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

はじめに

『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。

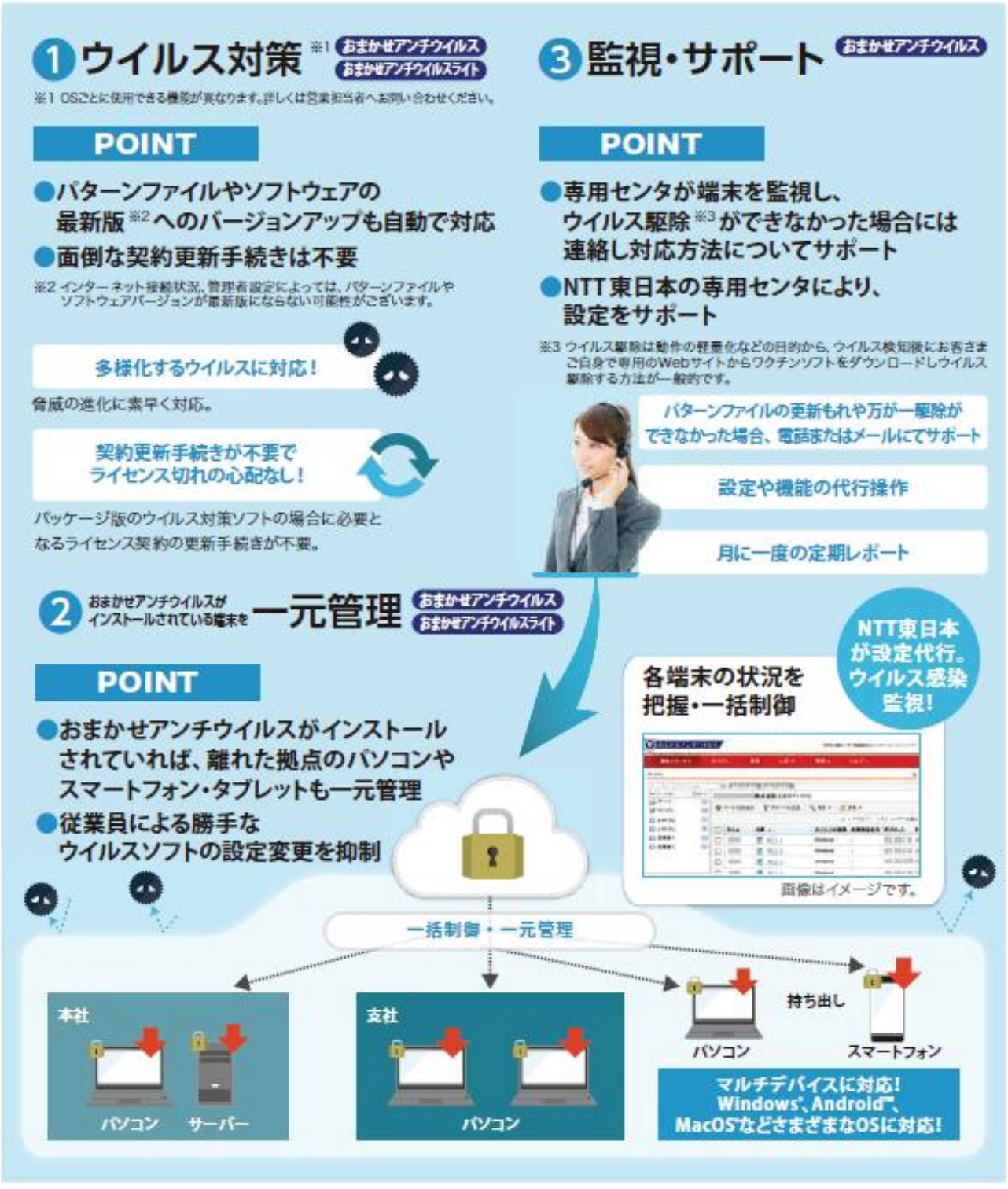
目次

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



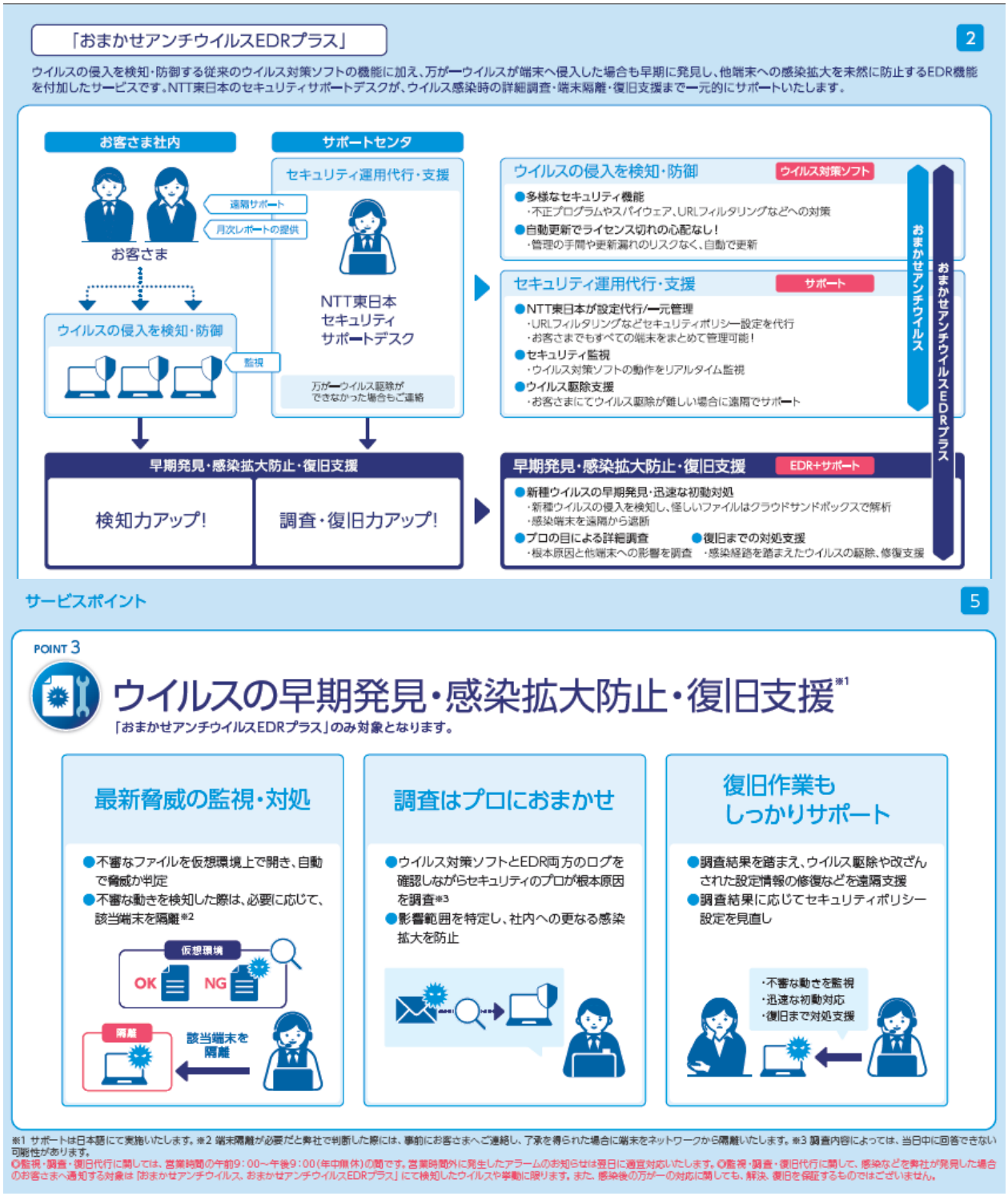
※　③の監視・設定代行は『おまかせアンチウイルス　ライト』では提供しておりません。

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



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

サービス提供までの流れ

お客さま

お申込み

NTT東日本　営業

情報取次

NTT東日本
サポートセンタ

おまかせアンチウイルスID等通知

おまかせアンチウイルスのご利用開始希望日に
メールで通知されます(※)

※お客さまの設定によっては、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	ウイルス/不正プログラム、スパイウェア、メール、フィッシングサイトなど幅広い脅威に対応することができ、脅威をブロック・隔離することができます。	○	○	○	○	○	○	–	–
		機械学習型検索	AIによる分析で不正プログラムに似た特性を示すと判定されたファイルを自動的に隔離	○	○	○	○	○	–	–	–
		挙動監視機能	プログラム単体では判定困難な場合でも、既知のウイルスと似た挙動を検知した際には自動的にプログラムの実行を停止	○	○	○	○	–	–	–	–
		ファイルレス攻撃対応	挙動監視、機械学習型検索、リアルタイム検索にて、メモリ上にのみ存在するウイルスを検知・隔離します。	○	○	○	○	–	–	–	–
		ランサムウェア対応	ランサムウェア（身代金要求ウイルス）に対し、各種セキュリティ機能を複合的に実施して防ぐと共に、ランサムウェア独自の挙動に対して有効な対処やファイルの復元を行います。	○	○	○	○	–	–	–	–
		仮想パッチ	セキュリティパッチを早急に適用する事が難しい環境へ、暫定的なセキュリティを担保するためのソリューションです。	○	○	○	○	–	–	–	–
		ファイアウォール機能	端末とネットワーク間の通信において、特定の種類のトラフィックを拒否または許可	○	○	○	○	–	–	–	–
		Webレピュテーション	フィッシング詐欺やウイルスが仕込まれたWebサイトなど、危険なサイトへのアクセスをブロック	○	○	○	○	○	○	○	○
		URLフィルタリング	業務上必要のないWebサイトへのアクセスを制御	○	○	○	○	○	–	–	○
		情報漏えい対策	機密データの転送を監視・ブロックします。	○	○	○	○	–	–	–	–
		デバイスコントロール	USBメモリなどに対し、「コピー」「移動」「開く」「保存」「削除」「実行」などの操作を制御	○	○	○	○	○	–	–	–
		アプリケーションコントロール	カテゴリ、ベンダー、アプリケーション名を指定してアプリケーションの利用を制限できます。	○	○	○	○	–	–	–	–
		パスワード/パスコード	エンドポイントの画面をロックするためのパスワードを設定するよう、ユーザに通知がされます。また、パスワードポリシー（文字数等）を指定することができます。	○	○	○	–	–	○	○	–
		クラウドサンドボックス	パターンファイルで検知困難な新種のウイルスをクラウド上の仮想環境で解析し、悪性なウイルスか判定	○	–	–	○	○	–	–	–
	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。

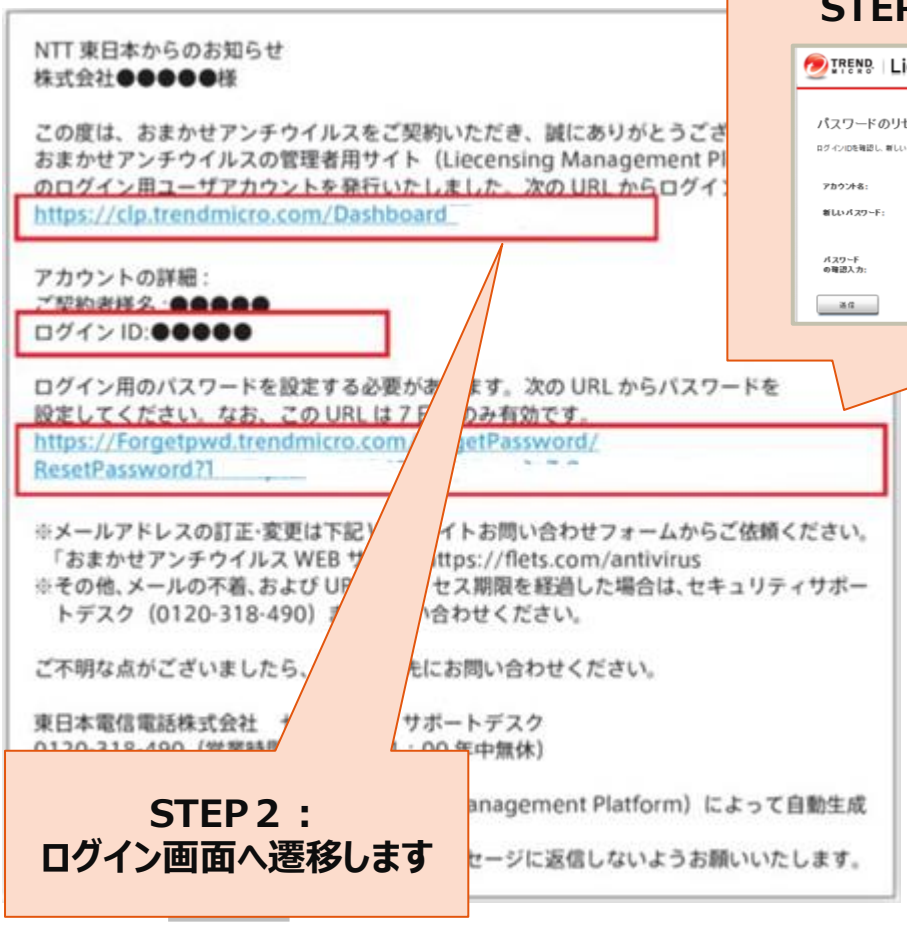
※他社の法人向けウイルス対策サービスをご利用中の場合、
アンインストールを行う際にアンインストールパスワードを要求される場合がございます。
その場合は、アンインストールパスワードを確認の上、アンインストールを実施します。

(※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。



STEP１：PWを設定します

STEP２：
ログイン画面へ遷移します

STEP３：
『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。

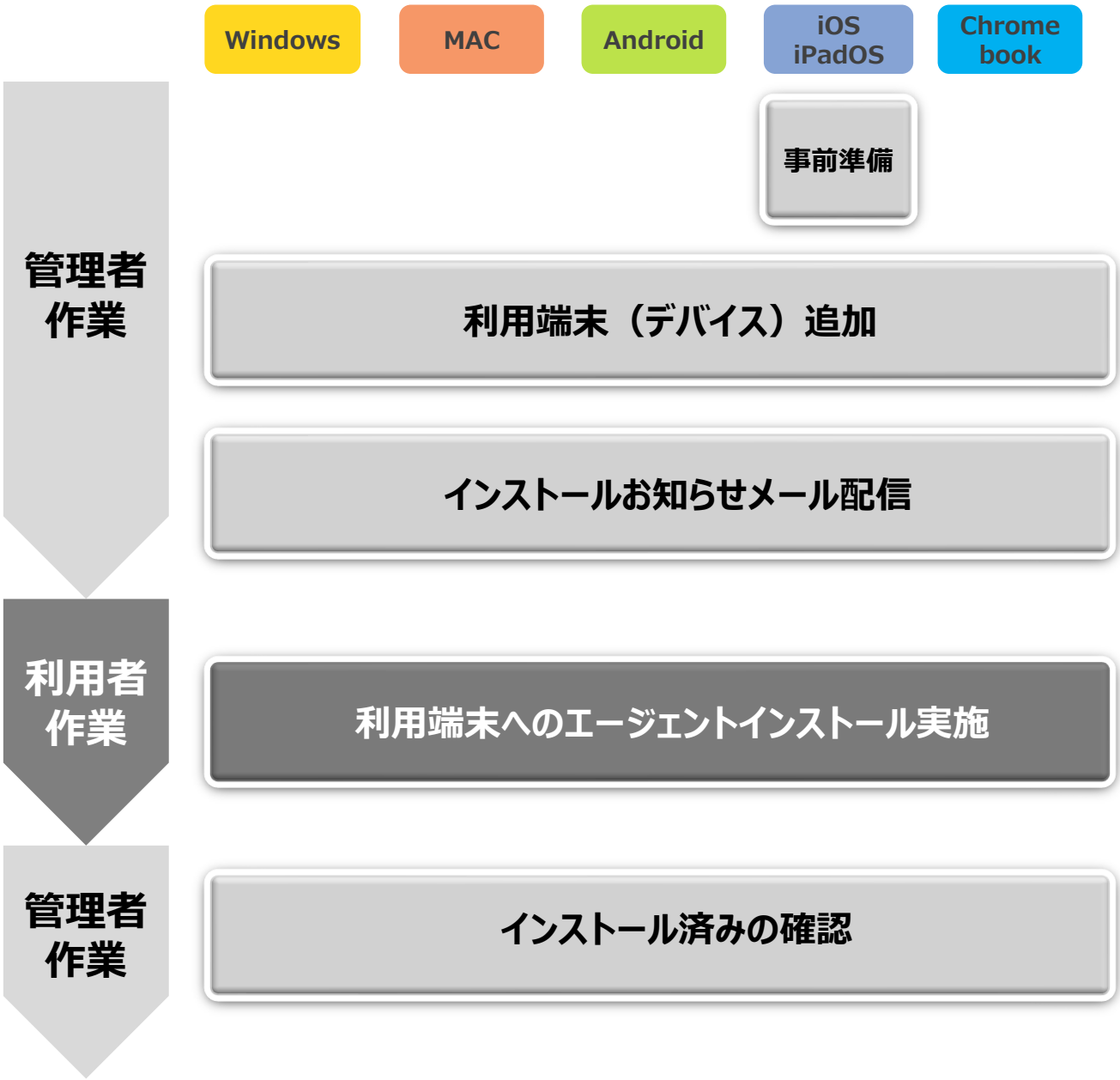
※二要素認証の設定手順はおまかせアンチウイルス公式HPに掲載されているマニュアルを参照ください。
おまかせアンチウイルス公式HP：https://business.ntt-east.co.jp/support/antivirus/

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

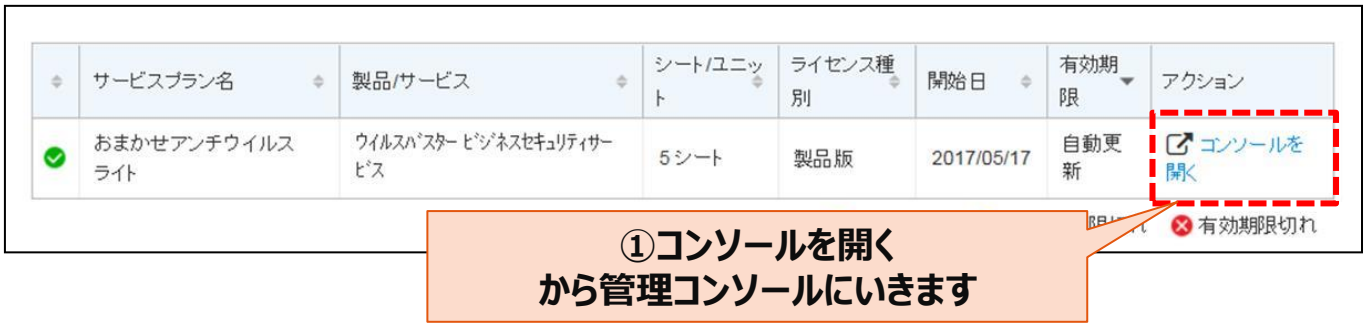
①ログインIDを入力

②設定したPWを入力

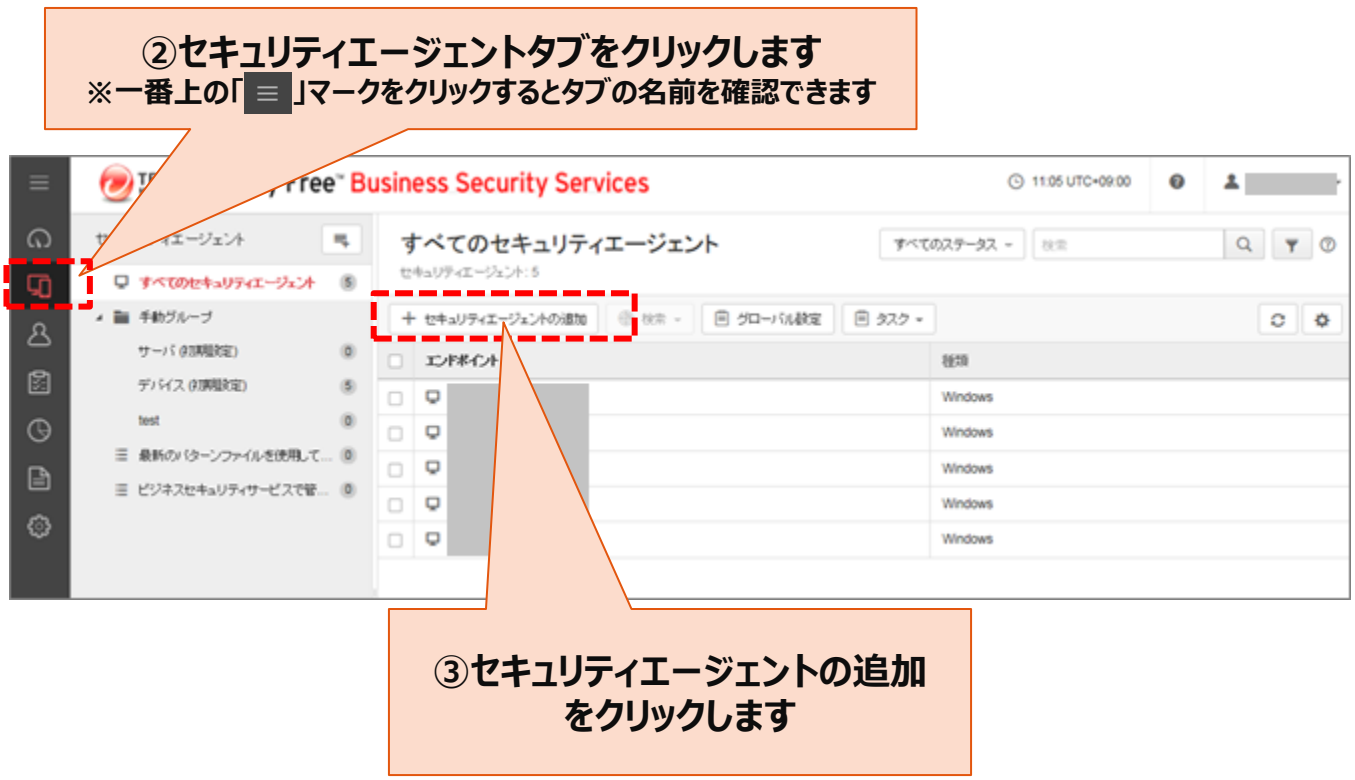
③ログインをクリック

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



※「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。

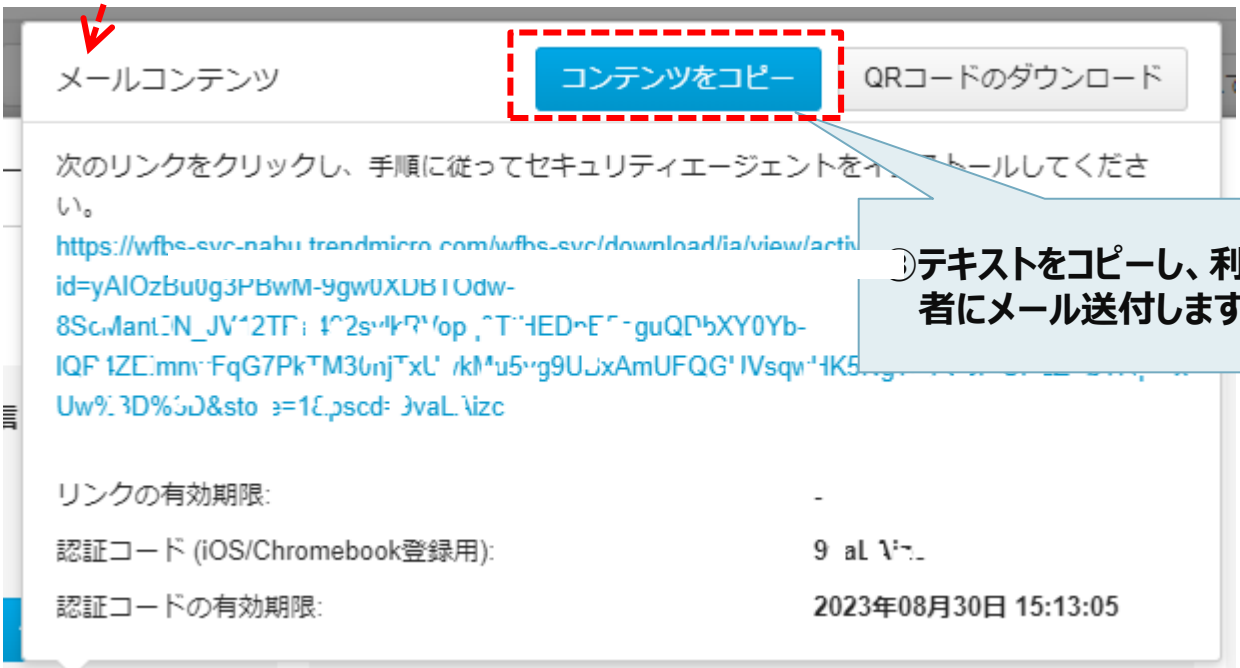


エージェントツールのインストール

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、コチラをクリックします

①管理者の端末にインストールする場合は、コチラをクリックします



③テキストをコピーし、利用者にメール送付します

エージェントツールのインストール

Windows

管理者作業 → 利用者作業

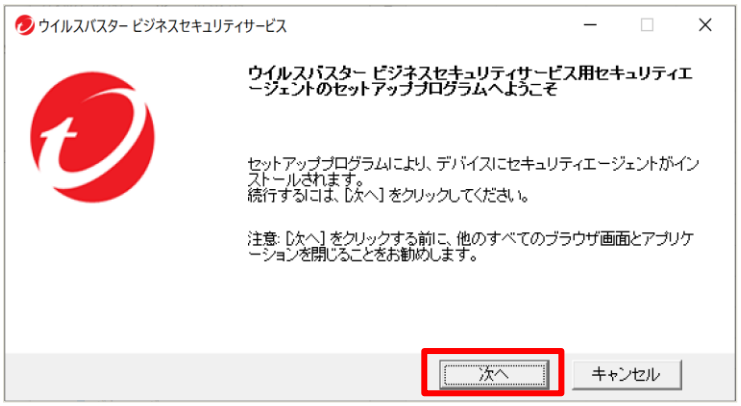
【EDRプラスをご利用の場合】
Windowsエージェントは、EDR機能は自動で有効化されるため、有効化作業は不要となります
EDRプラスを新規でご利用される場合は、下記手順に従い、アンチウイルスエージェントのインストール作業を実施してください
※MacのEDR有効化は有効化作業が必要なため、後の「EDRエージェント有効化」を参照ください

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。

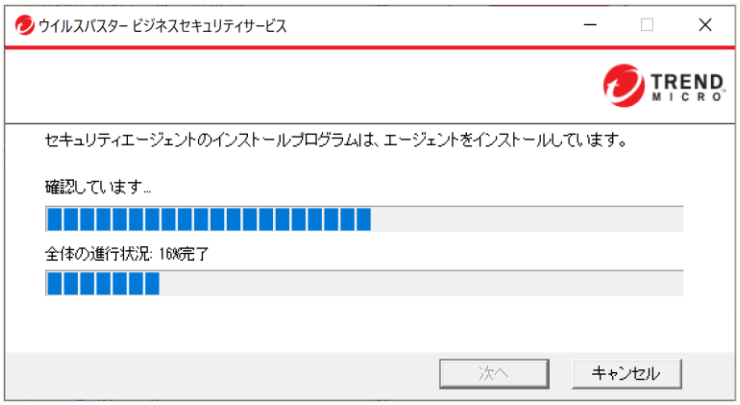


エージェントツールのインストール

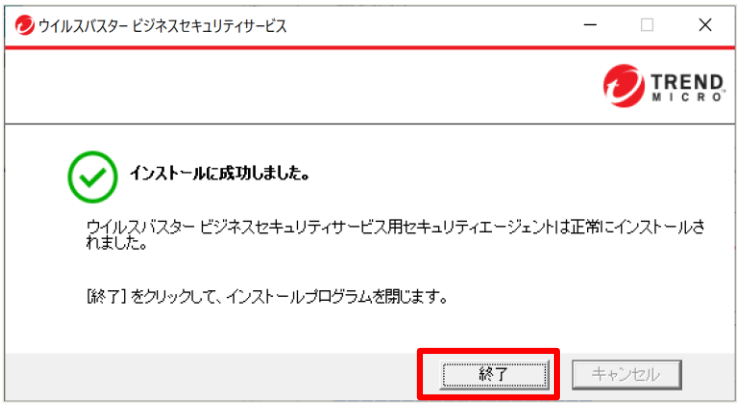
Windows

管理者作業 利用者作業

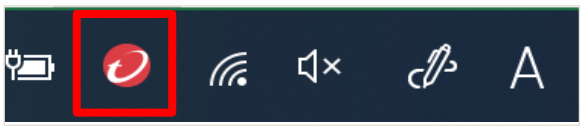
5. インストールが開始されます。



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。

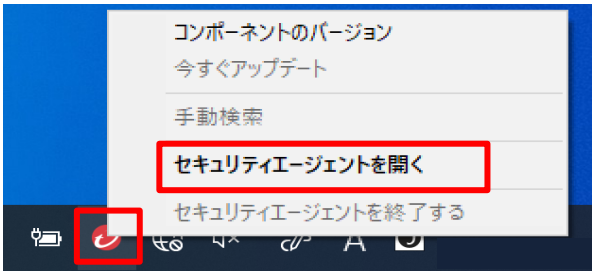


エージェントツールのインストール

Windows

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。



番号	機能	詳細
1	ステータス	セキュリティエージェントのメイン画面に表示されるアイコンやその意味と対処内容を示しています。
		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	ユーザツール	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。

エージェントツールのインストール

MAC

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。

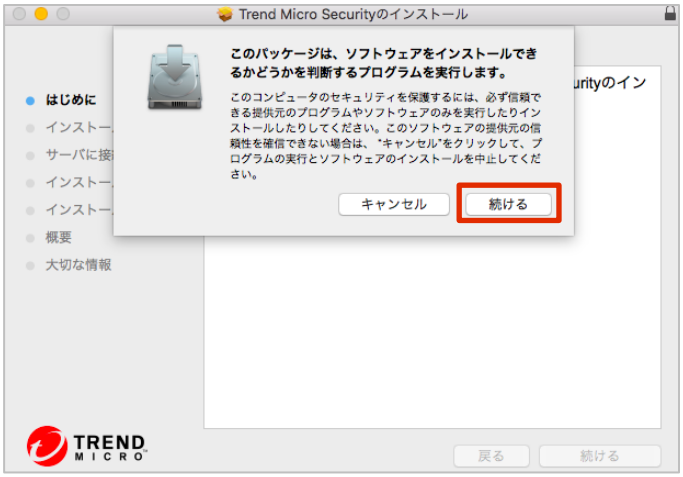
3．ダウンロード完了後、「WFBS-SVC_Agent_Installer.pkg」をクリックし、インストールを実行します。

エージェントツールのインストール

MAC

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

MAC

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。

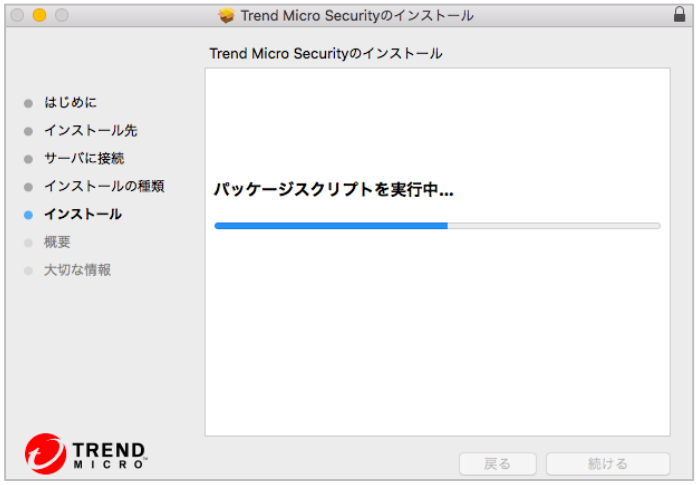
6．「インストーラが新しいソフトウェアをインストールしようとしています。」と表示された場合は、名前(ご利用のMac OSのユーザ名)とパスワードを入力し、[ソフトウェアをインストール]をクリックします。

エージェントツールのインストール

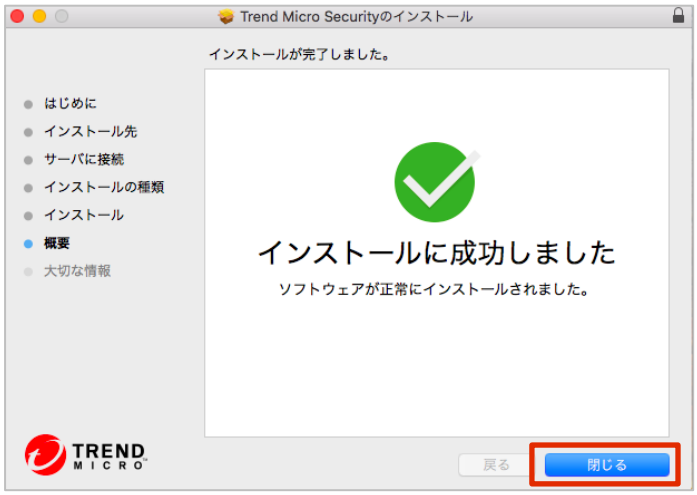
MAC

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。



エージェントツールのインストール

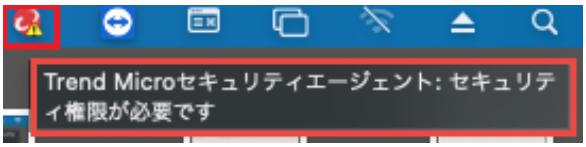
MAC

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。

エージェントツールのインストール

MAC

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。

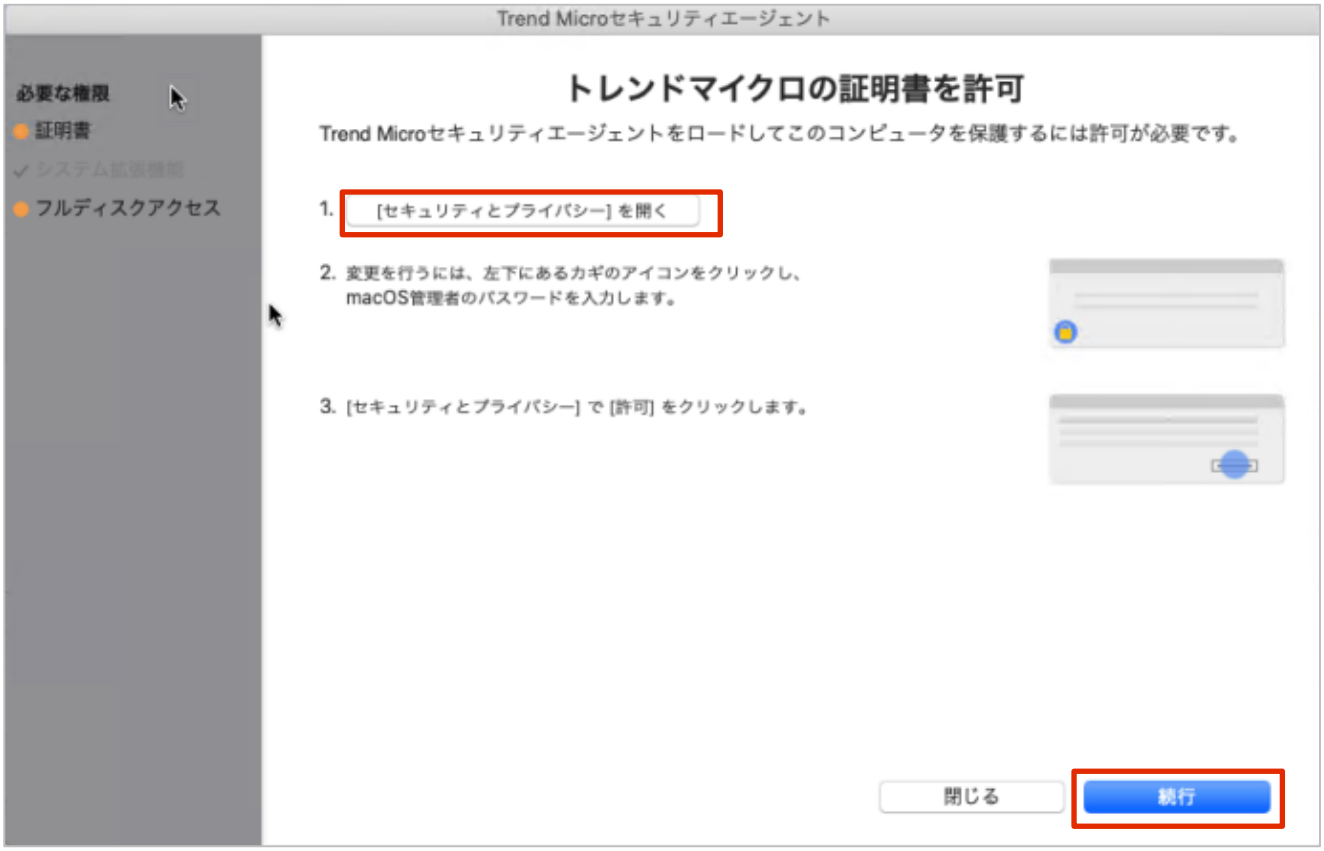
2．「セキュリティ権限が必要」と表示されますので [詳細を表示] をクリックします。

エージェントツールのインストール

MAC

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。

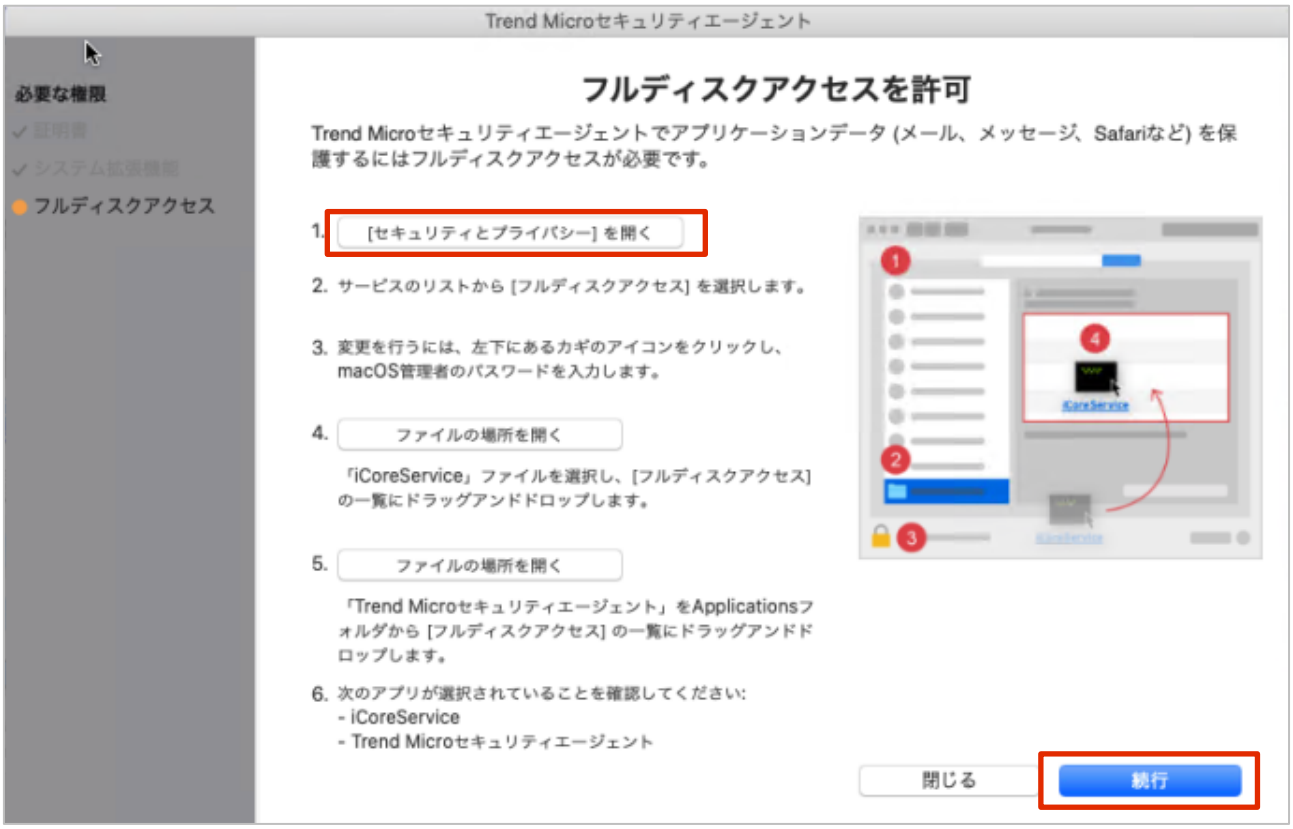
3-3. [続行] をクリックします。

エージェントツールのインストール

MAC

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。

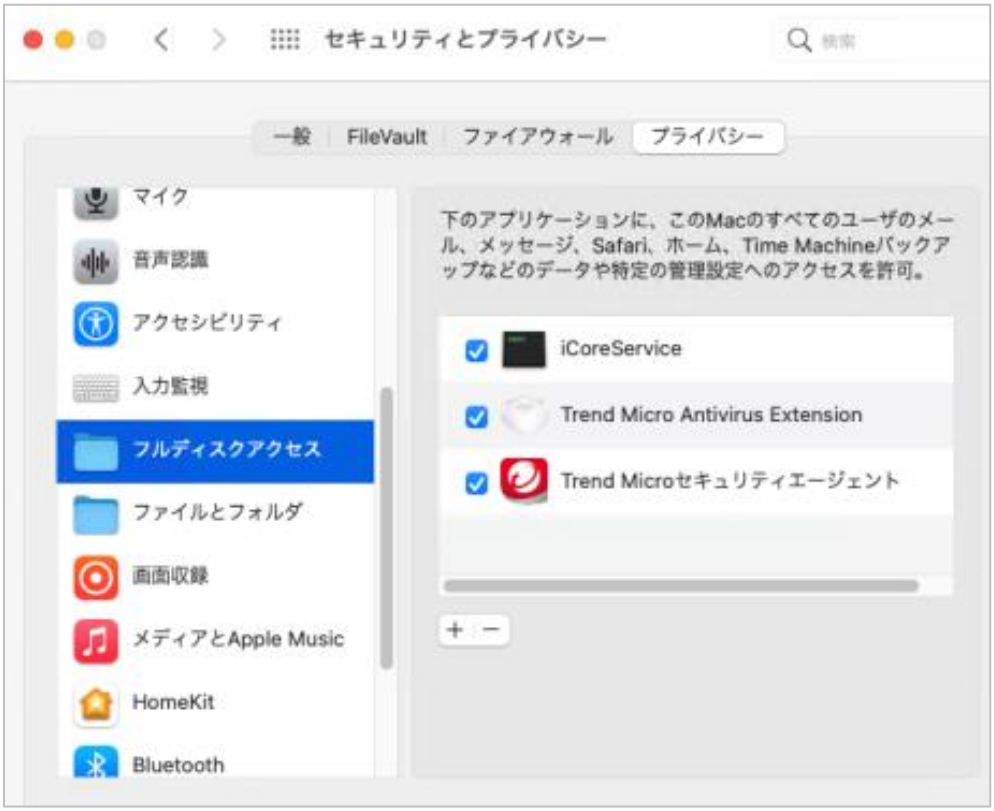
※ macOS 11 Big Sur をご利用の場合は、「TrendMicro Antivirus Extension」についても追加とチェックが必要となります。

エージェントツールのインストール

MAC

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。

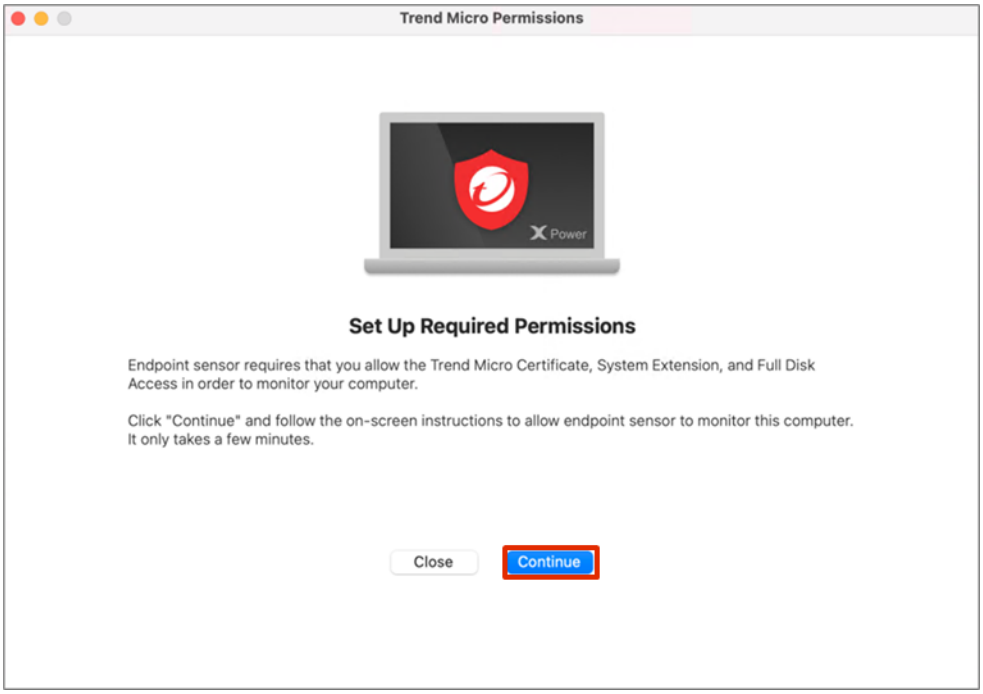
（Macのみ）EDRエージェント有効化

MAC

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。



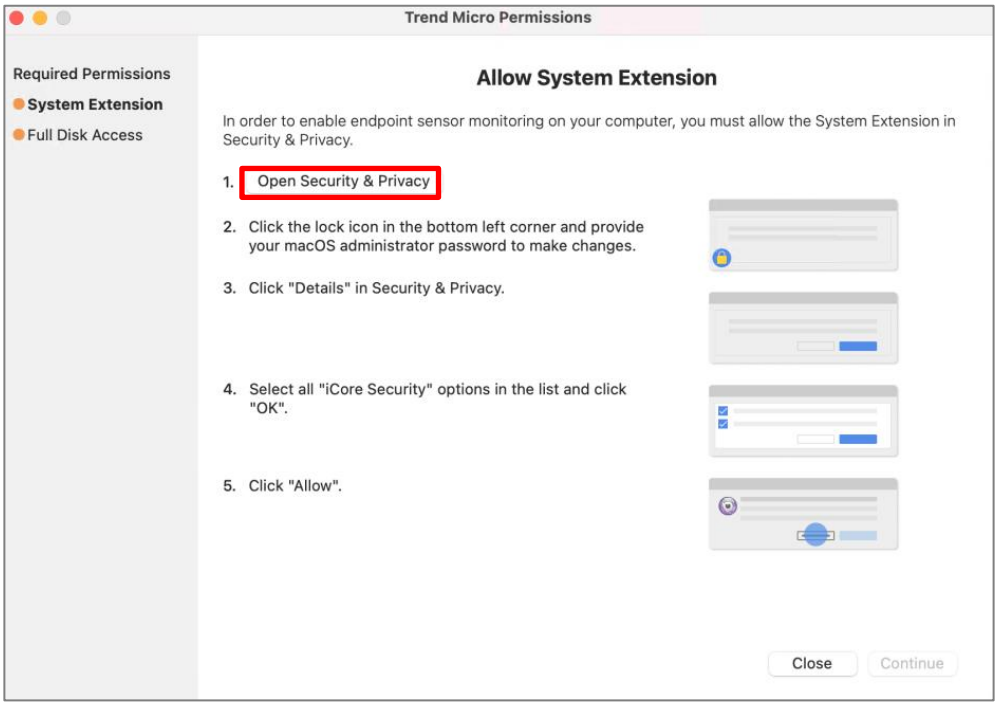
２．以下画面が表示された場合は、「システム設定を開く」をクリックします。

（Macのみ） EDRエージェント有効化

MAC

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。

（Macのみ）EDRエージェント有効化

MAC

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

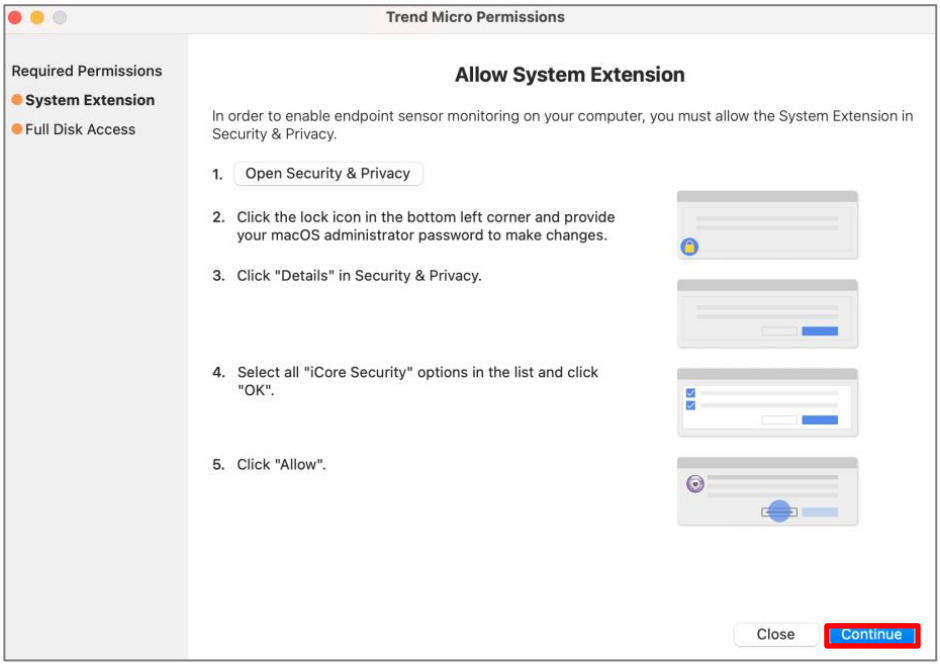
7. 以下画面において、許可をクリックします

（Macのみ）EDRエージェント有効化

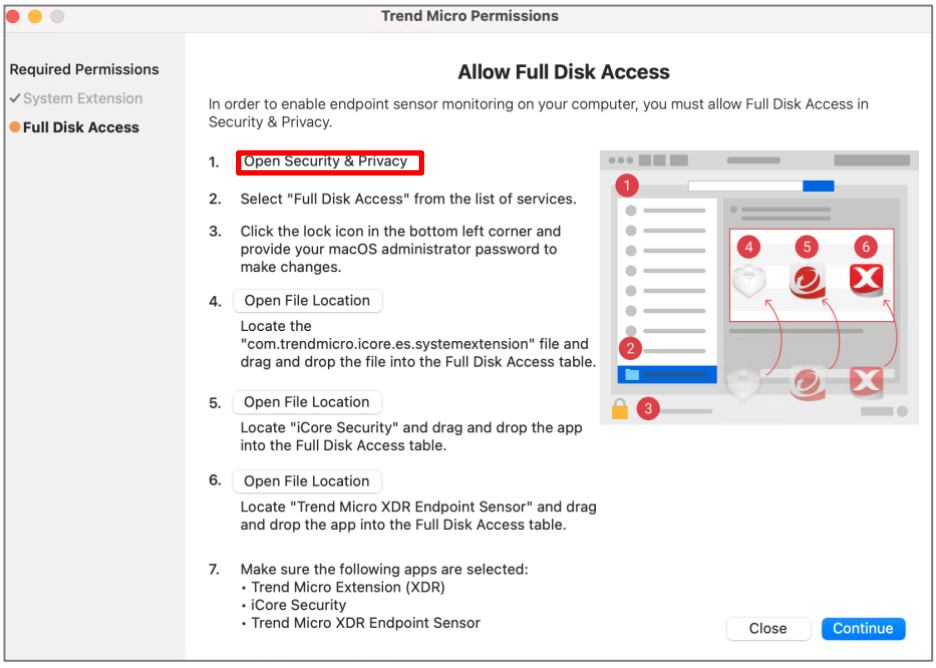
MAC

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。

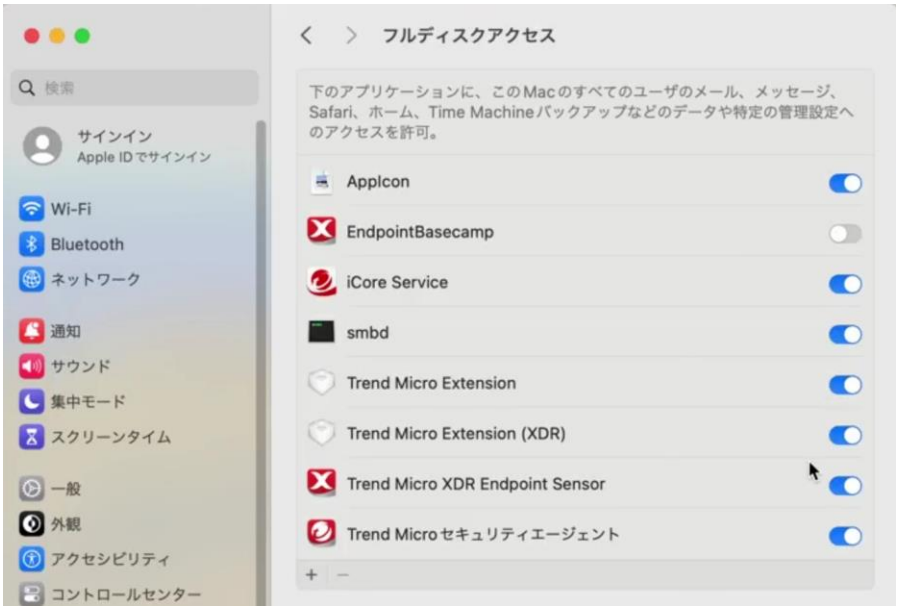


（Macのみ）EDRエージェント有効化

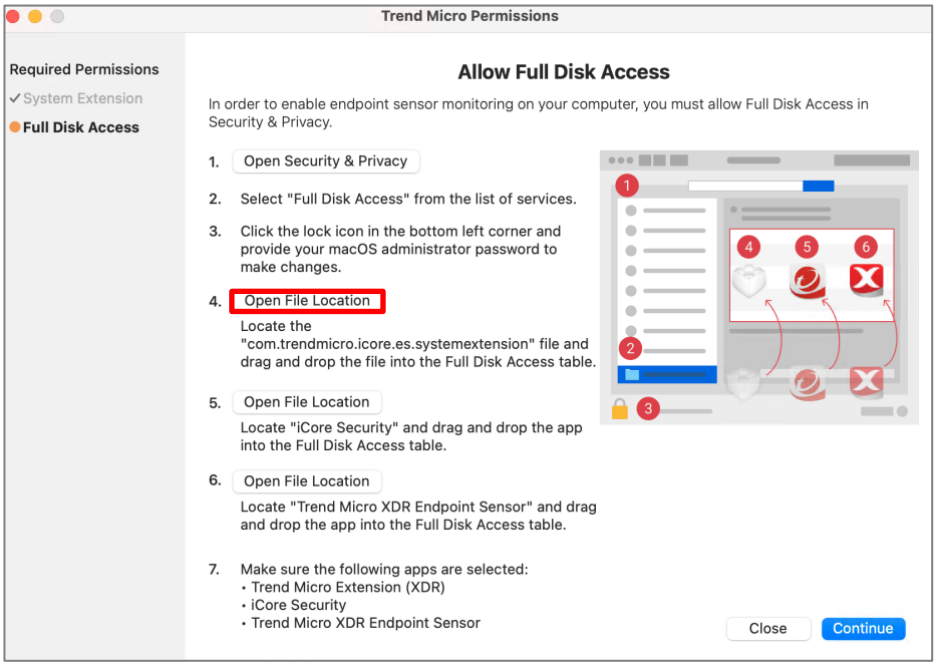
MAC

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。

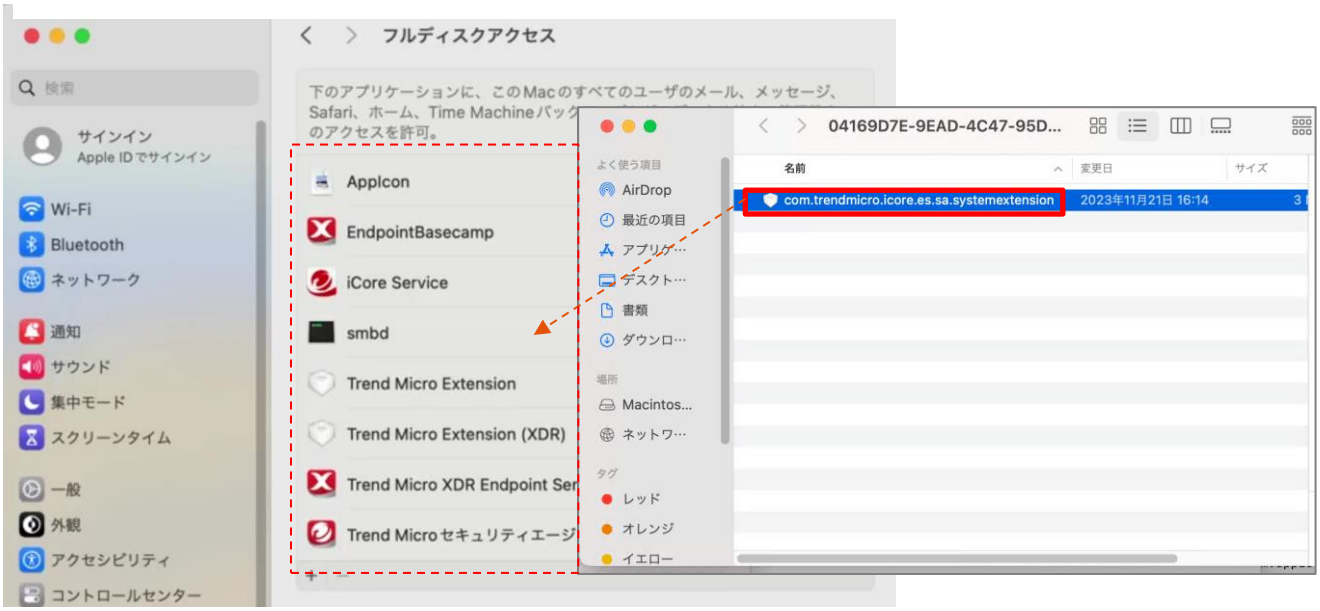


（Macのみ）EDRエージェント有効化

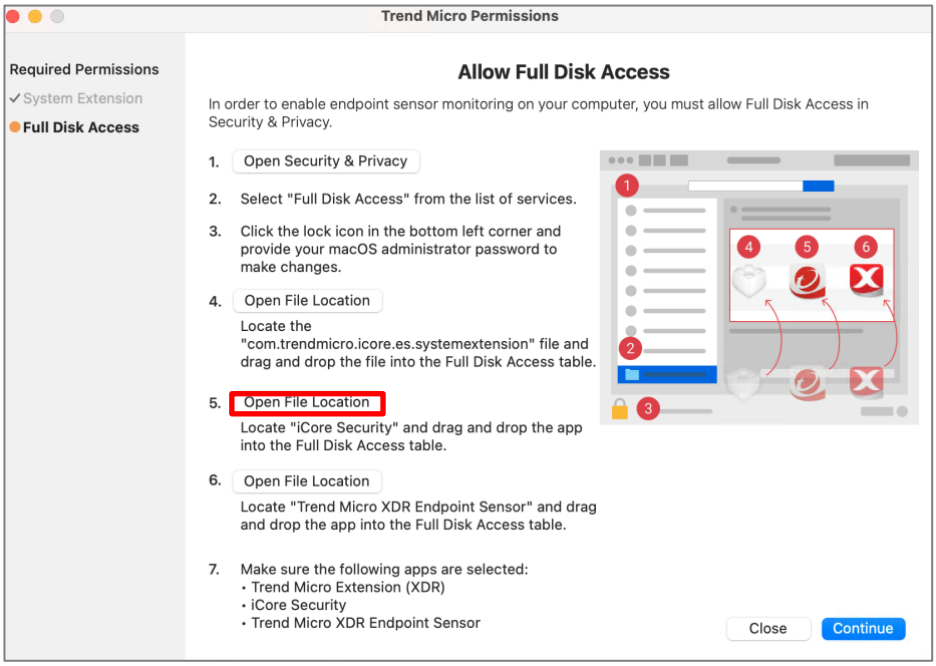
MAC

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。

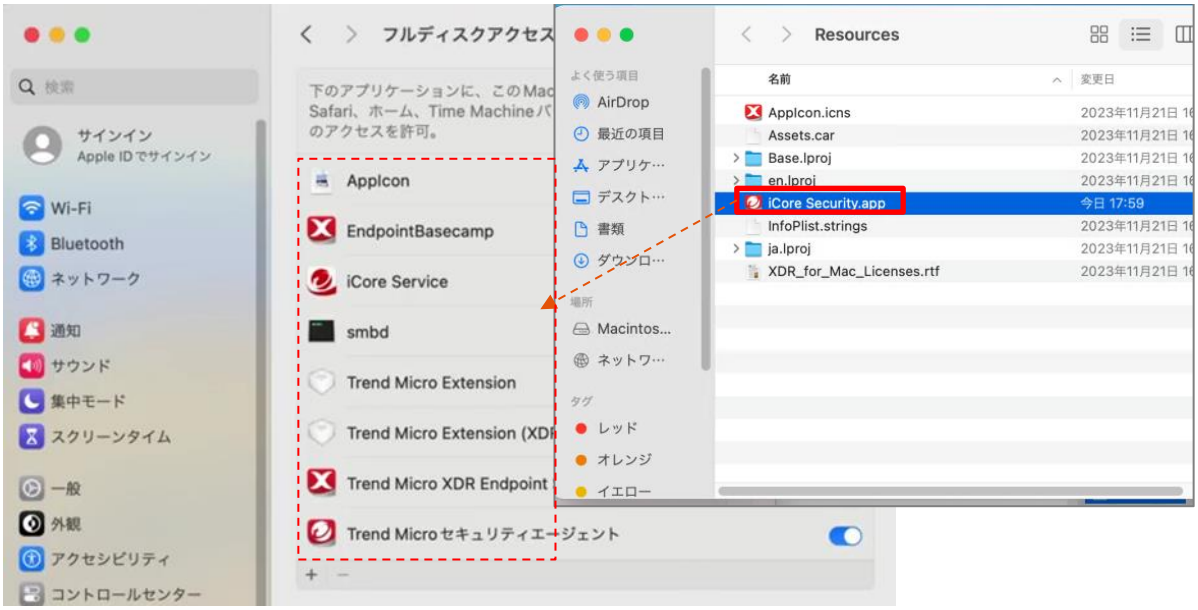


（Macのみ）EDRエージェント有効化

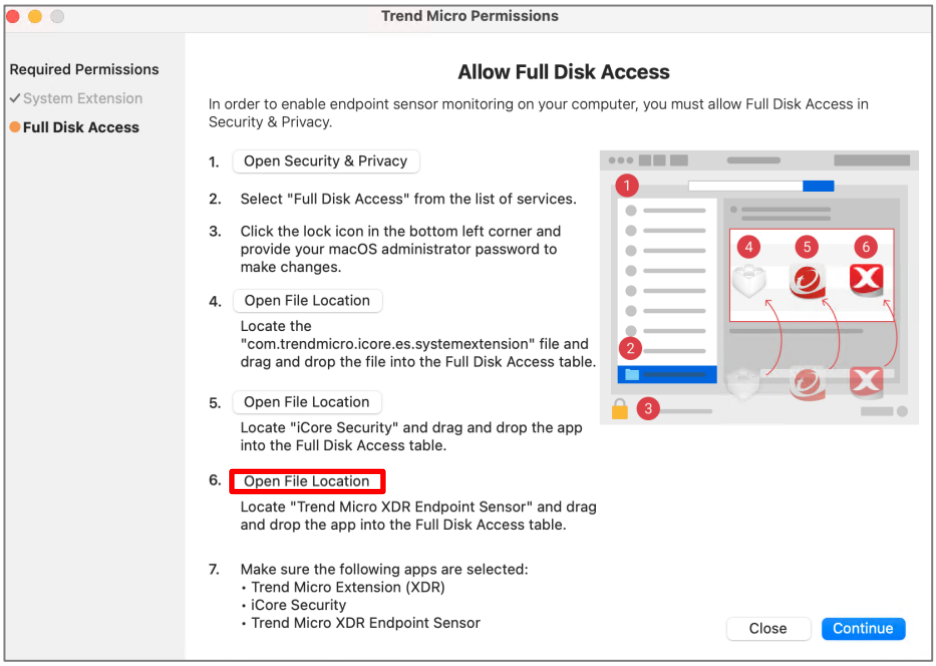
MAC

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。

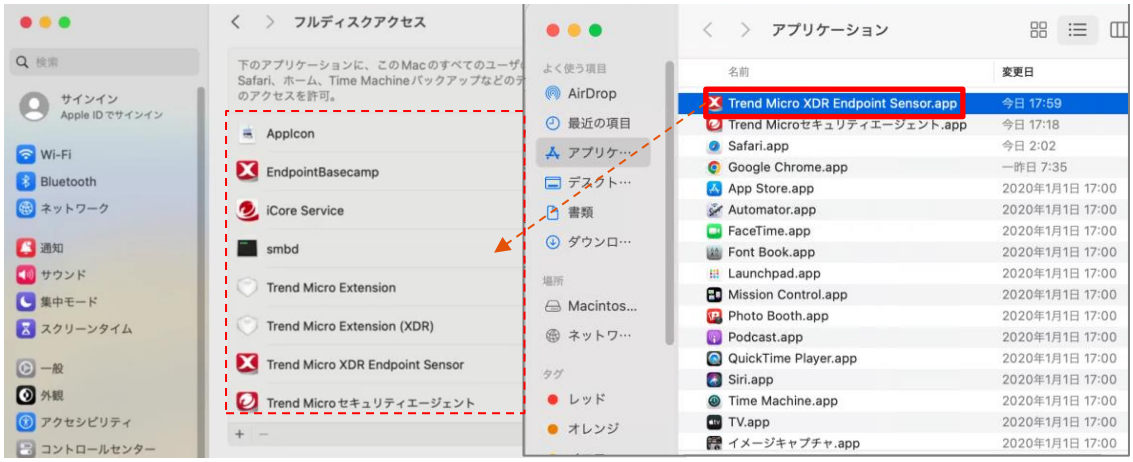


（Macのみ）EDRエージェント有効化

MAC

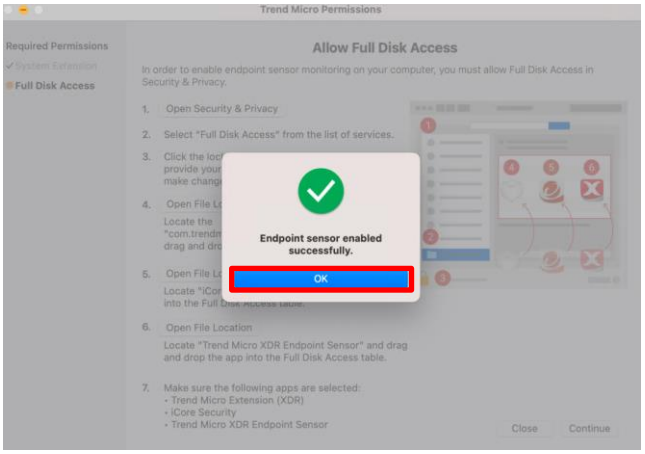
管理者作業 利用者作業

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



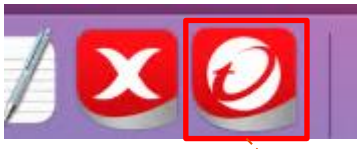
（Macのみ）EDRエージェント有効化

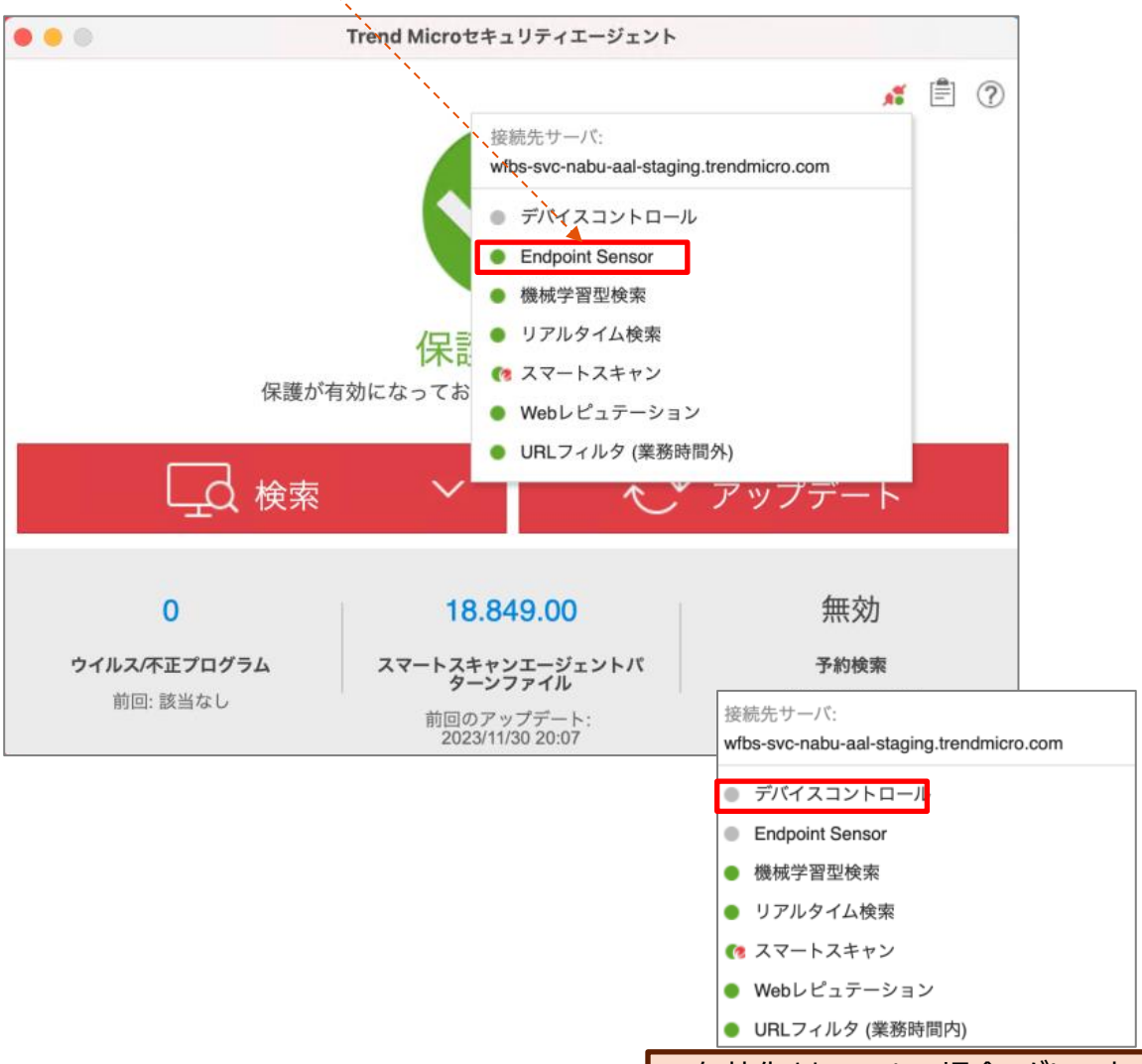
MAC

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

（Macのみ）EDRのアンインストール

MAC

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。

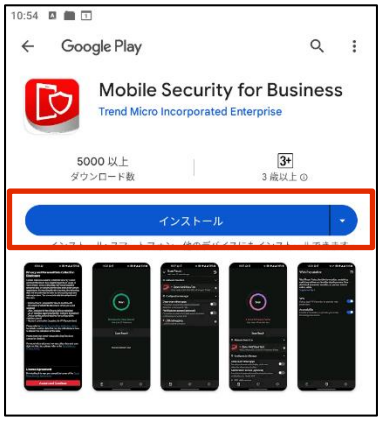
エージェントのインストール

Android

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。

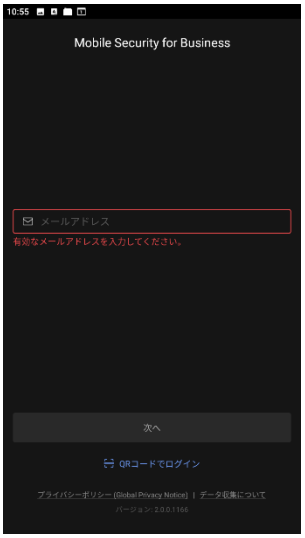
4 .インストールが完了したら開くをタップします。

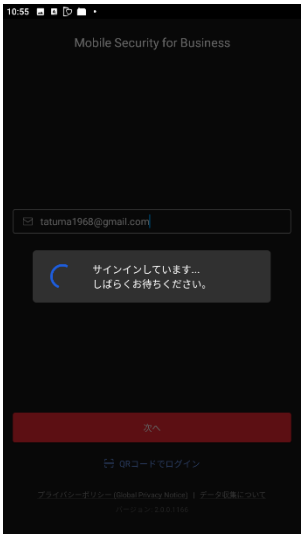
エージェントのインストール

Android

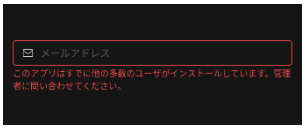
管理者作業 利用者作業

5.メールアドレスを入力してサインインします



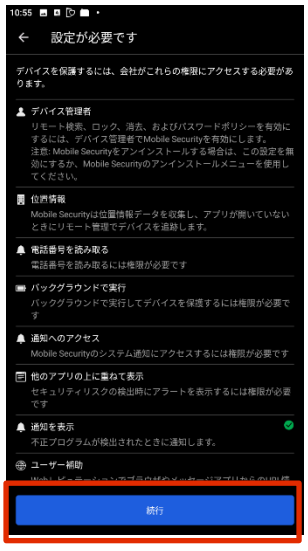


「このアプリではすでに他の多数のユーザがインストールしています。管理者に問い合わせてください。」



※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。

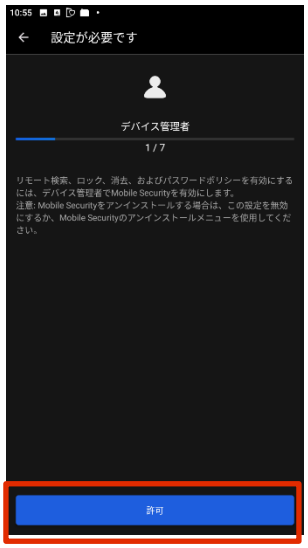


エージェントのインストール

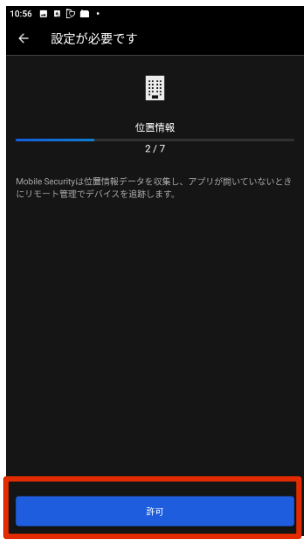
Android

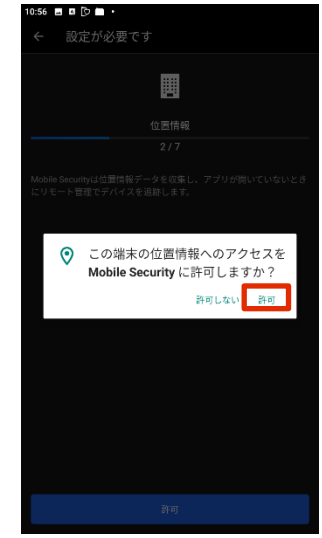
管理者作業 利用者作業

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。



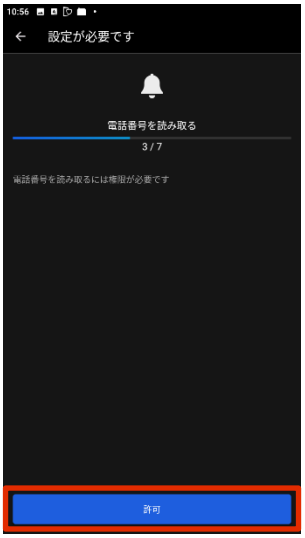


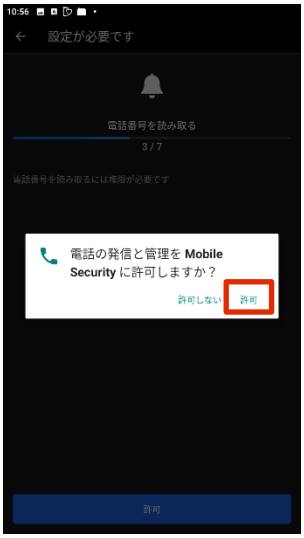
エージェントのインストール

Android

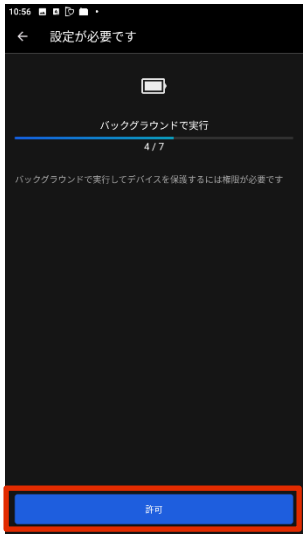
管理者作業 利用者作業

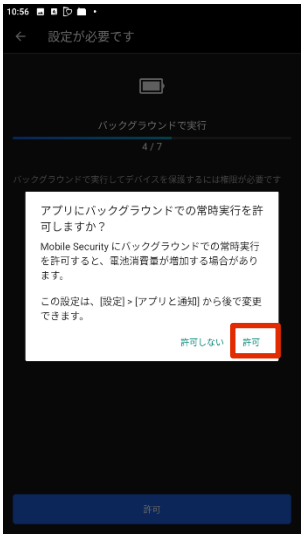
9.電話の発信と管理を許可します。





10.バックグラウンドでの実行を許可します。



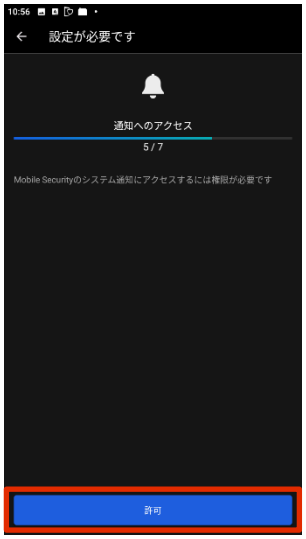


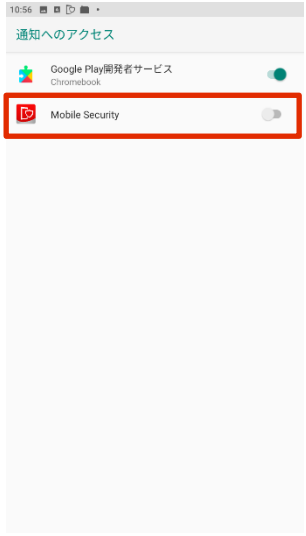
エージェントのインストール

Android

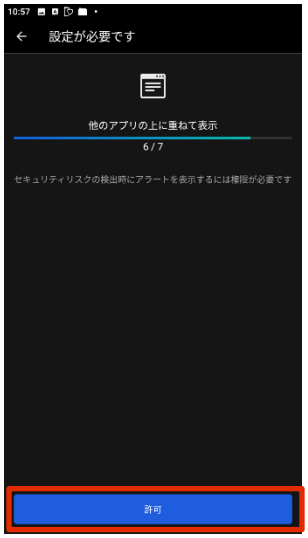
管理者作業 利用者作業

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。

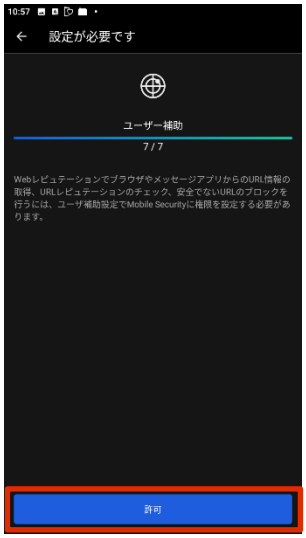


エージェントのインストール

Android

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。

エージェントのインストール

Android

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。

エージェントツールのインストール

iPadOS iOS

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。

エージェントツールのインストール

iPadOS　iOS

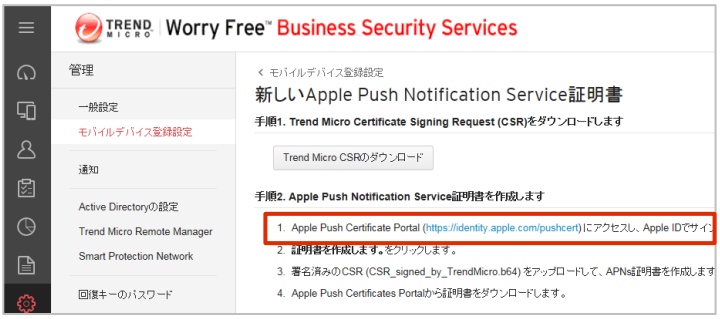
管理者作業　利用者作業

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。）



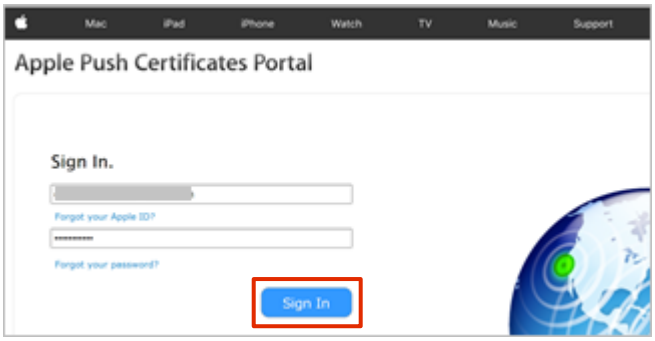
Apple Push Certificate Portal
https://identity.apple.com/pushcert/

エージェントツールのインストール

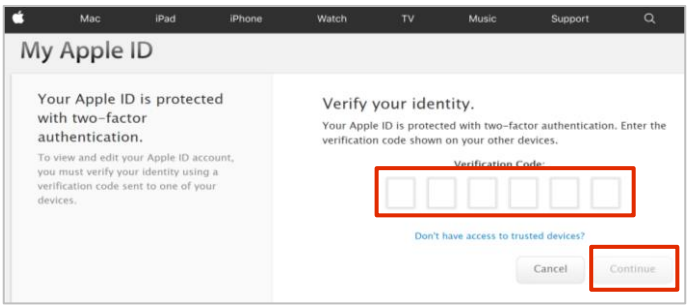
iPadOS　iOS

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。

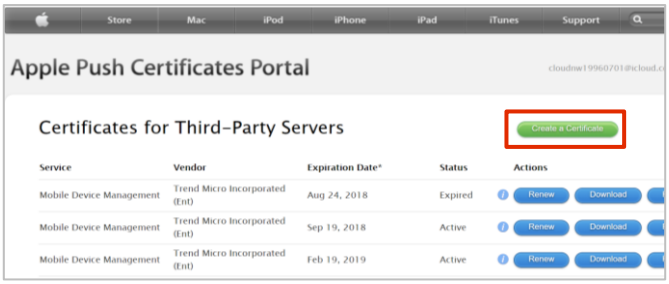
※確認コードの取得方法はOSのバージョンおよび利用状況によって異なります。詳しくは下記をご確認ください。
https://support.apple.com/ja-jp/HT204974

エージェントツールのインストール

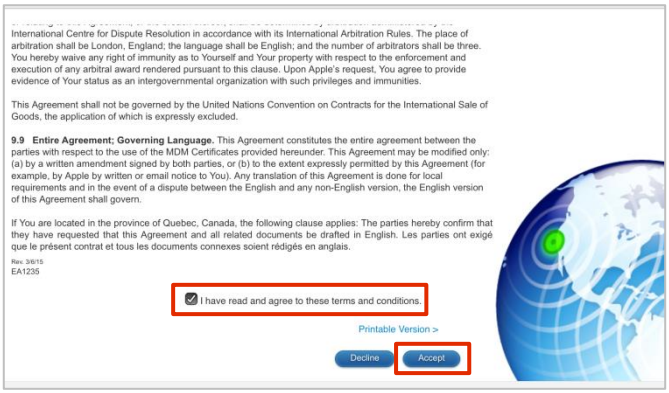
iPadOS iOS

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。



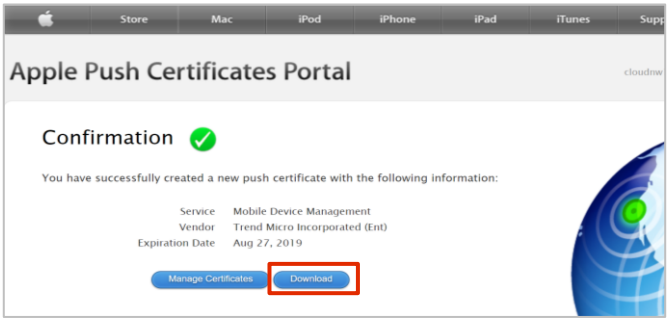
8．「Create a New Push Certificate」画面が表示されます。[ファイルを選択]をクリックし、3でダウンロードしたCSRファイルを選択し、[Upload]ボタンをクリックします。

エージェントツールのインストール

iPadOS　iOS

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。

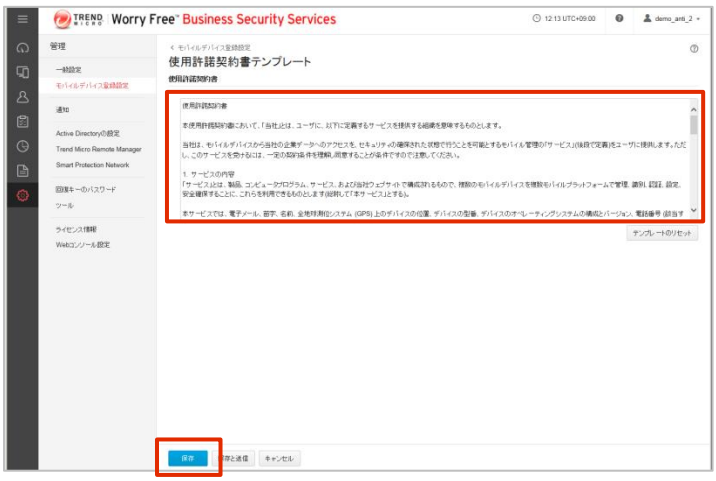
エージェントツールのインストール

iPadOS　iOS

管理者作業　利用者作業

１２．「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。

１３．編集が完了したら[保存]をクリックします。



１４．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。)

エージェントツールのインストール

iPadOS　iOS

管理者作業　利用者作業

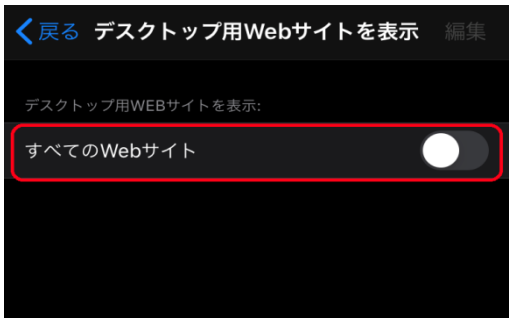
iOS および iPadOSでは、初期設定でSafariの「デスクトップ用Webサイト」が有効になっています。

※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。

エージェントツールのインストール

iPadOS　iOS

管理者作業　利用者作業

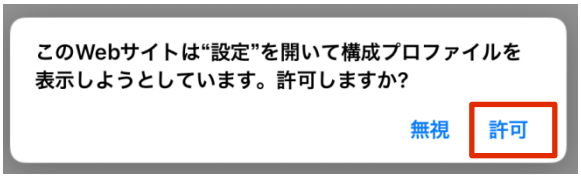
4. iOSデバイスでブラウザを開き、管理者から周知されたインストール用のリンクを入力します。

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。

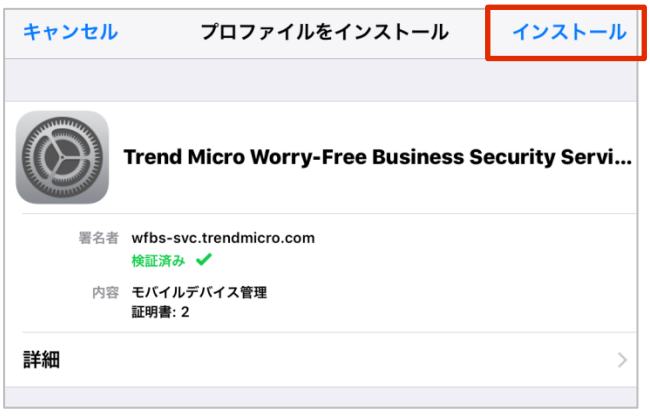
6. 使用許諾契約書が表示されます。確認の上、[同意する]をタップします。

7. [続行]をタップします。

8. [許可]をタップします。



9. 「プロファイルをインストール」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。



エージェントツールのインストール

iPadOS　iOS

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。

エージェントツールのインストール

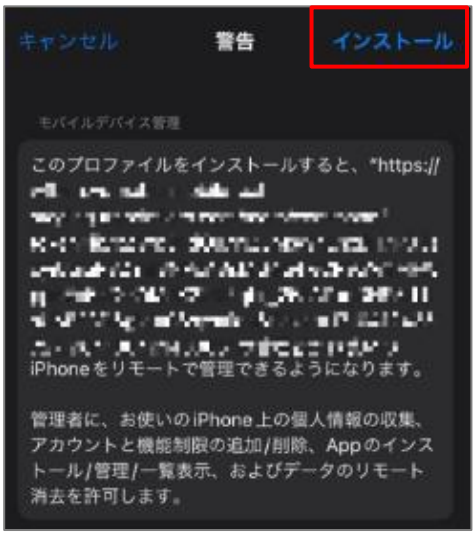
iPadOS iOS

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。



エージェントツールのインストール

iPadOS　iOS

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。

エージェントツールのインストール

iPadOS iOS

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。

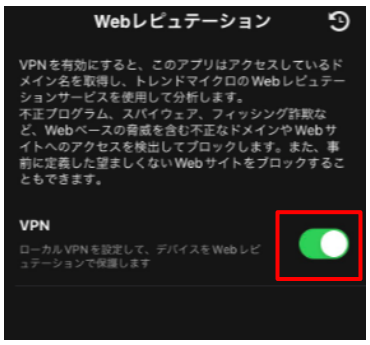
エージェントツールのインストール

iPadOS　iOS

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。



エージェントツールのインストール

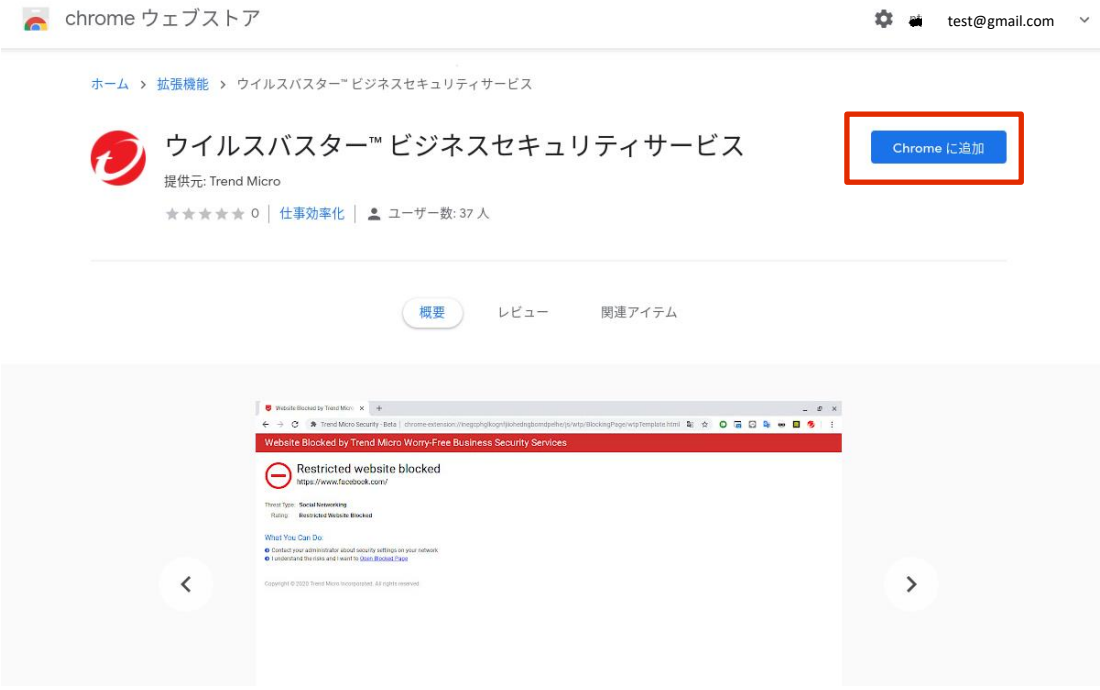
Chromebook

管理者作業 利用者作業

1．Chromebook上で、インストーラリンクをクリック

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

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。

エージェントツールのインストール

Chromebook

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

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 》

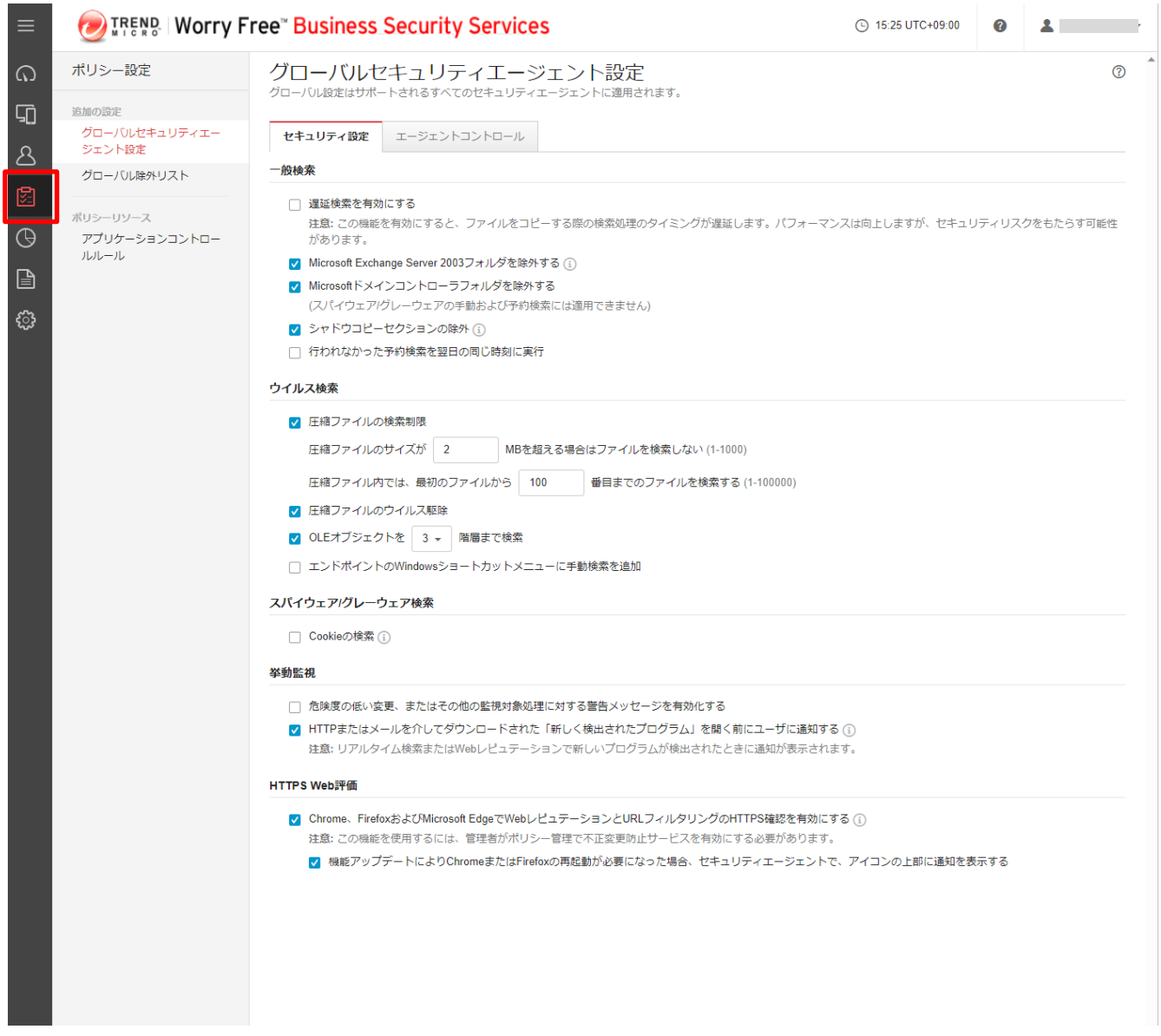
①「セキュリティエージェント」タブを押下します。
②「手動グループ」が表示されるため、設定したいグループを選択します。
※「すべてのセキュリティエージェント」には全端末情報が一覧で表示されます。
グループとは異なりますのでご注意ください。
③「ポリシーの設定」を押下します。
④設定するOSを選択します。

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。



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。

「保存」を押して終了です。

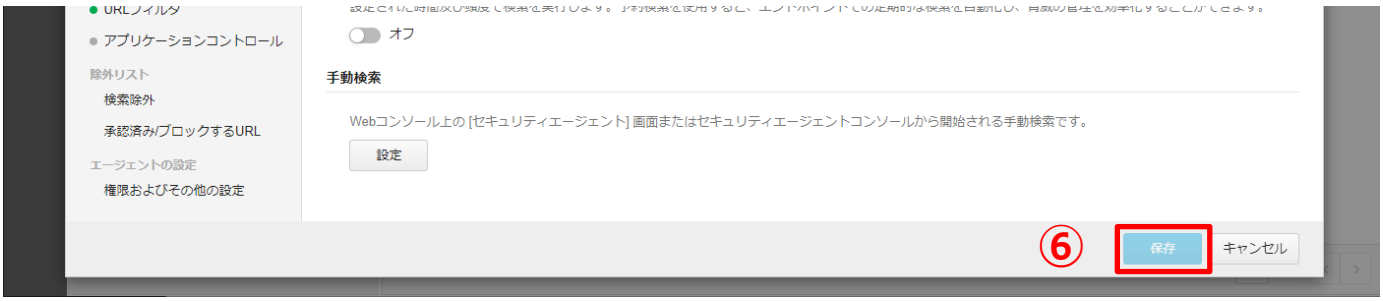
スマートスキャンとは：エージェントでは、脅威の特定に独自の検索エンジンが使用されますが、ローカルパターンファイルのみを使用するのではなく、クラウド上にあるスキャンサーバに格納されているパターンファイルを主に利用する方法

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。

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。



「保存」を押して終了です。

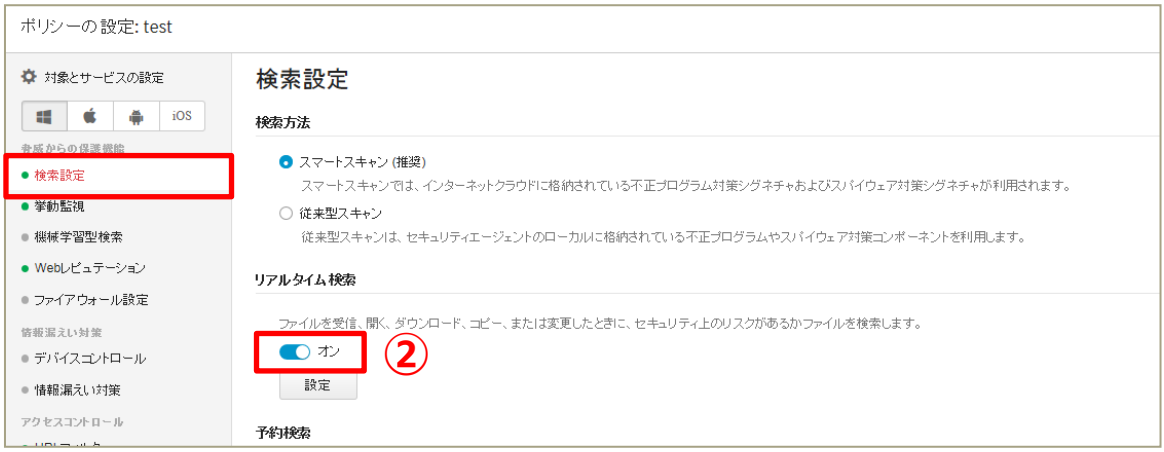
機能を設定する（グループ：検索設定-ファイルレス攻撃対応）

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

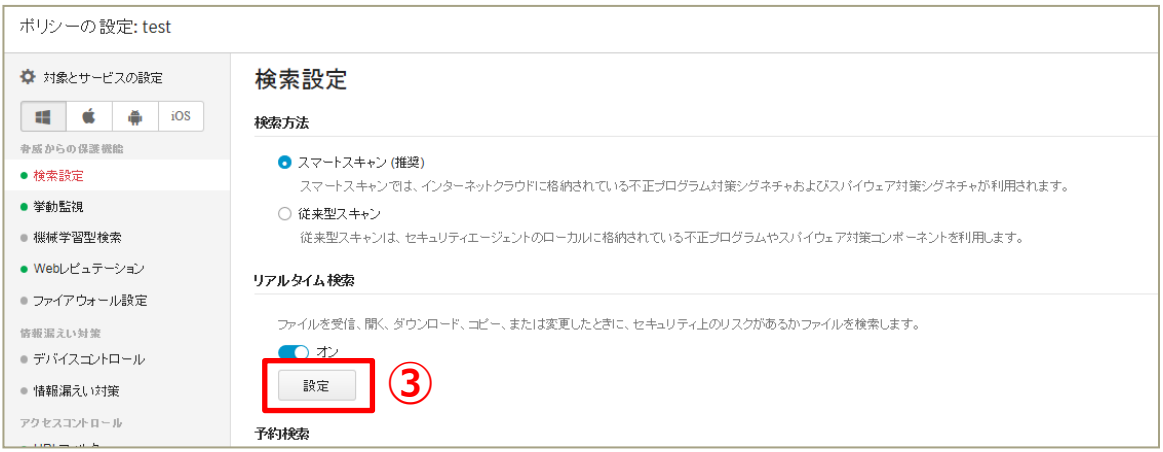
《 項目１ 》 ※項目番号は上記表を参照



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 》



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 》

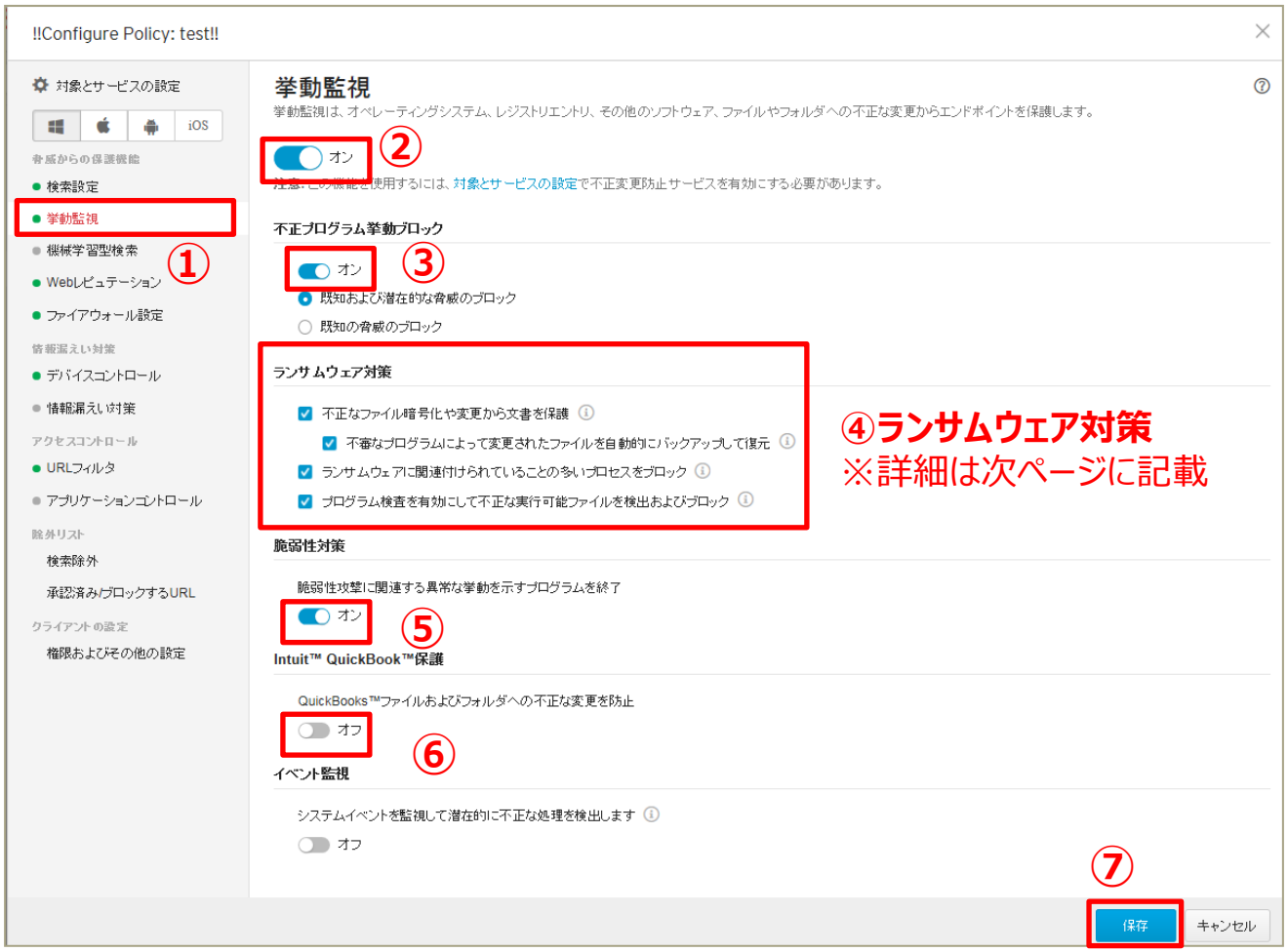
《 項目５ 》

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：挙動監視）

挙動監視機能を有効にします。

プログラムやOS、レジスト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。

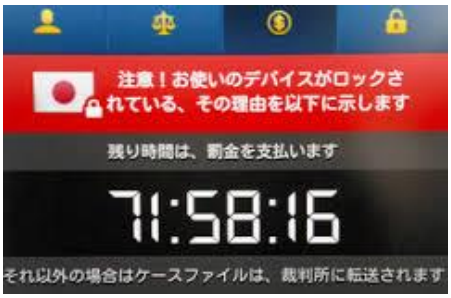


「保存」を押して終了です。

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）

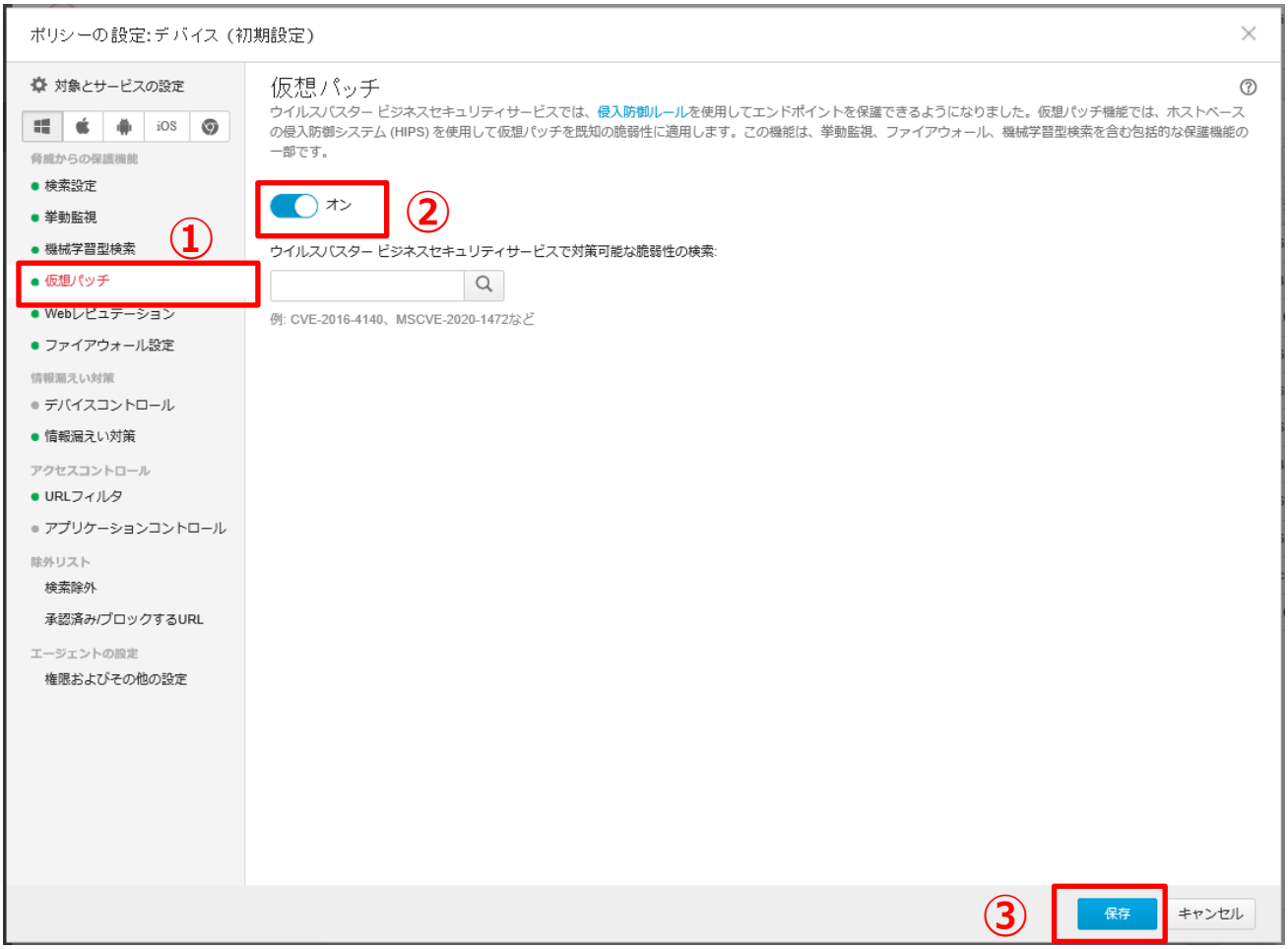
機械学習型検索を設定します。
→未知の脅威でも、不振な挙動から脅威を判別します。
※ここでは、未知の脅威を隔離・終了する設定を行います。

「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。

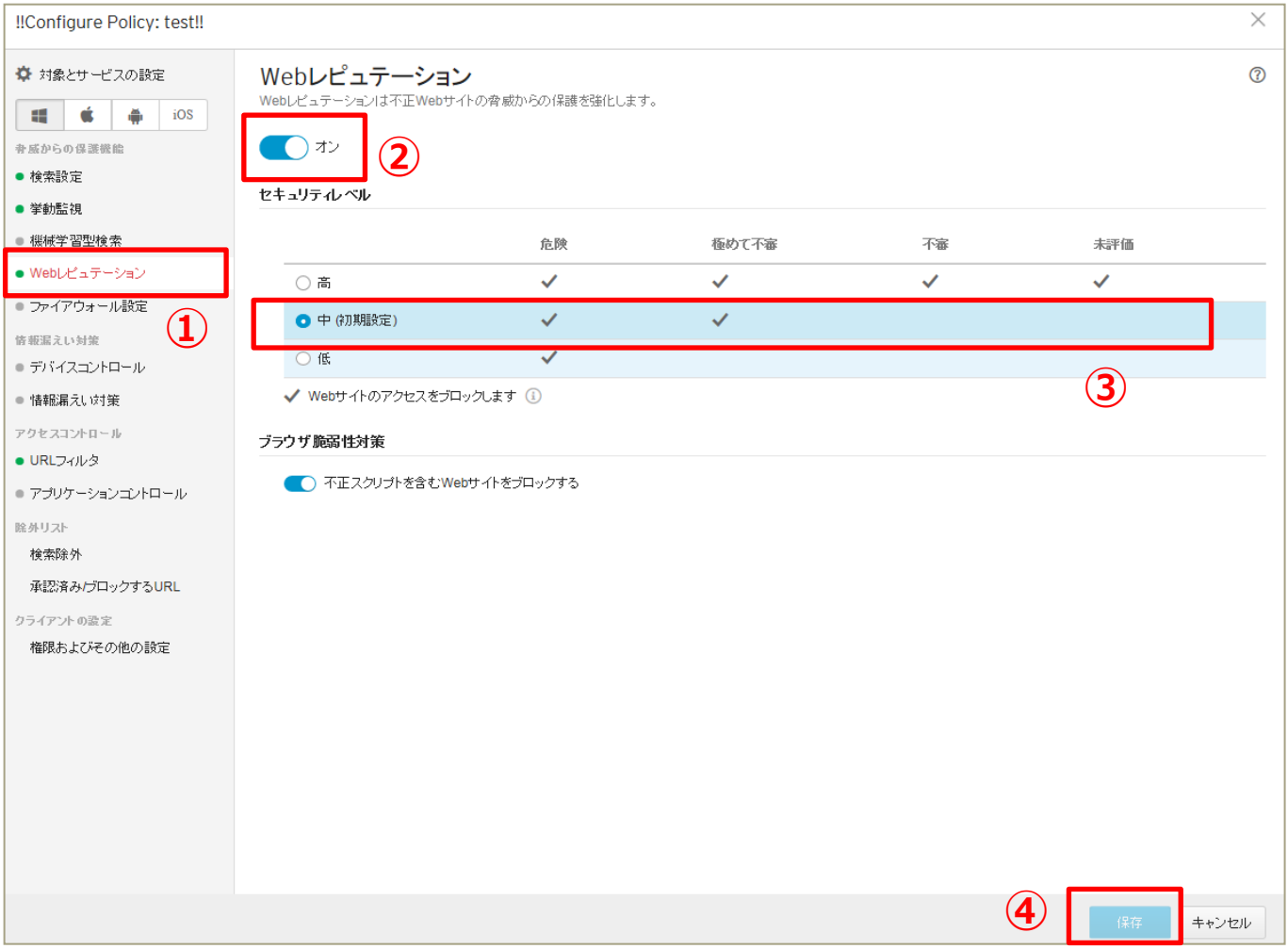


「保存」を押して終了です。

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。

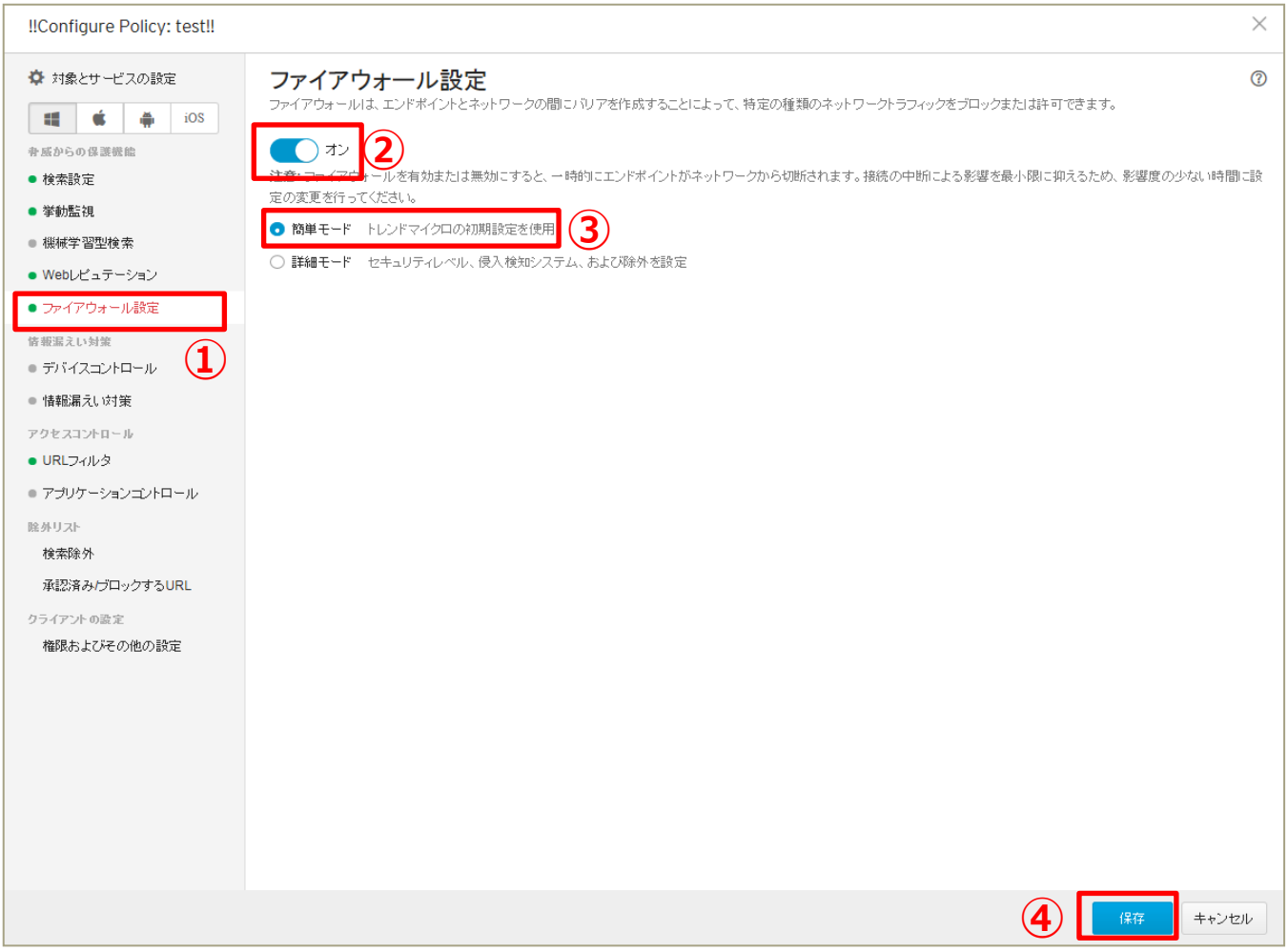


「保存」を押して終了です。

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。



「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。

「保存」を押して終了です。

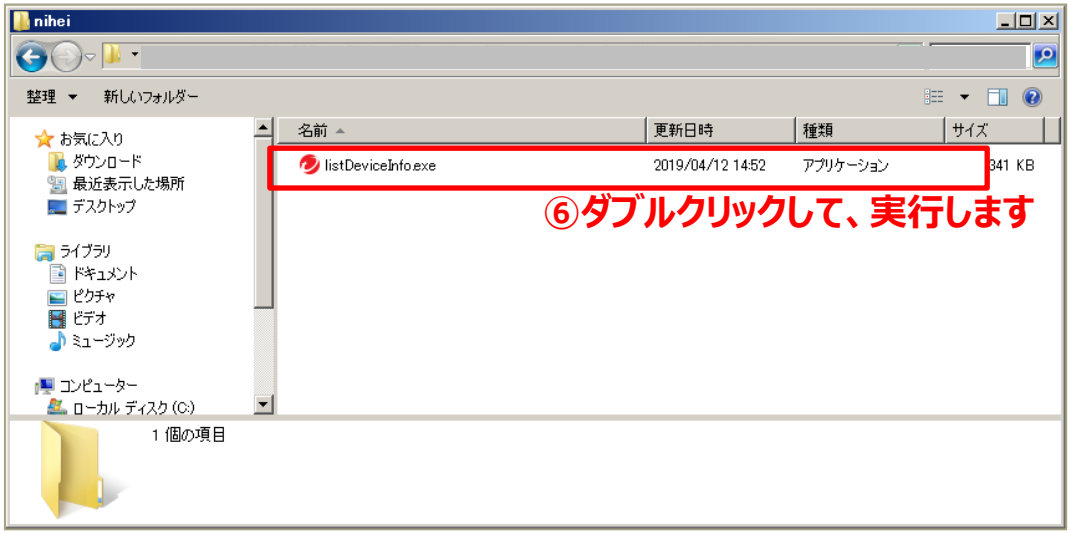
機能を設定する（全端末：デバイスコントロール）

《 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。

機能を設定する（全端末：デバイスコントロール）

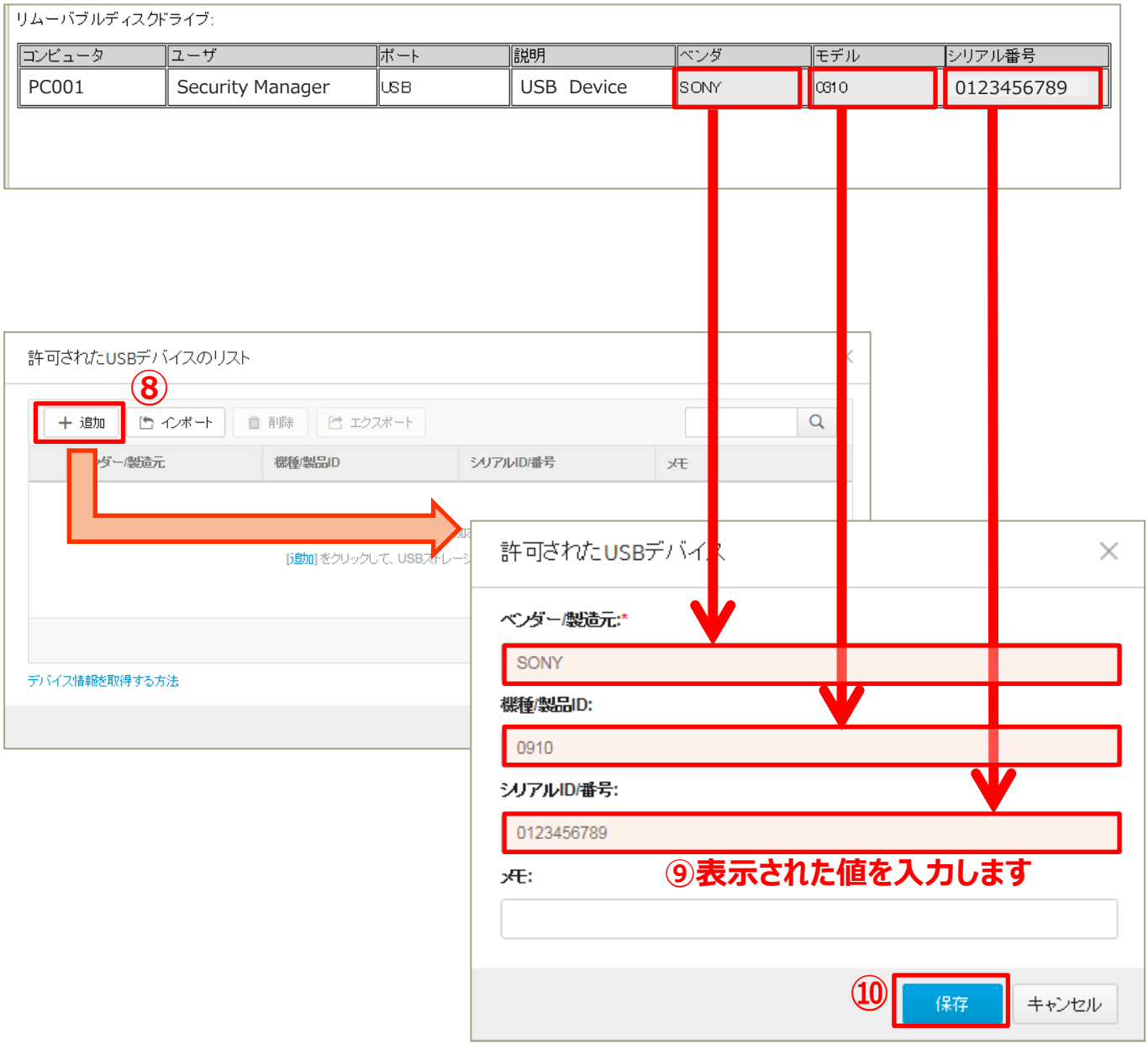
⑤「名前をつけて保存」をクリックし、任意のフォルダに保存します



⑥ダブルクリックして、実行します

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

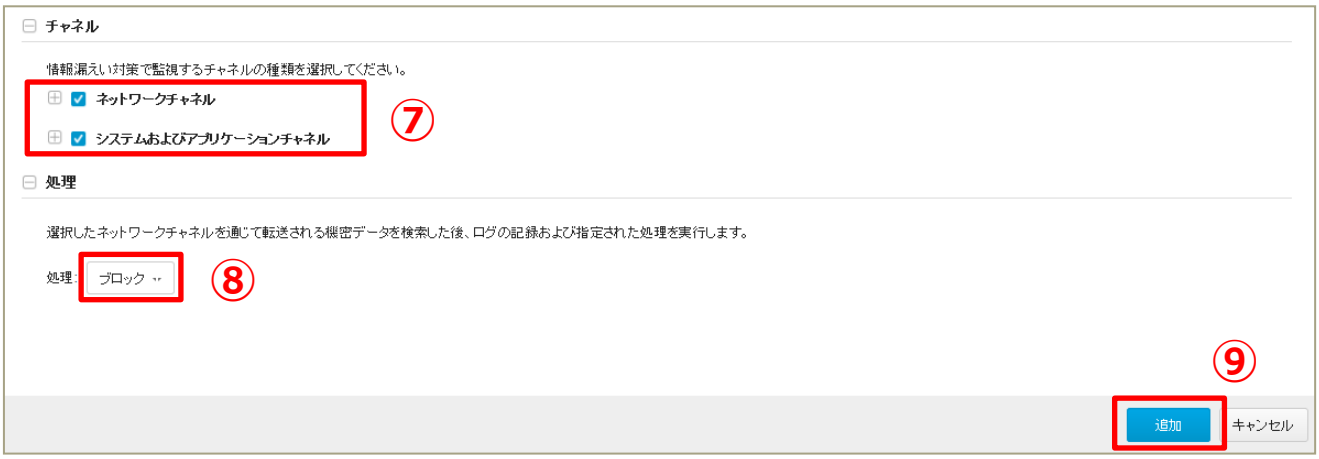


「保存」を押して終了です。

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。

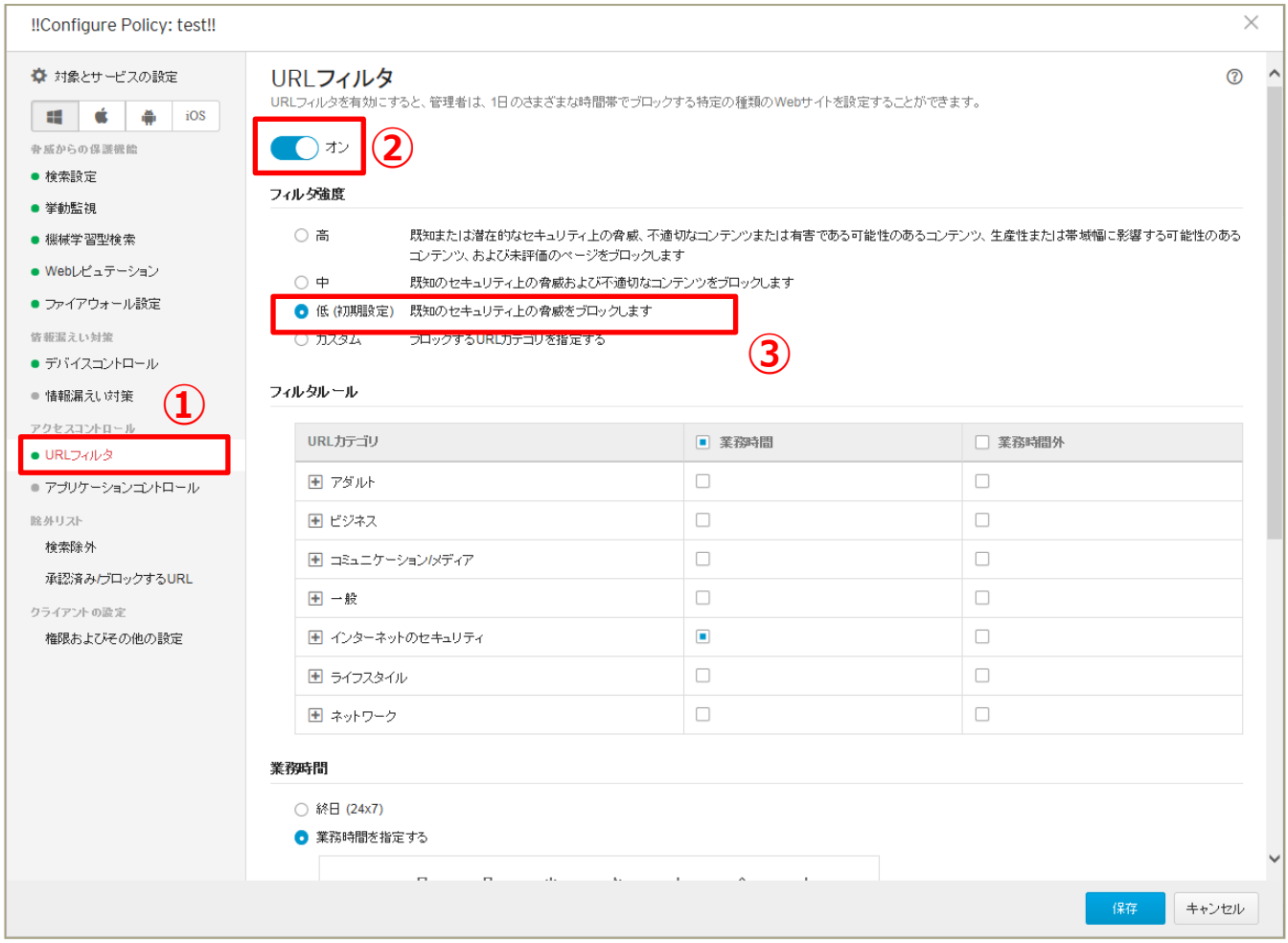
機能を設定する（グループ：情報漏えい対策）



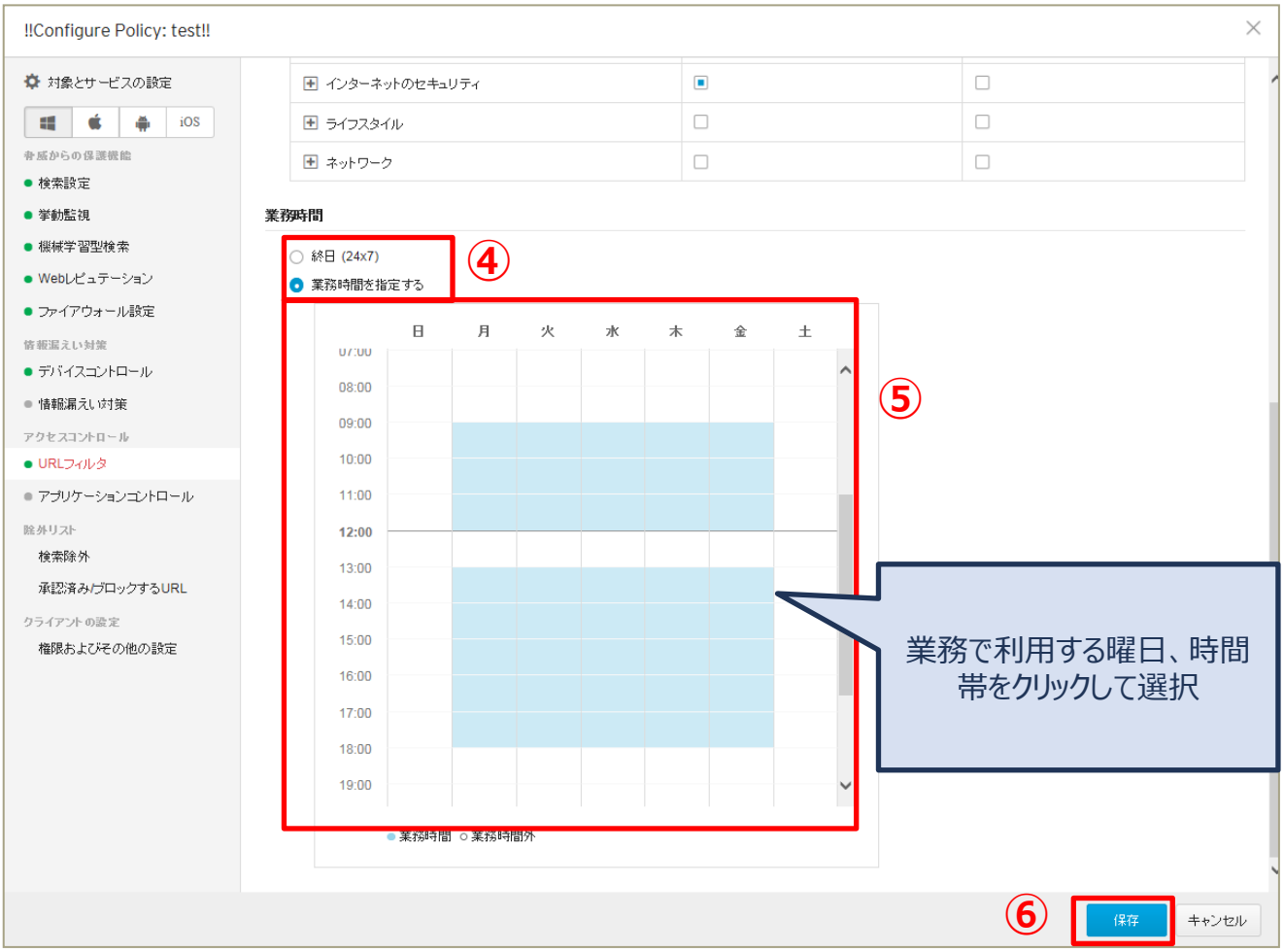
「保存」を押して終了です。

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。



機能を設定する（グループ：URLフィルタ）



「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）

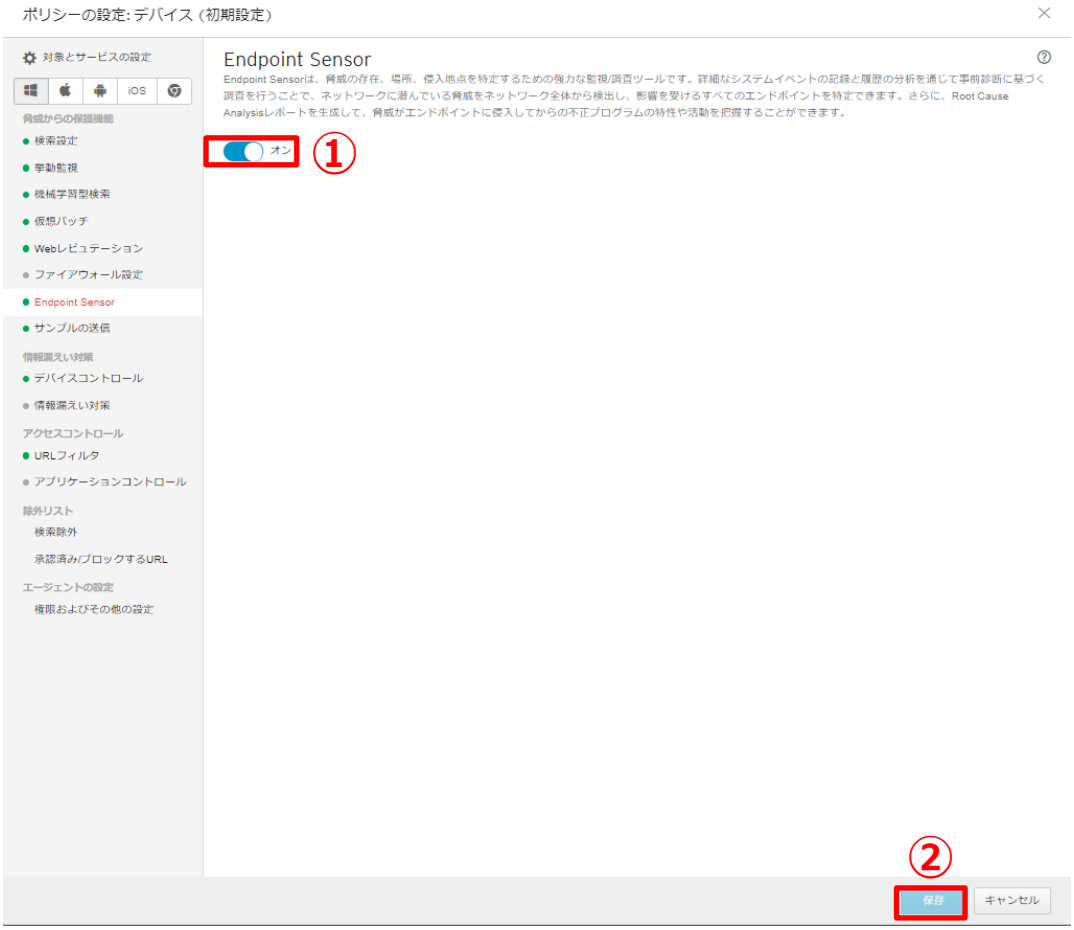
アプリケーションコントロール機能を有効にします。
→指定したアプリケーションの利用を制限します。
※ここでは簡易モードで設定をしています。

「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



「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）

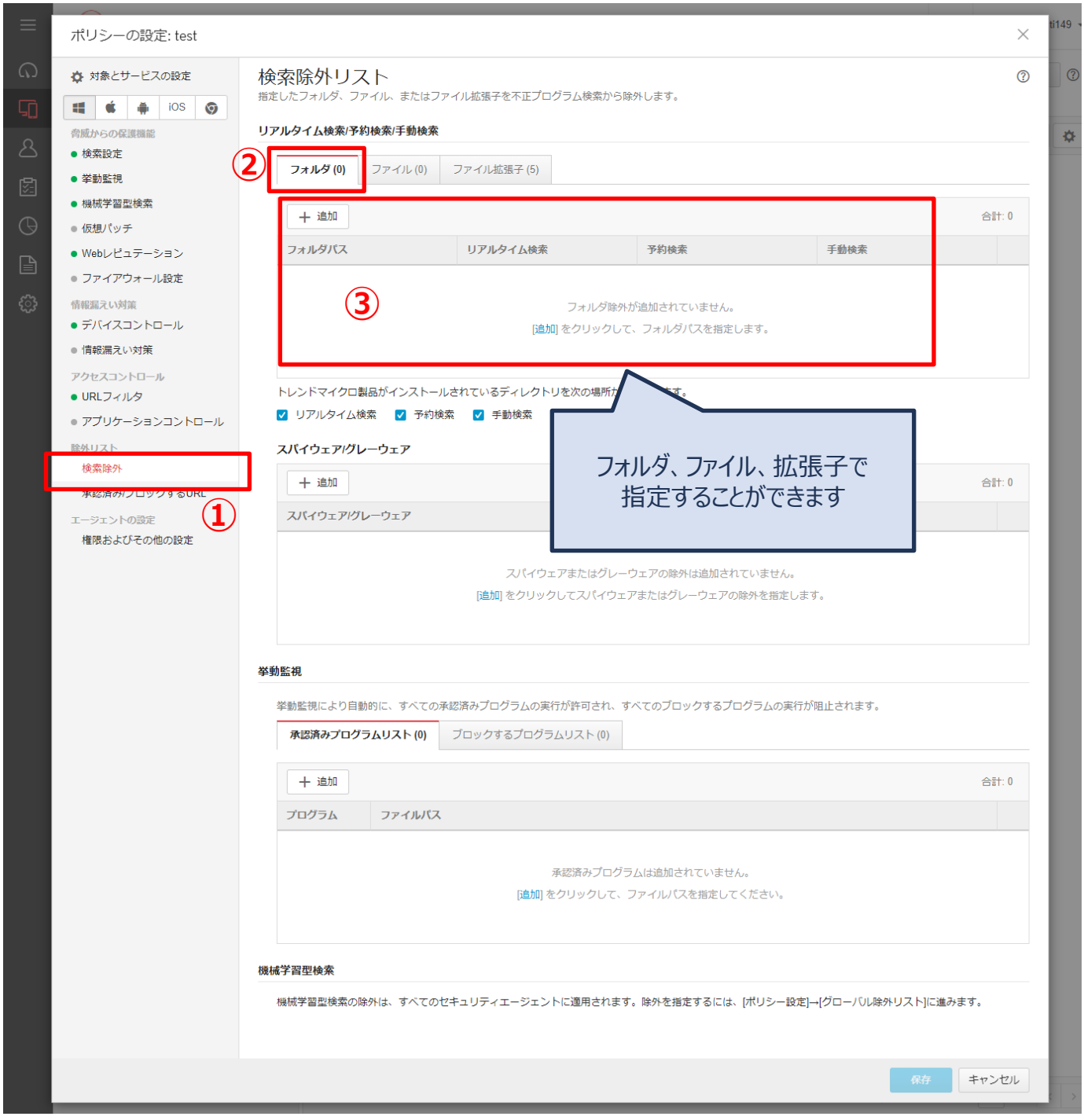
端末のロックを解除する際に、パスワードの入力を要求します。
※ここではAndroidの中レベルの設定をしています。

「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）

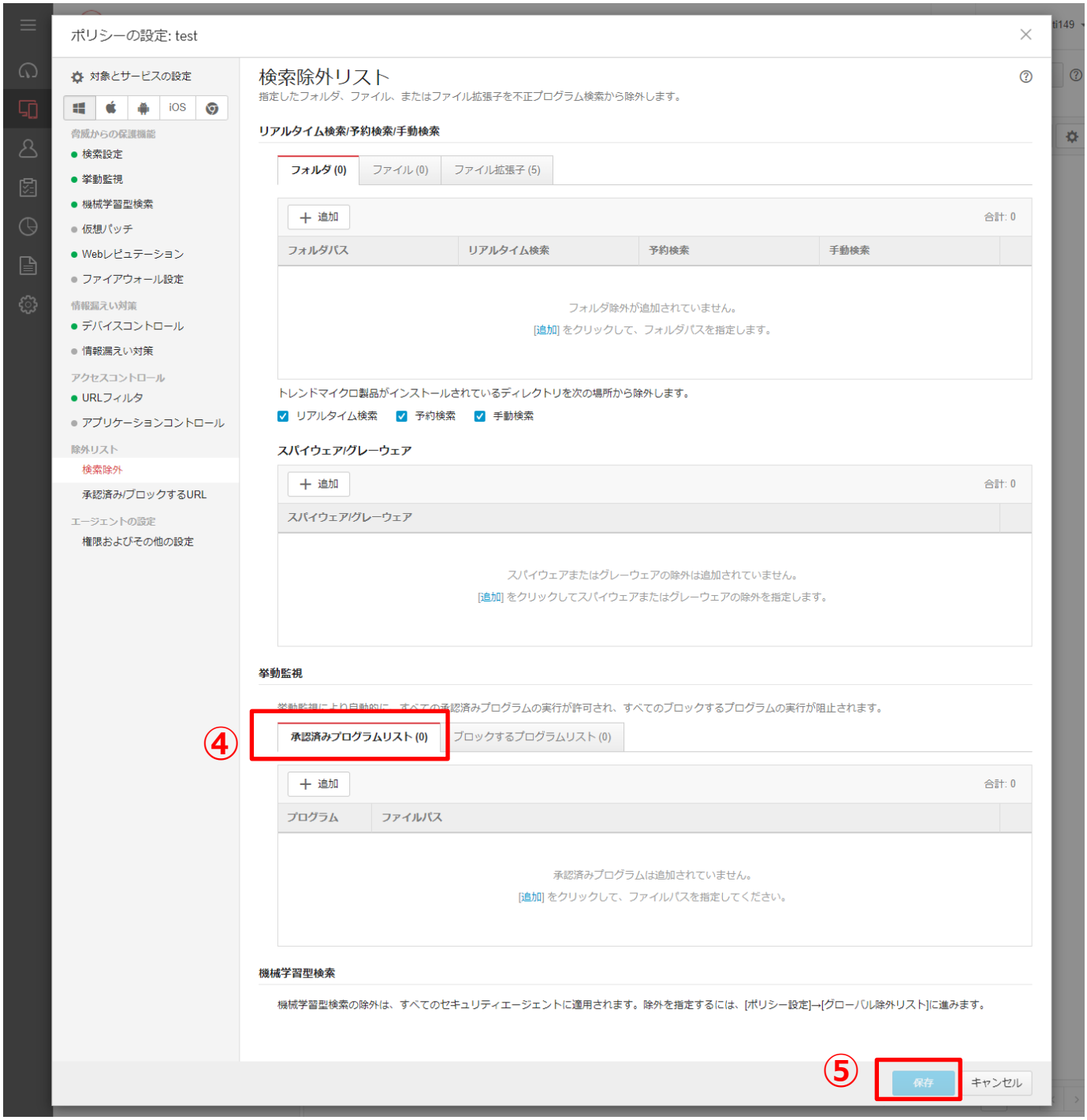
指定したフォルダ、ファイル、またはファイル拡張子を不正プログラム検索から除外します。

《 リアルタイム検索/予約検索/手動検索から除外する場合 》



機能を設定する（グループ：除外設定）

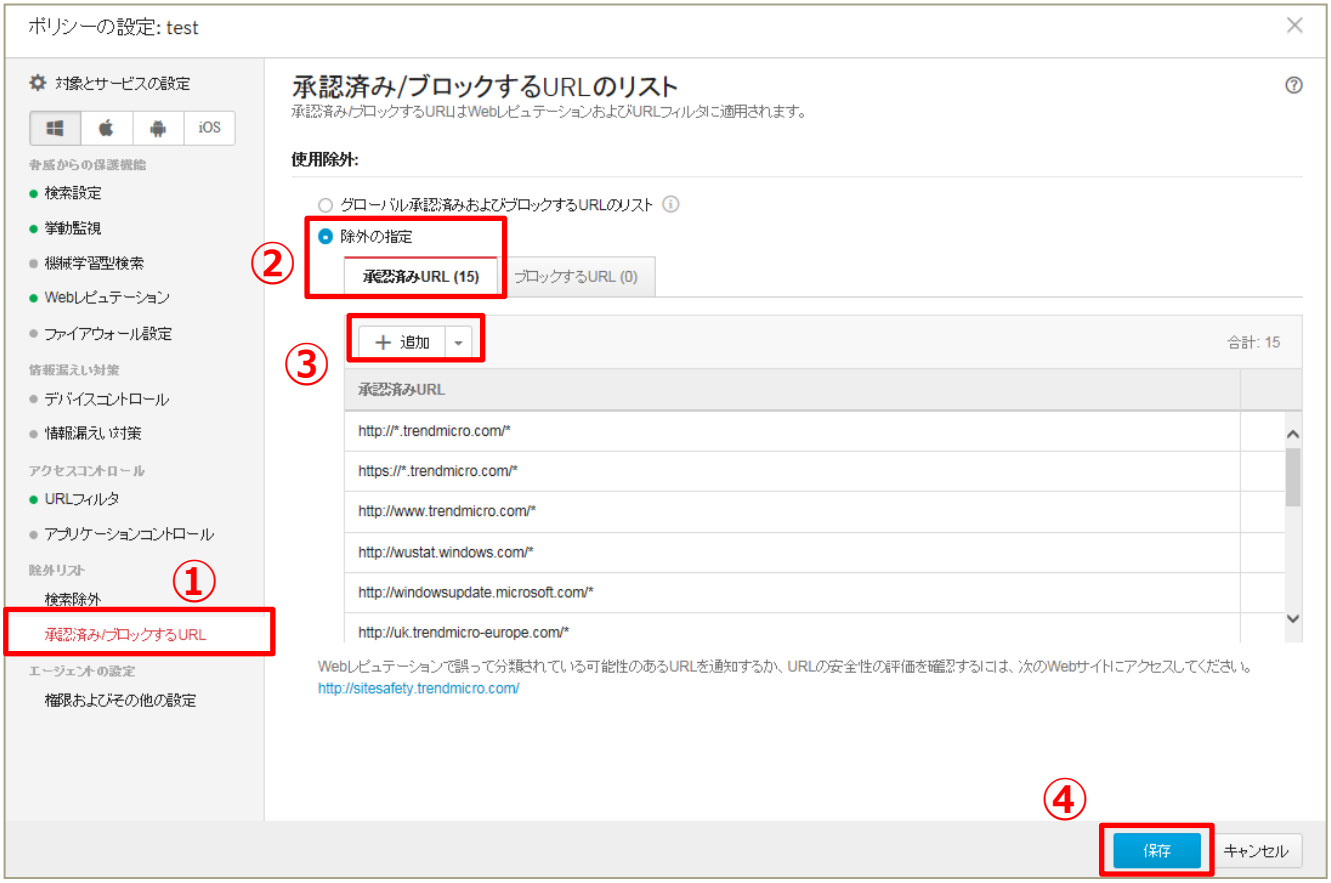
《 挙動監視から除外する場合 》



「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。



「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。

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。

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。

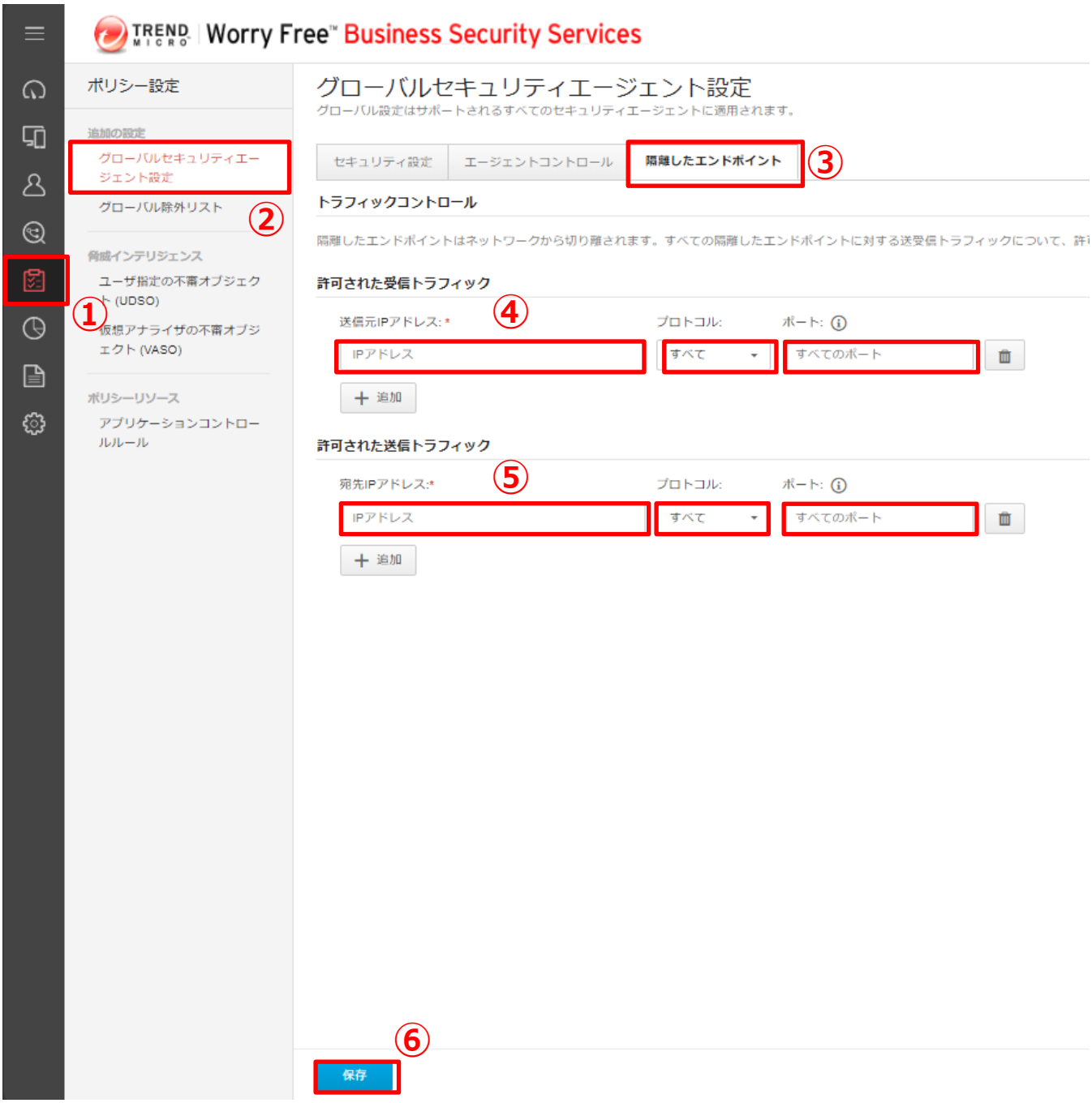
- ウイルス/不正プログラム対策
- Webレピュテーション
- 挙動監視
- 機械学習型検索

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



「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

「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

「保存」を押して終了です。

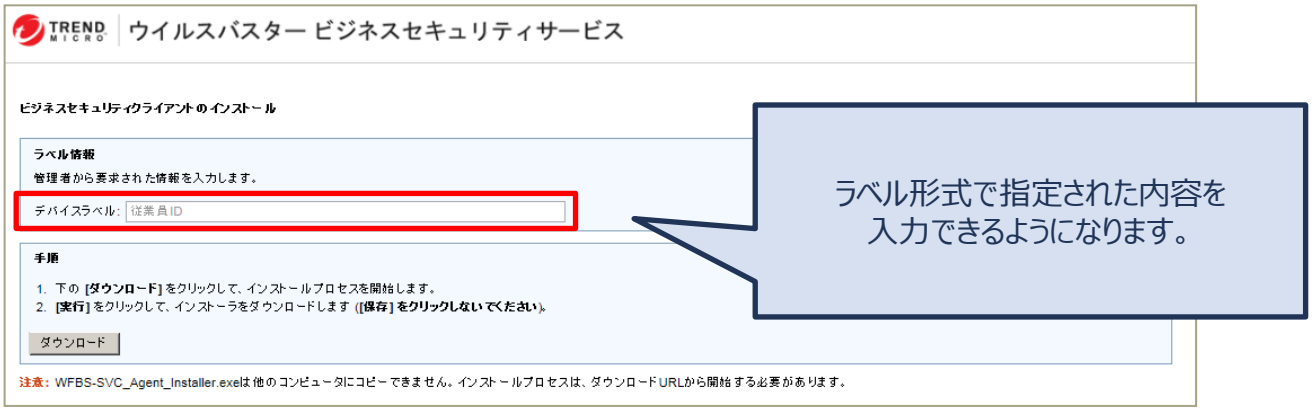
機能を設定する（管理：ラベル表示）

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。

「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。

「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

●iPadOS/iOSを選択した場合

※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(※)

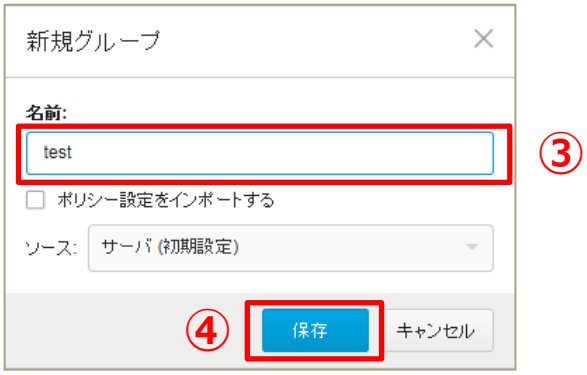
機能を設定する（全端末：除外設定）

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。

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）

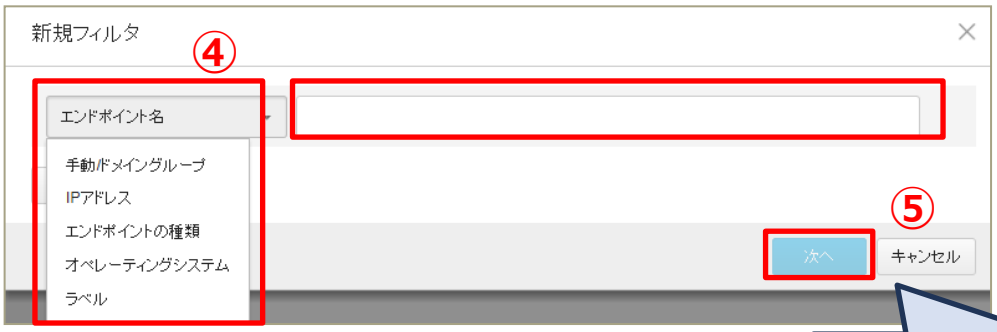
ライセンス数が多い場合など、グループを作成し管理を容易にすることができます。
※ここでは[test]グループを追加しています。



「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。



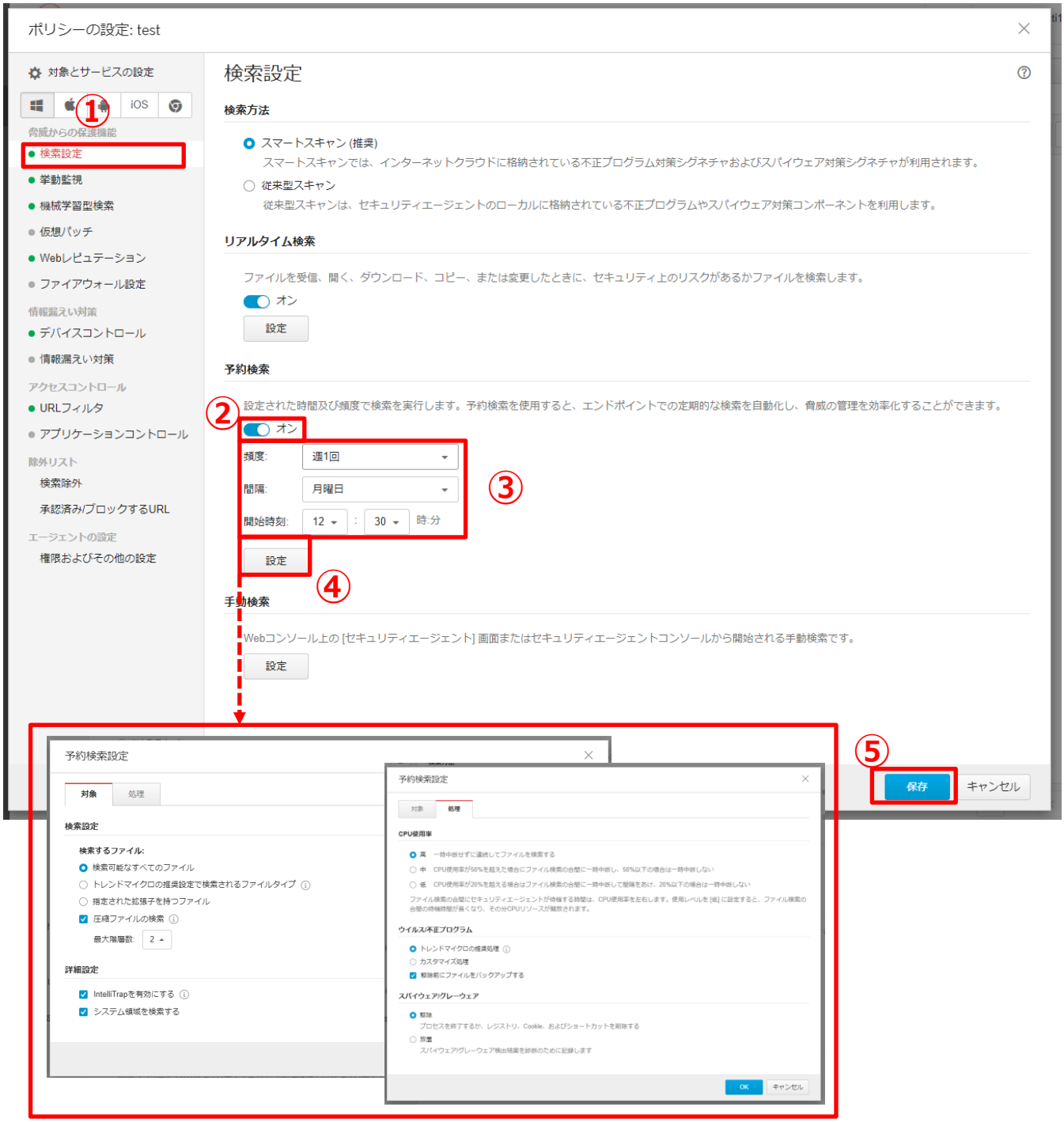
フィルタの条件を指定（AND条件）

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。



「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。

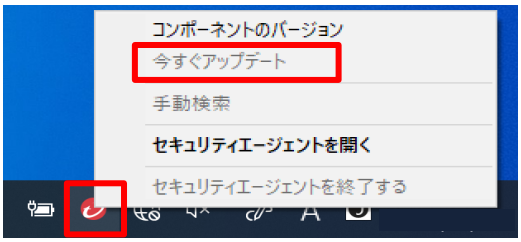
「アップデート」を押して終了です。

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）

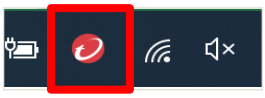
方法(2)：エージェントから手動でアップデートする

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