信して複数のエンドポイントにインストールする方法。インストール後、セキュリティエージェントは Apex One (Mac) サーバに自動的に登録されます。

重要

Apex One (Mac) サーバでのセキュリティエージェント ID の重複の問題を解決するには、TMMakeGoldenImage ツールをマスター OS イメージに含めます。ツールを入手して、次の Web サイトの手順に従ってください。

https://success.trendmicro.com/dcx/s/solution/1115416?language=ja

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、133 ページの「サーバおよびセキュリティエージェントのアップグレード」を参照してください。

Apex One (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いくつかあります。

- Apex One (Mac) Web コンソールで、[エージェント] > [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、セキュリティ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セキュリティエージェントプログラムを削除します。削除するセキュリティ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。

  Apex One (Mac) セキュリティエージェントのアンインストールについては、52 ページの「エージェントのアンインストール」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¥ActiveUpdate¥ClientInstall¥`に移動します。
- Apex Central Web コンソールから

詳細については、Trend Micro Apex Central 管理者ガイドを参照してください。

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 Apex One (Mac) 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、サーバへのセキュリティ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、37 ページの「エージェントのインストール方法と設定ファイル」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。

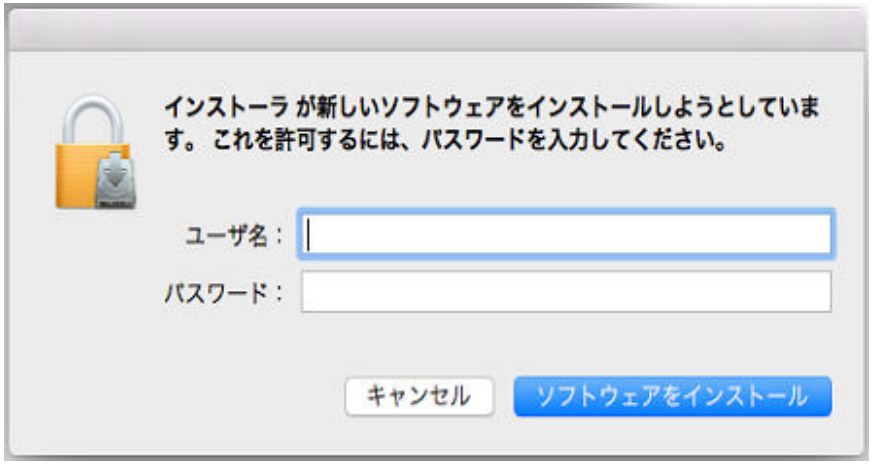
7. 留意事項を読み、[続ける] をクリックします。

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。

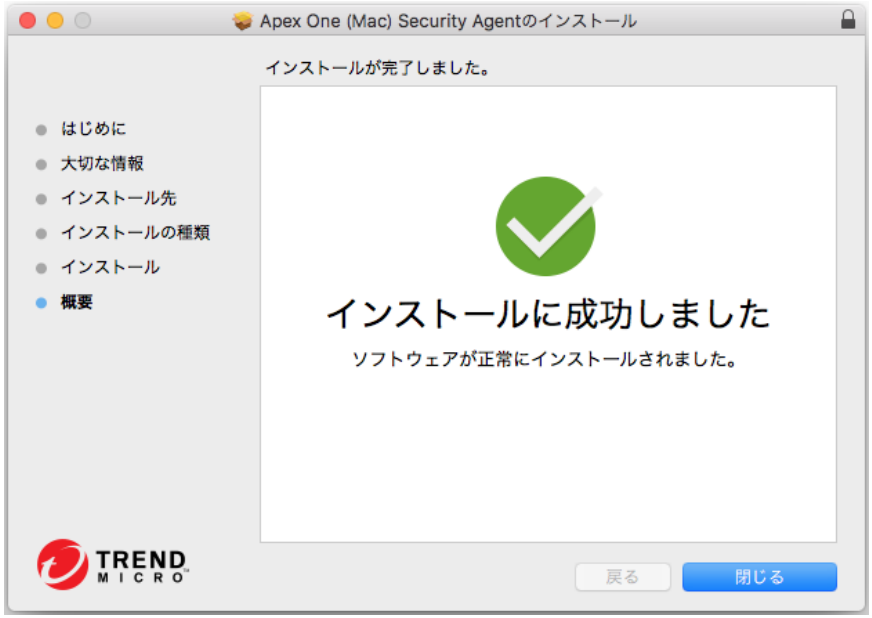
9. [名前] と [パスワード] を入力して、インストールプロセスを開始します。

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。



セキュリティエージェントは、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、セキュリティ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、46 ページの「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。

エージェントのインストール後のタスク

手順

1. サポートされている macOS™バージョンを実行しているエンドポイントにセキュリティエージェントを初めてインストールする場合は、セキュリティエージェントを機能させるために必要な権限を許可するように求めるセットアップウィザードが表示されます。画面に表示される指示に従って設定を完了します。

   次に手順の概要を示します。 macOS™ バージョンに必要のない権限設定は、セットアップウィザードによって自動的にスキップされます。

   macOS 13 以上の場合:

   a. [[プライバシーとセキュリティ] を開く] をクリックするか、アップルメニューにアクセスして、[システム設定] > [プライバシーとセキュリティ] に移動します。

   b. [セキュリティ] セクションまでスクロールし、[詳細] をクリックします。

   c. 変更を許可するには、macOS 管理者のパスワードを入力し、[ロックを解除] または [設定を変更] をクリックします。

   d. 切り替えスイッチをクリックしてすべての iCore Service エントリをオンにし、[OK] をクリックします。

   e. [許可] をクリックし、セキュリティエージェントにネットワークコンテンツのフィルタを許可します。

   f. [続行] をクリックします。

g. [フルディスクアクセスを開く] をクリックするか、アップルメニューにアクセスして、[システム設定] > [プライバシーとセキュリティ] > [フルディスクアクセス] に移動します。

h. [ファイルの場所を開く] をクリックして、`com.trendmicro.icore.es.systemextension` ファイルを探します。次に、ファイルを [フルディスクアクセス] テーブルにドラッグアンドドロップします。

i. [ファイルの場所を開く] をクリックして、`Apex One (Mac)` セキュリティエージェントを [アプリケーション] フォルダから [フルディスクアクセス] テーブルにドラッグアンドドロップし、表示される画面で [後で] をクリックします。

j. [ファイルの場所を開く] をクリックして、`iCore Service` ファイルを探します。次に、ファイルを [フルディスクアクセス] テーブルにドラッグアンドドロップします。

k. 切り替えスイッチをクリックして、次のアプリをオンにします。

- iCore Service
- Apex One (Mac) セキュリティエージェント
- Trend Micro Extension (使用可能な場合)

l. [続行] をクリックします。

m. 変更を適用するには、コンピュータを再起動してください。

macOS 10.14、10.15、11、および 12 の場合:

a. [[セキュリティとプライバシー] を開く] をクリックするか、アップルメニューにアクセスして、[システム環境設定] > [セキュリティとプライバシー] > [一般] の順に移動します。

b. 変更を行うには、左下隅にあるカギのアイコンをクリックし、macOS 管理者のパスワードを入力します。

c. [許可] をクリックして、トレンドマイクロの証明書をインストールします。

d. [続行] をクリックします。

e. [セキュリティとプライバシー] 画面で、[許可] をクリックします。

f. 「Trend Micro Inc.」のオプションをすべて選択し、[OK] をクリックします。

g. [許可] をクリックし、セキュリティエージェントにネットワークコンテンツのフィルタを許可します。

h. [続行] をクリックします。

i. [セキュリティとプライバシー] 画面で、サービスのリストから [フルディスクアクセス] を選択します。

j. [ファイルの場所を開く] をクリックして、`iCore Service` ファイルを探します。次に、ファイルを [フルディスクアクセス] テーブルにドラッグアンドドロップします。

k. [ファイルの場所を開く] をクリックし、[アプリケーション] フォルダから [フルディスクアクセス] テーブルに `Apex One (Mac)` セキュリティエージェントをドラッグアンドドロップします。

l. 次のアプリが選択されていることを確認します。

- iCore Service
- Apex One (Mac) セキュリティエージェント
- Trend Micro Extension (使用可能な場合)

m. [続行] をクリックします。

n. 変更を適用するには、コンピュータを再起動してください。

2. トレンドマイクロツールバー for Mac の拡張機能をインストールして有効にするよう求めるアラート通知が表示されます。お使いの Web ブラウザに応じて、次の手順を実行します。

- Safari 17 以上:

  a. アラート通知のウィンドウで、[拡張機能を有効にする] をクリックします。

     設定の概要画面が表示されます。

  b. [Safari 拡張機能を開く] をクリックします。

  c. [トレンドマイクロツールバー for Mac] オプションを選択して拡張機能を有効にします。

d. [権限] セクションで、[すべての Web サイトで常に許可...] をクリックします。

e. すべての Web サイトでこの拡張機能を許可するかどうかを尋ねられたら、[すべての Web サイトで常に許可] をクリックします。

- Safari 16 以下:

  a. アラート通知のウィンドウで、[拡張機能を有効にする] をクリックします。

     設定の概要画面が表示されます。

  b. [Safari 拡張機能を開く] をクリックします。

  c. [トレンドマイクロツールバー for Mac] オプションを選択して拡張機能を有効にします。

- Firefox:

  a. アラート通知のウィンドウで、[拡張機能を有効にする] をクリックします。

     設定の概要画面が表示されます。

  b. [ファイルの場所を開く] をクリックし、`Trend Micro Toolbar for Mac extension.xpi` ファイルを選択します。次に、Firefox ウィンドウにこのファイルをドラッグアンドドロップしてインストールします。

  c. [追加] をクリックして、トレンドマイクロツールバー for Mac 拡張機能をインストールします。

- (macOS 11.0 以上では必須) Google Chrome:

  a. アラート通知のウィンドウで、[拡張機能を有効にする] をクリックします。

     設定の概要画面が表示されます。

  b. [ファイルの場所を開く] をクリックして `Trend Micro Toolbar For Mac (Chrome).mobileconfig` ファイルを探し、ダブルクリックします。

c. [プロファイルを開く] をクリックします。

d. [プロファイル] 画面で `Trend Micro Toolbar for Mac (Chrome)` を選択し、[インストール...] をクリックします。

e. [インストール] をクリックします。

f. メッセージが表示されたら、macOS 管理者のパスワードを入力し、[OK] をクリックします。

g. Google Chrome を再起動して、変更を適用します。

3. 以下を確認します。

- セキュリティ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。
- Apex One (Mac) 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セキュリティ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。

4. エージェントコンソールで [アップデート] をクリックし、Apex One (Mac) 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、Apex One (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、62 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。

セキュリティ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。

5. エンドポイントで手動検索を開始するには、[検索] をクリックし、次の検索オプションのいずれかを選択します。

   - クイック検索: 一般的にセキュリティリスクとなるエンドポイント上の領域を検索します。セキュリティエージェントのパターンファイルには、検索するエンドポイント上の領域に関する情報が含まれます。
   - カスタム検索: 指定されたファイルまたはフォルダを検索します。感染の疑いがあるファイルやフォルダがある場合は、カスタム検索を実行します。

- コンピュータ全体の検索: コンピュータ上のすべてのファイルを検索します。暗号化されたファイルやパスワードで保護されたファイルは除外されます。

次に進む前に

インストール後にセキュリティエージェントで問題が発生した場合は、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再インストールしてみてください。

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. Apex One (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。Apex One (Mac) Web コンソールで、[エージェント] > [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. [続行] をクリックして、システム拡張機能を削除します (macOS 11.0 以上の場合)。
5. 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、Apex One (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

Apex One (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。

セキュリティエージェントでは、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 Apex One (Mac)サーバから受け取ります。セキュリティエージェントでは、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 Apex One (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。

コンポーネント	説明
エージェントプログラム	セキュリティ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。
高度な脅威検索エンジン (ユニバーサル)	高度な脅威検索エンジンは、ウイルス、不正プログラム、ソフトウェア (Java や Flash など) の脆弱性の悪用を防ぎます。トレンドマイクロのウイルス検索エンジンと統合されており、署名と挙動に基づいた強力なヒューリスティック検出を実行します。
ダメージクリーンナップエンジン (ユニバーサル)	ダメージクリーンナップエンジンは、トロイの木馬とそのプロセスを検索し、削除します。
ダメージクリーンナップテンプレート	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使用され、トロイの木馬のファイルとプロセスを特定してエンジンで除去できるようにします。
Mac ヒューリスティックパターンファイル	Mac ヒューリスティックパターンファイルは、Mac プラットフォームを標的にした不正プログラムを特定するためにスマートスキャンで使用されます。
スマートスキャンエージェントパターンファイル	脅威を特定するためにセキュリティエージェントが使用するパターンファイル。このパターンファイルはエージェントエンドポイントに格納されています。
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、Apex One (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。

コンポーネント	説明
ウイルス検索エンジン (ユニバーサル)	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。 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
ウイルスパターンファイル	Apex One (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。

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、Apex One (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 Apex One (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、Apex One (Mac) サーバおよびセキュリティ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 ↓ Apex One (Mac) サーバ ↓ セキュリティエージェント	Apex One (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、セキュリティ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 ↓ セキュリティエージェント	セキュリティエージェントは、Apex One (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

Apex One (Mac)サーバは、次のコンポーネントをダウンロードして、セキュリティ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 (32 ビット/64 ビット)
- ダメージクリーンナップエンジン (64 ビット)
- ダメージクリーンナップテンプレート

- スマートスキャンエージェントパターンファイル
- Apex One (Mac)セキュリティエージェント
- Mac ヒューリスティックパターンファイル
- 高度な脅威検索エンジン (64 ビット)

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セキュリティ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 Apex One (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、サーバのアップデートにおける IPv6 の制限事項について、162 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セキュリティ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] > [エージェント管理] > [タスク] > [アップデート] に移動して、セキュリティ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. [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:
  - Apex One (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、60 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。
  - Apex Central からアップデートを取得するには、Apex Central サーバアドレスを入力します。

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 Apex One (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、162 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

Apex One (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、62 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:Apex One (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、61 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、Apex One (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. [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、Apex One (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。Apex One (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、Apex One (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、Apex One (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. [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セキュリティ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セキュリティエージェントをアップデートしてください。セキュリティエージェントが Apex One (Mac) サーバまたは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

セキュリティ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、68 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、67 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、アップデートを促す通知が、サーバからセキュリティエージェントへすぐに送信されます。 詳細については、65 ページの「エージェントの自動アップデート設定」を参照してください。 • 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 つまたは複数のセキュリティ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セキュリティ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、66 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、セキュリティエージェントは Apex One (Mac) サーバからコンポーネントをダウンロードします。Apex One (Mac) サーバからアップデートする際、セキュリティエージェントには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ダウンロードされます。セキュリティエージェン

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 Apex One (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。

セキュリティエージェントをアップデートする前に、Apex One (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。

Apex One (Mac) サーバのアップデート方法については、58 ページの「サーバアップデート」を参照してください。

Apex One (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、またはすべてのセキュリティエージェントを設定します。

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の設定」を参照してください。

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、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、163 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

- セキュリティエージェントでは、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セキュリティエージェントアイコンによって、製品がアップデートされていることが示されます。セキュリティ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、セキュリティ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、すべてのセキュリティ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。

エージェントの自動アップデート設定

自動アップデートを利用すると、すべてのセキュリティエージェントにアップデートを促す通知を送信する手間を省いて、エンドポイントに最新のコンポーネントがインストールされていないリスクを回避できます。

自動アップデート中、Apex One (Mac)セキュリティエージェントには、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もダウンロードされます。セキュリティエージェントでは、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 Apex One (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。

Apex One (Mac) サーバは、最新のコンポーネントをダウンロードした後で、オンラインのセキュリティエージェントにコンポーネントをアップロードするよう通知できます。オフラインのセキュリティエージェントには、再起動してサーバに接続したときにアップロードを通知できます。必要に応じて、アップデート後、Trend Micro Apex One (Mac)セキュリティエージェントエンドポイントで [検索開始] (手動検索) を実行してください。

1. [アップデート] > [エージェントの自動アップデート] をクリックします。
2. オプションを選択します。

表 5-2. イベント起動アップデート

オプション	説明
新しいコンポーネントをダウンロード後、ただちにエージェントでコンポーネントのアップデートを開始する	Apex One (Mac) サーバはアップデートを完了するとすぐに、セキュリティエージェントにアップデートするよう通知します。
エージェントを再起動してサーバに接続した後にコンポーネントのアップデートを開始する	アップデートが実行されなかったセキュリティエージェントは、サーバとの接続を確立するとただちにコンポーネントをダウンロードします。セキュリティエージェントがオフラインの場合や、インストール先のエンドポイントが稼働中でない場合、アップデートされない可能性があります。

注意

初期設定では、アップデート通知は Trend Micro Apex One (Mac) サーバに最大 7 日間保持されます。セキュリティエージェントがこの期間以内にオンラインになると、オフラインのセキュリティエージェントはアップデート通知を受け取ります。

3. [保存] をクリックします。

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、62 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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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. [Apex One (Mac) サーバに接続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アップデートをダウンロードする] を選択して、外部セキュリティエージェントが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できるようにします。

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、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、163 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. コンポーネントのアップデートの続行を許可し、Apex One (Mac) セキュリティエージェントのアップグレードを阻止する場合は、[エージェントにコンポーネントのアップデートを許可するが、エージェントプログラムのアップグレードと HotFix のインストールを禁止する] を選択します。

6. 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 Apex One (Mac) サーバがセキュリティ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のセキュリティ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のセキュリティ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。
7. エージェントツリーで 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

[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、62 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セキュリティエージェントがすべて示されます。

3. アップデートするセキュリティ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セキュリティ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 Apex One (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、62 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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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セキュリティ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 Apex One (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。Apex One (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。Apex One (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。

Apex One (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。

Apex One (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。

検索方法の種類

Apex One (Mac) セキュリティエージェントは、セキュリティリスクを検索するときに、2 つの検索方法のいずれかを使用できます。スマートスキャンと従来型スキャンです。

- スマートスキャン

  このドキュメントでは、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では、ローカル検索と、ファイルレピュテーションサービスが提供するインターネットクエリを使用できます。

- 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」と呼ばれます。従来型スキャンエージェントでは、エージェントエンドポイント上にすべての Apex One (Mac) コンポーネントが格納され、ファイルがローカルで検索されます。

初期設定の検索方法

新規にインストールされた Apex One (Mac) サーバの初期設定の検索方法はスマートスキャンです。

検索方法の比較

次の表に、2 つの検索方法を比較したものです。

表 6-1. 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
対応バージョン	このバージョンの Apex One (Mac) で利用できます。	このバージョンの Apex One (Mac) で利用できます。

比較基準	従来型スキャン	スマートスキャン
検索動作	従来型スキャンエージェントは、ローカルエンドポイントに対して検索を実行します。	• スマートスキャンエージェントは、ローカルエンドポイントに対して検索を実行します。 • セキュリティエージェントが検索時にファイルのリスクを判断できない場合、セキュリティエージェントはスキャンクエリを Smart Protection ソースに送信することで、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、検索クエリ結果を「キャッシュ」します。
使用するコンポーネントとアップデートされたコンポーネント	Mac ヒューリスティック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、アップデート元で利用可能なすべてのコンポーネント。	ウイルスパターンファイルおよびスパイウェア監視パターンファイル以外の、アップデート元で利用可能なすべてのコンポーネント。
一般的なアップデート元	Apex One (Mac) サーバ	Apex One (Mac) サーバ

検索方法の変更

手順

1. [エージェント] > [エージェント管理] に進みます。
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セキュリティエージェントを含めるか、特定のグループまたはセキュリティエージェントを選択します。
3. [設定] > [検索方法] をクリックします。
4. [従来型スキャン] または [スマートスキャン] を選択します。

5. エージェントツリーで 1 つ以上のグループまたはセキュリティエージェントを選択した場合は、[保存] をクリックします。ルートアイコンをクリックした場合は、次のオプションから選択します。

   - すべてのエージェントに適用: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

スマートスキャンから従来型スキャンへの切り替え

次の表は、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る場合のその他の注意点を示しています。

表 6-2. 従来型スキャンに切り替えるときの注意点

注意点	詳細
切り替えるセキュリティエージェントの数	一度に切り替えるセキュリティエージェントの数を少なくすることで、Trend Micro Apex One (Mac) サーバおよび Smart Protection Server のリソースを効率よく使用できます。これらのサーバは、セキュリティエージェントが検索方法を変更している間も、その他の重要なタスクを実行できます。
タイミング	従来型スキャンに戻すと、多くの場合、セキュリティエージェントは Trend Micro Apex One (Mac) サーバからウイルスパターンファイルおよびスパイウェア監視パターンファイルの完全版をダウンロードします。これらのパターンファイルは、従来型スキャンエージェントのみが使用します。 ダウンロード処理を短時間で完了できるよう、ピーク時間を避けて切り替えを実施することを検討してください。また、サーバからのセキュリティエージェントのアップデートが 1 件も予定されていないタイミングを推奨します。

注意点	詳細
エージェントツリーの設定	検索方法は、ルート、グループ、または個々のセキュリティエージェントレベルで設定できます。従来型スキャンに切り替えるときには、次の操作が可能です。 • 新しいグループを作成し、検索方法として従来型スキャンを割り当てる。このグループに移動したすべてのセキュリティエージェントで従来型スキャンが使用されます。セキュリティエージェントを移動するときは、設定の [新しいグループの設定を選択したエージェントに適用する] を有効にしてください。 • グループを選択し、従来型スキャンを使用するように設定する。このグループに属しているスマートスキャンエージェントは、従来型スキャンに切り替わります。 • グループから 1 つまたは複数のスマートスキャンエージェントを選択し、従来型スキャンに切り替える。 注意 グループの検索方法に変更を加えると、個々のセキュリティエージェントに設定してある検索方法がオーバーライドされます。

従来型スキャンからスマートスキャンへの切り替え

セキュリティエージェントを従来型スキャンからスマートスキャンに切り替える場合は、Apex One サーバで Smart Protection サービスが設定済みであることを確認してください。詳細については、Apex One のドキュメントを参照してください。

次の表は、セキュリティエージェントをスマートスキャンに切り替える場合のその他の注意点を示しています。

表 6-3. スマートスキャンに切り替える場合の注意点

注意点	詳細
製品ライセンス	スマートスキャンを使用する場合は、Apex One サーバで次のサービスのライセンスを有効にしてあることと、そのライセンスの有効期限が過ぎていないことを確認してください。 • ウイルス対策 • Web レピュテーションおよびスパイウェア対策
Apex One (Mac) サーバ	セキュリティエージェントが Apex One (Mac) サーバに接続できることを確認します。スマートスキャンに切り替えるように通知されるのはオンラインのセキュリティエージェントだけです。オフラインのセキュリティ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。スタンドアロンのセキュリティエージェントは、オンラインになったとき、またはセキュリティエージェントに予約アップデート権限がある場合は予約アップデートが実行されたときに通知されます。 Trend Micro Apex One (Mac) サーバに最新のコンポーネントが配置されていることも確認してください。スマートスキャンエージェントは、サーバから Mac ヒューリスティック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をダウンロードする必要があります。コンポーネントをアップデートするには、58 ページの「サーバアップデート」を参照してください。
切り替えるセキュリティエージェントの数	一度に切り替えるセキュリティエージェントの数を少なくすることで、Apex One (Mac) サーバのリソースを効率よく使用できます。セキュリティエージェントが検索方法を変更している間も、Apex One (Mac) サーバはその他の重要なタスクを実行できます。
タイミング	初めてスマートスキャンに切り替えるときは、セキュリティエージェントは Apex One (Mac) サーバから Mac ヒューリスティック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の完全版をダウンロードする必要があります。スマートスキャンパターンファイルはスマートスキャンエージェントのみが使用します。 ダウンロード処理を短時間で完了できるよう、ピーク時間を避けて切り替えを実施することを検討してください。また、サーバからのセキュリティエージェントのアップデートが 1 件も予定されていないタイミングを推奨します。

注意点	詳細
エージェントツリーの設定	検索方法は、ルート、グループ、または個々のエージェントレベルで設定できます。スマートスキャンに切り替えるときには、次の操作を実行できます。 • 新しいグループを作成し、検索方法としてスマートスキャンを割り当てる。このグループに追加するすべてのセキュリティエージェントでスマートスキャンが使用されます。セキュリティエージェントを移動するときは、設定の [新しいグループの設定を選択したエージェントに適用する] を有効にしてください。 • グループを選択し、スマートスキャンを使用するように設定する。このグループに属している従来型スキャンエージェントは、スマートスキャンに切り替わります。 • グループから 1 つまたは複数の従来型スキャンエージェントを選択し、スマートスキャンに切り替える。 注意 グループの検索方法に変更を加えると、個々のセキュリティエージェントに設定してある検索方法がオーバーライドされます。

注意点	詳細
IPv6 のサポート	スマートスキャンエージェントは、Smart Protection ソースに検索クエリを送信します。 IPv6 シングルスタックスマートスキャンエージェントは、次のような IPv4 シングルスタックソースにクエリを直接送信することはできません。 • Smart Protection Server 3.0 (統合またはスタンドアロン) 注意 Smart Protection Server に対する IPv6 のサポートは、バージョン 2.5 から開始されます。 • Trend Micro Smart Protection Network 同様に、IPv4 シングルスタックスマートスキャンエージェントは、IPv6 シングルスタック Smart Protection Server にクエリを送信できません。 スマートスキャンエージェントがソースに接続するためには、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 (DeleGate など) が必要です。

検索の種類

Apex One (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が用意されています。

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。 80 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。 83 ページの「手動検索」を参照してください。

検索の種類	説明
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。 86 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。 92 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。Apex One (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。Apex One (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は、1 つ以上のセキュリティ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セキュリティ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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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. チェックボックスをオンにして、リアルタイム検索を有効にします。
5. [対象] タブをクリックし、ファイルのアクティビティと検索の詳細を設定します。

詳細については、81 ページの「リアルタイム検索: [対象] タブ」を参照してください。

6. [処理] タブをクリックし、Apex One (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。

   詳細については、82 ページの「リアルタイム検索: [処理] タブ」を参照してください。

7. エージェントツリーで 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

リアルタイム検索: [対象] タブ

手順

1. [ファイルに対するユーザのアクティビティ] で、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。

   - 次のファイルを検索: 作成された/変更されたファイル: エンドポイントに取り込まれた新しいファイル (ファイルのダウンロード後など)、または変更されたファイルを検索します。
   - 次のファイルを検索: 読み込まれた/実行されたファイル: ファイルが開かれたときに検索します。
   - 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/実行されたファイル

- 次のファイルを検索: 作成された/変更された/実行されたファイル

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。

2. [検索設定] で、次のオプションを 1 つ以上選択します。

   - 圧縮ファイルの検索: アーカイブファイル内の個々のファイルを検索します

     詳細については、92 ページの「サポートされる圧縮ファイルの種類」を参照してください。

   - ネットワークドライブの検索: 他のエンドポイントに物理的に配置されていて、ローカルエンドポイントにマッピングされているディレクトリを検索します

リアルタイム検索: [処理] タブ

[処理] タブでは、セキュリティ上の脅威が検出されたときに Apex One (Mac) で実行する処理を設定します。

手順

1. [処理] で、検出時の処理を指定します。

オプション	説明
トレンドマイクロの推奨処理を使用	トレンドマイクロの推奨処理とは、セキュリティリスクの種類ごとに事前に割り当てられている一連の検索処理です。特定の種類のセキュリティリスクに適した検出時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使用することを推奨します。 トレンドマイクロの推奨処理の設定は、最新のセキュリティリスクや最新の攻撃手段からエンドポイントを保護できるようにパターンファイルで絶えず更新されます。

オプション	説明
すべての種類のセキュリティリスクに同じ処理を使用	このオプションは、潜在的なウイルス/不正プログラムを除くすべての種類のセキュリティリスクに同じ処理を実行する場合に選択します。潜在的なウイルス/不正プログラムに対する処理は常に「放置」です。 1 次処理として「駆除」を選択していて駆除に失敗した場合、Apex One (Mac) が実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。 検索時の処理の詳細は、93 ページの「検出時の処理」を参照してください。

2. リアルタイム検索中に Apex One (Mac) でセキュリティリスクが検出されたときに通知メッセージを表示するには、[ウイルス/不正プログラムが検出された場合にエージェントエンドポイントに通知メッセージを表示する] を選択します。

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。

手動検索の設定は、1 つ以上のセキュリティ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セキュリティ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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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. [対象] タブをクリックし、検索の詳細と CPU 使用率を設定します。

   詳細については、84 ページの「手動検索: [対象] タブ」を参照してください。

5. [処理] タブをクリックし、Apex One (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。

   詳細については、86 ページの「手動検索: [処理] タブ」を参照してください。

6. エージェントツリーで 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

手動検索: [対象] タブ

手順

1. [検索対象ファイル] セクションで、次のいずれかを選択します。

   - 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。検索できないファイルには、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、ユーザ指定の検索制限を超えるファイルがあります。

注意

すべてのファイルの検索には多くの時間とリソースを消費するため、状況によっては不要な場合もあります。このため、セキュリティエージェントで検索するファイルの数を制限することも可能です。

- Mach-O ファイルのみを検索: エンドポイント上の Mach-O ファイルのみを検索します。Apex One (Mac) セキュリティエージェントは、その他の種類のファイルに含まれる不正プログラムを検索しません。

注意

このオプションを選択する場合は、OS X および macOS プラットフォームを標的とする最新の不正プログラムによる攻撃から保護するためにスマートスキャン機能を有効にする必要があります。

2. [検索設定] で、次のオプションを 1 つ以上選択します。
   - 圧縮ファイルの検索: アーカイブファイル内の個々のファイルを検索します

     詳細については、92 ページの「サポートされる圧縮ファイルの種類」を参照してください。
   - ネットワークドライブの検索: 他のエンドポイントに物理的に配置されていて、ローカルエンドポイントにマッピングされているディレクトリを検索します
   - Time Machine の検索: Time Machine ドライブ上のファイルのみを検索します

     注意

     手動検索および予約検索の [Time Machine の検索] オプションを有効にした場合、不正プログラムの脅威は検出されますが、処理 (駆除、隔離、削除) は実行されなくなります。これは、Mac OS の権限の制限によるものです。検索処理が設定されている場合、製品ログには失敗として記録されます。

3. [CPU 使用率] セクションで必要な設定を行います。
   - 高: 間隔をあけず連続してファイルを検索する
   - 低: CPU 利用率が 20%を超えた場合は一時中断して間隔をあけ、20%以下の場合は一時中断しない

手動検索: [処理] タブ

[処理] タブでは、セキュリティ上の脅威が検出されたときに Apex One (Mac) で実行する処理を設定します。

オプション	説明
トレンドマイクロの推奨処理を使用	トレンドマイクロの推奨処理とは、セキュリティリスクの種類ごとに事前に割り当てられている一連の検索処理です。特定の種類のセキュリティリスクに適した検出時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使用することを推奨します。 トレンドマイクロの推奨処理の設定は、最新のセキュリティリスクや最新の攻撃手段からエンドポイントを保護できるようにパターンファイルで絶えず更新されます。
すべての種類のセキュリティリスクに同じ処理を使用	このオプションは、潜在的なウイルス/不正プログラムを除くすべての種類のセキュリティリスクに同じ処理を実行する場合に選択します。潜在的なウイルス/不正プログラムに対する処理は常に「放置」です。 1 次処理として「駆除」を選択していて駆除に失敗した場合、Apex One (Mac) が実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。 検索時の処理の詳細は、93 ページの「検出時の処理」を参照してください。

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。セキュリティエージェントの予約検索を使用して日々の検索を自動化することで、検索をより効率的に管理できます。

予約検索の設定は、1 つ以上のセキュリティ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セキュリティ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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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. [対象] タブをクリックし、検索の詳細、CPU 使用率、および検索スケジュールを設定します。

   詳細については、88 ページの「予約検索: [対象] タブ」を参照してください。
6. [処理] タブをクリックし、Apex One (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。

   詳細については、89 ページの「予約検索: [処理] タブ」を参照してください。
7. エージェントツリーで 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後

追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

予約検索: [対象] タブ

手順

1. [スケジュール] で、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、Apex One (Mac) によってその月の最終日に予約検索が実行されます。

2. [検索対象ファイル] セクションで、次のいずれかを選択します。

   - 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。検索できないファイルには、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、ユーザ指定の検索制限を超えるファイルがあります。

     注意
     すべてのファイルの検索には多くの時間とリソースを消費するため、状況によっては不要な場合もあります。このため、セキュリティエージェントで検索するファイルの数を制限することも可能です。

   - 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。
   - パスまたはフルパスを指定: 検索するファイルまたはディレクトリを手動で指定します。例: `/Shared/Files/mytext.txt` または `/Shared/Files`。

3. [検索設定] で、次のオプションを 1 つ以上選択します。

   - 圧縮ファイルの検索: アーカイブファイル内の個々のファイルを検索します

詳細については、92 ページの「サポートされる圧縮ファイルの種類」を参照してください。

- Time Machine の検索: Time Machine ドライブ上のファイルのみを検索します

注意

手動検索および予約検索の [Time Machine の検索] オプションを有効にした場合、不正プログラムの脅威は検出されますが、処理 (駆除、隔離、削除) は実行されなくなります。これは、Mac OS の権限の制限によるものです。検索処理が設定されている場合、製品ログには失敗として記録されます。

4. [CPU 使用率] セクションで必要な設定を行います。
   - 高: 間隔をあけず連続してファイルを検索する
   - 低: CPU 利用率が 20%を超えた場合は一時中断して間隔をあけ、20%以下の場合は一時中断しない

予約検索: [処理] タブ

[処理] タブでは、セキュリティ上の脅威が検出されたときに Apex One (Mac) で実行する処理を設定します。

手順

1. [処理] で、検出時の処理を指定します。

オプション	説明
トレンドマイクロの推奨処理を使用	トレンドマイクロの推奨処理とは、セキュリティリスクの種類ごとに事前に割り当てられている一連の検索処理です。特定の種類のセキュリティリスクに適した検出時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使用することを推奨します。 トレンドマイクロの推奨処理の設定は、最新のセキュリティリスクや最新の攻撃手段からエンドポイントを保護できるようにパターンファイルで絶えず更新されます。
すべての種類のセキュリティリスクに同じ処理を使用	このオプションは、潜在的なウイルス/不正プログラムを除くすべての種類のセキュリティリスクに同じ処理を実行する場合に選択します。潜在的なウイルス/不正プログラムに対する処理は常に「放置」です。 1 次処理として「駆除」を選択していて駆除に失敗した場合、Apex One (Mac) が実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。 検索時の処理の詳細は、93 ページの「検出時の処理」を参照してください。

2. [予約検索権限] で、ユーザによる予約検索の保留またはスキップを許可するかどうかを指定します。

権限	説明
予約検索の延期	「予約検索の延期」権限を持つユーザは、次の処理を実行できます。 • 予約検索を実行前に延期し、延期期間を指定できます。予約検索は 1 回だけ延期できます。 • 予約検索が進行中の場合、ユーザは検索を停止して後で再開できます。ユーザは、検索を再開するまでの経過時間を指定します。検索を再開すると、前に検索されたファイルがすべて再検索されます。予約検索を停止して再開できるのは 1 回だけです。 次に対応する時間数および分数を設定します。 • 最大延期期間 • 検索を再開するまでの最大経過時間
予約検索のスキップおよび停止	この権限を持つユーザは、次の処理を実行できます。 • 予約検索が実行される前にそれをスキップできます。 • 予約検索の実行中にそれを停止できます。

3. [予約検索設定] で、通知とバッテリ電力の設定を指定します。

設定	説明
予約検索の実行前に通知を表示	このオプションを有効にすると、予約検索を実行する数分前に、エンドポイントに通知メッセージが表示されるようになります。このメッセージでは、検索のスケジュール (日時)、およびユーザの予約検索権限 (予約検索の保留、スキップ、または停止など) が通知されます。 通知メッセージを表示するタイミングを分数で設定します。
予約検索を自動停止するまでの経過時間: __ 時間 __ 分	指定した時間が経過してもセキュリティエージェントによる検索が完了しない場合に検索を停止します。検索中に検出されたセキュリティリスクはセキュリティエージェントを通じてただちにユーザに通知されます。

設定	説明
ノート PC のバッテリ残量が__%よりも少なく、AC アダプタが接続されていない場合は、予約検索をスキップする	ノート PC のバッテリ残量が少なく、AC アダプタが電源に接続されていない場合、予約検索をスキップします。バッテリ残量が少なくても、AC アダプタが電源に接続されている場合は、検索が続行されます。バッテリ残量が少なくなっても、実行中の検索は中止されません。

検索開始

検索開始は、Apex One (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、87 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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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。

サポートされる圧縮ファイルの種類

Apex One (Mac) は次の種類の圧縮ファイルをサポートしています。

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
.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

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、Apex One (Mac) が実行する処理を指定します。

Apex One (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、Apex One (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。

Apex One (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	Apex One (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	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、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。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。
駆除	Apex One (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、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。

ウイルス検出時の処理	詳細
放置	Apex One (Mac) は、感染ファイルに対する処理を実行せず、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。 Apex One (Mac) は、誤検出を防止するため、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、Apex One (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、Apex One (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、Apex One (Mac) は「x_probable_virus」がトロイの木馬のプログラムとして検出するようになり、トロイの木馬の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。 注意 この処理は、リアルタイム検索に対しては使用できません。
アクセス拒否	Apex One (Mac) では、感染ファイルを開いたり、実行したりしようとする操作を検出すると、その操作を即時にブロックします。 ユーザは感染ファイルを手動で削除できます。

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、Apex One (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	Apex One (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	Apex One (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、「95 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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

検索のキャッシュ設定

検索を実行するたびに、セキュリティ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、セキュリティ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、セキュリティエージェントは、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、セキュリティエージェントはファイルの検索を省略します。
- 検索されたファイルのキャッシュに存在しない場合、セキュリティ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、Apex One (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、セキュリティエージェントはファイルの検索を省略します。
- 承認済みファイルのキャッシュに存在しない場合、セキュリティ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、99 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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

信頼済みプログラムリスト

セキュリティエージェントは、リアルタイム検索やイベント記録時に信頼済みプロセスの検索をスキップするよう設定できます。信頼済みプログラムリストにプログラムを追加すると、セキュリティエージェントでは、そのプログラムとそのプログラムで開始されるすべてのプロセスがリアルタイム検索とイベント記録の対象から除外されます。エンドポイントに対する検索のパフォーマンスを向上させるには、信頼済みプログラムリストに信頼するプログラムを追加してください。

注意

信頼済みプログラムリストに追加するファイルの要件は次のとおりです。

- システムディレクトリに格納されていない。
- 有効なデジタル署名がある。

信頼済みプログラムリストにプログラムを追加すると、セキュリティエージェントでは、そのプログラムが自動的に次の処理から除外されます。

- リアルタイム検索のファイル確認
- リアルタイム検索のプロセス検索
- イベント記録

信頼済みプログラムリストの設定

信頼済みプログラムリストを設定すると、特定のプログラムとそのプログラムから呼び出された子プロセスを、リアルタイム検索の対象から除外できます。

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セキュリティエージェントを含めるか、特定のグループまたはセキュリティエージェントを選択します。
3. [設定] > [信頼済みプログラムリスト] の順にクリックします。
4. 検索から除外するプログラムのフルパスを入力します。
5. [+追加] をクリックします。
6. リストからプログラムを削除するには、[削除] アイコンをクリックします。
7. 信頼済みプログラムリストをエクスポートするには、[エクスポート] をクリックし、ファイルのエクスポート先を選択します。

注意

Apex One (Mac) は、DAT 形式でこのリストを保存します。

8. 信頼済みプログラムリストをインポートするには、[インポート] をクリックし、ファイルの場所を選択します。
   a. [参照...] をクリックし、DAT ファイルの場所を選択します。
   b. [インポート] をクリックします。
9. エージェントツリーで 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

検索ログの表示

手動検索または予約検索を実行すると、Apex One (Mac)セキュリティエージェントでは、その検索に関する情報を含む検索ログが作成されます。検索ログを表示するには、Apex One (Mac) サーバコンソールまたはエージェントコンソールにアクセスします。

手順

1. [エージェント] > [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セキュリティエージェントを含めるか、特定のグループまたはセキュリティエージェントを選択します。

3. [ログ] > [検索ログ] 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。

   [検索ログ] 画面が表示されます。
5. 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。

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、136 ページの「ログの管理」を参照してください。

セキュリティリスク通知とログ

Apex One (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 Apex One (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。

Apex One (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

Apex One (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

Apex One (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。Apex One (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。

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	エージェントグループ名
%ii	エンドポイント IP アドレス
%nm	エンドポイント MAC アドレス
%p	セキュリティリスクの場所
%y	検出の日時

変数	説明
%a	実行された検索処理

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 Apex One (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 Apex One (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。Apex One (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、104 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、Apex One (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、固有ソースの数を 10、検出数を 100、期間を 5 時間と指定すると、5 時間以内に 10 個のセキュリティエージェントによって合計 101 個のセキュリティリスクが報告された時点で、Apex One (Mac) から通知が送信されます。すべてのインスタンスが同じセキュリティエージェントで 5 時間以内に検出された場合、Apex One (Mac) から通知は送信されません。

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。セキュリティエージェント名またはグループ名、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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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、108 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、136 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。Apex One (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、Apex One (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、Apex One (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、Apex One (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、110 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。
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。

駆除できないファイル	説明と解決策
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。

セキュリティリスクの検出数のリセット

[検出数のリセット] 画面に移動して、セキュリティリスクの検出数を 0 にリセットできます。

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セキュリティエージェントを含めるか、特定のグループまたはセキュリティエージェントを選択します。
3. [ログ] > [検出数のリセット] をクリックします。

   注意

   [セキュリティリスク] フィールドには、選択したセキュリティエージェント、選択したグループ内のすべてのセキュリティエージェントまたはすべてのセキュリティエージェントについて検出数の合計が表示されます。

4. [リセット] をクリックします。
5. [OK] をクリックします。

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 Apex One (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。

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

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、Apex One (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。使用するポリシーを決定するために、Apex One (Mac) はセキュリティエージェントの場所をチェックします。セキュリティエージェントが Apex One (Mac) サーバに接続できる場合、セキュリティエージェントの場所は「内部」になります。サーバに接続できない場合、セキュリティ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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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. 外部のセキュリティ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、外部のセキュリティエージェントは Web レピュテーションクエリを 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、163 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として、[高]、[中]、[低] のいずれかを選択します。

注意

Apex One (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、Apex One (Mac) は Web からの脅威であることが判明している URL のみをブロックします。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. 内部のセキュリティ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、内部のセキュリティエージェントは 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、163 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. 内部のセキュリティエージェントから Web レピュテーションクエリを Smart Protection Server に送信するには、[Smart Protection Server にクエリを送信する] を選択します。

- このオプションを有効にすると、セキュリティエージェントは Apex One セキュリティエージェントによって使用されている

Smart Protection ソースリストを参照して、クエリの送信先となる Smart Protection Server を決定します。

重要

このオプションを有効にする前に、30 ページの「Trend Micro Smart Protection」のガイドラインをお読みください。

- このオプションが無効な場合、セキュリティエージェントは Web レピュテーションクエリを Smart Protection Network に送信します。エンドポイントからクエリを送信するためにはインターネット接続が必要です。

d. 使用可能な Web レピュテーションのセキュリティレベルとして、[高]、[中]、[低] のいずれかを選択します。

注意

Apex One (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、Apex One (Mac) は Web からの脅威であることが判明している URL のみをブロックします。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。

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

---

e. 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。

f. セキュリティエージェントに、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。Apex One (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 に対して適切な処理を実行する場合には、セキュリティエージェントからのログの送信を許可します。

6. エージェントツリーで 1 つ以上のグループまたはセキュリティ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

またはセキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

承認済み URL リストと URL ブロックリストの設定

安全と考える Web サイトを承認済みリストに、管理者が危険と判断する Web サイトをブロックリストに追加します。Apex One (Mac) でこれらの Web サイトへのアクセスが検出されると、そのアクセスは自動的に許可またはブロックされ、Smart Protection ソースにもクエリは送信されません。

手順

1. [エージェント] > [Web レピュテーションの承認済み URL リスト/URL ブロックリスト] 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. [承認済みリストに追加] または [ブロックリストに追加] をクリックします。
4. エントリを削除するには、[表示] ドロップダウンリストからオプションを選択し、URL の横の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、内部セキュリティエージェントを設定します。Apex One (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セキュリティエージェントを含めるか、特定のグループまたはセキュリティ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。
   - Apex One (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、136 ページの「ログの管理」を参照してください。

第 8 章

デバイスコントロールの使用

この章では、デバイスコントロール機能を使用して、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。

デバイスコントロール

デバイスコントロールを使用すると、エンドポイントに接続された外部ストレージデバイスやネットワークリソースへのアクセスを制御できます。デバイスコントロールを使用するとデータの紛失や漏えいを防止でき、ファイル検索と組み合わせて使用することで、セキュリティリスクから保護することができます。

内部エージェントと外部エージェントに対してデバイスコントロールポリシーを設定できます。通常は、外部エージェントに対してより厳格なポリシーを設定します。

ポリシーはエージェントツリーできめ細かく設定できます。各ポリシーは、エージェントグループや個々のセキュリティエージェントに適用できます。1 つのポリシーをすべてのセキュリティエージェントに適用することもできます。

ストレージデバイスに対する権限

ストレージデバイスに対するデバイスコントロール権限は、次の場合に使用されます。

- USB ストレージデバイス、CD/DVD、SD カード、ネットワークドライブ、および Thunderbolt SATA ストレージデバイスへのアクセスを許可する場合。これらのデバイスへのフルアクセスを許可したり、アクセスレベルを制限したりすることができます。
- 承認済み USB ストレージデバイスのリストを設定する場合。デバイスコントロールでは、承認済みデバイスのリストに追加されている USB ストレージデバイスを除く、すべての USB ストレージデバイスへのアクセスをブロックできます。承認済みデバイスに対するフルアクセスを付与したり、アクセスレベルを制限したりすることができます。

次の表は、ストレージデバイスの権限をリストしたものです。

表 8-1. ストレージデバイスに対するデバイスコントロール権限

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 これは、デバイスにファイルを保存、移動、およびコピーできることを意味します。
読み取り専用	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
ブロック	禁止される操作: すべて デバイスとデバイスに含まれるファイルは、ユーザには (Finder などに) 表示されません。	禁止される操作: 保存、移動、コピー

注意

読み取り専用権限はネットワークドライブには適用できません。

デバイスコントロールの設定

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セキュリティエージェントを含めるか、特定のグループまたはセキュリティエージェントを選択します。
3. [設定] > [デバイスコントロール設定] をクリックします。
4. [外部エージェント] タブをクリックして外部エージェントの設定を行うか、[内部エージェント] タブをクリックして内部エージェントの設定を行います。
5. [デバイスコントロールを有効にする] を選択します。

6. [デバイス] で、ストレージデバイスごとに権限を選択します。

   権限の詳細については、122 ページの「ストレージデバイスに対する権限」を参照してください。

7. (オプション) USB ストレージデバイスの権限が [ブロック] になっている場合は、[USB ストレージデバイス承認済みリスト] で承認済みデバイスのリストを設定できます。ユーザはこれらのデバイスにアクセスでき、管理者は権限を使用してアクセスレベルを制御できます。

   ヒント

   承認済み USB デバイスのリストでは、アスタリスク (*) ワイルドカードを使用できます。フィールドにアスタリスク (*) を使用すると、他のフィールドの条件と一致するデバイスがすべてリストに追加されます。たとえば、[製造元]-[製品 ID]-* と指定すると、シリアル番号に関係なく、指定した製造元と製品タイプの USB デバイスがすべて承認済みリストに追加されます。

   a. USB ストレージデバイスの製造元、製品 ID、シリアル番号を入力します。

   b. [追加] をクリックします。

      ヒント

      リストからデバイスを削除するには、エントリを選択して [削除] をクリックします。

   c. デバイスの権限を選択します。

      権限の詳細については、122 ページの「ストレージデバイスに対する権限」を参照してください。

      注意

      承認済みリストの USB ストレージデバイスには、[デバイス] セクションの USB ストレージデバイスに設定された権限よりも高いレベルの権限が必要です。

8. [通知] で、[新しいデバイスが検出された場合にエージェントエンドポイントに通知メッセージを表示する] オプションを選択すると、新しいストレージデバイスがエンドポイントに接続されたときに通知が表示されます。通知には、新しいストレージデバイスのアクセス権限が表示されます。

9. エージェントツリーで 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

デバイスリストツール

コンピュータに接続された外部デバイスを照会するには、Windows コンピュータでデバイスリストツールをローカルに実行します。このツールは、外部デバイスを検索し、デバイス情報をブラウザ画面に表示します。この情報は、デバイスコントロールのデバイス設定を指定するときに使用できます。

デバイスリストツールの実行

注意

デバイスリストツールは、macOS または OS X を実行しているエンドポイントをサポートしていません。

手順

1. Apex One (Mac) 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¥ListDeviceInfo` に移動します。
2. 外部デバイスを対象の Windows コンピュータに接続します。
3. `listDeviceInfo.exe` を Windows コンピュータにコピーします。
4. Windows コンピュータで、`listDeviceInfo.exe` を実行します。
5. 表示されたブラウザ画面でデバイス情報を確認します。デバイスコントロールは、次の情報を使用します。
   - ベンダまたは製造元
   - モデルまたは製品 ID
   - シリアル ID またはシリアル番号

セキュリティエージェント向けのデバイスコントロール通知の設定

デバイスコントロール違反が発生したことをエンドユーザに通知するために、セキュリティエージェントエンドポイントに通知メッセージを表示するように Apex One (Mac)を設定できます。

手順

1. [通知] > [エージェント通知] に移動します。
2. [デバイスコントロール違反] で、初期設定のメッセージをそのまま使用するか変更します。

   次の表は、通知メッセージ表示用のデータを表すために使用できるトークン変数を示しています。

トークン	説明
%DeviceType%	セキュリティエージェントエンドポイント向けのデバイスの種類 (「USB ストレージデバイス」など)

トークン	説明
%Permission%	デバイスコントロールポリシー設定 (「ブロック」など)

3. [保存] をクリックします。

デバイスコントロールログの表示

新しいストレージデバイスをエンドポイントに接続すると、Apex One (Mac) セキュリティエージェントでは、デバイスコントロール設定に基づいたアクセス権限を使用してイベントのログエントリが作成されます。

手順

1. [エージェント] > [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セキュリティエージェントを含めるか、特定のグループまたはセキュリティエージェントを選択します。
3. [ログ] > [デバイスコントロールログ] をクリックします。
4. ログ条件を指定して [ログの表示] をクリックします。

   [デバイスコントロールログ] 画面が表示されます。
5. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] 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。

第 9 章

サーバおよびセキュリティエージェントの管理

この章では、Apex One (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。

権限とその他の設定

[権限とその他の設定] 画面では、セキュリティエージェントが使用するファイルを他のプログラムやユーザによって変更または削除されないように、エージェントセルフプロテクション機能を設定できます。

[エージェントで使用するファイルの保護] を有効にした状態で、セキュリティエージェントがエンドポイントで実行されている場合、Apex One (Mac) によって次のファイルとフォルダがロックされます。

- /Library/Application Support/TrendMicro/RPD
- /Users/*/Library/Application Support/TrendMicro/dlpmac.app
- /Library/LaunchDaemons/com.trendmicro.tmes.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.rpd.plist
- /Users/*/Library/Application Support/TrendMicro/chromeNativeDLP
- /Users/*/Library/Application Support/TrendMicro/firefoxNativeDLP

注意

Apex One (Mac) では`/Library/Application Support/TrendMicro/Tools` フォルダにファイルを追加できますが、このフォルダからファイルを削除することはできません。

エージェントセルフプロテクションの設定

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セキュリティエージェントを含めるか、特定のグループまたはセキュリティエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [セキュリティエージェントセルフプロテクション] で、[セキュリティエージェントで使用するファイルの保護] を選択します。

5. エージェントツリーで 1 つ以上のグループまたはセキュリティ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セキュリティ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: すべての既存のセキュリティエージェント、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セキュリティエージェントに、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セキュリティエージェントにのみ設定を適用します。今後追加されるグループに加えられるセキュリティエージェントにのみ設定を適用します。

ソフトウェア安全性評価サービスの有効化

ソフトウェア安全性評価サービスは、トレンドマイクロデータセンターに照会し、ウイルス対策検索によって検出されたプログラムの安全性を確認する機能です。ソフトウェア安全性評価サービスは、誤検出を減らす必要がある場合に有効にしてください。

手順

1. [エージェント] > [ソフトウェア安全性評価サービス] に移動します。
2. [ウイルス対策検索のソフトウェア安全性評価サービスを有効にする] を選択します。
3. [保存] をクリックします。

注意

- ネットワーク内のエンドポイントがインターネットへのアクセスにプロキシサーバを必要とする場合は、内部エージェント用にプロキシ設定を指定します。
- 詳細については、143 ページの「エージェント/サーバ間の通信の設定」を参照してください。

機械学習型検索の有効化

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。

この機能を有効にするには、[エージェント] > [エージェント管理] > [設定] > [機械学習型検索設定] に移動し、[機械学習型検索を有効にする] を選択します。

注意

ネットワーク内のエンドポイントがインターネットへのアクセスにプロキシサーバを必要とする場合は、内部エージェント用にプロキシ設定を指定します。

詳細については、143 ページの「エージェント/サーバ間の通信の設定」を参照してください。

サーバおよびセキュリティ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、Apex One (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、すぐにサーバとセキュリティ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、サーバおよびセキュリティエージェントに8 ページの「サーバのインストール要件」および36 ページの「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

重要

Apex One (Mac) Patch 2 以降をインストールするか、または Apex One (Mac) Patch 2 以降を適用する前に、Microsoft インターネットインフォメーションサービス (IIS) の証明書の有効期限が切れていないことを確認してください。

詳細については、https://success.trendmicro.com/dcx/s/solution/000283035?language=ja を参照してください。

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¥OfficeScan¥Addon¥TMSM`
    - `C:¥Program Files¥Trend Micro¥Apex One¥Addon¥TMSM`

    または

    - `C:¥Program Files (x86)¥Trend Micro¥OfficeScan¥Addon¥TMSM`

    - C:¥Program Files (x86)¥Trend Micro¥Apex One¥Addon¥TMSM
  - バックアップするファイル:
    - ..¥apache-activemq¥conf¥.*
    - ..¥apache-activemq¥bin¥wrapper.conf
    - .¥ServerInfo.plist
- データベースファイル。138 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. Apex One またはウイルスバスター Corp. Web コンソールを開いて、メインメニューの [プラグイン] をクリックします。
2. [Apex One (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 <サーバのインストールフォルダ>¥PCCSRV¥Download にダウンロードされます。

   <サーバのインストールフォルダ> は通常、C:¥Program Files¥Trend Micro¥OfficeScan または C:¥Program Files¥Trend Micro¥Apex One 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、Apex One またはウイルスバスター Corp.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、[ログ] > [サーバアップデート] をクリックします。
4. Apex One (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. [Apex One (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。

セキュリティエージェントのアップグレード

注意

エージェントのアップグレードを可能にするには、[エージェント管理] > [設定] > [アップデート設定] 画面で [エージェントにコンポーネントのアップデートを許可するが、エージェントプログラムのアップグレードと HotFix のインストールを禁止する] チェックボックスをオフにします。

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 [Apex One (Mac) エージェント] 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セキュリティ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、[Apex One (Mac) エージェント] 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 Apex One (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。

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、[アップデートステータス] の [プログラム] 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

Apex One (Mac) では、セキュリティリスクの検出、ブロックされた URL、検索、およびデバイスコントロールイベント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セキュリティ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

Apex One (Mac) ライセンスの表示、アクティベーション、および更新は、Web コンソールで実行します。

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	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	有効	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、162 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。
- 前回のアップデート: ライセンスが前回アップデートされた日時。

3. 新しいアクティベーションコードを指定するには、[新しいコード] をクリックします。
4. 表示された画面で、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。

   この画面には、トレンドマイクロの Web サイトへのリンクも表示されます。このリンクに進むと、ライセンスに関する詳細情報を表示できます。

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 Apex One (Mac)
   - Apex One (Mac) Main Service
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、138 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 Apex One (Mac)
   - Apex One (Mac) Main Service
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。

本リリースでの Apex Central および Control Manager の統合

本リリースの Apex One (Mac) では、Apex Central B4476 以降をサポートします。本リリースでは、Apex Central から Apex One (Mac) ポリシーを作成、管理、および配信し、エンドポイントを監視できます。

エンドポイントは、Apex Central の [Apex One (Mac) キーパフォーマンスインジケータ] ウィジェットを使用して監視できます。

詳細については、140 ページの「キーパフォーマンスインジケータウィジェット」を参照してください。

詳細については、Apex Central ドキュメントを参照してください。

注意

Apex Central または Control Manager を Apex One (Mac)サーバのアップデート元に指定することもできます。詳細については、59 ページの「サーバアップデート元の設定」を参照してください。

キーパフォーマンスインジケータウィジェット

Apex Central の [ダッシュボード] 画面にあるこのウィジェットを使用して、選択した条件に基づく Apex One (Mac) キーパフォーマンスインジケータ (KPI) を表示します。

ウィジェットを [ダッシュボード] 画面に追加する方法の詳細については、Apex Central または Control Manager のドキュメントを参照してください。

ヒント

初期設定では、このウィジェットは 15 回発生したイベントを「重要」( )、30 回発生したイベントを「重大」( ) としてマークします。必要に応じて、イベントしきい値をカスタマイズしてイベントを重要または重大とマークしてください。

サーバ接続設定

ウィジェットに表示するデータを取得する Apex Central サーバを指定します。

1. Apex Central で、[ダッシュボード] 画面に進みます。
2. [Apex One (Mac) キーパフォーマンスインジケータ] ウィジェットが追加されているタブをクリックします。
3. ウィジェットの右上のメニュー ( ) から、[サーバ設定] アイコン ( ) を選択します。

4. 1 つ以上の Apex One (Mac) サーバを選択します。
5. [保存] をクリックします。

キーパフォーマンスインジケータの設定

Apex Central または Control Manager の [ダッシュボード] で [Apex One (Mac) キーパフォーマンスインジケータ] ウィジェットにアクセスし、以下のインジケータ関連タスクを実行します。

表 9-1. KPI ウィジェットのインジケータタスク

タスク	手順
新しいインジケータを追加する	1. [インジケータの追加] をクリックします。[インジケータの追加] 画面が表示されます。 2. [名前] ドロップダウンリストからオプションを選択し、必要に応じて設定をカスタマイズします。 3. [保存] をクリックします。
インジケータを編集する	1. リスト内のインジケータをクリックします。[インジケータの編集] 画面が表示されます。 2. 設定をカスタマイズします。 3. [保存] をクリックします。
インジケータを削除する	1. リスト内のインジケータをクリックします。[インジケータの編集] 画面が表示されます。 2. [削除] をクリックします。 3. [OK] をクリックします。

タスク	手順
イベントしきい値を指定する	1. [インジケータの追加] または [インジケータの編集] 画面で、[アラートを有効にする] を選択します。 2. イベントの種類ごとに、イベントの最小発生件数を入力します。 3. [保存] をクリックします。 注意 次の両方の条件に当てはまる場合、[件数] 列に重要または重大アイコンが表示されます。 • このインジケータに対応するイベント発生件数がしきい値以上である。 • [アラートを有効にする] が選択されている。

ウィジェットの設定

Apex Central または Control Manager の [ダッシュボード] 画面で、ウィジェットの右上にあるメニューから [ウィジェット設定] を選択し、以下のタスクを実行します。

表 9-2. KPI のウィジェット設定

タスク	手順
ウィジェットタイトルを編集する	テキストフィールドにウィジェットタイトルを入力します。
毎日のアップデート時間を設定する	ドロップダウンリストから、毎日ウィジェットデータを生成する時間を選択します。 ヒント ウィジェットデータを手動で更新するには、更新 ( ) アイコンをクリックします。

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。Apex One (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。

重要

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計画がある場合や、Apex One の待機ポートを変更したりプロキシ設定を変更したり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。セキュリティエージェント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。

サーバは、セキュリティエージェントのバージョンに応じて、次のいずれかの待機ポート経由でセキュリティエージェントと通信します。

- セキュリティエージェントバージョン 3.5.3xxx 以上: 4343

  セキュリティエージェントでは、Apex One で設定されているのと同じ待機ポートを使用します (初期設定では 4343 です)。

- セキュリティエージェントバージョン 3.5.2xxx 以前: 61617

  セキュリティエージェントでは、既存のサーバおよび待機ポートの設定を使用します。この設定は変更できません。

注意

- 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、上記のポート番号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 Apex One 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。

手順

1. [管理] > [エージェント/サーバ間の通信] に移動します。

   [サーバ名と待機ポート] セクションには、サーバアドレスと待機ポートの情報が表示されます。

2. [プロキシ設定] でオプションを選択します。
   - プロキシなし: このオプションは、セキュリティエージェントを直接サーバに接続する場合に選択します。
   - システムのプロキシ設定をエージェントで使用: このオプションは、システムのプロキシ設定をエージェントコンソールで使用する場合に選択します。
   - エージェントをサーバに接続する際には、次のプロキシ設定を使用します: プロキシ設定を行うには、このオプションを選択し、表示されるフィールドを設定します。
     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。

3. [保存] をクリックします。
4. 設定を適用するために Apex One (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。

オフラインセキュリティエージェント

Apex One (Mac) は、次の場合にセキュリティエージェントをオフラインとして表示します。

- エージェントのアンインストールプログラム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た後に、サーバからセキュリティエージェントの登録を解除していない場合。
- サーバからセキュリティエージェントの登録を解除せずに、エンドポイントのハードドライブを再フォーマットした場合。
- エージェントファイルを手動で削除した場合。
- セキュリティエージェントを長期間にわたってアンロードまたは無効な状態にしておいた場合。

エージェントツリーにアクティブなセキュリティエージェントだけが表示されるようにするには、エージェントツリーからオフラインのセキュリティエージェントを自動的に削除するように Apex One (Mac) を設定します。

オフラインセキュリティエージェントの自動削除

手順

1. [管理] > [オフラインエージェント] の順に選択します。
2. [オフラインのエージェントの自動削除を有効にする] を選択します。

3. Apex One (Mac) でセキュリティエージェントを停止中と見なす日数を選択します。
4. [保存] をクリックします。

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
		セキュリティ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。
		セキュリティエージェントは稼働中ですが、上位サーバに接続していません。
		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。速やかにセキュリティエージェントをアップデートしてください。
		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セキュリティエージェントによって検出されました。
		セキュリティ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。
		セキュリティエージェントは、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。
		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、セキュリティエージェントを再起動する必要があります。
		セキュリティエージェントでスマートスキャンまたは Web レピュテーションサービスを使用できません。ネットワーク接続を確認してください。

トレイアイコン	メニューアイコン	説明
		セキュリティ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、セキュリティエージェント の機能の一部を使用できません。 詳細については、136 ページの「ライセンスの管理」を参照してください。
		セキュリティ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。 セキュリティエージェントが上位サーバに登録されてない場合は、すべての機能 (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、パターンファイルのアップデートを含む) が無効になります。
		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、有効期限が切れています。ライセンスの有効期限が切れている場合、セキュリティエージェントの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セキュリティエージェントがインストールされました。
		セキュリティエージェントが正常に機能していません。セキュリティ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。
		セキュリティ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 10 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、Apex One (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、8 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 Apex One (Mac)
   - Apex One Plug-in Manager
   - Apex One (Mac) Main Service
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
   - Apex One: `C:¥Program Files¥Trend Micro¥Apex One¥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。Apex One Web コンソールのバナーで、「Apex One」の「A」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、Apex One (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、Apex One (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. Apex One (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. Apex One (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¥OfficeScan¥Addon¥TMSM¥apache-activemq¥data¥*.*` または `C:¥Program Files¥Trend Micro¥Apex One¥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、Apex One (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¥Wow6432Node¥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¥Wow6432Node¥TrendMicro¥OfficeScan¥service¥AoS¥OSCE_ADDON_xxxx`)。
4. Apex One Plug-in Manager 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。

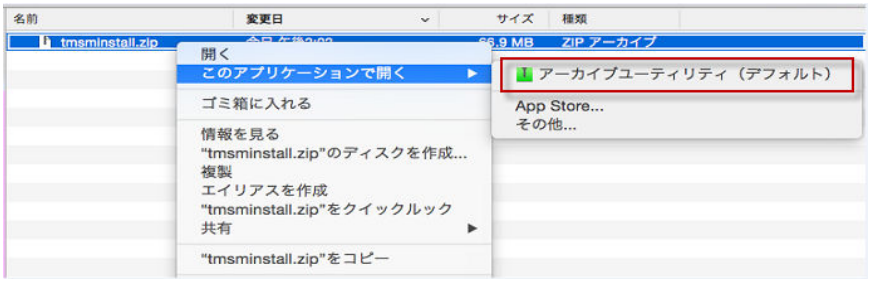
エージェントのインストール

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` または `tmsminstall.mpkg.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`) またはファイル (`tmsminstall.mpkg`) が破損しました。

手順

1. 解凍されたフォルダ (`tmsminstall`) またはファイル (`tmsminstall.mpkg`) 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。

- パッケージが `tmsminstall.zip` の場合:

```
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
```

- パッケージが tmsminstall.mpkg.zip の場合:

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

エージェント/サーバ間の通信

問題:

セキュリティエージェントがサーバと通信できません。

Apex One サーバで Web ホストの証明書をアップデートした場合、セキュリティエージェントはサーバに再接続する前に自動で新しい証明書を認証します。この処理にはしばらく時間がかかる場合があります。この処理の間、セキュリティエージェントはサーバとの接続を切断されます。

セキュリティエージェントが新しい証明書を認証したことを確かめるには、次に示すファイルがアップデートされ、最新のタイムスタンプが表示されていることを確認します。

- セキュリティエージェントのエンドポイント:

  ```
  /Library/Application Support/TrendMicro/common/conf/website.pem
  ```

- Apex One サーバ:

  - <TMSM>¥TMSM_HTML¥ActiveUpdate¥ClientInstall¥tmsminstall.zip

- <TMSM>¥TMSM_HTML¥A0FB621601F4D0FAB00B64F415A2C68C¥ClientInstall¥ServerInfoHttps.zip
- <TMSM>¥TMSM_HTML¥A0FB621601F4D0FAB00B64F415A2C68C¥ClientInstall¥ServerInfoHttpsLocal.zip

証明書の認証が完了した後もセキュリティエージェントがサーバに接続しない場合は、次の手順に従ってログを確認してください。

手順

1. サーバで、<サーバのインストールフォルダ>\debug.log からログを取得します。
2. セキュリティエージェントエンドポイントで、155 ページの「エージェントの一般的なエラー」の手順に従ってログを収集します。
3. 「error」または「fail」をキーワードとして使用し、ログを検索します。

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。

- 156 ページの「トラブルシューティングのリソース」
- 157 ページの「製品サポート情報」
- 158 ページの「トレンドマイクロへのウイルス解析依頼」
- 159 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/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 A

Apex One (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 Apex One (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、Apex One (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。

Apex One (Mac) サーバおよびセキュリティエージェントの IPv6 サポート

IPv6 のサポートは、IPv6 要件を満たす Apex One (Mac) サーバおよび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。

Apex One (Mac) セキュリティエージェントの IPv6 要件

Apex One (Mac) セキュリティ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、セキュリティエージェントに 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、Apex One (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。

項目	制限事項
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。Apex One (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、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 Apex One (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。

- Apex One (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。Apex One (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

Apex Central の統合, 139
IPv6 のサポート, 162
　制限事項, 162, 163
Smart Protection
　Web レピュテーションサービス, 30
　ファイルレピュテーションサービス, 30
Trend Micro Control Manager の統合, 139
Web からの脅威, 114
Web コンソール, 16
　概要, 16
Web レピュテーション, 114
Web レピュテーションサービス, 30

あ

ウィジェット, 26, 29
ウイルス/不正プログラムの検索
　結果, 108
エージェント/サーバ間の通信, 143, 154
エージェントセルフプロテクション, 130
エージェントツリー, 19
　一般的なタスク, 19
エージェントの移動, 25

か

権限
　ストレージデバイス, 122
検索の種類, 79
検索方法
　初期設定, 73
コンポーネント, 29

さ

従来型スキャン, 73–75
　スマートスキャンへ切り替える, 75
使用開始, 16
ストレージデバイス
　権限, 122
スマートスキャン, 73–75
　従来型スキャンから切り替える, 75
スマートフィードバック, 31
設定
　概要, 16

た

ダメージクリーンナップサービス, 3
デバイスコントロール, 121, 122
　権限, 122
　ストレージデバイス, 122
　通知, 126
　ログ, 127
デバイスリストツール, 125
トラブルシューティング
　エージェント/サーバ間の通信, 154
トロイの木馬プログラム, 3

は

ファイルレピュテーションサービス, 30
プログラム, 29