

おまかせアンチウイルス 初期設定簡易マニュアル

Ver5

2025年1月

東日本電信電話株式会社

『おまかせサイバーみまもり セキュリティパッケージ』を ご利用の方へ

本資料は、「おまかせアンチウイルス」をご利用の皆様に向けて作成されたものですが、「おまかせサイバーみまもり セキュリティパッケージ」をご利用の皆様にも、共通の資料としてご活用いただけます。

「おまかせサイバーみまもり セキュリティパッケージ」をご利用の方は『おまかせアンチウイルス』及び『おまかせアンチウイルスEDRプラス』という表記を『端末セキュリティ』へ読み替えてご確認ください。

目次

項目		ページ番号
サービスの概要		4
サービス提供までの流れ		6
機能一覧		7
ご利用までの流れ		8
事前準備		9
サービスへのログイン		10
エージェントインストール	エージェントインストールの流れ	12
	Windows	16
	Mac	19
	Android	38
	iPadOS/iOS	45
	Chromebook	58
機能の設定(Windows)		60

サービス概要

◆おまかせアンチウイルス概要

中小規模の企業向けのエンドポイント向けクラウド型セキュリティサービス

1 ウイルス対策 ※1 **おまかせアンチウイルス** **おまかせアンチウイルスライト**

※1 OSごとに使用できる機能が異なります。詳しくは営業担当者へお問い合わせください。

POINT

- パターンファイルやソフトウェアの最新版 ※2 へのバージョンアップも自動で対応
- 面倒な契約更新手続きは不要

※2 インターネット接続状況、管理者設定によっては、パターンファイルやソフトウェアバージョンが最新版にならない可能性があります。

多様化するウイルスに対応!

脅威の進化に素早く対応。

契約更新手続きが不要で
ライセンス切れの心配なし!

パッケージ版のウイルス対策ソフトの場合に必要な
なるライセンス契約の更新手続きが不要。

3 監視・サポート **おまかせアンチウイルス**

POINT

- 専用センタが端末を監視し、ウイルス駆除 ※3 ができなかった場合には連絡し対応方法についてサポート
- NTT東日本の専用センタにより、設定をサポート

※3 ウイルス駆除は動作の軽量化などの目的から、ウイルス検知後にお客さまご自身で専用のWebサイトからワクテンソフトをダウンロードしウイルス駆除する方法が一般的です。

パターンファイルの更新もれや万が一駆除が
できなかった場合、電話またはメールにてサポート

設定や機能の代行操作

月に一度の定期レポート



2 おまかせアンチウイルスがインストールされている端末を **一元管理** **おまかせアンチウイルス** **おまかせアンチウイルスライト**

POINT

- おまかせアンチウイルスがインストールされていれば、離れた拠点のパソコンやスマートフォン・タブレットも一元管理
- 従業員による勝手なウイルスソフトの設定変更を抑制

各端末の状況を
把握・一括制御

NTT東日本
が設定代行。
ウイルス感染
監視!



画像はイメージです。

一括制御・一元管理

本社

パソコン サーバー

支社

パソコン

持ち出し

パソコン スマートフォン

マルチデバイスに対応!
Windows®、Android™、
MacOSなどさまざまなOSに対応!

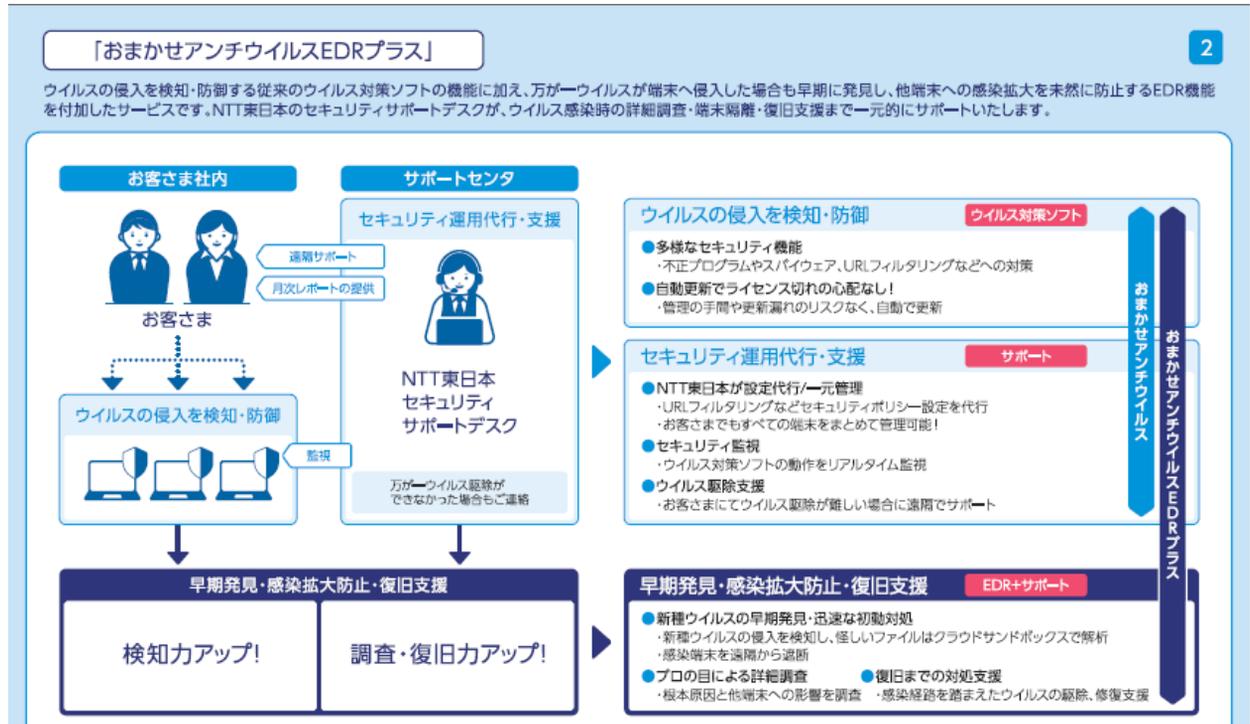
※ ③の監視・設定代行は『おまかせアンチウイルス ライト』では提供していません。

サービス概要 (おまかせアンチウイルス EDRプラス)

◆おまかせアンチウイルス EDRプラス概要

中小企業向けエンドポイント向けクラウド型EDRセキュリティサービス

※おまかせアンチウイルスとEDRプラスオプションを契約した場合の表記となります



サービスポイント

5

POINT 3



ウイルスの早期発見・感染拡大防止・復旧支援^{※1}

「おまかせアンチウイルスEDRプラス」のみ対象となります。

最新脅威の監視・対処

- 不審なファイルを仮想環境上で開き、自動で脅威か判定
- 不審な動きを検知した際は、必要に応じて、該当端末を隔離^{※2}

調査はプロにおまかせ

- ウイルス対策ソフトとEDR両方のログを確認しながらセキュリティのプロが根本原因を調査^{※3}
- 影響範囲を特定し、社内への更なる感染拡大を防止

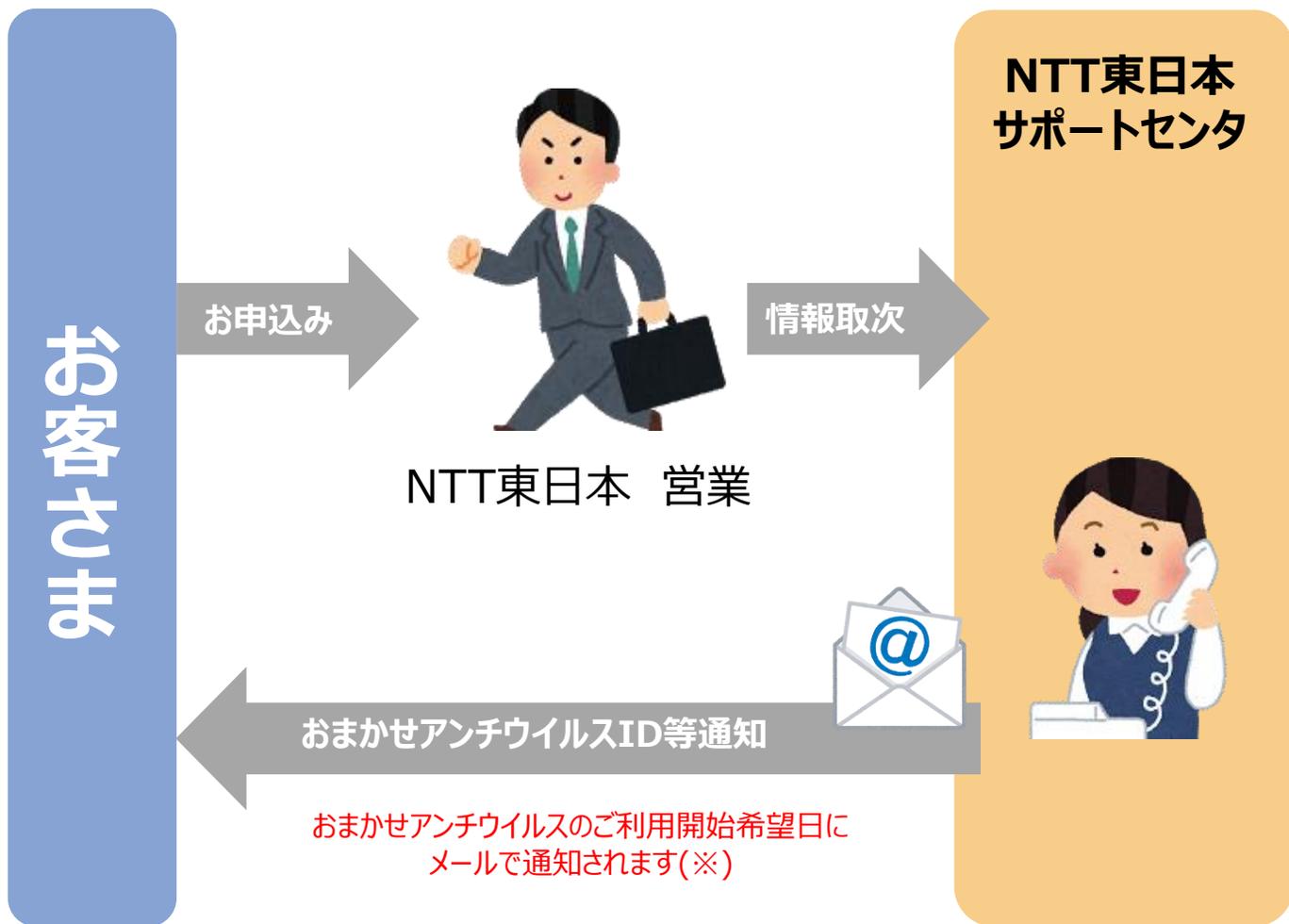
復旧作業も しっかりサポート

- 調査結果を踏まえ、ウイルス駆除や改ざんされた設定情報の修復などを遠隔支援
- 調査結果に応じてセキュリティポリシー設定を見直し

※1 サポートは日本語にて実施いたします。※2 端末隔離が必要だと弊社で判断した際には、事前にお客さまへご連絡し、了承を得られた場合に端末をネットワークから隔離いたします。※3 調査内容によっては、当日中に回答できない可能性があります。
 ○監視・調査・復旧代行に関しては、営業時間の午前9:00～午後9:00(年中無休)の間です。営業時間外に発生したアラームのお知らせは翌日に適宜対応いたします。○監視・調査・復旧代行に関して、感染などを弊社が発見した場合のお客さまへ通知する対象は「おまかせアンチウイルス」・「おまかせアンチウイルスEDRプラス」にて検知したウイルスや挙動に限ります。また、感染後の方への対応に関しても、解決、復旧を保証するものではありません。

※ EDRプラスオプションは『おまかせアンチウイルス ライト』では提供していません。

サービス提供までの流れ



- ※お客様の設定によっては、メールが迷惑メールフォルダなどに振り分けられる場合がございます。
- ※パスワード設定URLのアクセス期限は事前にお申込みいただいたご利用開始日から1週間以内です。
- ※送付先メールアドレスは別途送付書面「開通のご案内」をご確認ください。
- ※メールアドレスの訂正・変更は下記WEBサイトお問い合わせフォームからご依頼ください。
「おまかせアンチウイルスWEBサイト」<https://business.ntt-east.co.jp/service/antivirus/>
- ※その他、メールの不着、およびURLのアクセス期限を経過した場合は、セキュリティサポートデスクまでお問い合わせください。

開始

PC等におまかせアンチウイルスをインストールし、
ご利用開始

機能一覧

カテゴリ	機能名	説明	対応プラン			対応OS				
			EDR プラス	スタン ダード	ライ ット	Windows	Mac OS	Android	iOS/iPadOS	Chromebook
セキュリティ機能	侵入前防御	ウイルス対策/セキュリティリスク保護	○	○	○	○	○	○	-	-
		機械学習型検索	○	○	○	○	○	-	-	-
		挙動監視機能	○	○	○	○	-	-	-	-
		ファイルレス攻撃対応	○	○	○	○	-	-	-	-
		ランサムウェア対応	○	○	○	○	-	-	-	-
		仮想パッチ	○	○	○	○	-	-	-	-
		ファイアウォール機能	○	○	○	○	-	-	-	-
		Webレピュテーション	○	○	○	○	○	○	○	○
		URLフィルタリング	○	○	○	○	○	-	-	○
		情報漏えい対策	○	○	○	○	-	-	-	-
		デバイスコントロール	○	○	○	○	○	-	-	-
		アプリケーションコントロール	○	○	○	○	-	-	-	-
	パスワード/パスコード	○	○	○	-	-	○	○	-	
クラウドサンドボックス	○	-	-	○	○	-	-	-		
侵入後対処	EDR機能	EDR機能（Endpoint Detection and Response）が端末内のファイル操作、プログラム実行等様々な端末のログを監視し、不審な挙動を検知した場合、侵入経路や実行履歴、影響範囲を管理画面に表示	○	-	-	○	○	-	-	-
	遠隔端末隔離	感染を広げる可能性が高い感染端末を早期にネットワークから遮断	○	-	-	○	○	-	-	-
監視/サポート	インストールサポート	おまかせアンチウイルスエージェントのインストール支援	○	○	○	○	○	○	○	○
	設定代行	アンインストール禁止や、USB禁止など、WEB管理画面のセキュリティ設定を代行	○	○	-	○	○	○	○	○
	感染監視	端末にインストールされているおまかせアンチウイルスの検知状況や防御、隔離等の実行状況を監視	○	○	-	○	○	○	○	○
	EDRログ分析	EDR機能を活用して、端末のログを分析し、ウイルスかどうかの判定および感染原因や影響範囲を特定	○	-	-	○	○	-	-	-
	初動対応支援	感染の疑いがある場合は、管理者へ通知し、感染拡大防止のために端末のNW隔離や不審なプログラムの一時的ブロックを支援	○	-	-	○	○	-	-	-
	対処復旧支援	万が一ウイルスに感染し支援が必要な場合には、管理者へ通知し、ウイルス駆除や対処を支援	○	○	-	○	○	○	○	○
	月次レポート	月に一度、ウイルス対策や挙動監視機能、URLフィルタリングなどの検知状況をまとめたレポートを提供 月に一度、EDR機能の検知状況およびセキュリティ推奨設定をまとめたレポートを提供	○	○	-	○	○	-	-	-
基本機能	一元管理機能	ウイルスの検知状況や各端末のポリシー設定をWEB管理画面にて一元管理	○	○	○	○	○	○	○	○

ご利用までの流れ

【STEP1】 事前準備

既存でご利用中のウイルス対策ソフト及びMDMソフトをアンインストールする

【STEP2】 サービスへのログイン

- 1 開通日に届くメールを準備します。
※件名：【NTT東日本】おまかせアンチウイルス・おまかせサイバーみまもり・おまかせデータレスPC新規アカウント発行のお知らせ
- 2 パスワードを設定します。
- 3 管理者用URLをクリックし、ログイン画面を開きます。
- 4 アカウント名、手順2で設定したパスワードを入力し、ログインします。

【STEP3】 エージェントツールのインストール ※利用者へメール通知する方法で記載

- 1 エージェントインストール用URLを利用者へ通知する。
- 2 エージェントをインストールする機器でURLをクリックし、インストーラをダウンロードする。
- 3 インストーラを実行し、インストールする。

【STEP4】 各種機能を設定する

事前準備

既存でご利用中のウイルス対策ソフト及びMDMソフトのアンインストール

- ・**ウイルス対策ソフトやMDMソフト(※1)が入っている場合**、本サービスのインストールが行えない場合があるため、**事前にアンインストール**をお願い致します。
 - ※市販のウイルス対策ソフトは、本サービスインストール時に自動でアンインストールされますが、失敗する事例もあるため、必ず**手動でアンインストール**を実施ください。
- ・アンインストール後は、必ず**端末の再起動**を実施下さい。

<Windows10の場合>

- 「スタートボタンを右クリック」
 - ⇒「アプリと機能」
 - ⇒「プログラムのアンインストール」

<Macの場合>

- ・App Store からインストールしたアプリを削除するには、まず Launchpad を開きます。
 - ⇒ LaunchPad を起動後、どれか一つアプリを長押しします。
 - ⇒ アプリの左上に × マークが表示されます。
 - ⇒ 削除したいアプリの × マークをクリックします。
- ・App Store 以外からインストールしたアプリの場合、アンインストールプログラムが用意されている場合は、そのプログラムをクリックしてアンインストールを実施。

※他社の法人向けウイルス対策サービスをご利用中の場合、アンインストールを行う際にアンインストールパスワードを要求される場合がございます。その場合は、アンインストールパスワードを確認の上、アンインストールを実施します。

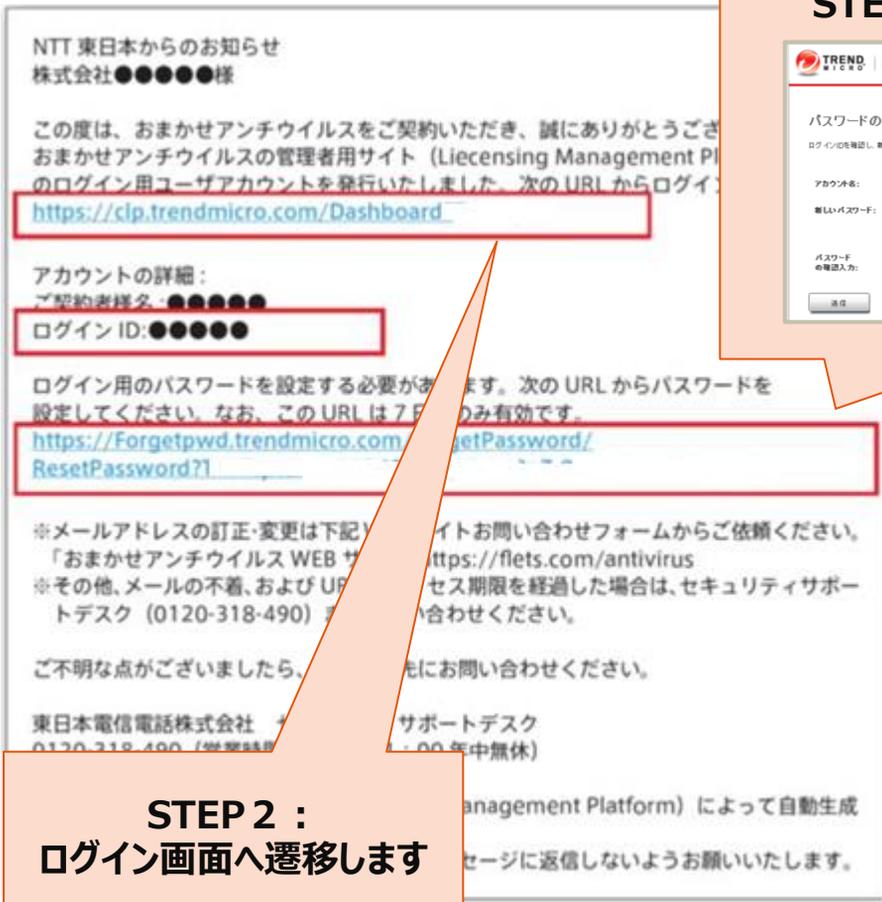
(※1)MDMとは…

モバイルデバイスマネジメントの略。スマートフォンやタブレット端末を安全に利用するための各種機能制限などを実施するサービスを指します。

サービスへのログイン

おまかせアンチウイルスご利用いただくために必要なPWを設定し、おまかせアンチウイルスにログインします。

件名：【NTT東日本】おまかせアンチウイルス・サイバーみまもり・データレスPC・クラウドアップセキュリティ新規アカウント発行のお知らせ のメールを使います。



STEP 1 : PWを設定します

STEP 2 : ログイン画面へ遷移します

STEP 3 : 『アカウントID (ログインID)』 『設定したPW』を入力し、ログイン

サービスへのログイン

二要素認証を設定していない場合、管理コンソールにログインをすると下記のメッセージが表示されます。

二要素認証とは…

- 管理コンソールのログインにあたり、従来の ID・パスワードに加えて“ワンタイムパスワード”を用いて認証を行うことで、セキュリティをさらに強化（第三者からの管理コンソールへの不正にログインを防止）することができます。
- ご利用の場合には、お手持ちの PC やスマートフォンに、第三者の提供するトークンアプリをインストール・設定する必要があります。
- トークンアプリは NTT 東日本およびトレンドマイクロ社の提供するものではなく、これをご利用になったことにより何らかの損害が発生した場合でも NTT 東日本およびトレンドマイクロ社では責任を負いかねますので、ご了承ください。

※二要素認証の設定手順はおまかせアンチウイルス公式HPに掲載されているマニュアルを参照ください。
おまかせアンチウイルス公式HP：<https://business.ntt-east.co.jp/support/antivirus/>

▲ セキュリティをさらに強化

サイバー犯罪が高度化するにつれて、不正アクセスからインターネットアカウントを保護するにはパスワード保護だけでは不十分な場合があります。アカウントを適切に保護するために、2要素認証をただちに有効にすることを強く推奨します。



2要素認証とは
2要素認証により、モバイルデバイスを使ってアカウントへのサインイン時に本人確認を行うことが可能になります。2要素認証によりセキュリティが強化され、パスワードが盗まれた場合でも、不正アクセスを防ぐことができます。
[詳細](#)

2要素認証が重要な理由
サイバー犯罪者によって本アカウントに不正アクセスされた場合、本コンソールからアクセス可能なトレンドマイクロ製品の保護をすべてオフにされる恐れがあります。それにより個人データ、企業機密、銀行情報への不正アクセスや、盗用、ランサムウェア、破損などの被害を受けやすくなる可能性があります。トレンドマイクロはアカウントを保護するために、2要素認証をただちに有効にすることを強く推奨します。

今後このメッセージを表示しない

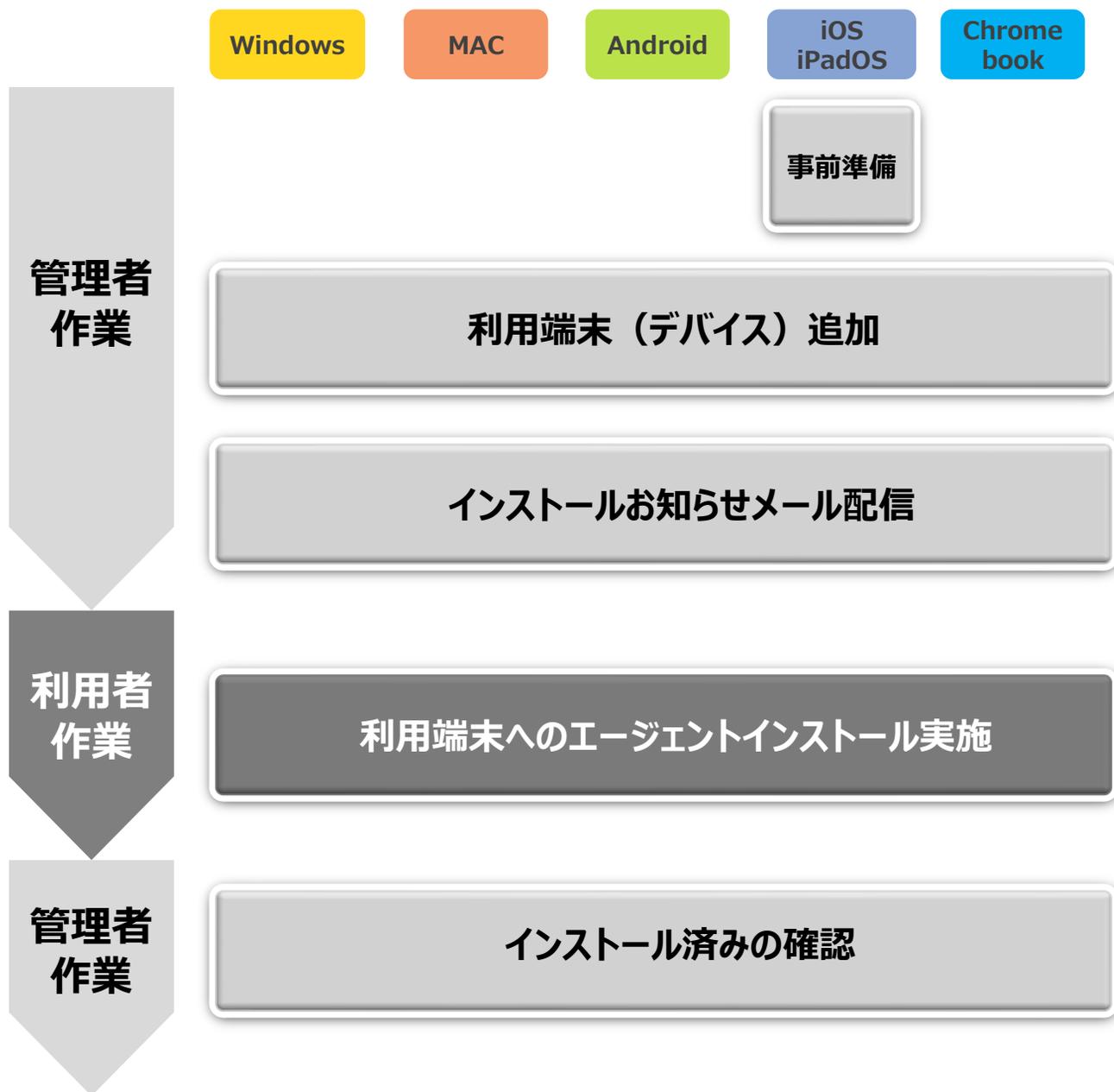
危険性を理解したうえで、スキップします

設定する場合はココをクリック

設定しない場合はココをクリック

エージェントのインストールの流れ

ウイルス対策を行いたい端末に対し、専用のエージェントのインストールが必要です。



次ページより、管理者作業および各OS毎のエージェントのインストール方法を記載しております。

エージェントツールのインストール

管理者作業

利用者作業

NTT 東日本

おまかせアンチウイルス

登録情報を入力してください

アカウント:

パスワード:

[パスワードのリセット \(パスワードをお忘れの場合\)](#)

アカウント名を記憶する

ログイン

アカウントをまだ取得していない場合 [今すぐ登録](#)

As a service provider, this platform gives you:

- Instant Provisioning - Provision your customer anytime.

① ログインIDを入力

② 設定したPWを入力

③ ログインをクリック

エージェントツールのインストール

管理者作業

利用者作業

サービスプラン名	製品/サービス	シート/ユニット	ライセンス種別	開始日	有効期限	アクション
おまかせアンチウイルス ライト	ウイルスバスター ビジネスセキュリティサービス	5シート	製品版	2017/05/17	自動更新	🔗 コンソールを開く

① コンソールを開くから管理コンソールにいきます

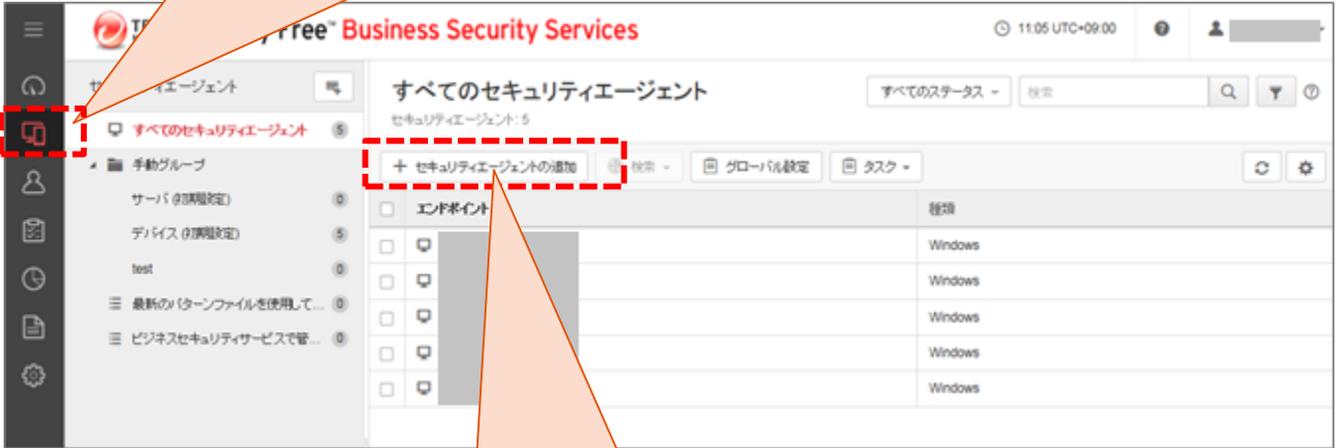
サービスプラン名	製品/サービス	シート/ユニット	ライセンス種別	開始日	有効期限
おまかせアンチウイルス EDRプラス	▼ Worry-Free Co-Managed XDR for Endpoint (3コンポーネント)	1シート	製品版	2024/02/07	自動更新

コンポーネント

- Worry-Free Managed Detection and Response
- ウイルスバスター ビジネスセキュリティサービス EDR
- ウイルスバスター ビジネスセキュリティサービス

※「おまかせアンチウイルスEDRプラス」の場合は、▼ボタンを押下し、「コンソールを開く」をクリックします。

② セキュリティエージェントタブをクリックします
※一番上の「☰」マークをクリックするとタブの名前を確認できます



③ セキュリティエージェントの追加をクリックします

エージェントツールのインストール

管理者作業

利用者作業



② 利用者の端末にインストールする場合は、こちらをクリックします

① 管理者の端末にインストールする場合は、こちらをクリックします



③ テキストをコピーし、利用者にメール送付します

管理者作業

利用者作業

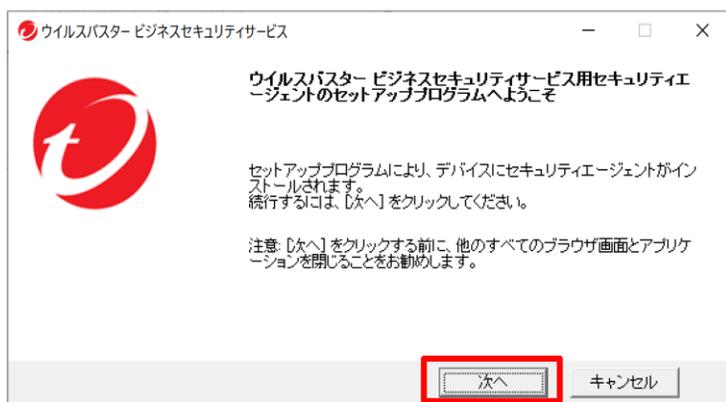
【EDRプラスをご利用の場合】

Windowsエージェントは、EDR機能は自動で有効化されるため、有効化作業は不要となります。EDRプラスを新規でご利用される場合は、下記手順に従い、アンチウイルスエージェントのインストール作業を実施してください。

※MacのEDR有効化は有効化作業が必要なため、後の「EDRエージェント有効化」を参照ください。

1. Windowsコンピュータでブラウザを開き、管理者から周知されたインストール用のリンクを入力します。
2. 下のような画面が表示されたら、[ダウンロード]をクリックします。インストールプロセスが開始されたら[実行]をクリックして、インストールを進めます。
※ラベル情報の記入欄が表示された場合、指定の内容を記入します。

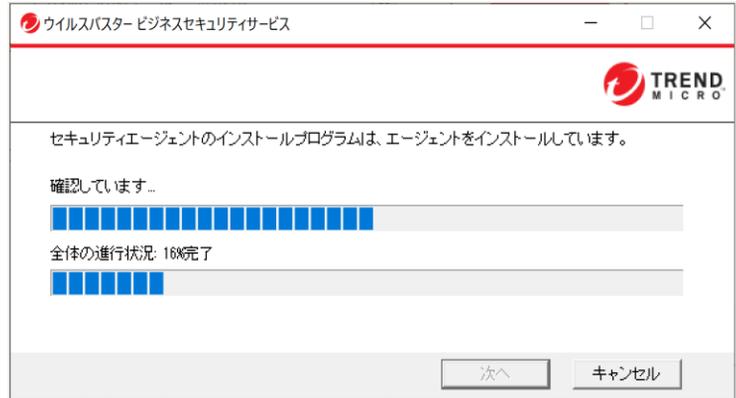
3. インストールプロセスが開始されたら[実行]をクリックして、インストールを進めます。
4. 下の画面が表示されたら、[次へ]をクリックします。



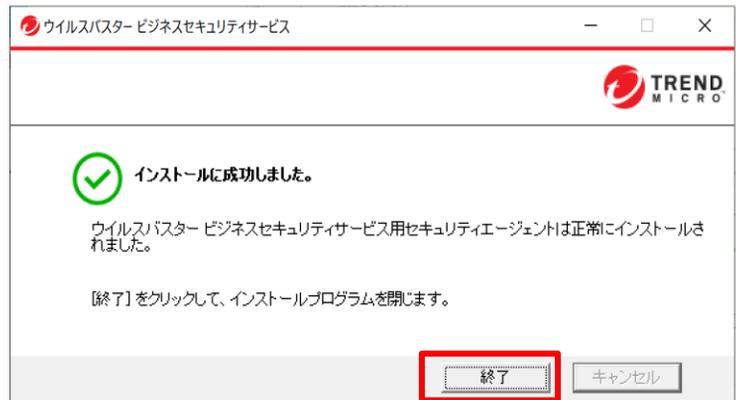
管理者作業

利用者作業

5. インストールが開始されます。



6. インストールが完了したら、[終了]をクリックして終了します。



7. タスクトレイ上に右記のようなアイコンが作成されます。インストールは完了です。

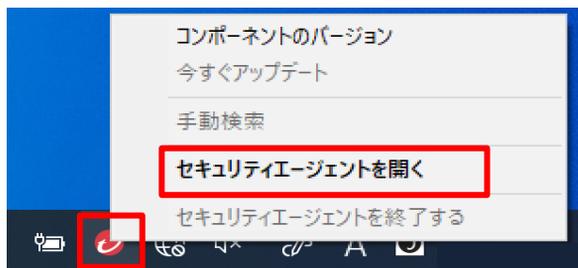


エージェントツールのインストール

管理者作業

利用者作業

セキュリティエージェントのアイコンを右クリックし、「セキュリティエージェントを開く」を選択すると、状況を確認することが出来ます。



1 : ステータス

2 : ログ

3 : 設定



4 : ツール

番号	機能	詳細
1	ステータス	 保護が有効
		 コンピュータの再起動が必要/危険な状態
		 今すぐアップデートが必要/Chromeの再起動が必要
		 スマートスキャン使用不可/コンピュータの再起動が必要/アップデートが必要
2	ログ	関連するログ情報が表示されます。
3	設定	エージェントの各設定の表示および設定に使用されます。
4	<u>ユーザツール</u>	トレンドマイクロが提供するその他のツールに関する情報が示されます。

※管理者によって機能設定の権限が与えられていない場合、表示されない項目があります。

管理者作業

利用者作業

1. Macコンピュータでブラウザを開き、管理者から周知されたインストール用のリンクを入力します。
2. 下のような画面が表示されたら、[ダウンロード]をクリックします。インストールパッケージ(WFBS-SVC_Agent_Installer.pkg)のダウンロードが開始されます。
※ラベル情報の記入欄が表示された場合、指定の内容を記入します。



TREND | ウイルスバスター ビジネスセキュリティサービス

ビジネスセキュリティクライアントのインストール

ラベル情報
管理者から提供された情報を入力します。

デバイスラベル:

手順

1. 下の [ダウンロード] をクリックして、インストールプロセスを開始します。
2. [実行] をクリックして、インストーラをダウンロードします。[保存] をクリックしないでください。

ダウンロード

注意: WFBS-SVC_Agent_Installer.exeは他のコンピュータにコピーできません。インストールプロセスは、ダウンロードURLから開始する必要があります。

3. ダウンロード完了後、「WFBS-SVC_Agent_Installer.pkg」をクリックし、インストールを実行します。

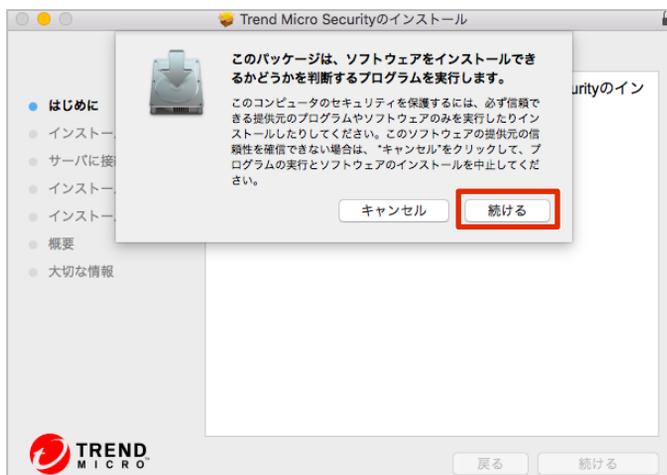


エージェントツールのインストール

管理者作業

利用者作業

4. [続ける]をクリックし、インストールを進めます。(3回繰り返す)

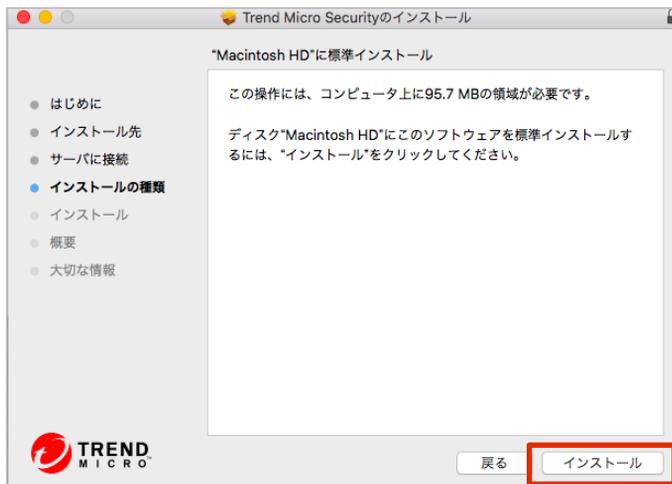


エージェントツールのインストール

管理者作業

利用者作業

5. 標準インストール確認画面が表示されます。[インストール]をクリックします。



6. 「インストーラが新しいソフトウェアをインストールしようとしています。」と表示された場合は、名前(ご利用のMac OSのユーザ名)とパスワードを入力し、[ソフトウェアをインストール]をクリックします。

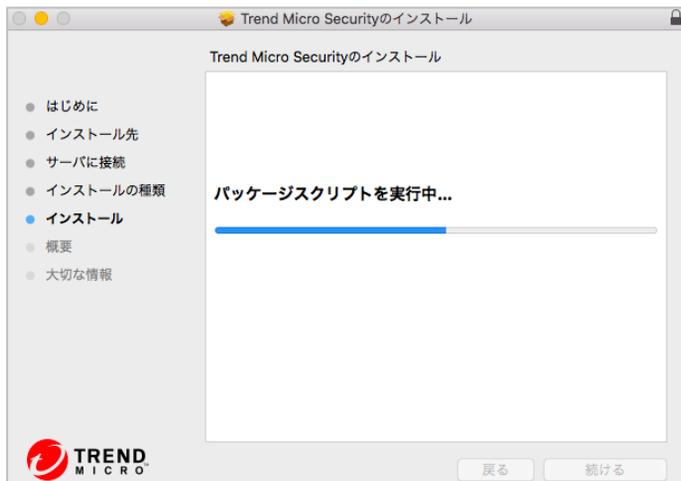


エージェントツールのインストール

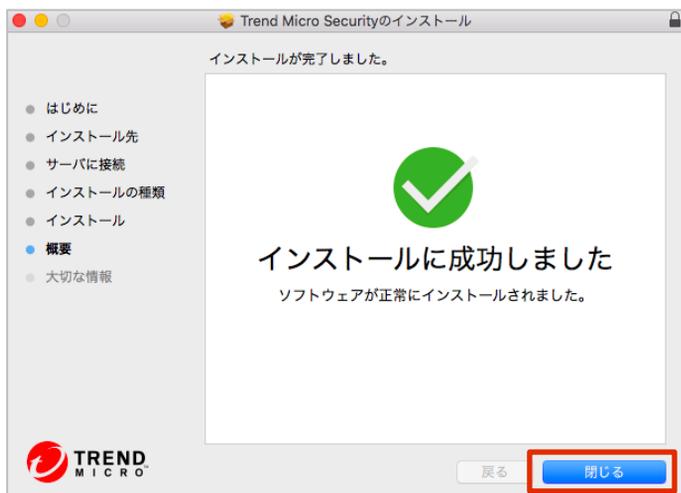
管理者作業

利用者作業

7. インストールが開始されます。画面が変わるまでお待ちください。



8. 「インストールに成功しました」というメッセージが表示されたら登録は完了です。「閉じる」をクリックして終了します。



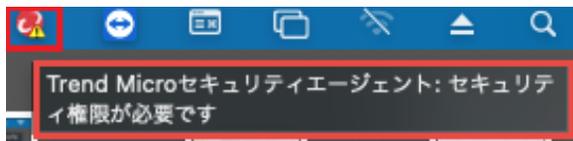
管理者作業

利用者作業

Macエージェントのアイコン上に警告が表示される時の対処方法

概要

おまかせアンチウイルス Mac版エージェントのアイコン上に警告が表示されます。また、アイコンにマウスオーバーすると「セキュリティ権限が必要です」と表示されます。



詳細

おまかせアンチウイルス Mac版エージェントは動作にあたりいくつかの権限を必要とします。2020年10月24日のメンテナンスにおいて、必要な権限が足りない場合はUI上から確認できるようになりました。おまかせアンチウイルスに必要な権限が不足している場合、アイコン上に警告が表示されます。警告が表示された場合は以下の作業を実施し、おまかせアンチウイルスに必要な権限を付与してください。

なお、おまかせアンチウイルスエージェントを新規にインストールした場合や、おまかせアンチウイルスエージェントがアップグレードされた場合には、下記の画面が表示されますので、その場合は [続行] をクリックし、次ページ以降の「作業手順」3.から作業を実施ください。



管理者作業

利用者作業

作業手順

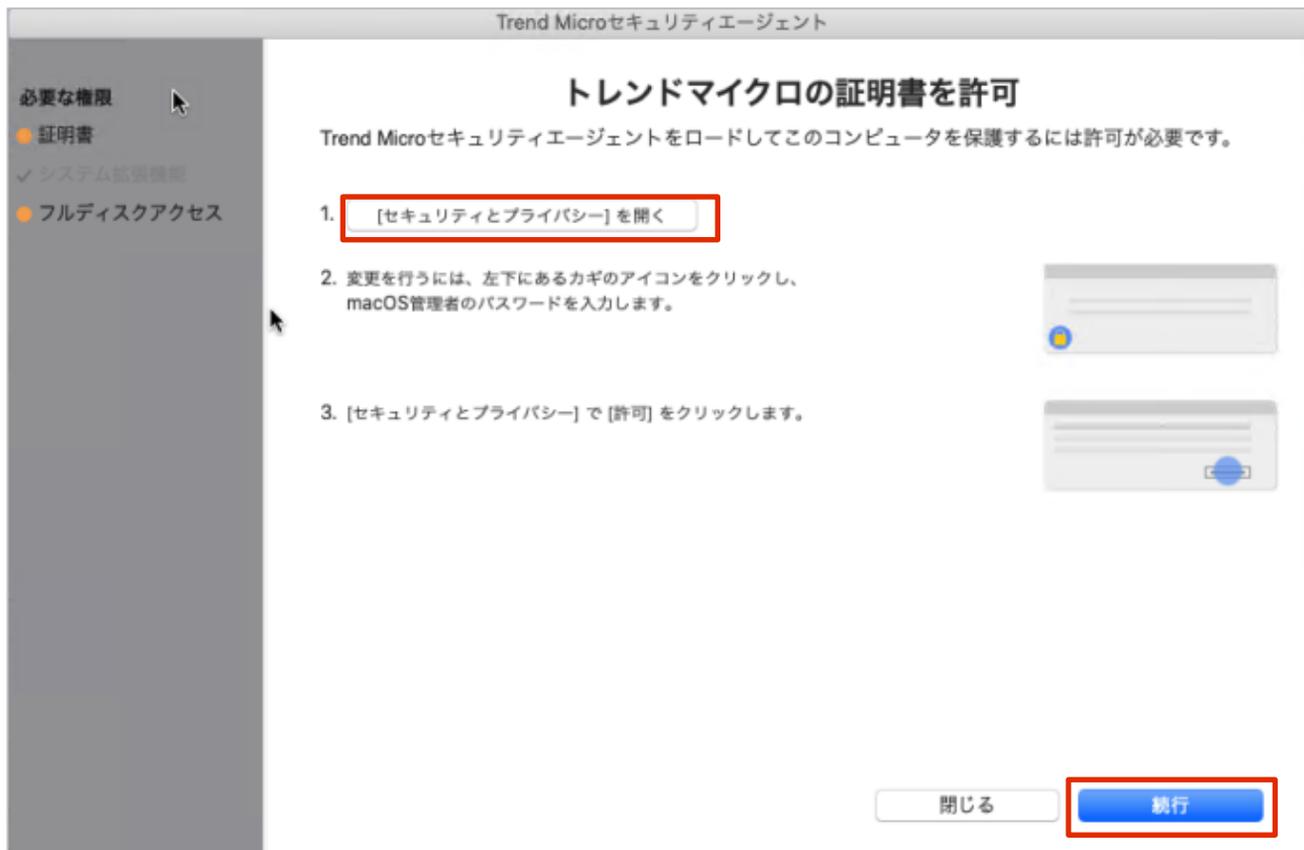
1. Mac端末上の「アプリケーション」から「Trend Microセキュリティエージェント」を選択して開きます。
2. 「セキュリティ権限が必要」と表示されますので [詳細を表示] をクリックします。



管理者作業

利用者作業

3. 「トレンドマイクロの証明書を許可」の画面で画面の指示にしたがって設定を行います。



3-1. 「セキュリティとプライバシー」画面を開きます。

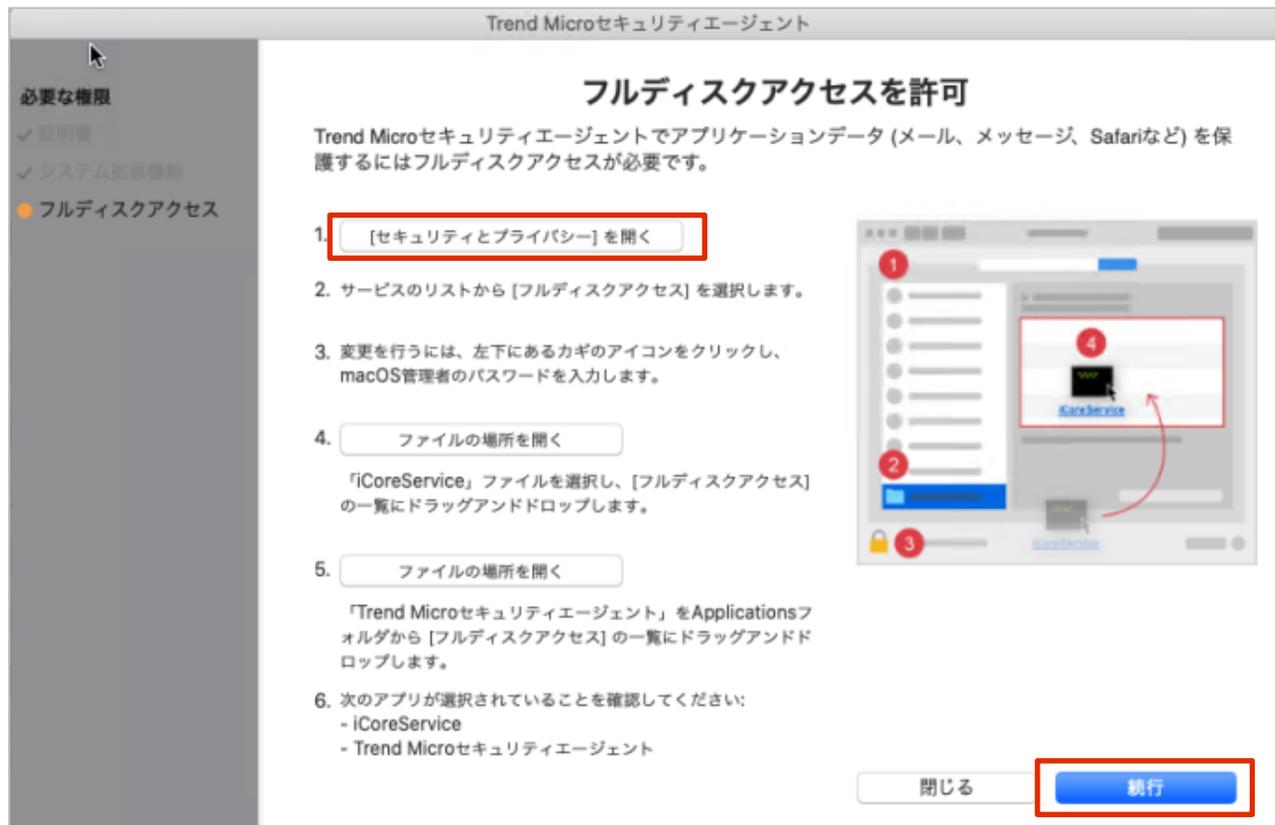
3-2. 「開発元「Trend Micro, Inc.」のシステムソフトウェアの読み込みがブロックされました」と記載がある横の「許可」ボタンをクリックします。複数の製品で承認が必要な場合、は許可ボタンをクリック後、署名元が表示されます。「Trend Micro, Inc.」にチェックボックスを入れて許可を完了してください。なお、すでに許可済みの場合、「Trend Micro, Inc.」は表示されませんので、その場合は本手順はスキップしてください。

3-3. [続行] をクリックします。

管理者作業

利用者作業

4. 「フルディスクアクセスを許可」の画面で画面の指示にしたがって設定を行います。



4-1. [セキュリティとプライバシー]画面を開きます。 ※イメージ図は次ページ参照

4-2. [プライバシー]タブを開き、画面左下のカギマークをクリックしてロックを解除します。

4-3. 続いて、[フルディスクアクセス]を開いて[+]をクリックします。

4-4. 「フルディスクアクセスを許可」の画面に戻り、4番の「ファイルの場所を開く」をクリックして表示された「iCoreService」を[フルディスクアクセス]の一覧にドラッグアンドドロップします。

4-5. 「フルディスクアクセスを許可」の画面に戻り、5番の「ファイルの場所を開く」をクリックして表示された「Trend Microセキュリティエージェント」を [フルディスクアクセス] の一覧にドラッグアンドドロップします。

※ 「iCoreService」につきましては、すでに追加されている場合でも、改めて4-4の手順をご実施ください。

※ 「Trend Microセキュリティエージェント」がすでに追加されている場合には、チェックが入っている事をご確認ください。もしチェックが入っていない場合には、チェックを入れてください。

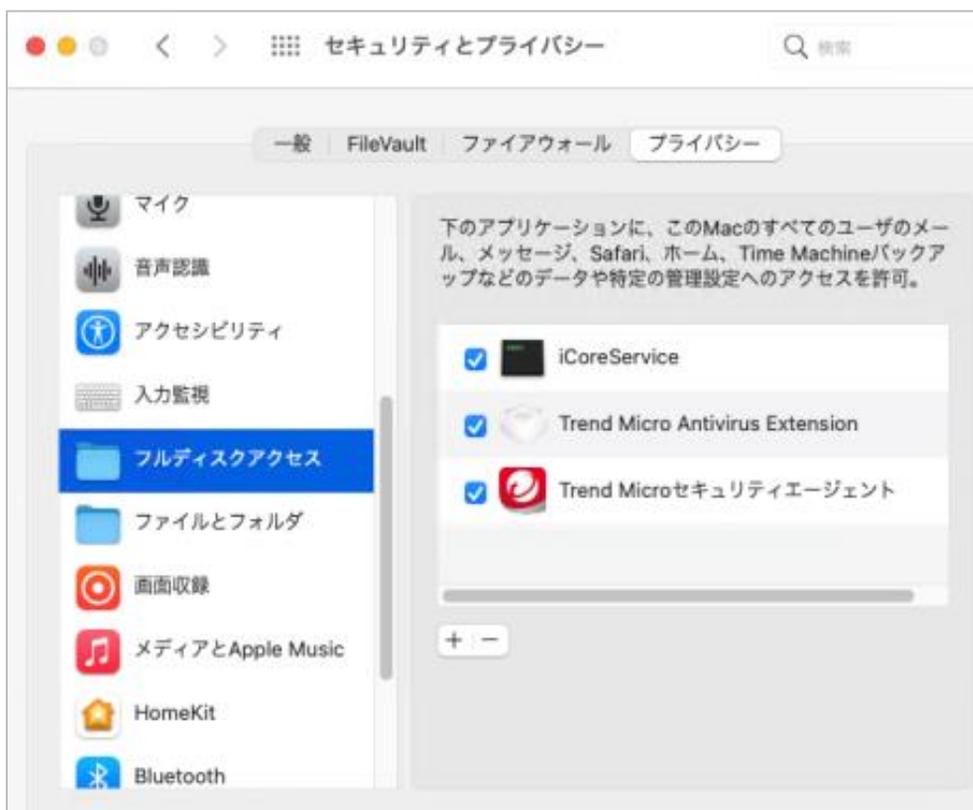
※ macOS 11 Big Sur をご利用の場合は、「TrendMicro Antivirus Extension」についても追加とチェックが必要となります。

エージェントツールのインストール

管理者作業

利用者作業

4-6. 「セキュリティとプライバシー」画面を閉じ、[続行] をクリックします。



5. [OK] をクリックすると自動的にセキュリティエージェントが再起動されます。再起動が完了したら必要な権限の付与設定は完了です。

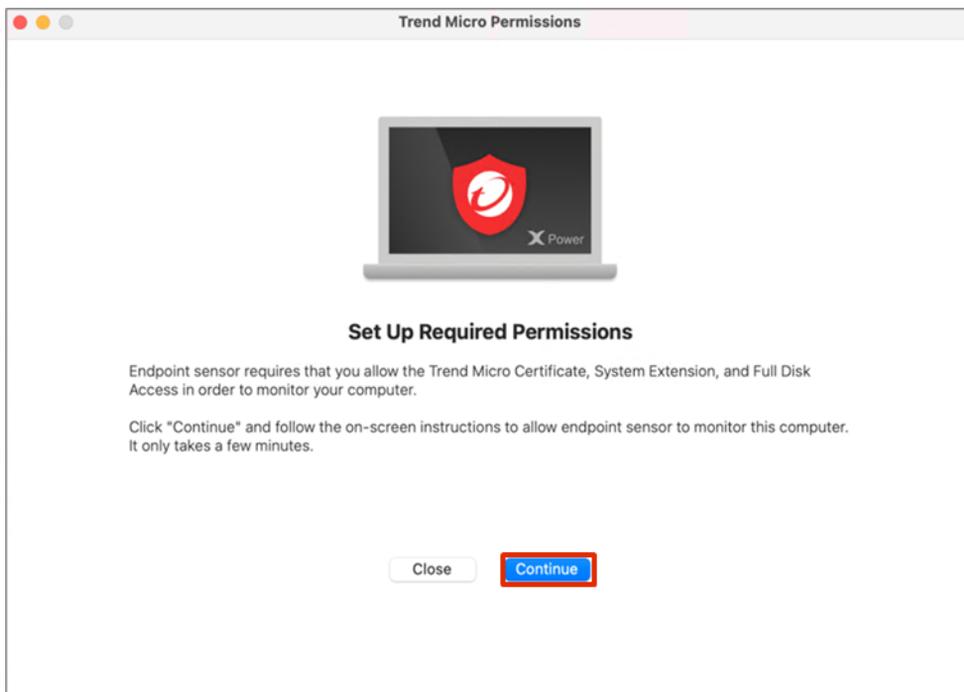


管理者作業**利用者作業****【EDRプラスをご利用の場合】**

Macについては、既におまかせアンチウイルスをインストール済みのお客様もEDRエージェントの有効化作業が必要となりますので、以下手順を参考に実施をお願いいたします。

1. 以下セットアップ画面において、「Continue」をクリックします

※「Close」を押下して表示されていない状況であれば、XDRアプリ  のアイコンをクリックすることで再度権限セットアップ画面の再表示が可能です。



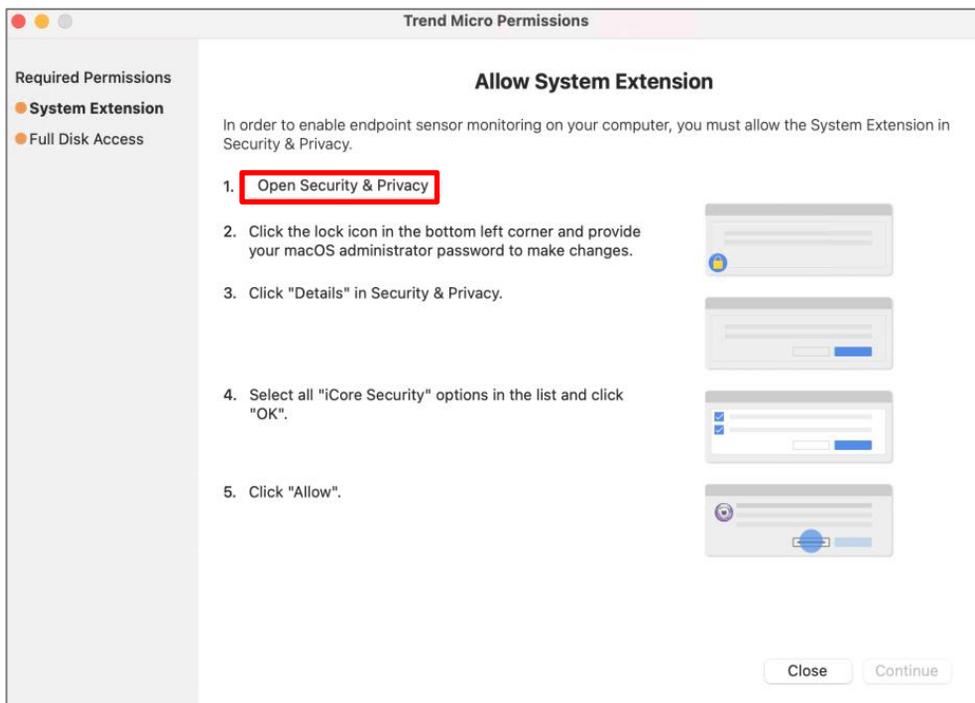
2. 以下画面が表示された場合は、「システム設定を開く」をクリックします。



管理者作業

利用者作業

3. 「Allow System Extension」画面において、「Open Security & Privacy」をクリックします



4. 「セキュリティとプライバシー」画面において、「詳細...」をクリックします。

一部のシステムソフトウェアでは、使用する前に確認が求められます。

詳細...

管理者作業利用者作業

5. 以下画面において、ユーザ名、パスワードを入力し、「設定を変更」をクリックします。



6. 以下画面において、iCoreサービスを全て選択し、OKをクリックします

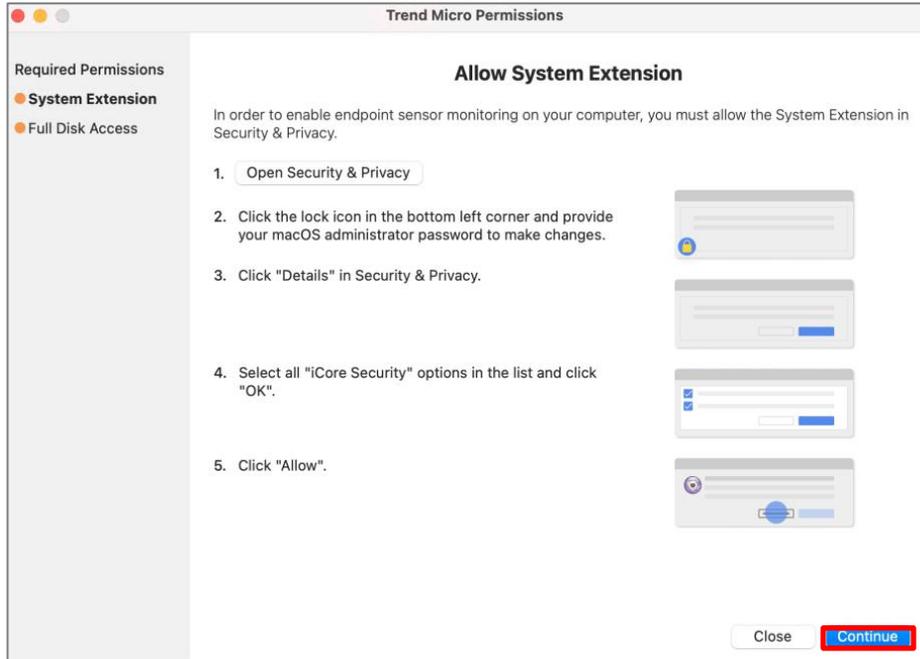


7. 以下画面において、許可をクリックします

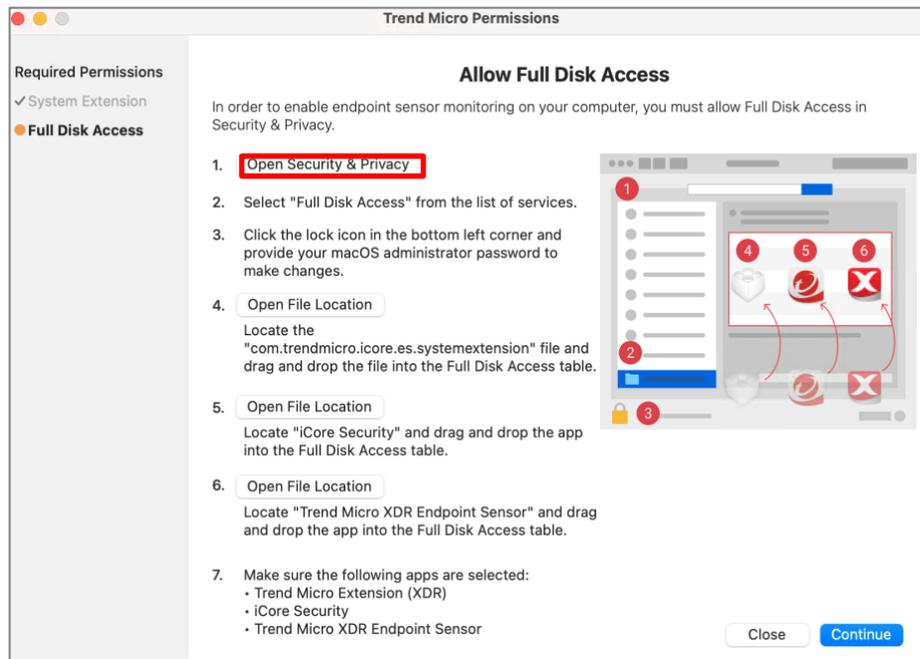


管理者作業利用者作業

8. 「Allow System Extension」の設定が完了したので、「Continue」をクリックします。

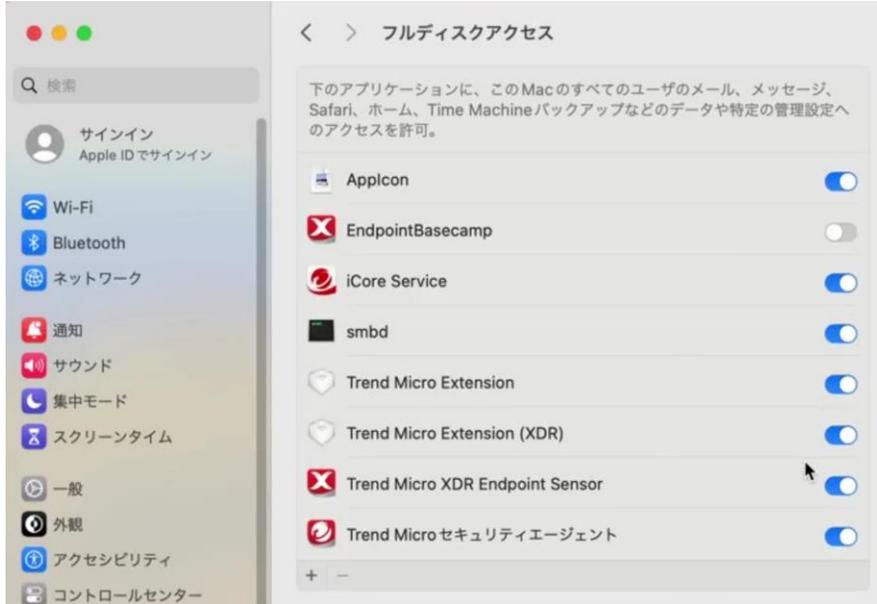


9. 「Allow Full Disk Access」画面にて、「Open Security & Privacy」をクリックします。

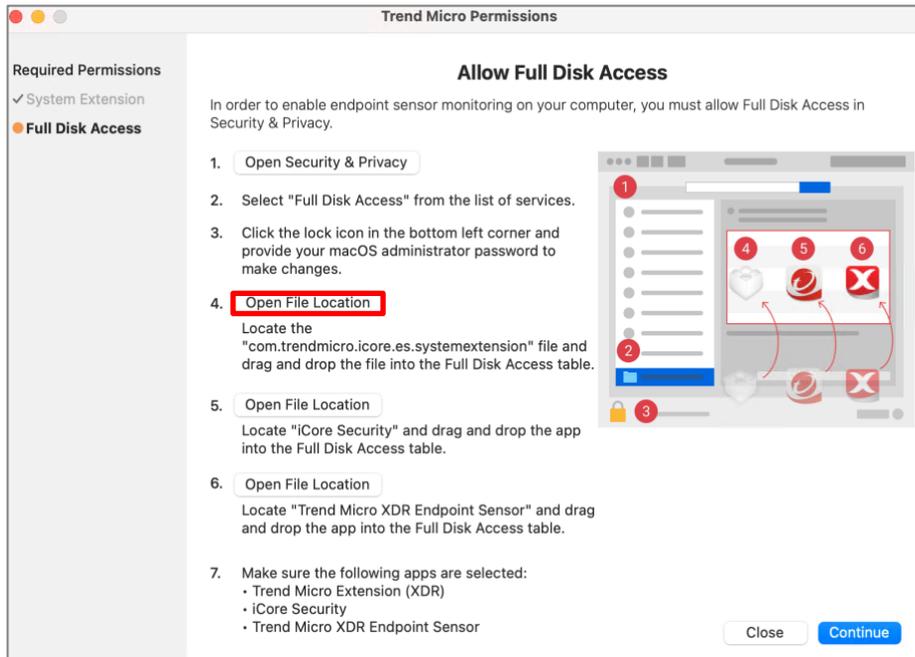


管理者作業利用者作業

10. 「フルディスクアクセス」を確認します。

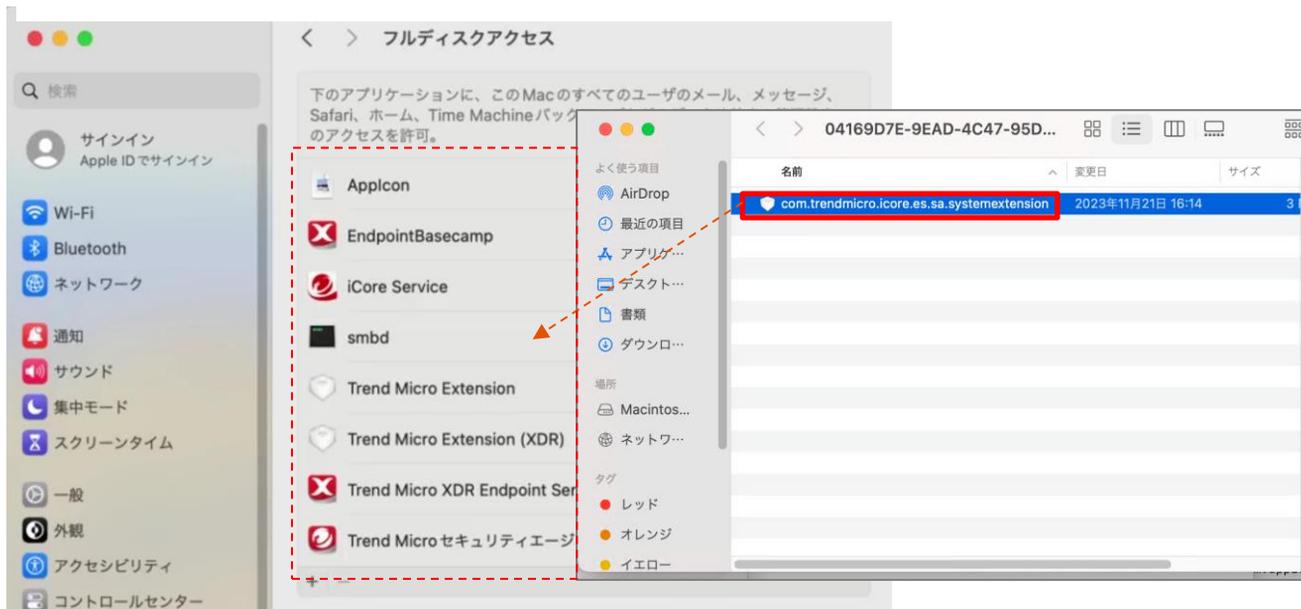


11. 「Allow Full Disk Access」画面にて、「4.Open File Location」をクリックします。

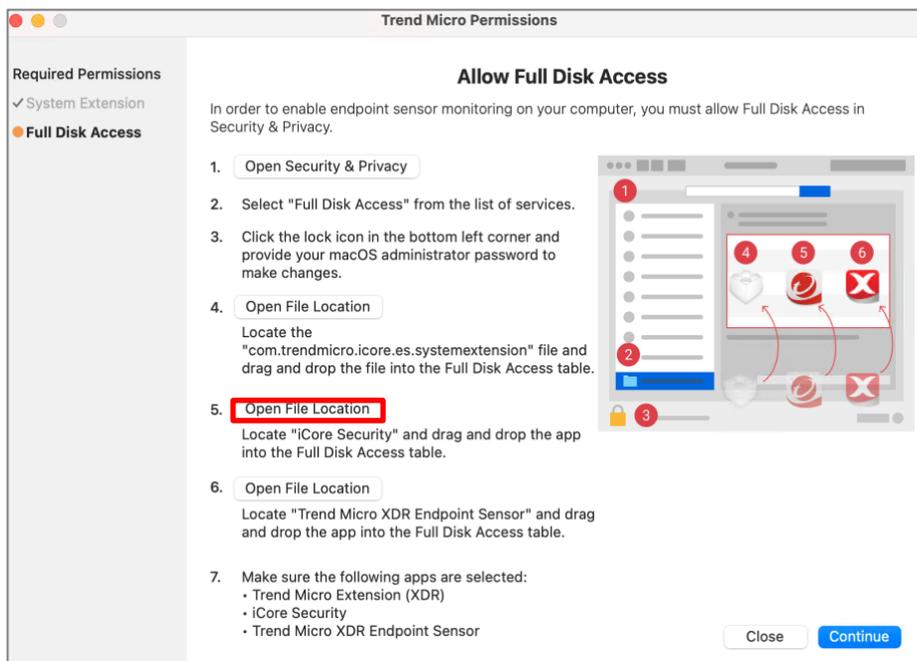


管理者作業利用者作業

12. 「フルディスクアクセス」を選択し、「com.trendmicro.icore.es.systemextension」をフルディスクアクセスの一覧にドラッグアンドドロップします。ドロップする該当アイコンがONに変わります。

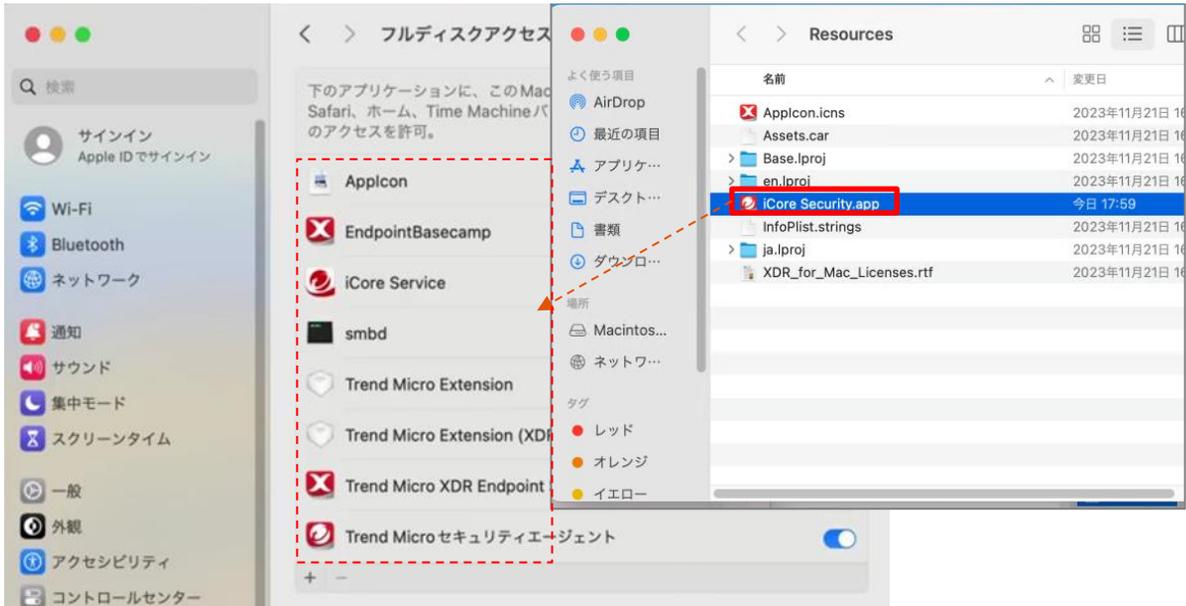


13. 「Allow Full Disk Access」画面にて、「5.Open File Location」をクリックします。

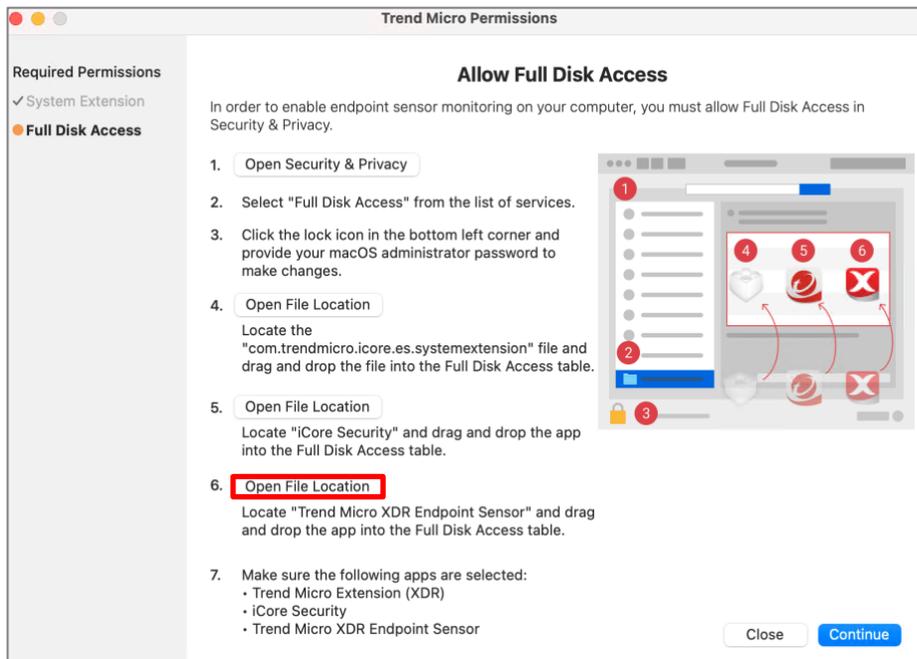


管理者作業利用者作業

14. 「フルディスクアクセス」を選択し、「iCore Security」をフルディスクアクセスの一覧にドラッグアンドドロップします。ドロップする該当アイコンがONに変わります。

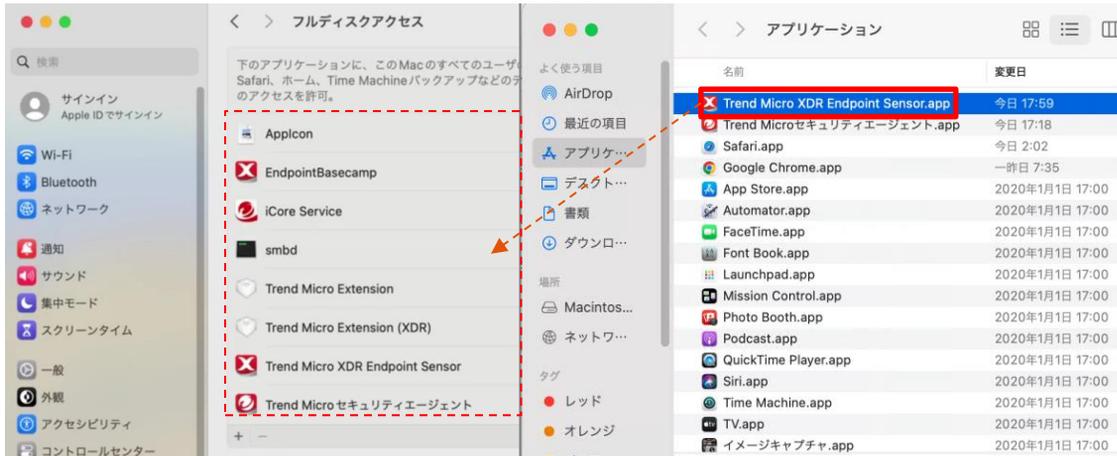


15. 「Allow Full Disk Access」画面にて、「6.Open File Location」をクリックします。



管理者作業利用者作業

16. 「フルディスクアクセス」を選択し、「Trend Micro XDR Endpoint Sensor」をフルディスクアクセスの一覧にドラッグアンドドロップします。ドロップする該当アイコンがONに変わります。



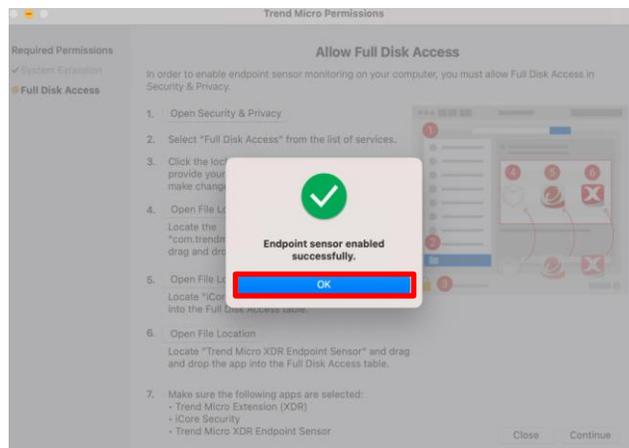
17. 以下画面が表示された場合、「あとで行う」をクリックします。



18. 以下画面にて、「OK」をクリックします。

※OSバージョン10.15では、端末再起動が必要です

※17で[終了して再度開く]をクリックした場合は、こちらの画面は表示されませんが、設定作業は正常に完了しています



管理者作業利用者作業

以上で、MacEDRの有効化作業は完了となります。

インストール完了しますと、以下赤枠のアイコン（おまかせアンチウイルス）をクリックすると「Endpoint Sensor」のステータスが、緑（有効化）になっております



有効化されていない場合、グレー表示

管理者作業

利用者作業

Mac版のEDRエージェントアンインストール作業については、専用のアンインストールツールが必要となりますので、NTT東日本セキュリティサポートデスクまでご連絡ください。

※管理コンソールの「ツール」よりダウンロード可能なアンインストーラ (WFBS-SVC_Agent_Uninstaller.app.zip) は使用しないでください。実行した場合、おまかせアンチウイルスエージェントのみアンインストールされEDRエージェントが残ってしまいます。

管理者作業

利用者作業

1. Androidデバイスからインストール用のリンクにアクセスします。
2. 下記のような画面が表示されたら、[インストール]をタップし、インストールを開始します。



3. インストールが開始されたら「インストール中...」が表示されます。



4. インストールが完了したら開くをタップします。



管理者作業

利用者作業

5. メールアドレスを入力してサインインします

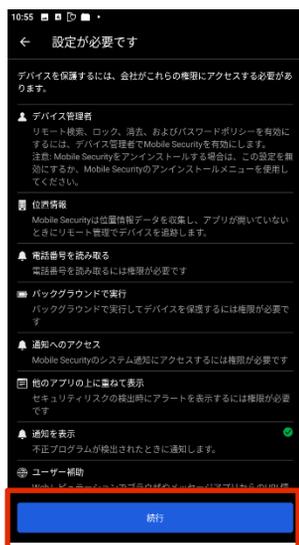


「このアプリではすでに他の多数のユーザがインストールしています。管理者に問い合わせてください。」



※上記のエラーメッセージが表示された場合は、ご契約いただいているライセンス数に空きがありませんので、以降のインストール作業を行うことができません。
管理画面よりご不要な端末を削除してからインストール作業を行ってください。

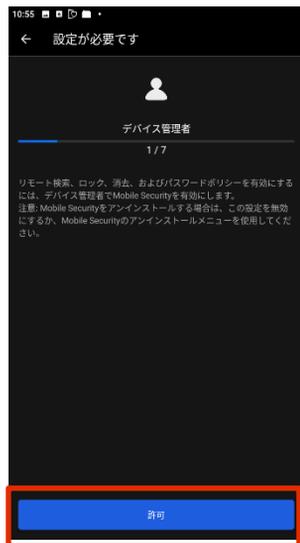
6. デバイス管理機能を有効にするか選択する画面で「続行」をタップします。



管理者作業

利用者作業

7. 端末管理アプリの有効化を行います。



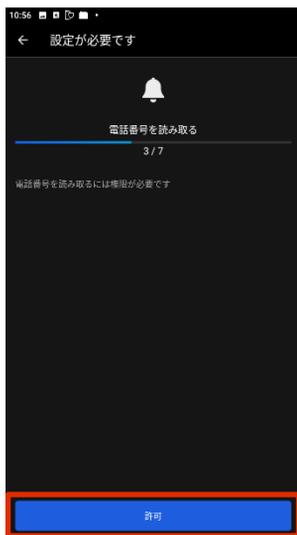
8. 位置情報へのアクセスを許可します。



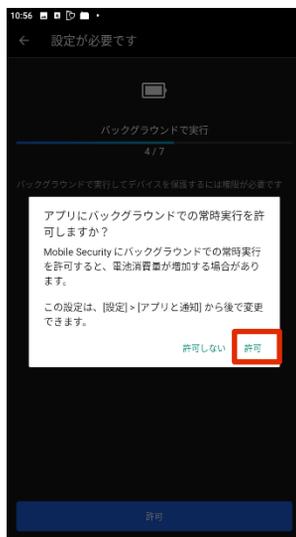
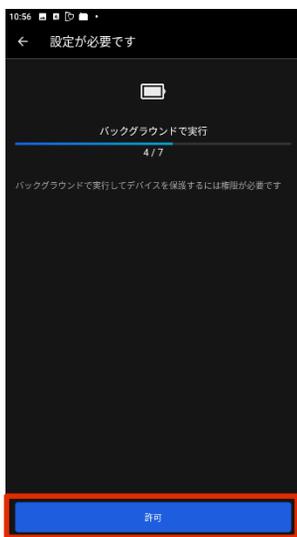
管理者作業

利用者作業

9. 電話の発信と管理を許可します。



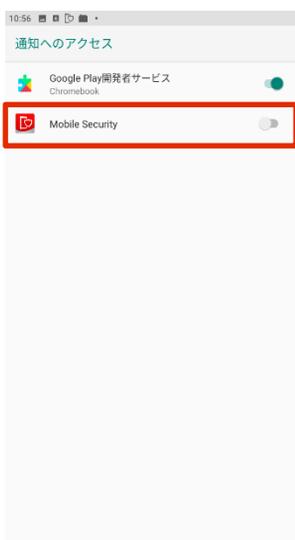
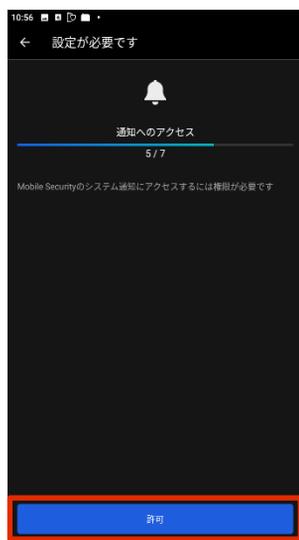
10. バックグラウンドでの実行を許可します。



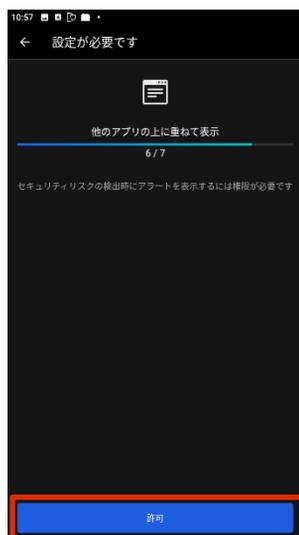
管理者作業

利用者作業

11.「通知へのアクセス」画面でスイッチを切り替え、設定を有効化します。



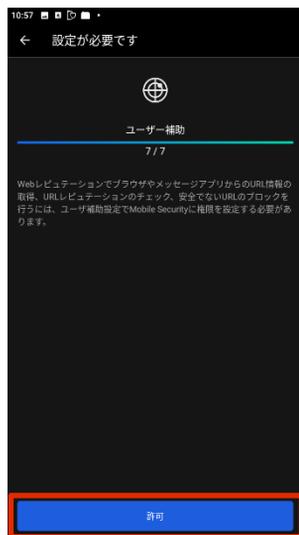
12.「他のアプリのうえに重ねて表示」画面でスイッチを切り替え、設定を有効化します。



管理者作業

利用者作業

13. ユーザー補助を許可します。



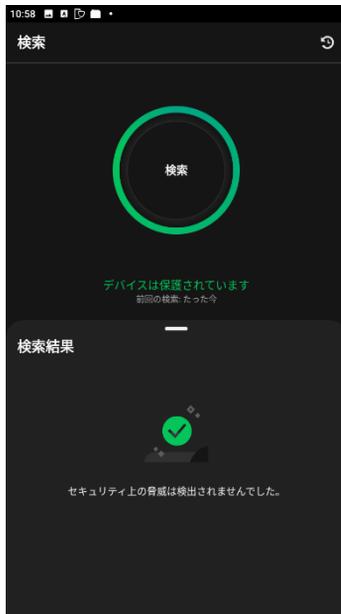
14. Mobile Securityの利用を開始します。



管理者作業

利用者作業

15. デバイスの登録が開始され、登録完了後に下記の画面が表示されたら登録は完了です。



16. Androidデバイス内に下記ようなアイコンが作成されます。



管理者作業利用者作業

はじめにお読みください

- Apple社のサイトへアクセスする際には、必ずSafariまたはGoogle Chromeでアクセスしてください。
- iPadOS/iOSモバイルデバイスを登録する際に、管理者はAPNs証明書を作成する必要があります。
 - ※ 1つの管理コンソール画面につき1つの証明書が必要です。
 - ※ ご利用端末数分の証明書は必要ありません。
- APNs証明書を作成するには、Apple IDが必要です。更新時には、作成時に使用したApple IDを紛失すると、各デバイスへ再インストールとなります。使用したApple IDは必ず保管しておいてください。
- iPadOS/iOSデバイスへは「Trend Micro Worry Free Business Security Service」がプロファイルとしてインストールされます。
- iOS,iPadOS端末へインストールする場合には、Web管理コンソールを利用するためのWindows/Mac端末が別途必要です。

管理者作業

利用者作業

1. 「管理」タブを開き、「モバイルデバイス登録設定」をクリックします。



2. [APNs証明書のアップロード]ボタンをクリックします。



3. [Trend Micro CSRのダウンロード]をクリックし、Trend Micro CSR (Certificate Signing Request) をダウンロードします。



4. Apple Push Certificate Portalサイトへアクセスします。(SafariまたはGoogle Chromeを使用してアクセスしてください。その他のブラウザの場合、表示が崩れたり正しい証明書が作成できないことがあります。)

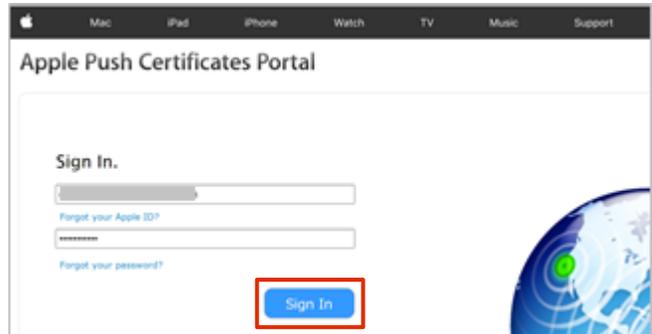


Apple Push Certificate Portal
<https://identity.apple.com/pushcert/>

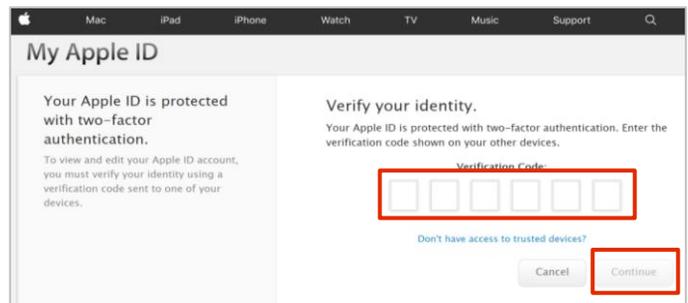
管理者作業

利用者作業

5. エージェントをインストールする端末で利用しているAppleIDを入力してサインインします。



指定したAppleIDで2ファクタ認証を有効としている場合、右の画面が表示されます。信頼されたデバイスで取得した確認コードを入力し、[Continue]ボタンをクリックします。



< 確認コードの取得方法 (iOS 10.3 以降) >

1. 信頼されたデバイスで[設定]を開き、ユーザ名をタップします。
2. [パスワードとセキュリティ]をタップします。



3. [確認コードを入手]をタップします。
4. 確認コードが表示されます。



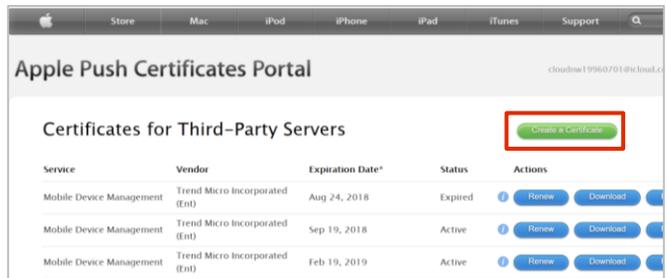
※確認コードの取得方法はOSのバージョンおよび利用状況によって異なります。詳しくは下記をご確認ください。

<https://support.apple.com/ja-jp/HT204974>

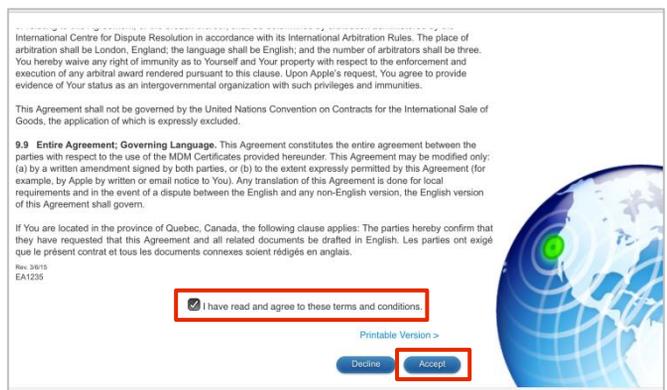
管理者作業

利用者作業

6. Certificates for Third-Party Servers 画面が表示されます。[Create a Certificate] ボタンをクリックします。



7. 「Terms of Use」画面が表示されます。内容を確認の上、「I have read and agree to these terms and conditions.」にチェックを入れ、[Accept]ボタンをクリックします。



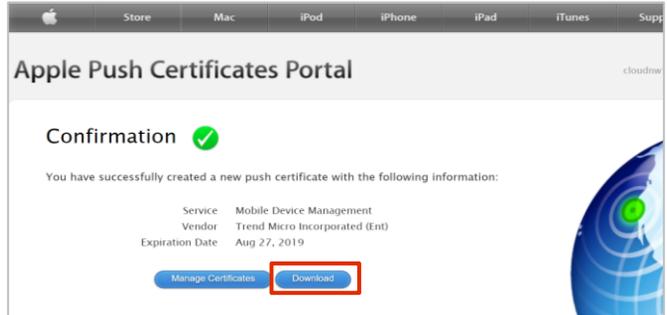
8. 「Create a New Push Certificate」画面が表示されます。[ファイルを選択]をクリックし、3でダウンロードしたCSRファイルを選択し、[Upload]ボタンをクリックします。



管理者作業

利用者作業

9. 「Confirmation」画面が表示されます。
[Download]ボタンをクリックして、証明書をダウンロードし、任意の場所へ保存します。



10. 管理コンソールへもどり、証明書を作成するために使用したApple IDを入力します。



11. [ファイルを選択]をクリックし、9で作成したAPNs証明書を選択し、[APNs証明書のアップロード]ボタンをクリックします。



管理者作業

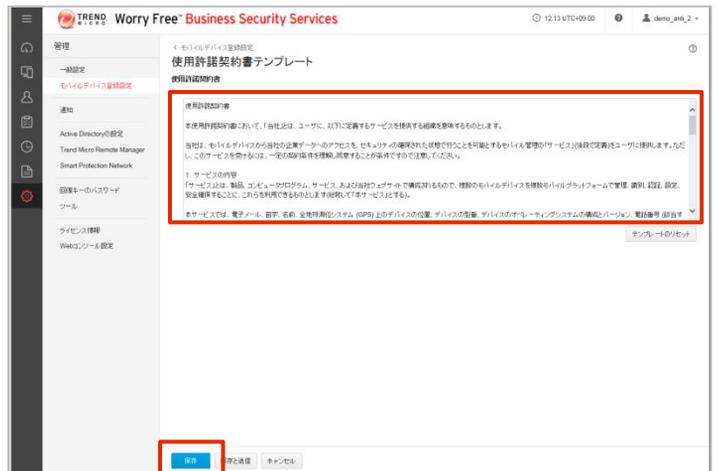
利用者作業

1 2. 「カスタマイズ」ボタンをクリックして使用許諾契約書を編集できます。

Android/iOSデバイスへのインストール時には「使用許諾契約書」が表示されます。エンドユーザはこの使用許諾契約書に同意してインストールします。この画面の初期設定では、テンプレートとしてお使いいただくことを想定した文章をご用意していますが、お客さまのご利用環境に合わせて文面を修正してお使いになることをお勧めします。



1 3. 編集が完了したら[保存]をクリックします。



1 4. 変更後は、利用許諾契約書の送付ができます。「送信」ボタンをクリックしメール送付します。(ご利用中のメールソフトが起動します。)



管理者作業利用者作業

iOS および iPadOSでは、初期設定でSafariの「デスクトップ用Webサイト」が有効になっています。

※インストール前に、一時的にSafariをモバイル用Webサイト表示にする必要があります。

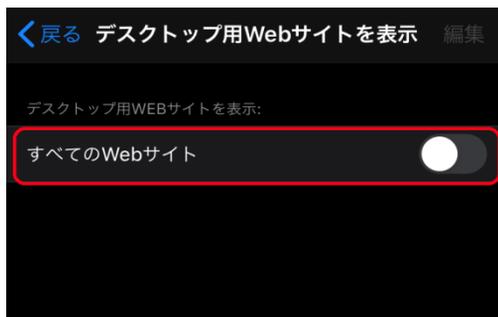
1. ホーム画面より [設定] >「Safari」をタップします。



2. 「デスクトップ用Webサイトを表示」をタップします。



3. 「すべてのWebサイト」をスライドし、オフにします。



※インストール完了後は、適宜設定を元に戻してください。

管理者作業

利用者作業

4. iOSデバイスでブラウザを開き、管理者から周知されたインストール用のリンクを入力します。

5. 右のような画面が表示されたら、管理者から周知された認証コードを入力し、[続行]をタップします。



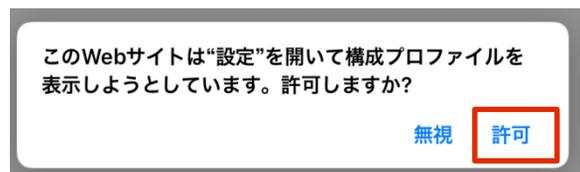
6. 使用許諾契約書が表示されます。確認の上、[同意する]をタップします。



7. [続行]をタップします。



8. [許可]をタップします。



9. 「プロフィールをインストール」の画面が表示されます。[インストール]ボタンをタップします。



管理者作業利用者作業

10. iOSの設定アプリを起動します。



11. 「一般」を選択します。



12. 「VPNとデバイス管理」を選択します。



管理者作業利用者作業

13. 「Trend Micro Worry-Free Business Security Services」を選択します。



14. 「インストール」を選択します。



15. 警告が表示されますが「インストール」を選択します。



管理者作業利用者作業

16. 「信頼」を選択します。



17. 「完了」を選択します。



18. Appのインストール確認が表示されますので、「インストール」を選択します。



管理者作業

利用者作業

19. アプリ(Mobile Security)がインストールされるので開きます。



20. 通知の送信を許可します。



21. 位置情報の使用を許可します。



管理者作業

利用者作業

22. アプリ(Mobile Security)がインストールされるので開きます。



23. Webレピュテーションを使用するためにVPNをONにします。



管理者作業

利用者作業

1. Chromebook上で、インストーリングをクリック
2. 拡張機能のインストール画面が表示されるので、ビジネスセキュリティの入手 をクリック

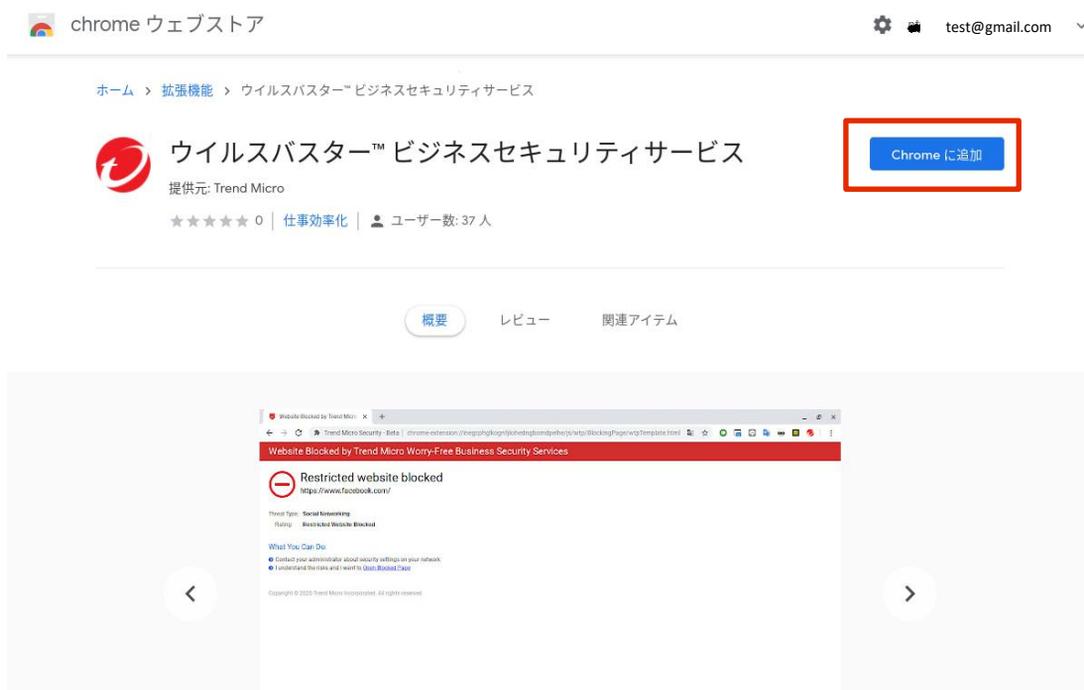
ビジネスセキュリティ拡張機能のインストール

ブラウザ拡張機能をインストールしてChromebookをセキュリティ上の脅威から保護します。

1. 次のボタンをクリックしてChromeウェブストアにアクセスします。

ビジネスセキュリティの入手

3. Chrome ウェブストア内の画面 が表示されるので、[Chrome に 追加 を クリック し モジュール を ダウンロード



※Chrome同期でブラウザの拡張機能が同期されている場合は、本ページの手順は不要です。拡張機能が同期されている場合は次の手順のみご参照ください。

管理者作業

利用者作業

4. ブラウザ右上のトレンドマイクロ拡張機能アイコンをクリック



5. 認証コード入力画面が表示されるので、認証コードを入力しアクティベートする (必要に応じてデバイス名を変更してください)

認証コード：通知された認証コード

デバイス名：ログイン中のgoogle アカウント名 (@より前) が自動表示されます

※管理コンソール上でエンドポイント名として表示

The screenshot shows the authentication screen for activating the protection feature. At the top, there is a header with the Trend Micro logo and a menu icon. Below the header, there is a message: "保護機能を有効にするには、以下の情報を指定してください。". Below the message, there are two input fields: "認証コード:" and "デバイス名:". The "デバイス名:" field is pre-filled with "lapurqj33 (Chromebook)". Below the input fields, there is a red button labeled "保護機能のアクティベート".

6. アクティベートが完了すると、ポリシーのステータスが表示されます



機能を設定する（画面構成）

ポリシー設定方法には大きく2つの方法があります。

1. グループごとにポリシーを定める方法

2. 全端末に適用されるポリシーを定める方法

《グループごとにセキュリティポリシーを定める場合》

- ①「セキュリティエージェント」タブを押下します。
- ②「手動グループ」が表示されるため、設定したいグループを選択します。
※「すべてのセキュリティエージェント」には全端末情報が一覧で表示されます。
グループとは異なりますのでご注意ください。
- ③「ポリシーの設定」を押下します。
- ④設定するOSを選択します。



機能を設定する（画面構成）

《 全端末に適用されるポリシー/ルールを定める場合 》

①「ポリシー」タブまたは「管理」タブを押下。

※設定する内容により、タブが異なりますのでご注意ください。

TREND MICRO Worry Free™ Business Security Services 15:25 UTC+09:00

ポリシー設定

追加の設定

- グローバルセキュリティエージェント設定
- グローバル除外リスト

ポリシーリソース

- アプリケーションコントロールルール

グローバルセキュリティエージェント設定

グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール

一般検索

- 遅延検索を有効にする
注意: この機能を有効にすると、ファイルをコピーする際の検索処理のタイミングが遅延します。パフォーマンスは向上しますが、セキュリティリスクをもたらす可能性があります。
- Microsoft Exchange Server 2003フォルダを除外する ①
- Microsoftドメインコントローラフォルダを除外する
(スパイウェア/グレーウェアの手動および予約検索には適用できません)
- シャドウコピーセクションの除外 ①
- 行われなかった予約検索を翌日の同じ時刻に実行

ウイルス検索

- 圧縮ファイルの検索制限
圧縮ファイルのサイズが MBを超える場合はファイルを検索しない (1-1000)
圧縮ファイル内では、最初のファイルから 番目までのファイルを検索する (1-100000)
- 圧縮ファイルのウイルス駆除
- OLEオブジェクトを 階層まで検索
- エンドポイントのWindowsショートカットメニューに手動検索を追加

スパイウェア/グレーウェア検索

- Cookieの検索 ①

挙動監視

- 危険度の低い変更、またはその他の監視対象処理に対する警告メッセージを有効化する
- HTTPまたはメールを介してダウンロードされた「新しく検出されたプログラム」を開く前にユーザーに通知する ①
注意: リアルタイム検索またはWebレピュテーションで新しいプログラムが検出されたときに通知が表示されます。

HTTPS Web評価

- Chrome、FirefoxおよびMicrosoft EdgeでWebレピュテーションとURLフィルタリングのHTTPS確認を有効にする ①
注意: この機能を使用するには、管理者がポリシー管理で不正変更防止サービスを有効にする必要があります。
- 機能アップデートによりChromeまたはFirefoxの再起動が必要になった場合、セキュリティエージェントで、アイコンの上部に通知を表示する

機能を設定する（グループ：検索設定）

デバイス内のウイルス検索方法を選択します。
※ここではスマートスキャンの利用を選択しています。

ポリシーの設定: test

対象とサービスの設定

検索設定 ①

検索設定 ②

検索方法

スマートスキャン (推奨)
スマートスキャンでは、インターネットクラウドに格納されている不正プログラム対策シグネチャおよびスパイウェア対策シグネチャが利用されます。

従来型スキャン
従来型スキャンは、セキュリティエージェントのローカルに格納されている不正プログラムやスパイウェア対策コンポーネントを利用します。

リアルタイム検索

ファイルを受信、開く、ダウンロード、コピー、または変更したときに、セキュリティ上のリスクがあるかファイルを検索します。

オン

設定

予約検索

設定された時間及び頻度で検索を実行します。予約検索を使用すると、エンドポイントでの定期的な検索を自動化し、脅威の管理を効率化することができます。

オフ

手動検索

Webコンソール上の [セキュリティエージェント] 画面またはセキュリティエージェントコンソールから開始される手動検索です。

設定

保存 ③ キャンセル

「保存」を押して終了です。

スマートスキャンとは：エージェントでは、脅威の特定に独自の検索エンジンが使用されますが、ローカルパターンファイルのみを使用するのではなく、クラウド上にあるスキャンサーバに格納されているパターンファイルを主に利用する方法

機能を設定する（グループ：検索設定-POP3メール検索）

POP3メール検索機能を有効にします。

→メールの受信時にウイルス検索を実施することができます。

ポリシーの設定: test

対象とサービスの設定

脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- 仮想パッチ
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済みブロックするURL

エージェントの設定

- 権限およびその他の設定

検索設定

検索方法

- スマートスキャン (推奨)
スマートスキャンでは、インターネットクラウドに格納されている不正プログラム対策シグネチャおよびスパイウェア対策シグネチャが利用されます。
- 従来型スキャン
従来型スキャンは、セキュリティエージェントのローカルに格納されている不正プログラムやスパイウェア対策コンポーネントを利用します。

リアルタイム検索

ファイルを受信、開く、ダウンロード、コピー、または変更したときに、セキュリティ上のリスクがあるかファイルを検索します。

オン

設定

予約検索

設定された時間及び頻度で検索を実行します。予約検索を使用すると、エンドポイントでの定期的な検索を自動化し、脅威の管理を効率化することができます。

オフ

手動検索

Webコンソール上の [セキュリティエージェント] 画面またはセキュリティエージェントコンソールから開始される手動検索です。

設定

保存 キャンセル

機能を設定する（グループ：検索設定-POP3メール検索）

POP3メール検索機能を有効にします。

→メールの受信時にウイルス検索を実施することができます。

リアルタイム検索設定

対象 処理

検索設定 ③

検索するファイル:

- 検索可能なすべてのファイル
- トレンドマイクロの推奨設定で検索されるファイルタイプ ⓘ
- 指定された拡張子を持つファイル

ファイルに対するユーザのアクティビティ

- 作成、変更、またはファイルの読み込み
- ファイルの読み込み
- 作成または変更

詳細設定 ④

- POP3メッセージを検索する
- IntelliTrapを有効にする ⓘ
- メモリで検出された不正プログラムの変種/亜種を隔離する ⓘ
注意: この機能を使用するには、管理者がリアルタイム検索と挙動監視を有効にしている必要があります。
- システムのシャットダウン時にフロッピーディスクを検索する
- 圧縮ファイルの検索 ⓘ
最大階層数: 2 ▲
- ユーザの許可なくプロセスを終了する可能性のあるアプリケーションを検索する
- Webおよびメールからダウンロードしたファイルに対するCVEセキュリティホールの検索を有効にする

⑤ OK キャンセル

● URLフィルタ

● アプリケーションコントロール

除外リスト

検索除外

承認済み/ブロックするURL

エージェントの設定

権限およびその他の設定

設定

設定を4分間隔で実行して検索結果をリフレッシュ。リアルタイム検索を使用すると、エージェントがリアルタイムで検出された脅威を自動的に、有効な脅威を削除して処理することができます。

オフ

手動検索

Webコンソール上の [セキュリティエージェント] 画面またはセキュリティエージェントコンソールから開始される手動検索です。

設定

⑥ 保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：検索設定-ファイルレス攻撃対応）

ファイルレス攻撃対応機能を有効にします。

→ハードディスクに保存されない(メモリ上にのみ存在)ウイルスを検出できます。

ファイルレス攻撃対応機能を有効にするためには、下記5項目全てを設定する必要があります。

機能	項目	設定内容
検索設定	1	リアルタイム検索を“オン”に設定
	2	[リアルタイム検索] - [設定] - [対象]タブを選択し、「メモリで検出された不正プログラムの変種/亜種を隔離する」にチェックをいれる
挙動監視	3	挙動監視を“オン”に設定
	4	「脆弱性攻撃に関連する異常な挙動を示すプログラムを終了」を“オン”に設定
機械学習型検索	5	機械学習型検索を“オン”に設定

《 項目 1 》 ※項目番号は上記表を参照

ポリシーの設定: test

対象とサービスの設定

検索設定

検索方法

- スマートスキャン (推奨)
スマートスキャンでは、インターネットクラウドに格納されている不正プログラム対策シグネチャおよびスバイウェア対策シグネチャが利用されます。
- 従来型スキャン
従来型スキャンは、セキュリティエージェントのローカルに格納されている不正プログラムやスバイウェア対策コンポーネントを利用します。

リアルタイム検索

ファイルを受信、開く、ダウンロード、コピー、または変更したときに、セキュリティ上のリスクがあるかファイルを検索します。

オン

設定

予約検索

機能を設定する (グループ: 検索設定-ファイルレス攻撃対応)

ファイルレス攻撃対応機能を有効にします。

→ハードディスクに保存されない(メモリ上にのみ存在)ウイルスを検出できます。

《 項目 2 》

ポリシーの設定: test

対象とサービスの設定

検索設定

検索方法

- スマートスキャン (推奨)
スマートスキャンでは、インターネットクラウドに格納されている不正プログラム対策シグネチャおよびバイウェア対策シグネチャが利用されます。
- 従来型スキャン
従来型スキャンは、セキュリティエージェントのローカルに格納されている不正プログラムやバイウェア対策コンポーネントを利用します。

リアルタイム検索

ファイルを受信、開く、ダウンロード、コピー、または変更したときに、セキュリティ上のリスクがあるかファイルを検索します。

オン

③

予約検索

リアルタイム検索設定

対象 処理

検索設定

検索するファイル:

- 検索可能なすべてのファイル
- トレンドマイクロの推奨設定で検索されるファイルタイプ ①
- 指定された拡張子を持つファイル

ファイルに対するユーザのアクティビティ

- 作成、変更、またはファイルの読み込み
- ファイルの読み込み
- 作成または変更

詳細設定

- POP3メッセージを検索する
- IntelliTrapを有効にする ①
- メモリで検出された不正プログラムの変種/亜種を隔離する ① ④
注意: この機能を使用するには、管理者がリアルタイム検索と挙動監視を有効にしている必要があります。
- システムのシャットダウン時にフロッピーディスクを検索する
- 圧縮ファイルの検索 ①
最大階層数: 2 ▲
- ユーザの許可なくプロセスを終了する可能性のあるアプリケーションを検索する
- Webおよびメールからダウンロードしたファイルに対するCVEセキュリティホールを検索を有効にする

⑤ キャンセル

機能を設定する (グループ: 検索設定-ファイルレス攻撃対応)

ファイルレス攻撃対応機能を有効にします。

→ハードディスクに保存されない(メモリ上にのみ存在)ウイルスを検出できます。

《 項目 3, 4 》

ポリシーの設定: test

対象とサービスの設定

OS: Windows, Apple, Android, iOS

脅威からの保護機能

- 検索設定 (6)
- **挙動監視** (7)
- 機械学習型検索
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済みブロックするURL

エージェントの設定

- 権限およびその他の設定

挙動監視

挙動監視は、オペレーティングシステム、レジストリエントリ、その他のソフトウェア、ファイルやフォルダへの不正な変更からエンドポイントを保護します。

注意: この機能を使用するには、対象とサービスの設定で不正変更防止サービスを有効にする必要があります。

オン (7)

不正プログラム挙動ブロック

オン

- 既知および潜在的な脅威のブロック
- 既知の脅威のブロック

ランサムウェア対策

- 不正なファイル暗号化や変更から文書を保護 (1)
- 不審なプログラムによって変更されたファイルを自動的にバックアップして復元 (1)
- ランサムウェアに関連付けられていることの多いプロセスをブロック (1)
- プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック (1)

脆弱性対策

脆弱性攻撃に関連する異常な挙動を示すプログラムを終了 (8)

オン

Intuit™ QuickBooks™ 保護

《 項目 5 》

ポリシーの設定: test

対象とサービスの設定

OS: Windows, Apple, Android, iOS

脅威からの保護機能

- 検索設定 (9)
- 挙動監視
- **機械学習型検索** (10)
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

機械学習型検索

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジーを使用して、あまり普及していない不審プロセスやファイルに含まれる未知のセキュリティリスクを検出します。

注意:

- 機械学習型検索を使用するには、挙動監視を有効にする必要があります。
- インターネット接続を利用できない場合は、機械学習型検索ローカルモデル (ファイル検出) を使用してポータブル実行可能ファイルの脅威に対する保護が継続されます。

検出設定

種類	処理
<input checked="" type="checkbox"/> ファイル	隔離
<input checked="" type="checkbox"/> プロセス	終了 (1)

保存 (11) キャンセル

項目 1 ~ 5 を全て設定し、「保存」を押して終了です。

機能を設定する（グループ：拳動監視）

拳動監視機能を有効にします。

プログラムやOS、レジストリなどを不正に変更されないように
エンドポイントを保護します。

!!Configure Policy: test!!

対象とサービスの設定

OS: Windows, Apple, Android, iOS

脅威からの保護機能

- 検索設定
- 挙動監視** (1)
- 機械学習型検索 (2)
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール

情報漏えい対策

- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済み/ブロックするURL
- クライアントの認定
- 権限およびその他の設定

挙動監視

挙動監視は、オペレーティングシステム、レジストリエントリ、その他のソフトウェア、ファイルやフォルダへの不正な変更からエンドポイントを保護します。

注意: この機能を使用するには、対象とサービスの設定で不正変更防止サービスを有効にする必要があります。

挙動監視 (3) オン (4)

不正プログラム挙動ブロック

オン (5) (6)

- 既知および潜在的な脅威のブロック
- 既知の脅威のブロック

ランサムウェア対策

- 不正なファイル暗号化や変更から文書を保護 (7)
- 不審なプログラムによって変更されたファイルを自動的にバックアップして復元 (8)
- ランサムウェアに関連付けられていることのないプロセスをブロック (9)
- プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック (10)

脆弱性対策

脆弱性攻撃に関連する異常な挙動を示すプログラムを終了

オン (11) (12)

Intuit™ QuickBook™保護

QuickBooks™ファイルおよびフォルダへの不正な変更を防止

オフ (13) (14)

イベント監視

システムイベントを監視して潜在的に不正な処理を検出します (15)

オフ (16)

保存 (17) キャンセル

④ランサムウェア対策
※詳細は次ページに記載

「保存」を押して終了です。

挙動監視機能とは： OS、レジストリエントリ、他のソフトウェア、ファイル、またはフォルダが不正に変更されないよう、コンピュータを監視し、保護する為の機能です

機能を設定する（グループ：挙動監視-ランサムウェア対策）

ランサムウェアはパソコン内に侵入してファイルやシステムの一部もしくはすべてを**使用不能**にし、その**復旧と引き換えに金銭を要求**する不正プログラムのことです。これまでは一般ユーザでの感染が多く報告されていましたが、企業でも感染報告が上がるようになってきています。



◆おまかせアンチウイルスのランサムウェア対応機能

I：不正なファイル暗号化や変更から文書を保護

ドキュメント、画像、音声ファイルなど特定のファイルの種類を監視対象とし、不審なプロセスが監視対象のドキュメント等に対して変更等を実施しようとした際にプロセスを停止し、実行元のプログラムの隔離を行います。

II：不審なプログラムによって変更されたファイルを自動的にバックアップして復元

暗号化・復号化を行うファイルを全て自動的にバックアップを取得し、ランサムウェアと思われる暗号化の場合、ファイルの復元を試みます。本機能は、「不正な暗号化や変更から文書を保護」が有効な場合に機能します。※バックアップは100MBまで実施し、超過の場合は古いファイルから自動的に削除されます。

III：ランサムウェアに関連付けられていることの多いプロセスをブロック

OSで利用されている実行ファイル等にインジェクションされるようなランサムウェアの挙動を監視し、不審な動作をブロックします。

IV：プログラム検査を有効にして不正な実行可能ファイルを検出ブロック

コンピュータのプロセス挙動監視を強化し、ランサムウェア特有の挙動をする実行可能ファイルを検出しブロックします。

機能を設定する（グループ：機械学習型検索）

機械学習型検索を設定します。

→未知の脅威でも、不振な挙動から脅威を判別します。

※ここでは、未知の脅威を隔離・終了する設定を行います。

!!Configure Policy: test!!

対象とサービスの設定

脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索**
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済みブロックするURL

クライアントの監定

- 権限およびその他の設定

機械学習型検索

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジーを使用して、リムーバブルストレージ、Web、メールを経由する不審なプロセスやファイルに含まれる蔓延前の未知のセキュリティリスクを検出します。

注意：機械学習型検索には以下が必要です。

- 挙動監視の有効化
- Smart Protection Networkに接続するためのインターネット接続

検出設定

種類	処理
<input checked="" type="checkbox"/> ファイル	隔離
<input checked="" type="checkbox"/> プロセス	終了

① ② ③ ④

保存 キャンセル

機械学習型検索を有効にすると自動でチェックされる

「保存」を押して終了です。

機械学習型検索とは：既存の機能では検出されない不審なファイルやプロセスが見つかった場合に、そのファイルやプロセスの特徴情報を元に統計的に当該ファイル等が脅威であるかの判断をすること

機能を設定する（グループ：仮想パッチ）

仮想パッチを設定します。

→OS やアプリケーションの脆弱性を突く攻撃パケットを検知/ブロックすることができます。

ポリシーの設定: デバイス (初期設定)

対象とサービスの設定

仮想パッチ

ウイルスバスター ビジネスセキュリティサービスでは、**侵入防御ルール**を使用してエンドポイントを保護できるようになりました。仮想パッチ機能では、ホストベースの侵入防御システム (HIPS) を使用して仮想パッチを既知の脆弱性に適用します。この機能は、挙動監視、ファイアウォール、機械学習型検索を含む包括的な保護機能の一部です。

ウイルスバスター ビジネスセキュリティサービスで対策可能な脆弱性の検索:

例: CVE-2016-4140、MSCVE-2020-1472など

① 仮想パッチ

② オン

③ 保存

「保存」を押して終了です。

仮想パッチとは：脆弱性そのものを修正する正規パッチとは異なり、脆弱性を突く攻撃をネットワークレイヤで検知およびブロックするものです。脆弱性発覚後、各ベンダーから正規パッチがリリースされるまでの間、仮想パッチにより、本脆弱性を衝く攻撃のリスクを軽減することができます。

機能を設定する（グループ：Webレピュテーション）

Webレピュテーション機能を有効にします。

→危険なWebサイトへのアクセスを制限します。

※ここではセキュリティレベル（中）を選択しています。

!!Configure Policy: test!!

対象とサービスの設定

Webレピュテーション

Webレピュテーションは不正Webサイトの脅威からの保護を強化します。

オン

セキュリティレベル

	危険	極めて不審	不審	未評価
<input type="radio"/> 高	✓	✓	✓	✓
<input checked="" type="radio"/> 中 (初期設定)	✓	✓		
<input type="radio"/> 低	✓			

Webサイトのアクセスをブロックします

ブラウザ脆弱性対策

不正スクリプトを含むWebサイトをブロックする

保存 キャンセル

「保存」を押して終了です。

Webレピュテーションとは：不正なWebサイトへのアクセスをブロックするWebセキュリティ機能

機能を設定する（グループ：ファイアウォール設定）

ファイアウォール機能を有効にします。

→インターネットからの攻撃をブロックします。

※ここでは簡易モードで設定をしています。

!!Configure Policy: test!!

対象とサービスの設定

背景からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- Webレビューテーション
- **ファイアウォール設定**
- 情報漏えい対策
- デバイスコントロール
- 情報漏えい対策
- アクセスコントロール
- URLフィルタ
- アプリケーションコントロール
- 除外リスト
- 検索除外
- 承認済みブロックするURL
- クライアントの設定
- 権限およびその他の設定

ファイアウォール設定

ファイアウォールは、エンドポイントとネットワークの間コリアを作成することによって、特定の種類のネットワークトラフィックをブロックまたは許可できます。

オン

注意: ファイアウォールを有効または無効にすると、一時的にエンドポイントがネットワークから切断されます。接続の中断による影響を最小限に抑えるため、影響度の少ない時間に設定の変更を行ってください。

簡単モード トレンドマイクロの初期設定を使用

詳細モード セキュリティレベル、侵入検知システム、および除外を設定

4 保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：デバイスコントロール）

USBインターフェースで接続するストレージ(USBメモリ等)の利用をコントロールします。

※ここでは、USBデバイスを読み取り専用にし、情報の持ち出しを禁止する設定を行います。

The screenshot shows the '!!Configure Policy: test!!' window with the 'Device Control' policy selected. The left sidebar has 'Device Control' highlighted (1). The main area shows the 'Device Control' policy is turned 'On' (2). Under 'Storage Devices', 'CD/DVD', 'Network Drives', and 'USB Storage Devices' are all set to 'Read-only' (3). Under 'Storage Devices', the checkbox for 'Block automatic execution of programs on USB storage devices' is unchecked. Under 'Mobile Devices', the 'Storage' dropdown is set to 'Full Control'. Under 'Storage Devices', the 'Storage Devices' section is highlighted (4) and contains a list of devices with 'Allow' selected for all: Bluetooth Adapters, COM and LPT Ports, IEEE 1394 Interfaces, Imaging Devices, Infrared Devices, Modems, Print Screen Keys, and Wireless NICs. A callout box notes that 'Storage Devices' and 'CD/DVD' are blockable but not logged. At the bottom, the 'Save' button is highlighted (5).

!!Configure Policy: test!!

対象とサービスの設定

デバイスコントロール

デバイスコントロールは、周辺デバイスへのアクセスを制御します。

オン

注意: この機能を有効にするには、対象とサービスの設定で不正変更防止サービスを有効にする必要があります。

ストレージデバイス

CD/DVD: 読み取り

ネットワークドライブ: 読み取り

USBストレージデバイス: 読み取り

USBストレージデバイスでの自動実行機能をブロックする

許可されたUSBデバイスの権限を設定する

許可されたプログラムを設定 (0)

モバイルデバイス

ストレージ: フルアクセス

ストレージ以外のデバイス

Bluetoothアダプタ: 許可 ブロック

COMおよびLPTポート: 許可 ブロック

IEEE 1394インターフェース: 許可 ブロック

イメージングデバイス: 許可 ブロック

赤外線デバイス: 許可 ブロック

モデム: 許可 ブロック

プリントスクリーンキー: 許可 ブロック

ワイヤレスNIC: 許可 ブロック

※以下はブロック可能ですが、ログには記録されません。

- ・ストレージ以外のデバイス
- ・CD/DVD

保存 キャンセル

「保存」を押して終了です。

機能を設定する（全端末：デバイスコントロール）

《 特定のUSBのみ常に許可する場合 》

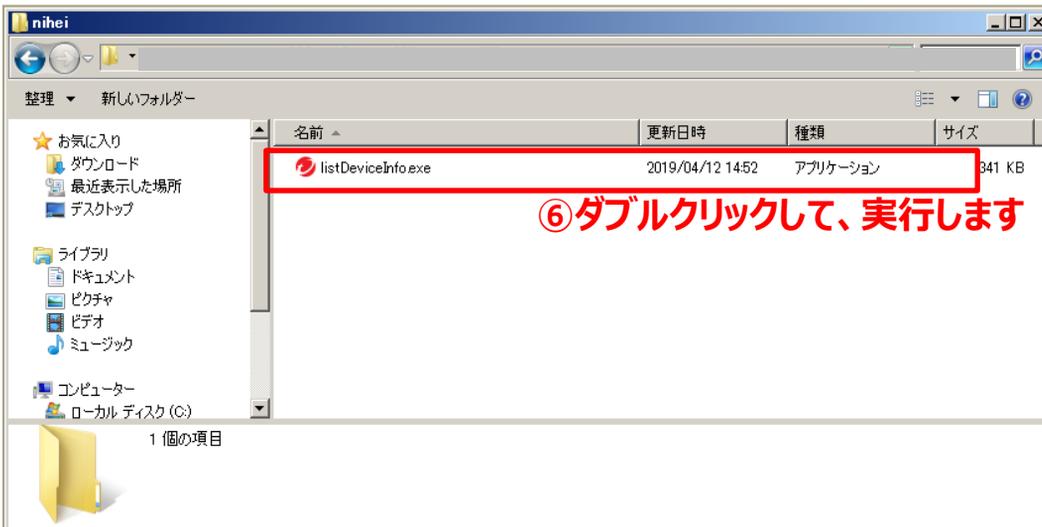
- ① 作業開始前に、許可したいUSBを手元に準備します。
- ② 許可したいUSBを端末に接続します。

The screenshot shows the Trend Micro Worry Free Business Security Services interface. The left sidebar contains a navigation menu with the following items: Policy Settings, Additional Settings, Global Security Agent Settings, **Global Exclusion List** (highlighted with a red box and a circled '1'), Policy Sources, Application Control Rules, and Settings. The main content area is titled 'グローバル除外リスト' (Global Exclusion List) and includes a sub-section 'Webレピュテーション / URLフィルタ' (Web Reputation / URL Filter). Under this section, there are several lists: '承認済みURLリスト (15)', 'ブロックするURLリスト (0)', '承認済みIPアドレスリスト (0)', and '許可されたプロセスのリスト (0)'. Below this is the '不正プログラム検索除外' (Malware Search Exclusion) section, which includes '信頼済みWindowsプログラムリスト (0)', '信頼済みMacプログラムリスト (0)', and '機械学習型検索除外リスト (0)'. The 'デバイスコントロール' (Device Control) section is highlighted with a red box and a circled '2', and it contains a list '許可されたUSBデバイスのリスト (3)'. The bottom right corner of the interface shows a search icon, a home icon, a refresh icon, a plus icon, and a settings icon.

機能を設定する（全端末：デバイスコントロール）



⑤「名前をつけて保存」をクリックし、任意のフォルダに保存します



機能を設定する（全端末：デバイスコントロール）

⑦ 端末に接続しているUSB情報が表示されます

リムーバブルディスクドライブ:

コンピュータ	ユーザ	ポート	説明	ベンダ	モデル	シリアル番号
PC001	Security Manager	USB	USB Device	SONY	0910	0123456789

許可されたUSBデバイスのリスト

⑧

+ 追加 インポート 削除 エクスポート

ベンダー/製造元	機種/製品ID	シリアルID/番号	メモ

デバイス情報を取得する方法

許可されたUSBデバイス

ベンダー/製造元:
SONY

機種/製品ID:
0910

シリアルID/番号:
0123456789

メモ:

⑨ 表示された値を入力します

⑩ 保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：情報漏えい対策）

情報漏えい対策機能を有効にします。

→機密データの転送を監視またはブロックします。

※ここでは「日本：パスポート番号」の転送ブロックの設定をしています。

!!Configure Policy: test!!

対象とサービスの設定

Windows Apple Android iOS

脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- Webレビューセッション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策** (1)
- アクセスコントロール
- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済み/ブロックするURL

クライアントの設定

- 権限およびその他の設定

情報漏えい対策

情報漏えい対策は、ネットワーク全体の機密データの転送を監視またはブロックします。

オン (2)

注意: 初めて情報漏えい対策を有効化する場合は、ユーザがエンドポイントを再起動し、設定を適用する必要があります。

ルール (3) 除外設定

情報漏えい対策ルールを作成して、機密データの転送を監視またはブロックします。

+ 追加 (4) コピー 削除 0/40

ルール (4)	テンプレート	チャンネル	処理	有効
ルールが定義されていません。 [追加] をクリックして、情報漏えい対策ルールを作成してください。				

保存 キャンセル

機能を設定する（グループ：情報漏えい対策）

情報漏えい対策ルールの設定

一般設定

このルールを有効にする

ルール名* test 5

説明:

テンプレート

情報漏えい対策テンプレートを選択し、監視する機密データの種類を定義してください。 [詳細情報](#)

すべてのテンプレート

テンプレート (1/239)	
<input type="checkbox"/>	台湾: 携帯電話番号
<input type="checkbox"/>	台湾: 日盛銀行の口座番号 6
<input type="checkbox"/>	台湾: 銀行口座番号
<input checked="" type="checkbox"/>	日本: パスポート番号
<input type="checkbox"/>	日本: マイナンバー (法人) 国の機関 10件以上で検出
<input type="checkbox"/>	日本: マイナンバー (法人) 地方公共団体 (団体コードあり) 10件以上で検出
<input type="checkbox"/>	日本: マイナンバー (法人) 地方公共団体 (団体コードなし) 10件以上で検出
<input type="checkbox"/>	日本: マイナンバー (法人) 設立登記のある法人 10件以上で検出
<input type="checkbox"/>	日本: マイナンバー (法人) 設立登記のない法人・人格なき社団・人格なき財団 10件以上で検出

チャンネル

情報漏えい対策で監視するチャンネルの種類を選択してください。

ネットワークチャンネル 7

システムおよびアプリケーションチャンネル

処理

選択したネットワークチャンネルを通じて転送される機密データを検索した後、ログの記録および指定された処理を実行します。

処理: ブロック 8

9

追加 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：URLフィルタ）

URLフィルタリングを設定します。

→カテゴリ別に閲覧するWebサイトを設定できます。

※ここではセキュリティレベル（低）を選択しています。

!!Configure Policy: test!!

対象とサービスの設定

各版からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- Webシミュレーション
- ファイアウォール設定

皆無漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済みブロックするURL

クライアントの認定

- 権限およびその他の設定

URLフィルタ

URLフィルタを有効にすると、管理者は、1日のさまざまな時間帯でブロックする特定の種類のWebサイトを設定することができます。

オン

フィルタ強度

- 高 既知または潜在的なセキュリティ上の脅威、不適切なコンテンツまたは有害である可能性のあるコンテンツ、生産性または帯域幅に影響する可能性のあるコンテンツ、および未評価のページをブロックします
- 中 既知のセキュリティ上の脅威および不適切なコンテンツをブロックします
- 低 (初期設定) 既知のセキュリティ上の脅威をブロックします
- カスタム ブロックするURLカテゴリを指定する

フィルタルール

URLカテゴリ	<input checked="" type="checkbox"/> 業務時間	<input type="checkbox"/> 業務時間外
アダルト	<input type="checkbox"/>	<input type="checkbox"/>
ビジネス	<input type="checkbox"/>	<input type="checkbox"/>
コミュニケーション/メディア	<input type="checkbox"/>	<input type="checkbox"/>
一般	<input type="checkbox"/>	<input type="checkbox"/>
インターネットのセキュリティ	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ライフスタイル	<input type="checkbox"/>	<input type="checkbox"/>
ネットワーク	<input type="checkbox"/>	<input type="checkbox"/>

業務時間

- 終日 (24x7)
- 業務時間を指定する

保存 キャンセル

機能を設定する（グループ：URLフィルタ）

!!Configure Policy: test!!

対象とサービスの設定

- インターネットのセキュリティ
- ライフスタイル
- ネットワーク

業務時間

終日 (24x7)

業務時間を指定する

U/V:UU	日	月	火	水	木	金	土
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							

● 業務時間 ○ 業務時間外

保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：アプリケーションコントロール）

アプリケーションコントロール機能を有効にします。
→指定したアプリケーションの利用を制限します。
※ここでは簡易モードで設定をしています。

ポリシーの設定: test

対象とサービスの設定

脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- 仮想パッチ
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール**

除外リスト

- 検索除外
- 承認済み/ブロックするURL

エージェントの設定

- 権限およびその他の設定

アプリケーションコントロール

エンドポイントでのアプリケーションの実行やインストールを制限するルールを作成します。

オン

ブロック: 指定したアプリケーションのエンドポイントでの実行をブロック

ロックダウン: 前回のインベントリ検索で確認されなかったアプリケーションをすべてブロック

トレンドマイクロの信頼済みベンダーのアプリケーションを除外 (推奨)

Microsoftの署名付きのプログラム (Windows Updateを含む) によるプロセスツリーを除外

ルール

+ ルールの割り当て 合計: 0

種類 ↑	ルール	概要
ルールが割り当てられていません。 [ルールの割り当て] をクリックしてアプリケーションコントロールルールを指定してください。		

許可ルールはブロックルールよりも優先されます。

保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：EDR機能 Endpoint Sensor）

※EDRプラスオプションをご利用されている場合の機能となります

Endpoint Sensorの機能を有効にします。

→端末の不審な挙動を検知およびクラウドサンドボックス機能を有効化します

ポリシーの設定: デバイス (初期設定)

Endpoint Sensor

Endpoint Sensorは、脅威の存在、場所、侵入地点を特定するための強力な監視/調査ツールです。詳細なシステムイベントの記録と履歴の分析を通じて事前診断に基づく調査を行うことで、ネットワークに潜んでいる脅威をネットワーク全体から検出し、影響を受けるすべてのエンドポイントを特定できます。さらに、Root Cause Analysisレポートを生成して、脅威がエンドポイントに侵入してからの不正プログラムの特性や活動を把握することができます。

①

②

保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：パスワード/パスコード）

端末のロックを解除する際に、パスワードの入力を要求します。
※ここではAndroidの中レベルの設定をしています。

ポリシーの設定: test

1 対象とサービスの設定

2

3

パスワード

デバイスのロックを解除する際に、PINまたはパスワードの入力を要求します。

4 オン

5

複雑さ

- 低
 - パターン
 - PIN: 同じ数字の繰り返し (1111など)、または連続する数字 (1234など) を使用できます
- 中
 - PIN: 4桁以上の数字、同じ数字の繰り返し (1111など)、および連続する数字 (1234など) は使用できません
 - 英字: 4文字以上 (A~Z、a~z)
 - 英数字: 4文字以上 (A~Z、a~z、0~9)
- 高
 - PIN: 8桁以上の数字、同じ数字の繰り返し (1111など)、および連続する数字 (1234など) は使用できません
 - 英字: 6文字以上 (A~Z、a~z)
 - 英数字: 6文字以上 (A~Z、a~z、0~9)

自動画面ロック

次の時間デバイスが操作されない場合、デバイスを自動的にロックする: 4 分

6 保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：除外設定）

指定したフォルダ、ファイル、またはファイル拡張子を不正プログラム検索から除外します。

《 リアルタイム検索/予約検索/手動検索から除外する場合 》

ポリシーの設定: test

対象とサービスの設定

検索除外

検索除外リスト

指定したフォルダ、ファイル、またはファイル拡張子を不正プログラム検索から除外します。

リアルタイム検索/予約検索/手動検索

② フォルダ (0) ファイル (0) ファイル拡張子 (5)

+ 追加				合計: 0
フォルダパス	リアルタイム検索	予約検索	手動検索	
③ フォルダ除外が追加されていません。 追加 をクリックして、フォルダパスを指定します。				

トレンドマイクロ製品がインストールされているディレクトリを次の場所から除外します。

リアルタイム検索 予約検索 手動検索

スパイウェア/グレーウェア

+ 追加

+ 追加				合計: 0
スパイウェア/グレーウェア				
スパイウェアまたはグレーウェアの除外は追加されていません。 追加 をクリックしてスパイウェアまたはグレーウェアの除外を指定します。				

挙動監視

挙動監視により自動的に、すべての承認済みプログラムの実行が許可され、すべてのブロックするプログラムの実行が阻止されます。

承認済みプログラムリスト (0) ブロックするプログラムリスト (0)

+ 追加		合計: 0
プログラム	ファイルパス	
承認済みプログラムは追加されていません。 追加 をクリックして、ファイルパスを指定してください。		

機械学習型検索

機械学習型検索の除外は、すべてのセキュリティエージェントに適用されます。除外を指定するには、[ポリシー設定]→[グローバル除外リスト]に進みます。

保存 キャンセル

機能を設定する（グループ：除外設定）

《 挙動監視から除外する場合 》

ポリシーの設定: test

対象とサービスの設定

検索除外リスト

検索除外リスト

指定したフォルダ、ファイル、またはファイル拡張子を不正プログラム検索から除外します。

リアルタイム検索/予約検索/手動検索

フォルダ (0) | ファイル (0) | ファイル拡張子 (5)

+ 追加 合計: 0

フォルダパス	リアルタイム検索	予約検索	手動検索
フォルダ除外が追加されていません。 [追加] をクリックして、フォルダパスを指定します。			

トレンドマイクロ製品がインストールされているディレクトリを次の場所から除外します。

リアルタイム検索 予約検索 手動検索

スパイウェア/グレーウェア

+ 追加 合計: 0

スパイウェア/グレーウェア
スパイウェアまたはグレーウェアの除外は追加されていません。 [追加] をクリックしてスパイウェアまたはグレーウェアの除外を指定します。

挙動監視

挙動監視により自動的に、すべての承認済みプログラムの実行が許可され、すべてのブロックするプログラムの実行が阻止されます。

承認済みプログラムリスト (0)	ブロックするプログラムリスト (0)
[追加] をクリックして、ファイルパスを指定してください。	

機械学習型検索

機械学習型検索の除外は、すべてのセキュリティエージェントに運用されます。除外を指定するには、[ポリシー設定]-[グループ/URL除外リスト]に進みます。

5 保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：承認済み/ブロックするURL）

WebレピュテーションおよびURLフィルタにおいて、常に許可/ブロックするURLを設定することができます。

ポリシーの設定: test

対象とサービスの設定

検索設定

掌動監視

機械学習型検索

Webレピュテーション

ファイアウォール設定

情報漏えい対策

デバイスコントロール

情報漏えい対策

アクセスコントロール

URLフィルタ

アプリケーションコントロール

除外リスト

検索除外

承認済み/ブロックするURL

エージェントの設定

権限およびその他の設定

承認済み/ブロックするURLのリスト

承認済み/ブロックするURLはWebレピュテーションおよびURLフィルタに適用されます。

使用除外:

グローバル承認済みおよびブロックするURLのリスト

除外の指定

承認済みURL (15) ブロックするURL (0)

+ 追加

合計: 15

承認済みURL
http://*.trendmicro.com/*
https://*.trendmicro.com/*
http://www.trendmicro.com/*
http://wustat.windows.com/*
http://windowsupdate.microsoft.com/*
http://uk.trendmicro-europe.com/*

Webレピュテーションで誤って分類されている可能性のあるURLを通知するか、URLの安全性の評価を確認するには、次のWebサイトにアクセスしてください。
<http://sitesafety.trendmicro.com/>

保存 キャンセル

「保存」を押して終了です。

機能を設定する（全端末：感染経路の可視化）

セキュリティイベントが検出されるまでの簡易的な経路が確認できます。

《 注意点 》

- ・ 設定が有効になった以降のログが対象となります。
有効にする前のログに関する感染経路は確認できません。
- ・ 設定を有効にすることで、ご利用端末にかかる負荷が大きくなります。
ご利用状況によっては、端末の動作が遅くなるなどの影響が出る可能性があります。

グローバルセキュリティエージェント設定
グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール ③

警告

7 日経過してもウイルスパターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

セキュリティエージェントのログ

WebレピュテーションおよびURLフィルタのログをサーバーに送信する

脅威イベントの詳細を強化型脅威分析のためにサーバーに送信する ④

監視サービス

セキュリティエージェントの監視サービスを有効にする:
セキュリティエージェントのステータスを 1 分間隔で確認
セキュリティエージェントを再起動できない場合、5 回まで再試行

管理者への問い合わせの通知

セキュリティエージェントに管理者への問い合わせ情報を表示する

アンインストール

セキュリティエージェントのアンインストール時にパスワード入力を要求する

終了ロック解除

セキュリティエージェントの終了時、または詳細設定のロック解除時にパスワード入力を要求する

保存 ⑤

追加で必要なリソース

本機能が有効の場合、無効の場合に比べてエンドポイントのリソースを多く使用するため、パフォーマンスに影響が出る可能性があります。

メモリ : 最大21MB程度／通常4MB程度
HDD : 最大213MB程度／通常40MB程度

「保存」を押して終了です。

機能を設定する（全端末：感染経路の可視化）

《 感染経路の確認方法 》

- ・ 感染経路はログ画面で確認することができます。

日時	カテゴリ	脅威違反	ファイルのパス/対象	処理結果	エンドポイント	ユーザ	詳細
2019年01月30日 17:3...	機械学習型検索	Ransom.Win32.TRX...	c:\users\kyoko\downlo...	隔離	DESKTOP-██████████	██████████	
2019年01月30日 17:3...	ウイルス/不正プログ...	Ransom.Win32.TRX...	c:\users\kyoko\downlo...	駆除	DESKTOP-██████████	██████████	
2019年01月30日 17:3...	ウイルス/不正プログ...	Ransom.Win32.TRX...	c:\users\kyoko\yappdat...	駆除	DESKTOP-██████████	██████████	



感染経路が確認可能な脅威ログのカテゴリ

下記4つで検知されたイベントについて、経路を確認することができます。

- ・ ウイルス/不正プログラム対策
- ・ Webレピュテーション
- ・ 挙動監視
- ・ 機械学習型検索

機能を設定する（全端末：隔離した端末の通信許可）

※EDRプラスオプションをご利用されている場合の機能となります

《 隔離した端末の通信許可方法 》

- ・ 隔離した端末において許可したい通信を設定することはできます。
 - 許可された受信トラフィック：IPアドレス、通信プロトコル、ポート番号
 - 許可された送信トラフィック：IPアドレス、通信プロトコル、ポート番号

グローバルセキュリティエージェント設定
グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール **隔離したエンドポイント** ③

トラフィックコントロール

隔離したエンドポイントはネットワークから切り離されます。すべての隔離したエンドポイントに対する送受信トラフィックについて、許可された受信トラフィック

許可された受信トラフィック

送信元IPアドレス:* ④ プロトコル: ポート: ①

IPアドレス すべて 全てのポート

+ 追加

許可された送信トラフィック

宛先IPアドレス:* ⑤ プロトコル: ポート: ①

IPアドレス すべて 全てのポート

+ 追加

保存 ⑥

「保存」を押して終了です。

機能を設定する（全端末：エージェントアンインストール防止）

エージェントのアンインストール防止を設定します。

→指定のパスワードを入力しないとアンインストールができないようにします

TREND MICRO | Worry Free™ Business Security Services

15:02 UTC+09:00

ポリシー設定 ②

追加の設定

グローバルセキュリティエージェント設定

グローバル除外リスト

ポリシーリソース

① アプリケーションコントロールルール

グローバルセキュリティエージェント設定

グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール ③

警告

7 日経過してもウイルスパターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

セキュリティエージェントのログ

WebレピュテーションおよびURLフィルタのログをサーバに送信する

脅威イベントの詳細を強化型脅威分析のためにサーバに送信する

監視サービス

セキュリティエージェントの監視サービスを有効にする:

セキュリティエージェントのステータスを 1 分間隔で確認

セキュリティエージェントを再起動できない場合、5 回まで再試行

管理者への問い合わせの通知

セキュリティエージェントに管理者への問い合わせ情報を表示する

アンインストール

セキュリティエージェントのアンインストール時にパスワード入力を要求する

パスワード: 4~20文字

パスワードの確認: ④

終了/ロック解除

セキュリティエージェントの終了時、または詳細設定のロック解除時にパスワード入力进行要求する

保存 ⑤

アンインストールに必要なパスワードを入力

「保存」を押して終了です。

機能を設定する（エージェント終了防止）

エージェントの終了防止を設定します。

→指定のパスワードを入力しないとエージェントの終了/ロック解除ができないようにします

TREND MICRO | Worry Free™ Business Security Services

15:04 UTC+09:00

ポリシー設定

追加の設定

グローバルセキュリティエージェント設定

グローバル除外リスト

ポリシーリソース

アプリケーションコントロールルール

グローバルセキュリティエージェント設定

グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定

エージェントコントロール

警告

7 日経過してもウイルスパターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

セキュリティエージェントのログ

WebレピュテーションおよびURLフィルタのログをサーバに送信する

脅威イベントの詳細を強化型脅威分析のためにサーバに送信する

監視サービス

セキュリティエージェントの監視サービスを有効にする:

セキュリティエージェントのステータスを 1 分間隔で確認

セキュリティエージェントを再起動できない場合、5 回まで再試行

管理者への問い合わせの通知

セキュリティエージェントに管理者への問い合わせ情報を表示する

アンインストール

セキュリティエージェントのアンインストール時にパスワード入力进行要求する

終了/ロック解除

セキュリティエージェントの終了時、または詳細設定のロック解除時にパスワード入力进行要求する

パスワード: 4~20文字

パスワードの確認:

保存

エージェントの終了に必要なパスワードを入力

「保存」を押して終了です。

機能を設定する（管理：ラベル表示）

管理者が各デバイスの名称を管理コンソール上で判別しやすいようにラベル登録することができます。

※ここではラベル形式に[従業員ID]を設定をしています。

管理 ② 一般設定

①

一般設定

モバイルデバイス登録設定

通知

Active Directoryの設定

Smart Protection Network

回復キーのパスワード

③

エンドポイントのラベル付け

この機能を使用すると、セキュリティエージェントのインストール中またはWebコンソール上の [セキュリティエージェント] 画面でエンドポイントをラベル付けることができます。詳細情報

エンドポイントのラベル付けを有効にする

エンドポイントのラベル付けのヒントとして、セキュリティエージェントのインストール中にラベル形式が表示されます。例: フルネーム、従業員ID、メールアドレス

ラベル形式: 従業員ID

セキュリティエージェントのインストール用リンク

ウイルスバスター ビジネスセキュリティサービスでは、ユーザにより処理がドリンクと認証コードの有効期限を設定するよう選択できます。

有効期限を 14 日後とする (1~999) ④

セキュリティエージェントツリーのクリーンナップ

ウイルスバスター ビジネスセキュリティサービスは、セキュリティエージェントがインストールされた特定のコンピュータにセキュリティエージェントがインストールされた場合、セキュリティエージェントを自動的に削除できます。接続が再度確立されると、サーバは削除されたWindowsおよびMacセキュリティエージェントを自動的に復元します。⑤

次の期間アクセスがないエージェントをセキュリティエージェントツリーから自動削除する: 30 日 (1~999)

トラブルシューティング

セキュリティエージェント

障害発生時に、デバッグログを有効化して下記の情報を収集することをトレンドマイクロのテクニカルサポートに許可する

Windowsエンドポイントの場合: デバッグログ、Windowsイベントログ、パフォーマンスカウンタのデータ、システム情報、カーネルダンプ、クラッシュ情報、セキュリティエージェントの設定 (レジストリ) など

Macエンドポイントの場合: デバッグログ、システム情報、カーネルダンプ、クラッシュ情報、システムプロファイラのデータ、セキュリティエージェントの設定 (.plist) など

Webコンソール

診断とトラブルシューティングを目的としたウイルスバスター ビジネスセキュリティサービスWebコンソールへのアクセスをトレンドマイクロのテクニカルサポートに許可する

保存 ⑤

「保存」を押して終了です。

機能を設定する（管理：ラベル表示）

【参考】エージェントインストール時の画面

「セキュリティエージェント」タブからラベルを入力・訂正することもできます。

機能を設定する（管理：通知）

ウイルス感染時等に、管理者へのメール通知を設定します。

The screenshot displays the '通知' (Notification) settings page in the Trend Micro Worry Free Business Security Services management console. The interface includes a sidebar with navigation options such as '一般設定', 'モバイルデバイス登録設定', and '通知'. The main content area shows a form for configuring email notifications, with fields for '送信者' (Sender), '受信者' (Recipient), and '件名の先頭文字列' (Subject prefix). A callout box provides an example subject line: '【おまかせアンチウイルスからの通知】'.

「保存」を押して終了です。

機能を設定する（グループ：リモートロック/消去）

端末の盗難・紛失時に、遠隔で端末をロックします。



● Androidを選択した場合



- タスク ▾
- リモート検索
- リモートロック
- パスワードをリセット
- リモート消去
- 今すぐアップデート

● iPadOS/iOSを選択した場合



- タスク ▾
- リモートロック
- Touch IDとパスコードをクリア
- リモート消去

※状況により消去出来ない場合があります

リモートロックとは：紛失した携帯端末を第三者が利用できないようにします
リモート消去とは：紛失した携帯端末のデータを消去します(※)

機能を設定する（全端末：除外設定）

指定したフォルダ、ファイル、またはファイル拡張子を不正プログラム検索から除外します。

The screenshot shows the Trend Micro Worry Free Business Security Services interface. On the left is a navigation sidebar with icons for Home, Add Settings, User, Exclusion List (highlighted with a red box and a circled '2'), Policy Sources, Application Control Rules (circled '1'), Documents, and Settings. The main content area is titled 'グローバル除外リスト' (Global Exclusion List) and includes a sub-header 'Webレピュテーション / URLフィルタ' (Web Reputation / URL Filter). It lists several exclusion categories: '承認済みURLリスト (15)', 'ブロックするURLリスト (0)', '承認済みIPアドレスリスト (0)', and '許可されたプロセスのリスト (0)'. Below this is the '不正プログラム検索除外' (Malware Search Exclusion) section, which includes '信頼済みWindowsプログラムリスト (0)', '信頼済みMacプログラムリスト (0)', and '機械学習型検索除外リスト (0)'. The final section is 'デバイスコントロール' (Device Control), with '許可されたUSBデバイスのリスト (0)'. A blue callout box at the bottom explains that items can be specified for exclusion based on security functions.

セキュリティ機能に応じて常に許可/ブロックしたいもの（URL/プログラムなど）を指定することができます

機能を設定する（グループ追加）

ライセンス数が多い場合など、グループを作成し管理を容易にすることができます。

※ここでは[test]グループを追加しています。



新規グループ

名前:
test

ポリシー設定をインポートする

ソース: サーバ (初期設定)

保存 キャンセル

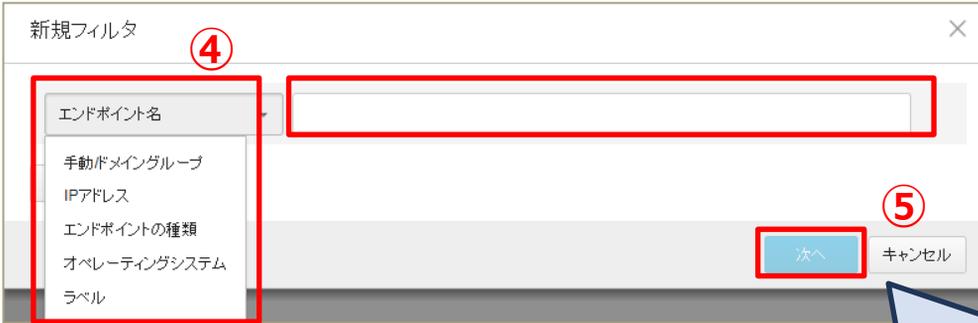


「手動グループ」の配下に新規グループが作成されます。

機能を設定する（フィルタ追加）

特定の条件に該当するエンドポイントを確認したい場合などは、フィルタを作成し管理を容易にすることができます。

※ここでは[test]フィルタを追加しています。



フィルタの条件を指定（AND条件）

フィルタ名を指定



「フィルタ機能の実装」の配下に新規フィルタが作成されます。

機能を設定する（グループ：予約検索）

金曜日のお昼にウイルスチェックするなど、デバイスの脅威を定期的に検索することができます。

ポリシーの設定: test

対象とサービスの設定

脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- 仮想パッチ
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済み/ブロックするURL

エージェントの設定

- 権限およびその他の設定

検索設定

検索方法

- スマートスキャン (推奨)
スマートスキャンでは、インターネットクラウドに格納されている不正プログラム対策シグネチャおよびスパイウェア対策シグネチャが利用されます。
- 従来型スキャン
従来型スキャンは、セキュリティエージェントのローカルに格納されている不正プログラムやスパイウェア対策コンポーネントを利用します。

リアルタイム検索

ファイルを受信、開く、ダウンロード、コピー、または変更したときに、セキュリティ上のリスクがあるかファイルを検索します。

オン

設定

予約検索

設定された時間及び頻度で検索を実行します。予約検索を使用すると、エンドポイントでの定期的な検索を自動化し、脅威の管理を効率化することができます。

オン

頻度: 週1回

間隔: 月曜日

開始時刻: 12 : 30 時分

設定

手動検索

Webコンソール上の [セキュリティエージェント] 画面またはセキュリティエージェントコンソールから開始される手動検索です。

設定

予約検索設定

対象 処理

検索設定

検索するファイル:

- 検索可能なすべてのファイル
- トレンドマイクロの推奨設定で検索されるファイルタイプ
- 指定された拡張子を持つファイル
- 圧縮ファイルの検索

最大階層数: 2

詳細設定

- IntelliTrapを有効にする
- システム領域を検索する

CPU使用率

- 高 一時中断せずに連続してファイルを検索する
- 中 CPU使用率が50%を超えた場合にファイル検索の合間に一時中断し、50%以下の場合は一時的に中断しない
- 低 CPU使用率が20%を超えた場合はファイル検索の合間に一時中断して回復を待ち、20%以下の場合は一時中断しない

ファイル検索の合間にセキュリティエージェントが待機する時間は、CPU使用率を左右します。使用レベルを [低] に設定すると、ファイル検索の合間の待機時間が長くなり、その分CPUリソースが解放されます。

ウイルス不正プログラム

- トレンドマイクロの推奨設定
- カスタマイズ設定
- 検出前にファイルをバックアップする

スパイウェアグレーウェア

- 削除 プロセスを終了するが、レジストリ、Cookie、およびショートカットを削除する
- 監視 スパイウェアグレーウェア検出結果を診断のために記録します

保存 キャンセル

「保存」を押して終了です。

機能を設定する（グループ：手動アップデート）

手動でパターンファイルをアップデートすることも可能です。
方法は(1)管理コンソールから、(2)エージェントからの2種類があります。

方法(1)：管理コンソールから手動でアップデートする



③でチェックしたエンドポイントのアップデートを行います。



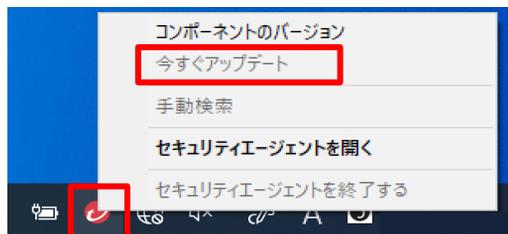
「アップデート」を押して終了です。

エージェントのアップデートが開始するまでに5～10分かかります。

機能を設定する（グループ：手動アップデート）

方法(2)：エージェントから手動でアップデートする

おまかせアンチウイルスがインストールされている
端末の常駐アイコン(赤い丸アイコン)を右クリックし
表示されたメニューから「今すぐアップデート」を
クリックします。



ファイルのダウンロードが始まります。



完了のメッセージが表示されますので
「閉じる」ボタンをクリックします。



常駐アイコン(赤い丸アイコン)を
ダブルクリックすることにより
ソフトウェアが最新か確認することが
出来ます。

緑色のアイコンが表示され、
「保護された状態であり、
ソフトウェアは最新です」の表示

