セキュリティおまかせプラン
エンドポイントセキュリティ・EDRセキュリティ
ご利用マニュアル
（Ver 2.0）

2024年　6月

西日本電信電話株式会社

改定履歴

No	Date	主な変更内容	Ver
1	2017/12/01	初版	1.0
2	2018/08/30	VBBSSのVer6.5へのバージョンアップによるUI変更箇所の画面イメージの修正	1.1
3	2019/06/14	インストール（ダウンロード用URLの確認）について変更	1.2
4	2022/11/14	10.（参考）チャット連携会社名取得方法を追加	1.3
5	2023/05/11	現行表記と画面イメージの修正	1.4
6	2023/07/27	インストール（Android）手順を変更	1.5
7	2023/09/29	Android VBBSS 旧エージェントから新エージェントへの移行手順を追加	1.6
8	2023/10/20	レポート通知メールの仕様変更、管理コンソールログイン時のPWリセット手順の追加	1.7
9	2024/04/23	iOSの新エージェントリリースのためインストール(iOS)手順を変更	1.8
10	2024/06/03	Mac対応のため手順追加・EDRセキュリティページについて追加	2.0

目次

目次

エンドポイントセキュリティ ・・・エンドポイントセキュリティ対象説明

EDRセキュリティ ・・・EDRセキュリティ対象説明

エンドポイント/EDRセキュリティ ・・・エンドポイントセキュリティ・EDRセキュリティ共通説明

1.エンドポイントセキュリティ概要

○ ウイルス対策機能だけでなく、企業用に特化したさまざまな管理機能を加えた総合的なエンドポイントセキュリティソフトです
○ AIの機械学習型検索を利用した高度なウイルス検知機能により、亜種のウイルスにも対応します
○ 管理サーバを通じてセキュリティサポートセンタと接続されており、設定変更や異常検知にも遠隔で対応可能です。

正しく利用しているだけで

中小企業・中堅企業で求められるレベルのセキュリティが備わる

スパイウェア対策
アドウェアやCookie、グレーウェアを含むスパイウェアの検知や、起動中のスパイウェアの検出・削除が可能です。

ウイルス対策
ウイルス対策・スパイウェア対策として、ファイルレピュテーション技術を用いた「スマートスキャン」機能を搭載。

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ているWebサイトなど、危険なWebサイトへのアクセスを未然にブロックします。

USBデバイス対策
デバイスコントロール機能を通して、USBなどの外部デバイスを介して広がるセキュリティ上の脅威をブロックします。

URLフィルタリング
業務上必要の無いWebサイトへのアクセス制御を行います。ルールを設定することで、お客さまのビジネス環境に応じて柔軟に規制対象のコンテンツを設定できます。

Mac OS対応
Windowsだけでなく、Mac OS向けアンチウイルスとWebレピュテーションを提供。単一のコンソールからWin,Mac両方の管理が可能に。

モバイルデバイス管理（MDM)機能
スマートフォン、タブレットといったモバイルに特有の脅威から守ります。AndroidとiOS向けのモバイルデバイス管理機能を搭載しています。

ランサムウェア対策（身代金要求型ウイルス）
国内でも感染例が増えているランサムウェア対策も可能。ランサムウェアの検出状況を可視化し、暗号化されたファイルの自動復旧機能も搭載しています。

- フィッシング詐欺対策
- POP3メール検索
- 脆弱性診断
- 大規模感染防止
- Webによるクライアント管理
- エージェントアンインストール／アンロード防止パスワード設定
- ワンタイムレポート
- メールでの自動通知
- 不正侵入防止
- 挙動監視
- スマートスキャン
- Webインストール
- グループごとのセキュリティ設定
- ダッシュボードによる脅威／管理情報のサマリー表示
- 日、週、月ごとのスケジュールレポート

機械学習による高度なウイルス対策

ＡＩが機械学習で亜種のウイルス等の新たな脅威を検知し、隔離駆除を試みます。

USB利用規制等の簡易MDM機能搭載

USB利用規制やリモートロック機能等の簡易ＭＤＭ機能がパッケージ化されています。

メンテナンスフリー

バージョンのアップデートは全てクラウド上で管理されており、インターネットに接続されていれば常に最新の状態が維持できます。

マルチデバイス対応

Windows OSだけでなく、Mac OSやiOS、Android OSでも利用できます。
※利用可能な機能はOSによって異なります。

2.エンドポイントセキュリティ　機能一覧　1/2

エンドポイントセキュリティで主に提供される機能として、「セキュリティ対策機能」「簡易ＭＤＭ機能」がご利用可能です。
提供機能はご利用端末のＯＳによって異なります。

		Windows	Mac	Android	iOS
セキュリティ対策	ウイルス対策	○	○	○	
		ウイルスの侵入を検知し、ブロック、隔離、削除を行います。 また、スマートスキャンを利用することで、最新のウイルスにいち 早く対応できます。			
	Webレピュテーション	○	○	○	○
		毎日リアルタイムで監視・更新されているトレンドマイクロの不正 Webサイトの評価データベース情報を基に、フィッシング詐欺やウ イルスが仕込まれているWebサイトなど、危険なWebサイトへの アクセスを未然にブロックします。			
	ファイアウォール	○			
		クライアントとネットワークの間に障壁を作り、特定の種類のネッ トワークトラフィックを拒否または許可できます。また、クライアントに対する攻撃が疑われるネットワークパケットのパターンを特 定できます。			
	挙動監視	○			
		OS、レジストリ、ソフトウェアに対する不正変更を監視・ブロックします。			
	ＰＯＰ３メール検索	○			
		POP3メールメッセージとその添付ファ イルを介して脅威が広まらないようにコンピュータをリアルタイムに保護できます。			
	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制御を行います。全体ま たはグループ単位でフィルタの強度、ルール、時間帯等を設定する ことで、お客さまのビジネス環境に応じて柔軟に規制対象のWebサ イトを設定できます			

2.エンドポイントセキュリティ　機能一覧　2/2

エンドポイントセキュリティで主に提供される機能として、「セキュリティ対策機能」「簡易ＭＤＭ機能」がご利用可能です。
提供機能はご利用端末のＯＳによって異なります。

		Windows	Mac	Android	iOS
セキュリティ対策	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。			
	機械学習型検索	○			
		AI(人工知能)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します。			
簡易MDM	ＵＳＢデバイスコントロール	○			
		USBストレージへのアクセス権限を適切に設定し、情報漏えいやウイルス感染を予防します。			
	リモートロック リモートワイプ			○	○
		端末の紛失時等に、遠隔で端末のロックや、ワイプ（初期化）が可能です。			

※対応ＯＳ等システム要件は以下ＵＲＬにてご確認いただきますよう、お願いいたします。
https://www.trendmicro.com/ja_jp/small-business/worry-free-services.html

3. EDRセキュリティ概要

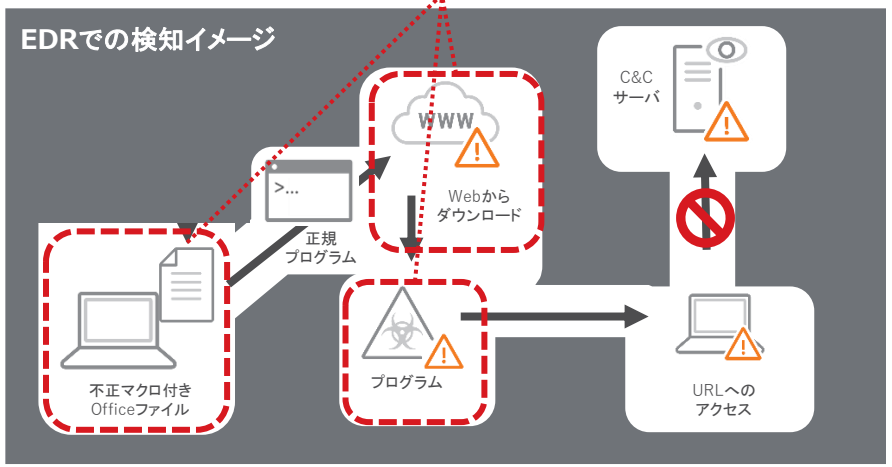
○ EDR（Endpoint Detection and Response）は、エンドポイント（クライアント端末、サーバなど）の操作や動作の監視を常時記録し、攻撃者による不正な挙動の兆候を検知します
○攻撃の全体像の可視化や、リモートによるエンドポイントの隔離機能などを提供することで、インシデントの根本原因の効率的な調査と迅速な対応を支援します

○EDRとは侵入してしまった脅威を「検知」し「対応」を支援する製品です。

○端末内の動作を記録することにより、一連の動作から不審な動きを迅速に検知することができます。

○検知した不審な動きに対し、端末の論理隔離などによる被害の最小化、また詳細な調査を実施することにより不審なファイル/URLの特定や、攻撃の経路、影響範囲などをインシデントレポートから可視化することができます。

EDRが可視化した攻撃の経路と不審なファイル/URL



セキュリティ

エンドポイントセキュリティ

脅威に対する
検知・処理を行う**事前対策**を
目的とした機能

＋

EDR

侵入した未知
の脅威の特定と処理を行う
事後対策を目的とした機能

サポート

EDRを使って脅威に対する監視や対応を
スペシャリストがお客様に代わって行うマネージドサービス

4. EDRセキュリティ　機能一覧

EDRセキュリティ提供機能はご利用端末のＯＳによって異なります。

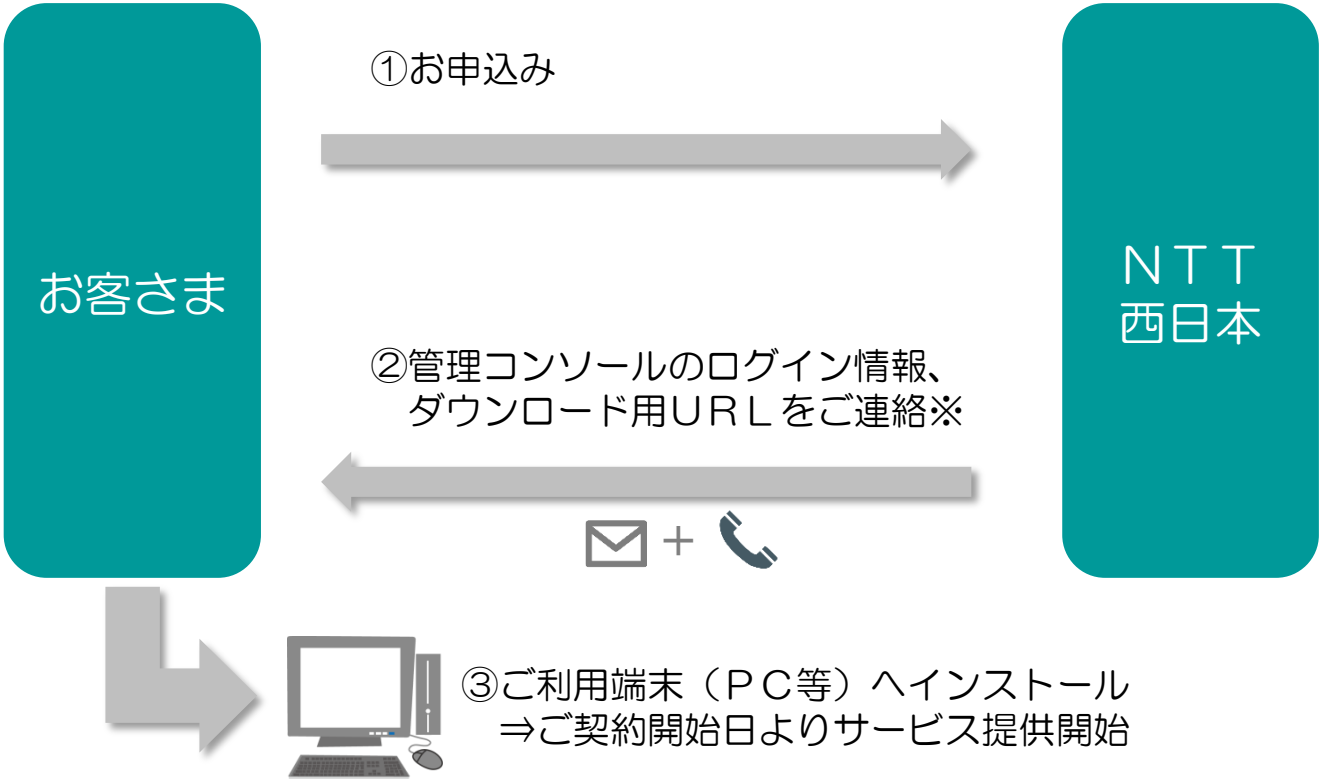
機能名		Windows	Mac OS	Android	iOS
セキュリティ対策	Webレピュテーション	○	○		
	機械学習型検索	○	○		
	挙動監視	○			
	仮想アナライザ	○	○		
	注意が必要なイベント通知	○	○		
	Endpoint Sensor	○	○		
	仮想パッチ	○			
	ファイアウォール	○			
	デバイスコントロール	○	○		
	情報漏えい対策	○			
	URLフィルタ	○	○		
	アプリケーションコントロール	○			
その他機能	レポート機能	○	○		
	モバイルデバイス制御機能				

EDRセキュリティについて
利用端末に専用ソフトウェアをインストールする必要があります。
利用端末のOSやソフト等との相性によっては、正常に動作しない場合があります。
遠隔サポート対象には、OS等の提供条件があります。
セキュリティ機能は、OSごとに提供機能が異なります。
定義ファイルやプログラムは、「フレッツ光」等接続環境下でダウンロード・更新を行い、常に最新の状態にしていただく必要があります。

※2024年6月3日よりMac　OSのEDRセキュリティ機能が提供されております。

5.ご提供の流れ

お申込みいただいたご契約者様には、メールにて、管理コンソールへのログイン情報と、エンドポイントセキュリティ/EDRセキュリティのダウンロード用ＵＲＬをご連絡させていただきます。ご利用端末へのインストールが完了いたしますと、ご契約開始日よりサービスをご利用いただけます。



※メールによるご連絡は、ご提供開始の２～３日前までを目安にお送りさせていただきます。
　サービスがご利用いただけるのは、ご契約開始日からとなりますので、ご注意いただきますようお願いいたします。
※メール送付後、お電話にて到着確認をさせていただきます。

6. 事前準備

・ウイルス対策ソフトやMDMソフトが入っている場合、本サービスで提供するエンドポイントセキュリティソフト・EDRセキュリティの両方で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

＜Windows 7/10 の場合＞
「スタート」⇒「コントロールパネル」⇒「プログラムのアンインストール」

＜Windows 8/8.1 の場合＞
以下のいずれかの方法でアンインストールできます。
・メトロ画面のアプリ一覧から「コントロールパネル」 ⇒「プログラムのアンインストール」
・メトロ画面のアプリ一覧から削除したいアプリを右クリックして 「アンインストール」をクリックする

Windows 8.1 の場合は、デスクトップ画面にて、以下の手順でも可能です。
「スタートボタンを右クリック」⇒「コントロールパネル」 ⇒「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、対象のプログラムをクリックしてアンインストールを実施。

7.管理コンソールへのログイン方法　1/2

ご登録いただいております「管理者様アドレス」宛に、メールにて、ログインに必要なURL・アカウントID情報をお送りいたします。
まず、パスワード設定用のＵＲＬをクリックいただき、パスワードの設定をお願いいたします。

＜メール例＞

□件名 【セキュリティおまかせプラン】新規アカウント発行のお知らせ
□送信元アドレス no-reply.security-omakase@west.ntt.co.jp
□本文

この度はNTT西日本 セキュリティおまかせプランへのお申込みありがとうございます。

お客様管理ポータルへのログイン用ユーザアカウントを発行致しました。次のURLからログインできます。
https://clp.trendmicro.com/Dashboard?T=xxxxx
アカウントの詳細:
アカウント名: TMF●●●●●●●●●●

ログイン用のパスワードを設定する必要があります。次のURLからパスワードを設定してください。なお、このURLは7日間のみ有効です。
https://●●●●●●●

変更後のパスワードは大切に保管いただきますようお願いします。パスワードを忘れるとお客様管理ポータルにログインできなくなります。

ご不明な点がございましたら、次の連絡先にお問い合わせください。

【本メールに関するお問い合わせ】
セキュリティおまかせプラン開通事務局
TEL：0120-xxx-xxxx（9:00-17:00　平日　※年末年始を除く）

【サポートに関するお問い合わせ】
セキュリティおまかせサポートセンタ
TEL：0800-xxx-xxxx（9:00-21:00 平日・土日祝　※年末年始を除く）

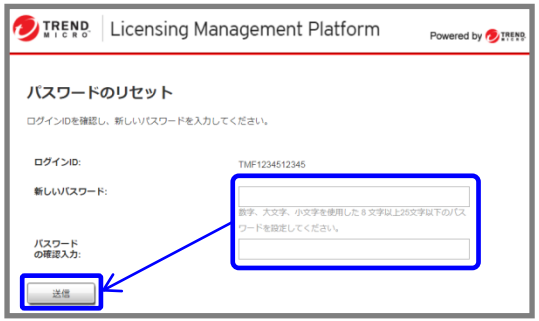
*このメールアドレスは配信専用です。このメッセージに返信しないようお願いいたします。

ログイン用ＵＲＬ

アカウント名

パスワード設定用ＵＲＬ

初めにこちらのＵＲＬより、
パスワードの設定をお願いします。



7.管理コンソールへのログイン方法　2/2

ログインURLをクリックし、アカウント名と設定したパスワードを入力し、ログインボタンを押します。ログインできますと、「セキュリティおまかせプラン」にてご契約のサービスが表示されますので、エンドポイントセキュリティ（ＶＢＢＳＳ）の「コンソールを開く」を選択します。

①ログイン画面へアクセス
https://clp.trendmicro.com/Dashboard?T=xxxxx

②ID/パスワードを入力し、「ログイン」をクリック

③割り当てられたサービスプランが表示されるので、エンドポイントセキュリティ（ｳｲﾙｽﾊﾞｽﾀｰﾋﾞｼﾞﾈｽｾｷｭﾘﾃｨｻｰﾋﾞｽ）の「コンソールを開く」をクリックします。

※表記が多少異なる場合がございます。
※初回ログイン時は、トレンドマイクロ株式会社のプライバシーポリシーが表示されますので、ご確認の上「OK」をクリックいただきますよう、お願いいたします。

④エンドポイントセキュリティの管理コンソールが立ち上がります。ログインは以上で完了です。

8. インストール（ダウンロード用URLの確認）1/3

エンドポイントセキュリティ/EDRセキュリティのダウンロード用ＵＲＬは、サービス提供開始前に送付しておりますメールもしくは、管理コンソールにてご確認いただけます。

メールでの確認方法

□件名　エンドポイントセキュリティ/EDRセキュリティのダウンロードURLのご案内
□送信元アドレス　sec-oma@west.ntt.co.jp
□本文

この度はNTT西日本 セキュリティおまかせプランへのお申込みありがとうございます。
本メールはエンドポイントセキュリティ　もしくは　EDRセキュリティ　を
ご契約いただいたお客様に送付しております。

インストールいただくソフトのダウンロードURLをご案内させていただきます。
なお、エンドポイントセキュリティ　と　EDRセキュリティ　でインストールするソフトは同一です。
※複数端末にインストールされる場合は、以下のURLをインストール端末に展開ください。

http://XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX　ダウンロード用ＵＲＬ

インストール方法・設定方法については、セキュリティおまかせプラン公式ホームページより、
ダウンロード頂くことが可能です。
セキュリティおまかせプラン公式ホームページURL：https://flets-w.com/solution/security_omakase/

尚、サービスが有効になるのは、ご利用開始予定日の●年●月●日からとなっております。

ご不明な点がございましたら、次の連絡先にお問い合わせください。

【本メールに関するお問い合わせ】
セキュリティおまかせプラン開通事務局
TEL：0120-xxx-xxxx（9:00-17:00　平日　※年末年始を除く）

【インストール方法に関するお問い合わせ】
セキュリティおまかせサポートセンタ
TEL：0800-xxx-xxxx　（9:00-21:00 平日・土日祝　※年末年始を除く）

【セキュリティおまかせプラン　サポートサイト】
サービスの使い方や、設定方法、よくあるご質問などを掲載しております。ご活用ください。
https://office-support.ntt-west.co.jp/security_omakase/

*このメールアドレスは配信専用です。このメッセージに返信しないようお願いいたします。

8. インストール（ダウンロード用URLの確認） 2/3

管理コンソールでの確認方法

①管理コンソールにて
「セキュリティエージェント」タブを選択

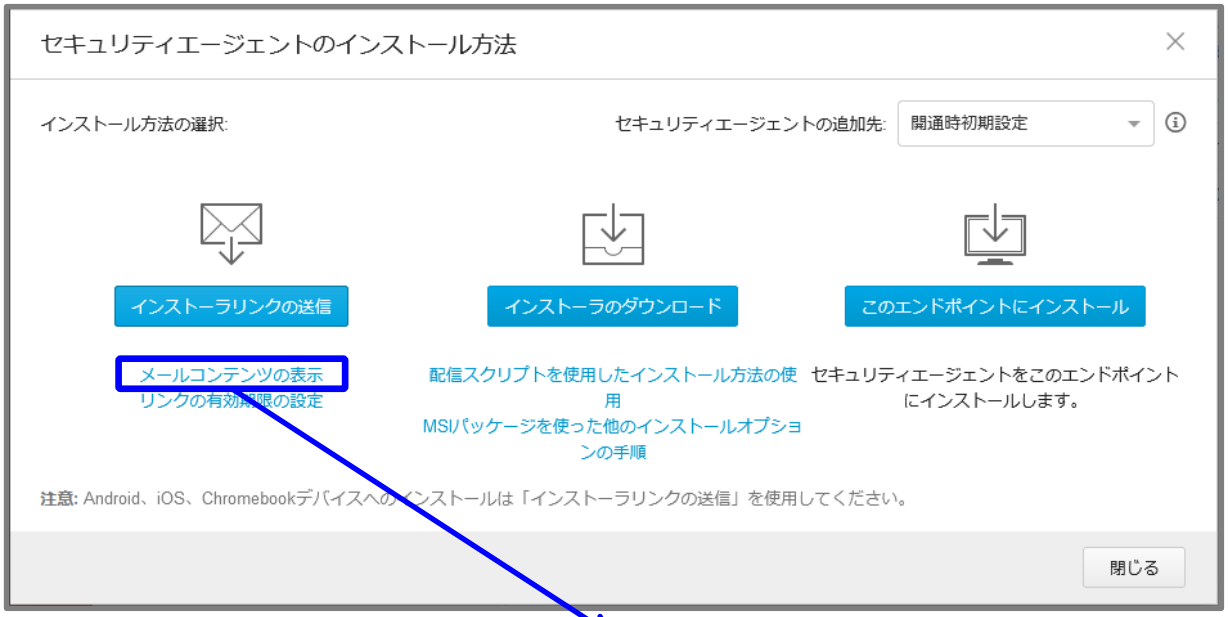
②グループのデバイス「開通時初期設定」を選択し、
「セキュリティエージェントの追加」を
クリックします。

※「開通時初期設定」とは、お申込み時に申請いただいた内容の設定情報を反映させたポリシーグループになります。新たなポリシーを作成する際は、「グループの追加」より、作成いただくことが可能です。
※「開通時初期設定」がない場合は「デバイス(初期設定)」を選択してください。

※サーバへインストールする際は、サーバ用のポリシーグループを選択ください。

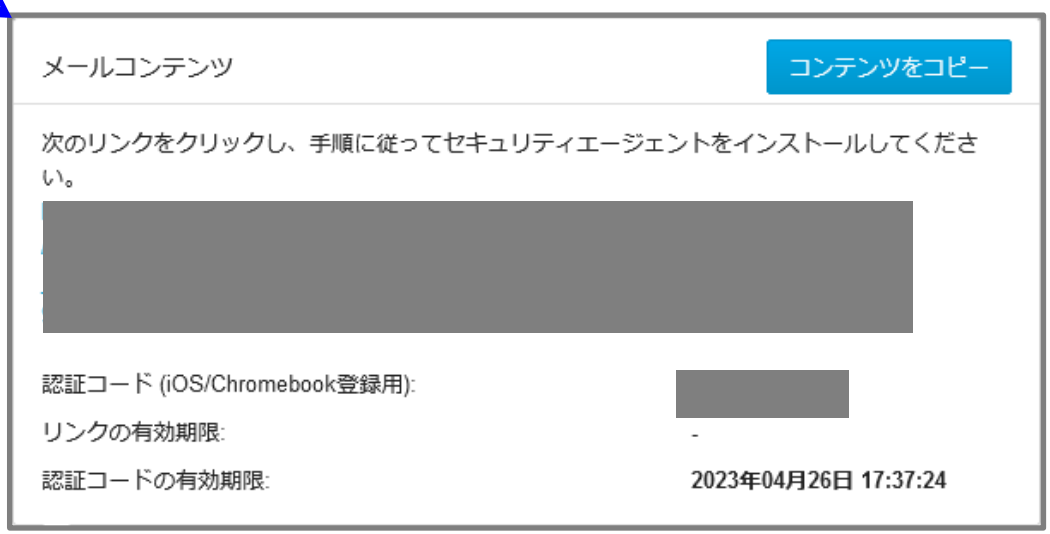
8. インストール（ダウンロード用URLの確認） 3/3

③インストール方法の選択画面にて、1つ目の項目にある
メールの詳細表示をクリックします。



④ダウンロード用ＵＲＬが表示されます。

複数端末にインストールされる場合は、本ＵＲＬを導入予定端末にメールで送付するか、共有サーバ等にテキストを保存する等の方法で、各端末にＵＲＬを展開します。



9. インストール（Windows）1/2

【メールを使用してインストールをする方法】
①1つ目の項目にある「インストーラリンクの送信」を
クリックします。

②インストール用のリンクを確認します。
Windows コンピュータへインストールする場合、この
インストール用のリンクをクリックしてインストールを
開始します。

③「インストーラーリンクの送信」から、自動で作成された
メールを送付し、エンドポイント側でリンクをクリックして
インストールを実施します。
また、「メールコンテンツの表示」から「コンテンツのコピー」で
内容をコピーしてメモ帳などに保存したものを配布して
インストールにご利用いただくこともできます。

④メールからリンクをクリック、またはブラウザを開きリンクを
入力して以下の画面から[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ていきます。
※注意　ハードディスク空き容量が約800MB必要となります。容量不足のエラーメッセージ
が表示される場合は、空き容量を確保し、再度インストールを実行します。

⑤次をクリックします。

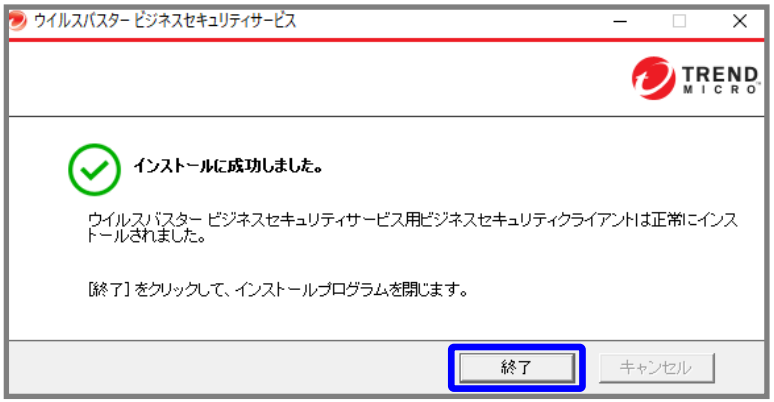
⑥インストールが開始されます。

⑦インストールが完了するまで待ちます。

9. インストール（Windows） 2 /2

⑧「インストールに成功しました」のメッセージが
表示されますので、「終了」をクリックします。

インストール作業は以上となります。



[参考]
インストールが完了したデバイスは、ご利用ＰＣのタスクトレイ上のアイコンと、
管理コンソールの「デバイス」画面にてご確認いただけます。

[タスクトレイ上のアイコン]

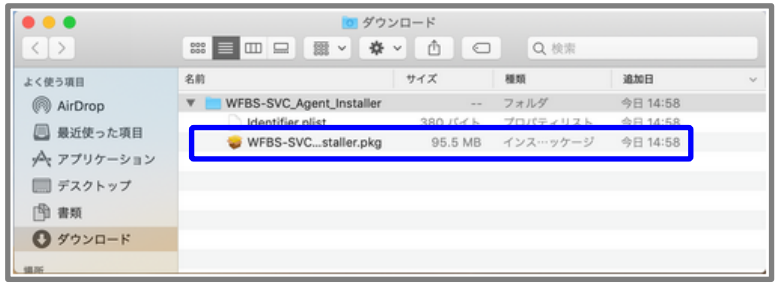
[管理コンソールのデバイス画面]

10. インストール（Mac OS）1/14

①「インストーラーリンクの送信」からメールで送られた
インストール用のリンクをクリックするか、
「インストーラのダウンロード」「このエンドポイントに
インストール」にて右の画面を開き、[ダウンロード]を
クリックします。
その後、インストーラ(WFBS-SVC_Agent_Installer.zip)
のダウンロードが開始されます。

②ダウンロード完了後、「WFBS-SVC_Agent_Installer.zip」
内の「WFBS-SVC_Agent_installer.pkg」をクリックし、
インストールを実行します。

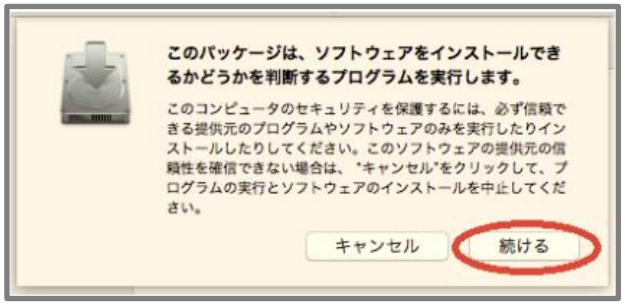
※注意
ハードディスク空き容量が64MB以上必要となります。容量不足のエラーメッセージが表示される場合は、空き容量を確保し、再度インストールを実行します。



〈以下のようなメッセージが出た場合〉
インストールパッケージを〝control〟キーを押したまま
クリックし、「開く」を使い実行します。
この方法はファイルを実行する時だけGateKeeper機能を無効にすることができます。

10.インストール（Mac OS）2/14

③「続ける」 をクリックし、インストールを進めます。

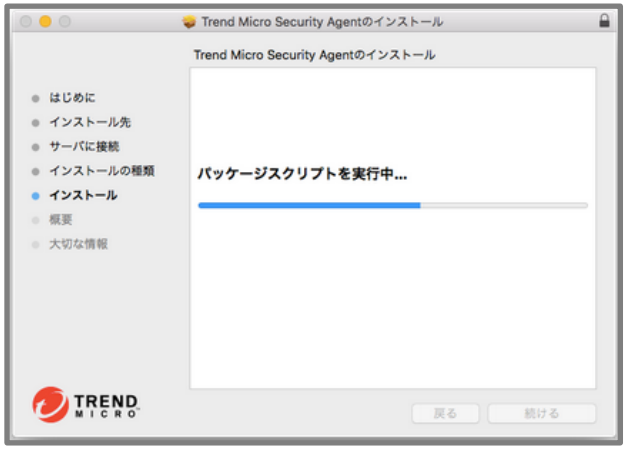


④「ようこそTrend Micro Securityインストーラへ」画面で
「続ける」をクリックし、インストールを進めます。

⑤「サーバーへの接続をテスト」画面で
「続ける」をクリックします。

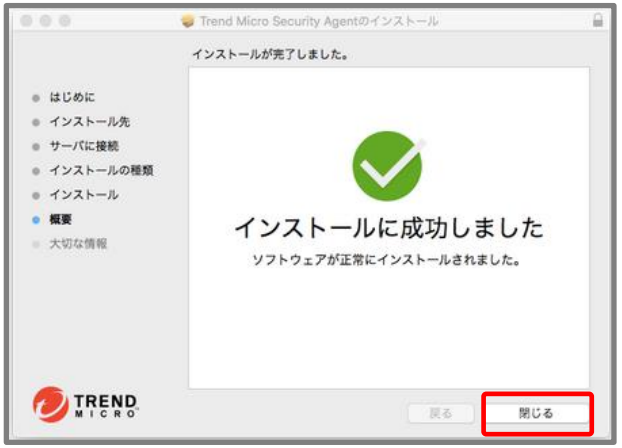
⑥「インストール」をクリックします。

⑦「インストール」が実行されます。



10.インストール（Mac OS）4/14

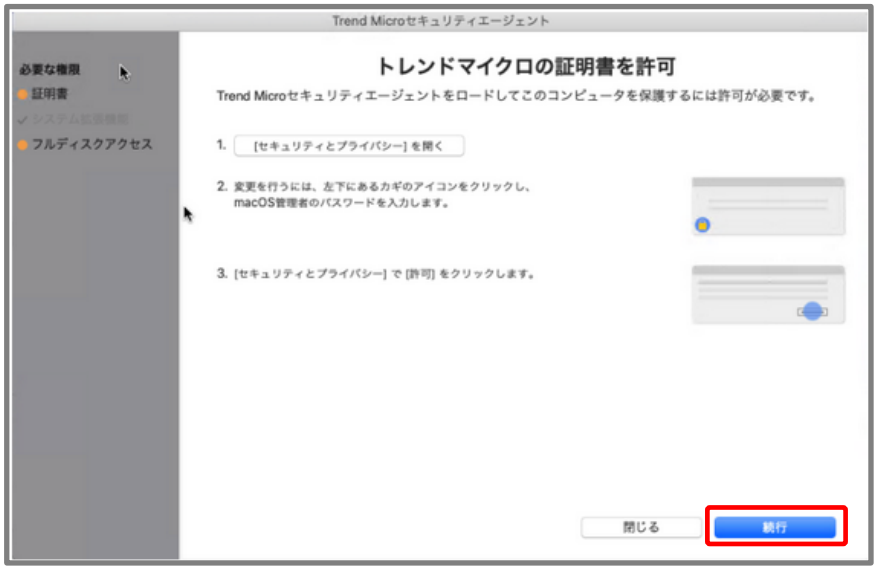
⑧「インストールに成功しました」というメッセージが表示されたら完了です。「閉じる」をクリックして終了します。



⑨macOS 10.14.x Mojave以降で新規インストールを実施した場合、右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、追加で必要な権限のセットアップをご実施ください。なお、ご利用のOSによって必要な作業が異なりますので、下記手順のうちご利用のOSに合わせた手順の実施をお願いいたします。

macOS 10.14.x Mojave以降 ～ macOS 10.15.x Catalina以前のOSをご利用の場合

⑩「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。



⑩-1．「セキュリティとプライバシー」画面を開きます。

⑩-2．「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。

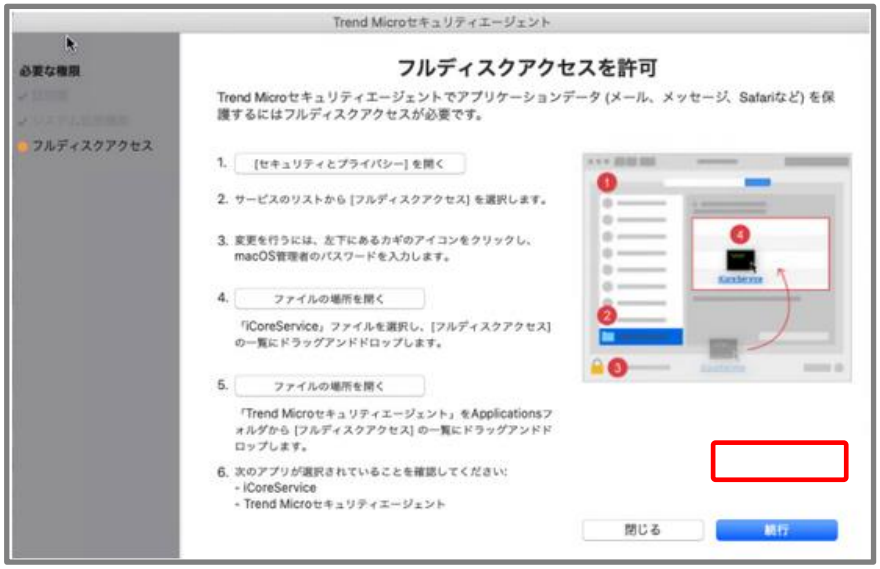
⑩-3. ［続行］をクリックします。

許可ボタンについて

「セキュリティとプライバシー」にはインストール後30分間「許可」ボタンが表示されます。
その間に許可をしなかった場合は、macOSを再起動することで再度「許可」ボタンが表示されます。

10.インストール（Mac OS）6/14 macOS10.14.x～15.x

⑪ 「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。



⑪-1. 「セキュリティとプライバシー」画面を開きます。「セキュリティとプライバシー」画面を開きます。

⑪-2 . [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。

⑪-3. 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。

⑪-4. 「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。

⑪-5. 「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。

⑪-6. 「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。

⑫［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。

⑬インストールが完了するとMacのアプリケーション内に以下のように表示されます。

Macエージェントを以前にインストールしたことがある場合、上記手順を実施することで、iCoreServiceが複数登録された状態になる場合がありますが、
そのままご利用いただいて問題ありません。

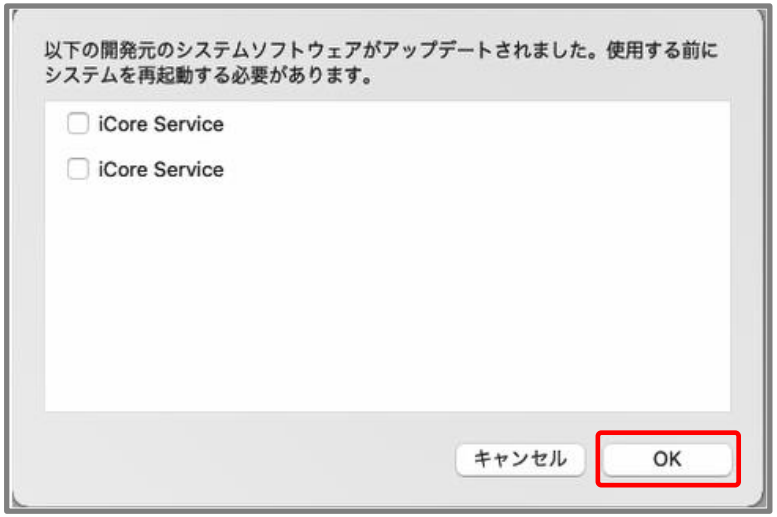
macOS 11 Big Sur 以降 ～ macOS Monterey 12.x 以前のOSをご利用の場合

⑩「システム拡張機能を許可」の画面で画面の指示にしたがって設定を行います。

⑩-1．「セキュリティとプライバシー」画面を開きます。

⑩-2．「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。」と記載がある横の「詳細」ボタンをクリックします。

⑩-3．リストから「iCoreService」の項目をすべて選択し、[OK] をクリックします。



10. インストール（Mac OS）9/14　macOS 12.x 以前

⑩-4. ″iCoreService″がネットワークコンテンツのフィルタリングを求めています」と表示されるので、[許可] をクリックします。

⑩-5. 「システム拡張機能を許可」の画面に戻り、[続行] をクリックします。

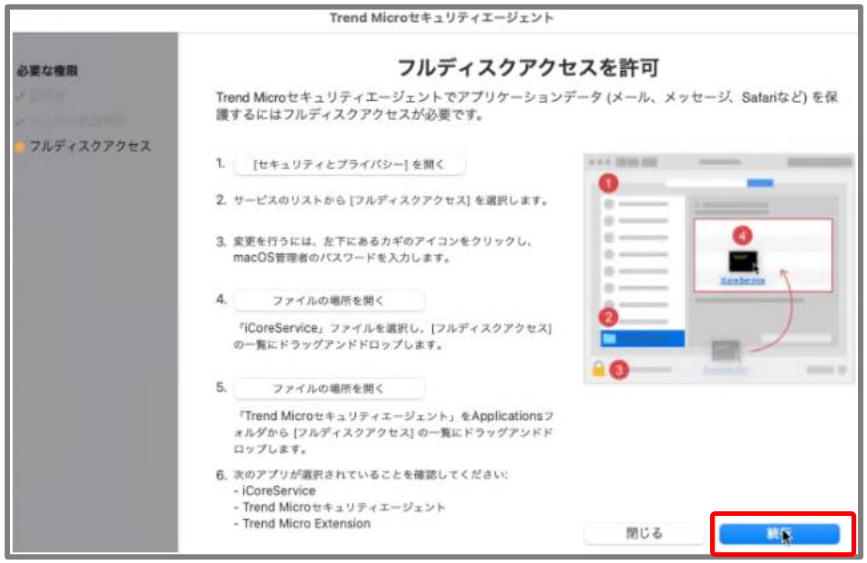
⑪「フルディスクアクセスを許可」の画面で画面の指示にしたがって設定を行います。

⑪-1. 「セキュリティとプライバシー」画面を開きます。

⑪-2 . [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。

⑪-3. 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。

⑪-4. 「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。



10. インストール（Mac OS）10/14　macOS 12.x 以前

⑪-5.　「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。なお、下記画面が表示された場合は［あとで行う］をクリックしてください。

⑪-6.　［フルディスクアクセス］の一覧に「iCoreService」「Trend Microセキュリティエージェント」「TrendMicro Extension」が表示されており、チェックがついていることを確認します。
チェックがついていない場合は、チェックを付けてください。

⑪-7.　「セキュリティとプライバシー」画面を閉じ、「フルディスクアクセスを許可」の画面で［続行］をクリックします。

⑫［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。

⑬インストールが完了するとMacのアプリケーション内に以下のように表示されます。

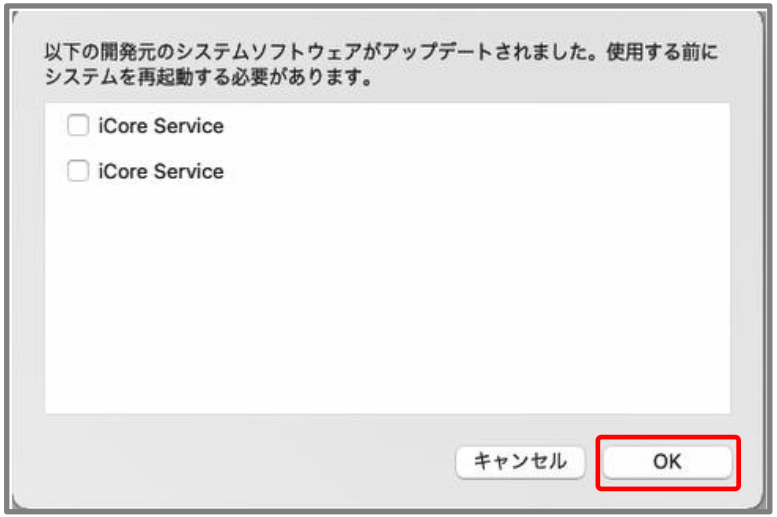
macOS Ventura 13.x 以降をご利用の場合

⑩ 「システム拡張機能を許可」の画面で画面の指示にしたがって設定を行います。

⑩-1. 「セキュリティとプライバシー」画面を開きます。

⑩-2 . 「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。」と記載がある横の「詳細」ボタンをクリックします。

⑩-3. リストから「iCoreService」の項目をすべて選択し、[OK] をクリックします。



10. インストール（Mac OS）12/14 macOS 13.x 以降

⑩-4 「″iCoreService″がネットワークコンテンツのフィルタリングを求めています」と表示されるので、[許可] をクリックします。

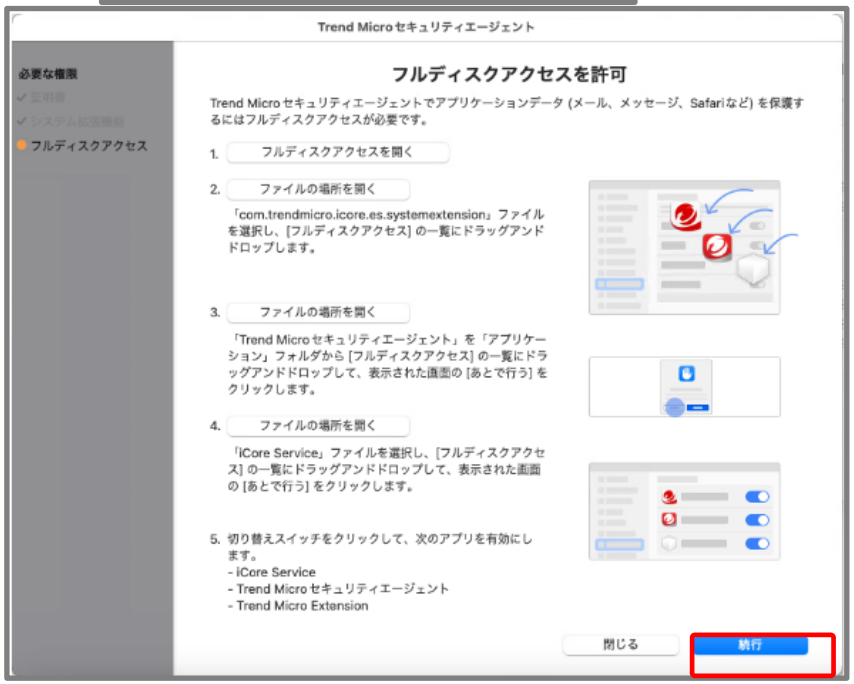
⑩-5. 「システム拡張機能を許可」の画面に戻り、[続行] をクリックします。

⑪ 「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。

⑪-1. [フルディスクアクセスを開く] をクリックし、フルディスクアクセスの画面を開きます。

⑪-2 . 「フルディスクアクセスを許可」の画面に戻り、2番の [ファイルの場所を開く] をクリックして表示された「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。

⑪-3. 「フルディスクアクセスを許可」の画面に戻り、3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。



10. インストール（Mac OS）13/14 macOS 13.x 以降

⑪-4. 「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。

⑪-5. 「フルディスクアクセスの画面においてそれぞれの切り替えスイッチが有効になっていることを確認後、「フルディスクアクセスを許可」画面の［続行］をクリックします。

⑫［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。

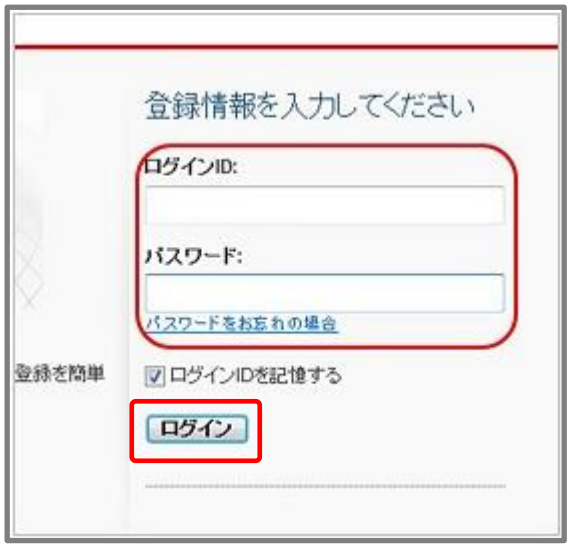
⑬インストールが完了するとMacのアプリケーション内に以下のように表示されます。

Macエージェントを以前にインストールしたことがある場合、上記手順を実施することで、iCoreServiceが複数登録された状態になる場合がありますが、そのままご利用いただいて問題ありません。

登録の確認

①管理コンソールに再度、ログインします。

②「セキュリティエージェント」メニューをクリックし、
「すべてのセキュリティエージェント」、
「手動グループ」または配下の任意のグループ内の
表示された画面内にインストールを実施したMacが
登録されていることを確認します。



11. Mac OS端末におけるEDRセキュリティのインストール手順について

事前準備

EDRセキュリティのアプリケーション（アプリケーション名：Trend Micro XDR Endpoint Sensor）は、
EDRセキュリティをご契約のお客様かつエンドポイントセキュリティがインストールされているMac端末に
自動インストールされます。

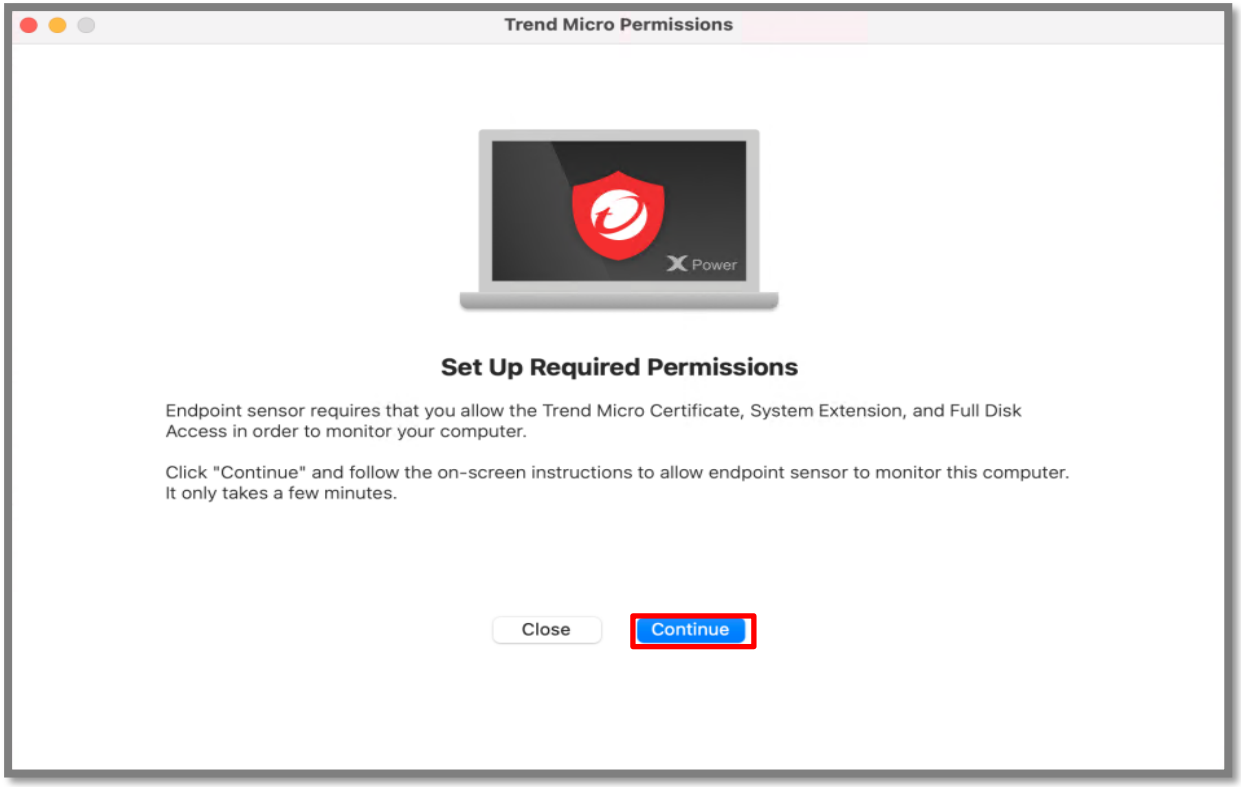
インストール後、EDRセキュリティの機能をご利用いただくには、EDRセキュリティ契約時の追加手順
（Mac OS）(34～44P)に沿った設定が必要となりますので、恐れ入りますがご確認のうえ、対応ください。
なお、エンドポイントセキュリティのインストール後、EDRセキュリティの自動インストールまで1営業日かかりますので、
ご了承ください。

また、一度インストールしたEDRセキュリティ　アプリケーションをアンインストールされる場合、
サポートセンターでの処理も必要となりますので、大変お手数をおかけしますが、サポートセンターまでご連絡を
お願いいたします。

12. EDRセキュリティ契約時の追加手順（Mac OS） 1/11

①EDRセキュリティのアプリケーション
（アプリケーション名：Trend Micro XDR Endpoint Sensor）が
自動インストールされると、
Mac端末上に権限のセットアップ画面が表示されます。

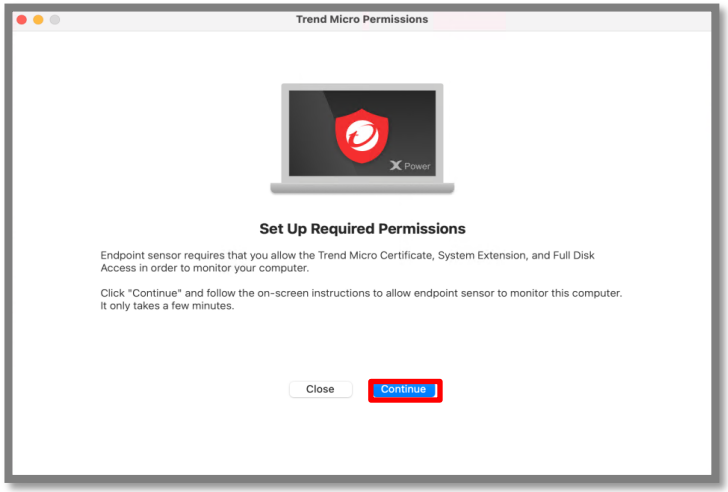
②「Continue」をクリックして権限のセットアップ作業を実施します。
※Closeボタンを押した場合は、端末上に表示されている
「 Trend Micro XDR Endpoint Sensor」アプリをクリックしていただ
きますと、再度設定画面を開くことが可能です。



12. EDRセキュリティ契約時の追加手順（Mac OS）2/11

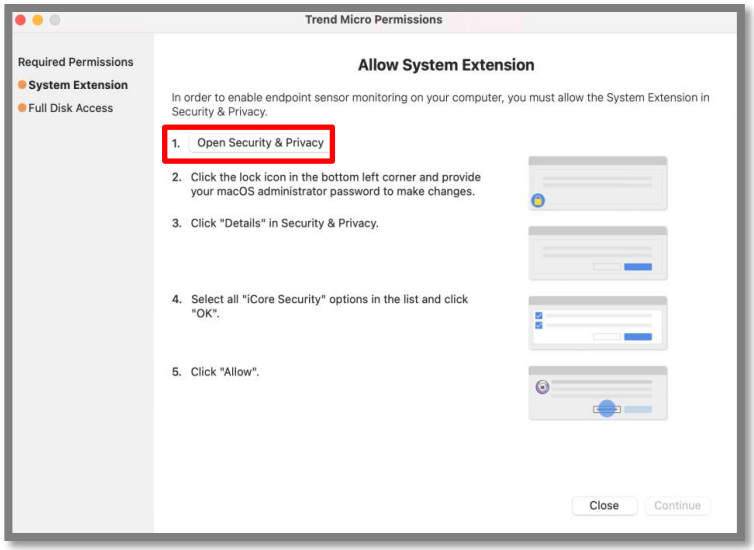
③「機能拡張がブロックされました」が表示されるので、
「OK」をクリックします。

④「Continue」をクリックして権限のセットアップ作業を実施します。



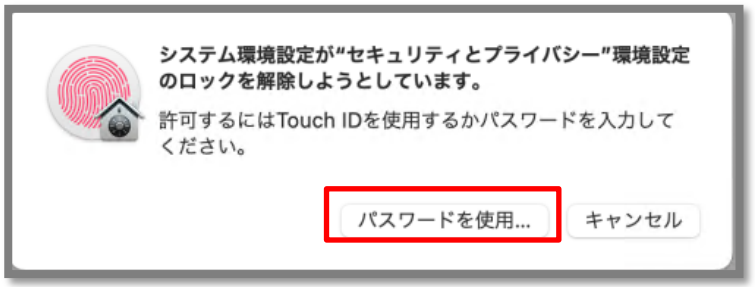
12. EDRセキュリティ契約時の追加手順（Mac OS）3/11

⑤「Allow　System Extension」が表示されるので、
「1.Open Security & Privacy」をクリックします。

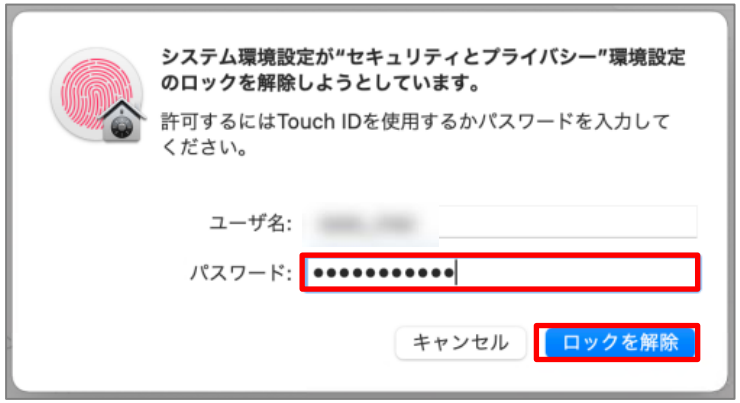


⑥「セキュリティとプライバシー画面」が表示されるので、
ロックされている場合はカギマークをクリックしてロック解除をします。

⑦「ロックの解除について」許可を求められる画面が表示されますので、「パスワードを使用」をクリックします。



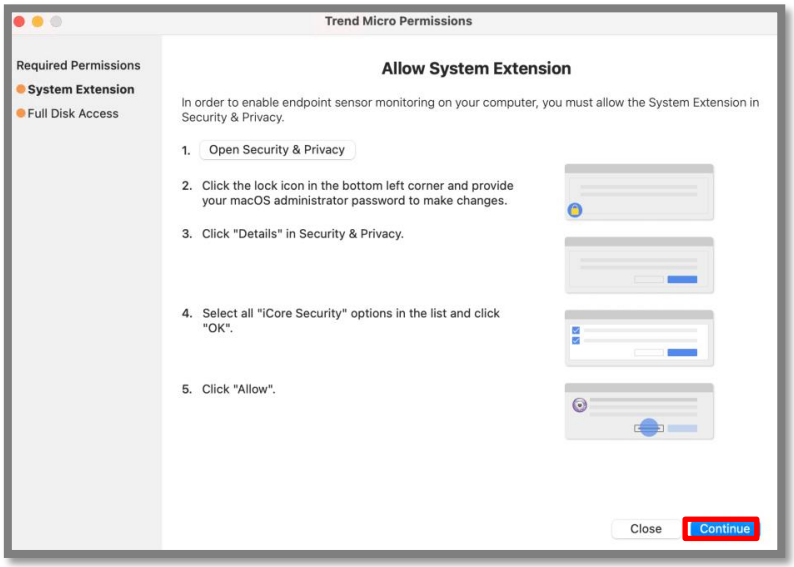
⑧パスワードを入力して、「ロックを解除」をクリックします。



12. EDRセキュリティ契約時の追加手順（Mac OS）5/11

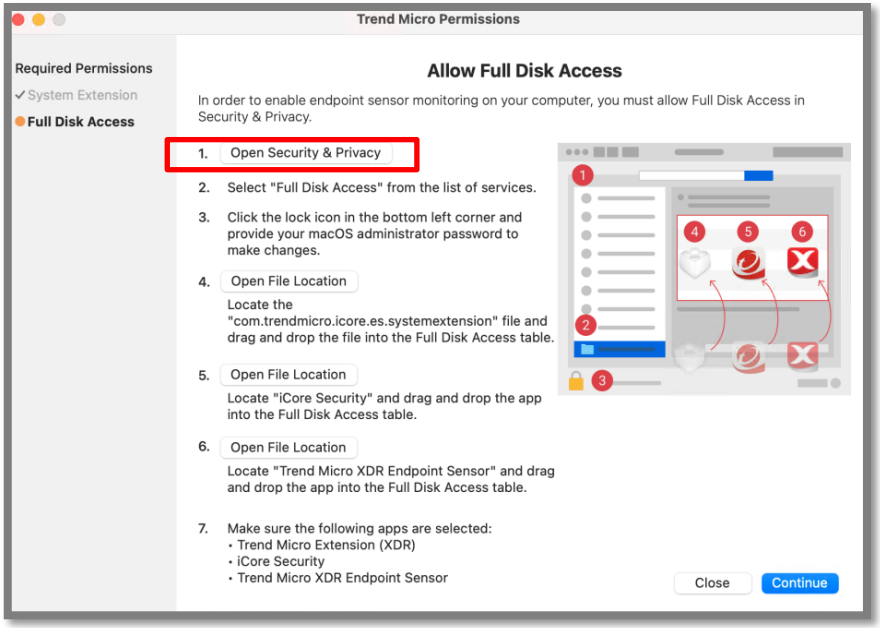
⑨「使用する前にシステムの再起動する必要があります」の画面が表示されましたら、「iCoreService」の項目をすべて選択し、[OK]をクリックします。

⑩「System Extension」の設定が完了しましたので、「Continue」をクリックします。
「Full　Disk Access」に進みます。

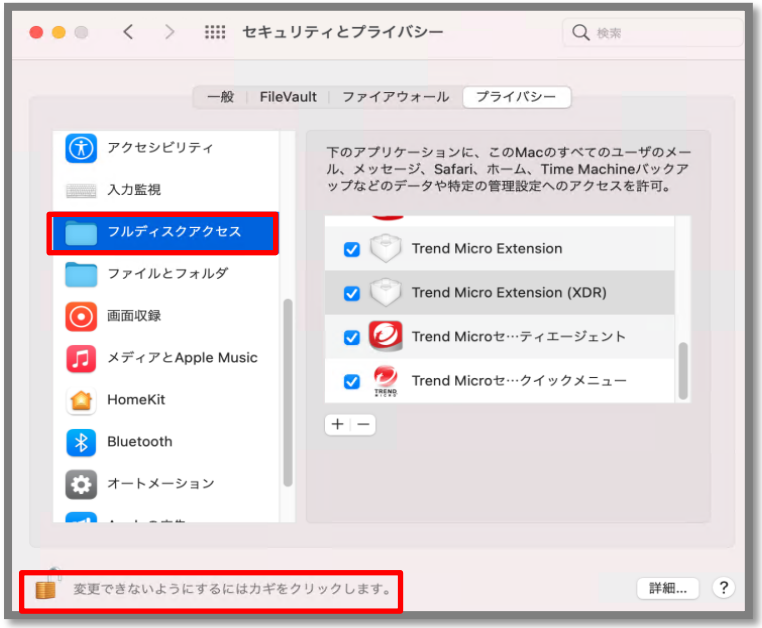


12. EDRセキュリティ契約時の追加手順（Mac OS）6/11

⑪「1.Open Security & Privacy」をクリックします。

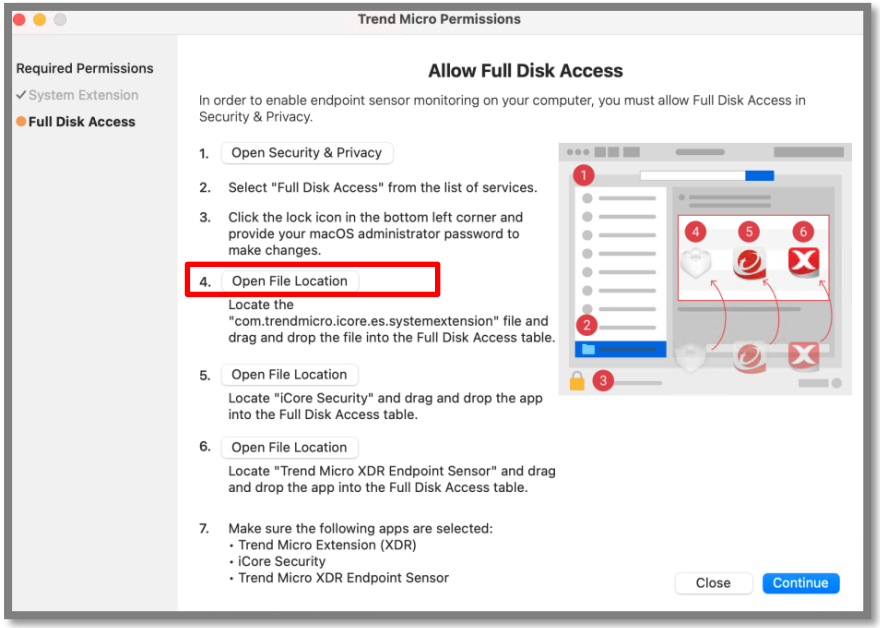


⑫「セキュリティとプライバシー」の画面が表示されますので、「フルディスクアクセス」が選択されていることを確認します。
※ロックされている場合は、カギマークをクリックしパスワード入力してロックを解除ください。
Allow Full Disk Access画面に戻ります。

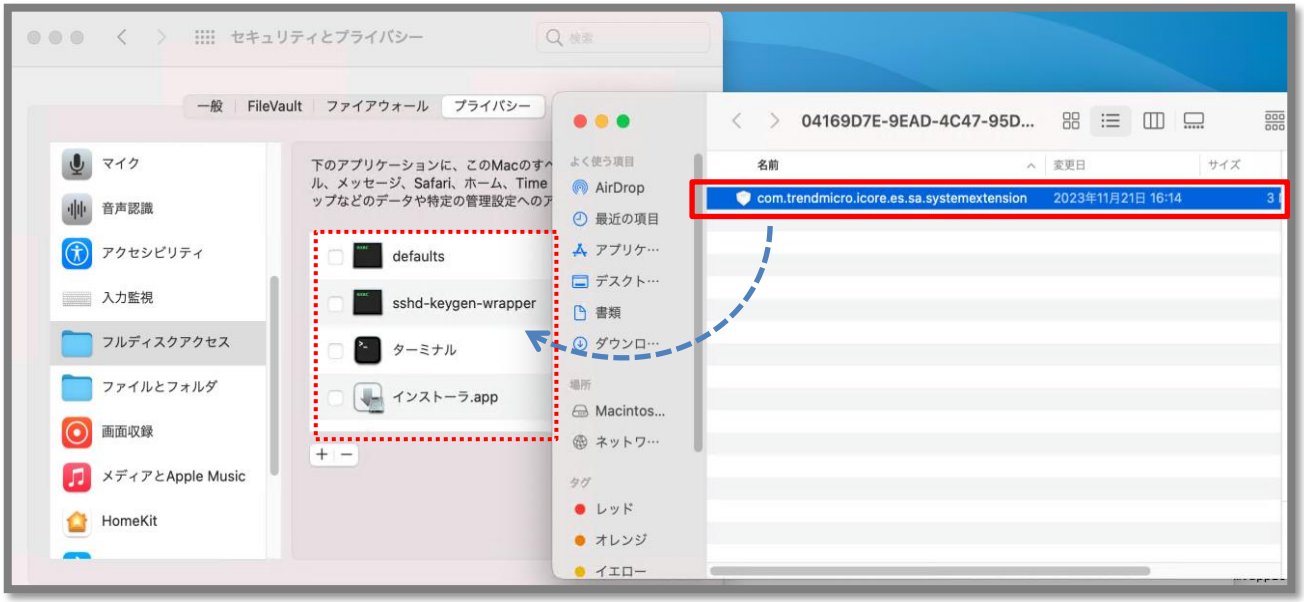


12. EDRセキュリティ契約時の追加手順（Mac OS）7/11

⑬「4.Open File Location」をクリックすると、
「com.trendmicro.icore.es.systemextension」が
表示されます。

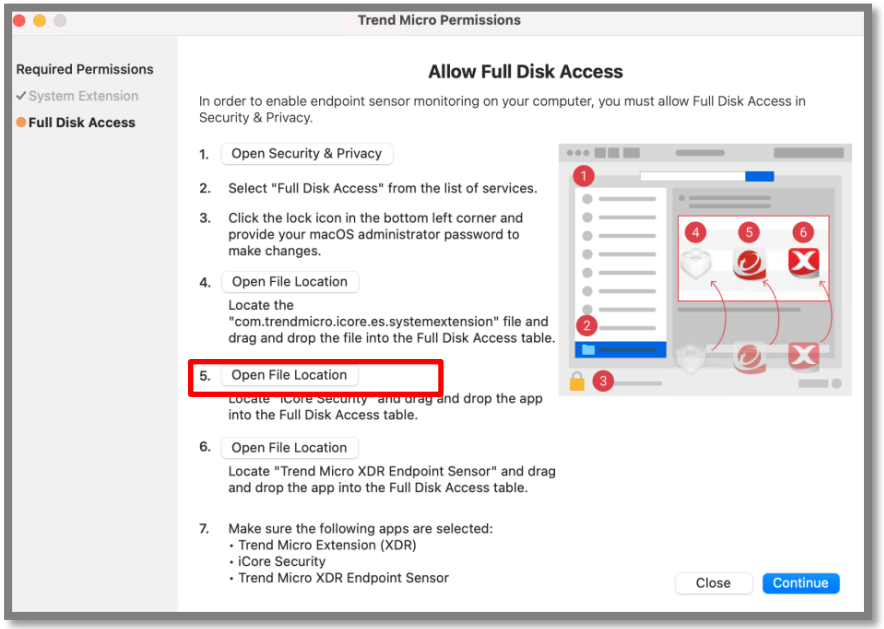


⑭「com.trendmicro.icore.es.systemextension」を
フルディスクアクセスの一覧に
ドラッグアンドドロップします。

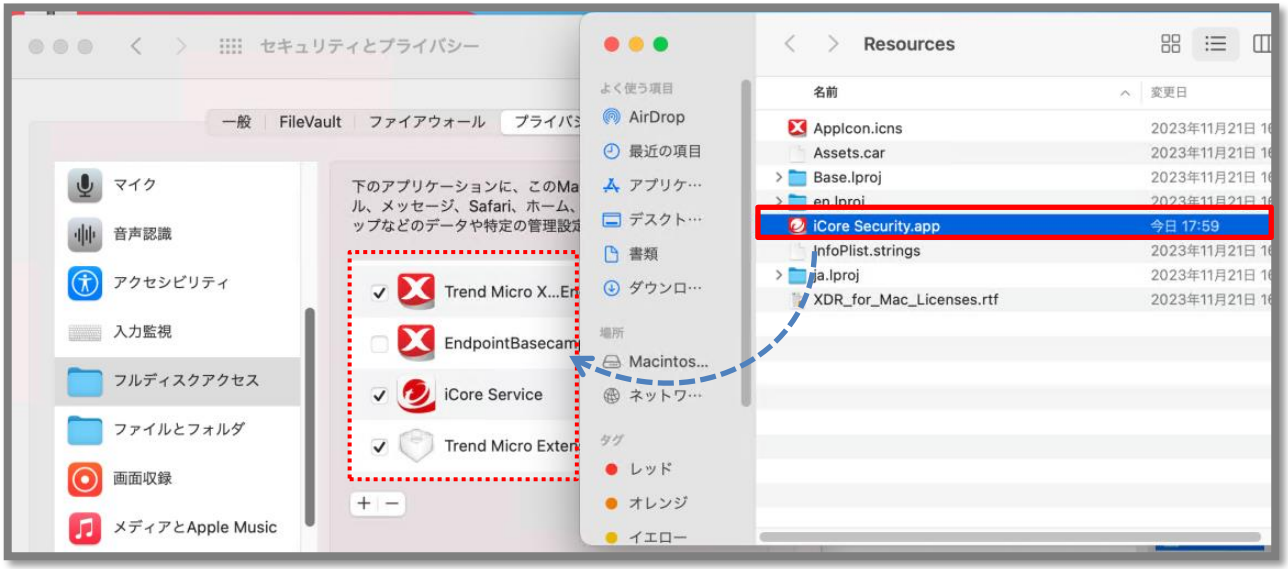


12. EDRセキュリティ契約時の追加手順（Mac OS）8/11

⑮「5.Open File Location」をクリックします。

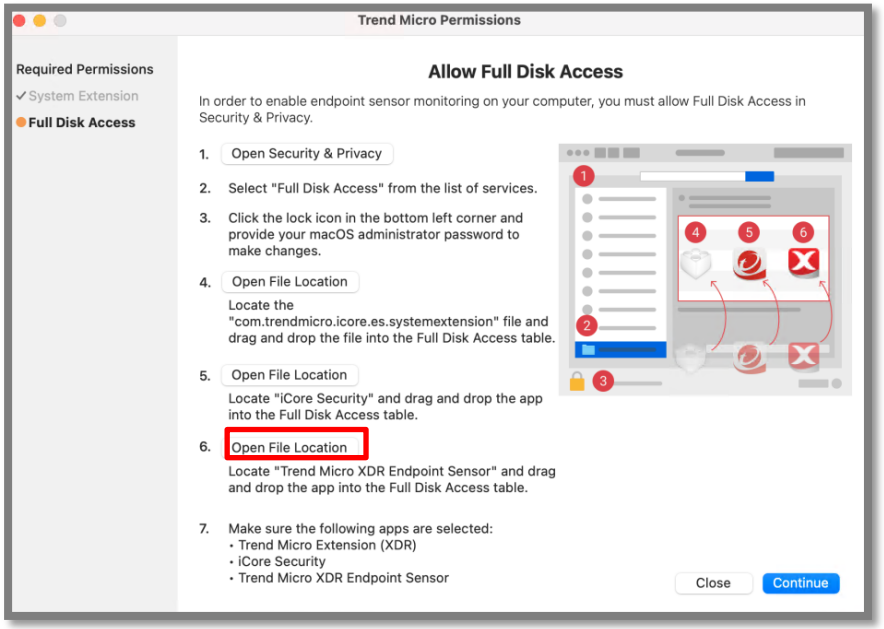


⑯「iCore Security」をフルディスクアクセスの一覧にドラッグアンドドロップします。
Allow Full Disk Access画面に戻ります。

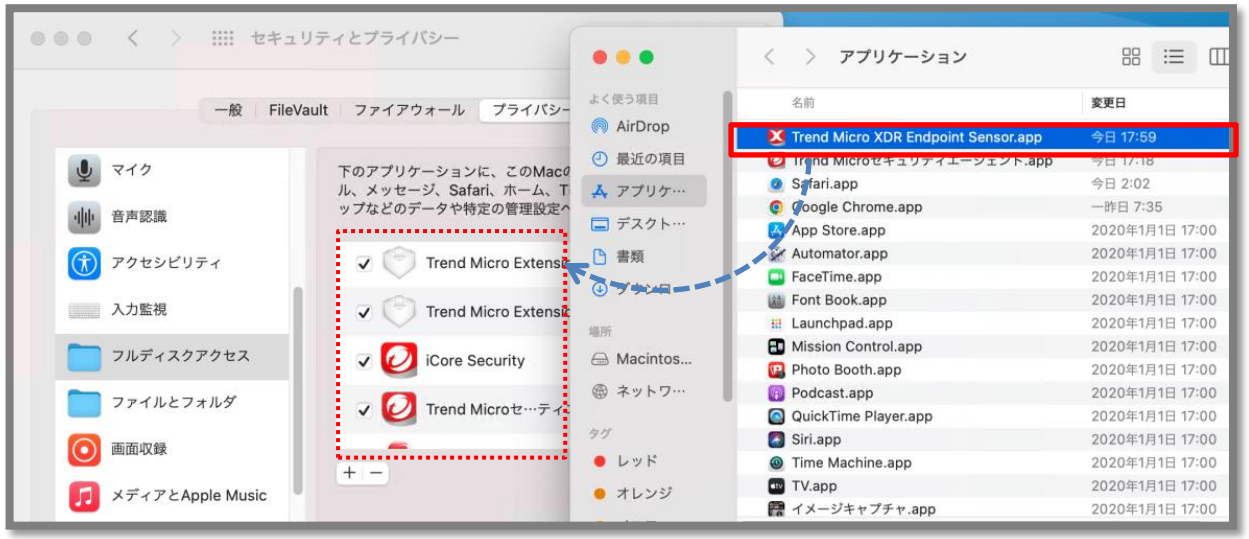


12. EDRセキュリティ契約時の追加手順（Mac OS）9/11

⑰「6.Open File Location」をクリックします。



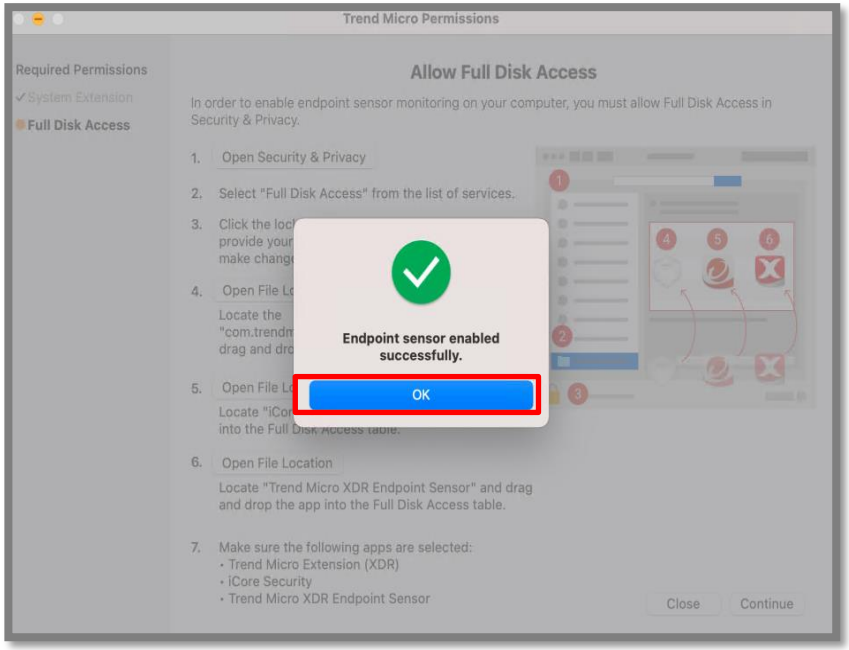
⑱「Trend Micro XDR Endpoint Sensor」をフルディスクアクセスの一覧にドラッグアンドドロップします。



12. EDRセキュリティ契約時の追加手順（Mac OS）10/11

⑲「Trend Micro XDR Endpoint Sensor.appには、終了するまでフルディスクアクセスがありません」の画面が表示されましたら、「あとで行う」をクリックします。

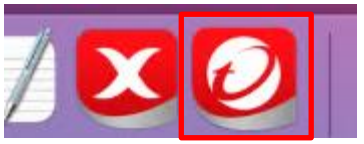
⑳「OK」をクリックしましたらセットアップは以上になります。
※OSバージョン10.15では、端末再起動が必要です。
※⑲で[終了して再度開く]をクリックした場合は、こちらの画面は表示されませんが、設定作業は正常に完了しています。



12. EDRセキュリティ契約時の追加手順（Mac OS）11/11

㉑インストールが完了すると、タスクバーに
「Trend Micro XDR Endpoint Sensor」
が追加されます。
別途インストールしたエンドポイントセキュリティ
アプリ（VBBSS）

をクリックして開きます。



㉒ツールバーエージェントコンソール上「Endpoint Sensor」のステータスがグリーン(有効)になります。

※未インストールや、「Endpoint Sensor」が無効の場合はグレー表示します。

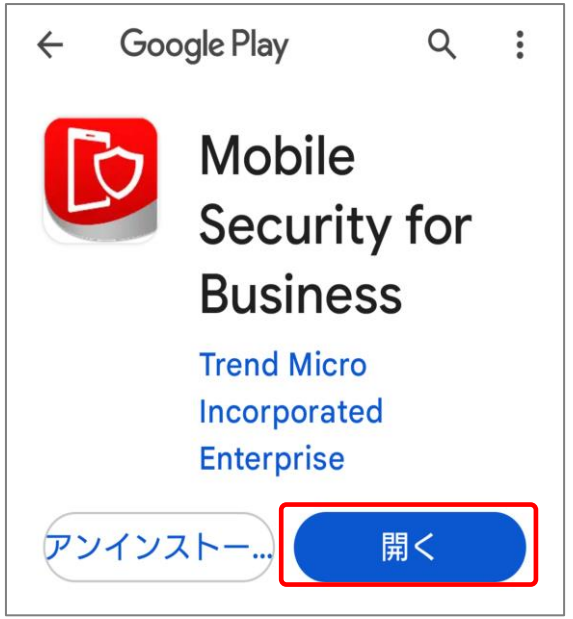
13. インストール（Android）1/17

①Android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。

右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。
※インストールが始まり、「インストール中…」が表示されます。

②インストールが完了したら、「開く」をタップします。

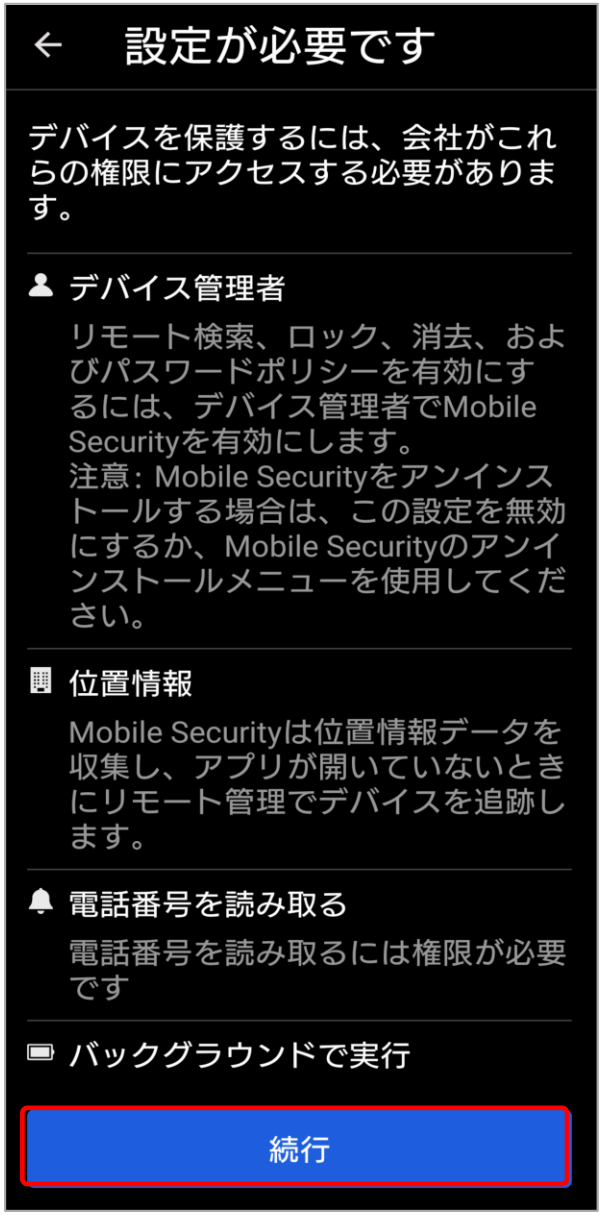
※「開く」をタップ後、Mobile Securityが起動し、「どの機能を使用しますか？
ウィルス対策 or すべての機能」と表示された場合は「すべての機能」を選択し、「続行」をタップします。



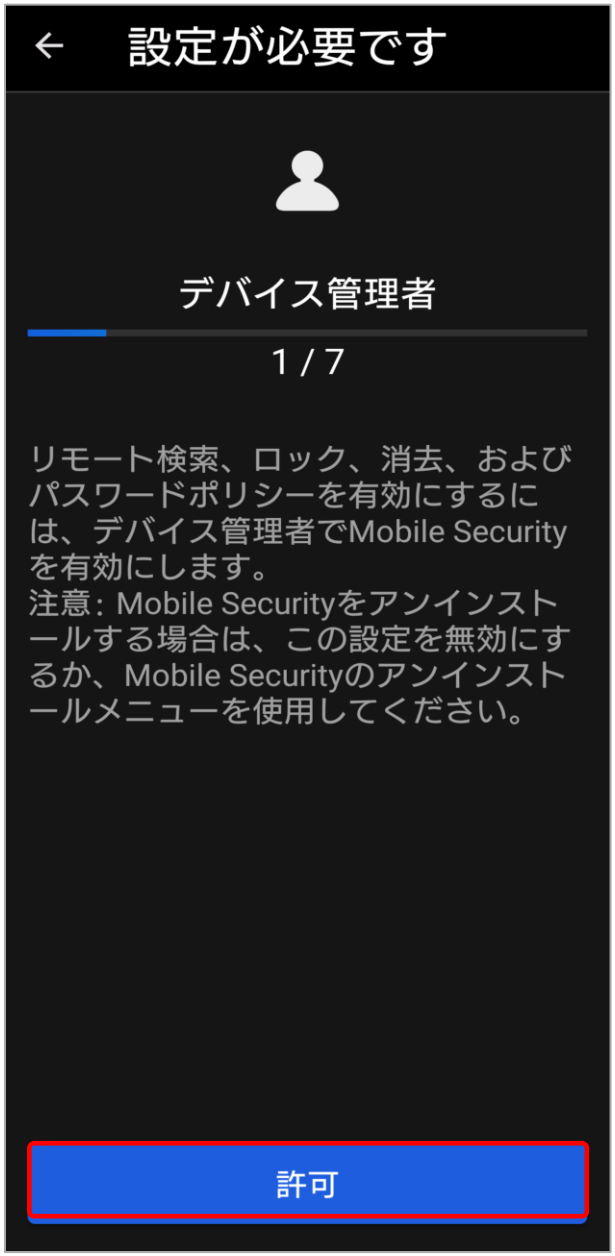
13. インストール（Android）2/17

③Mobile Security for Businessが起動し、
「サインインしています…　しばらくお待ちください。」と
表示されるため、待ちます。

④右のような画面が表示されるため、画面下部の「続行」をタップします。

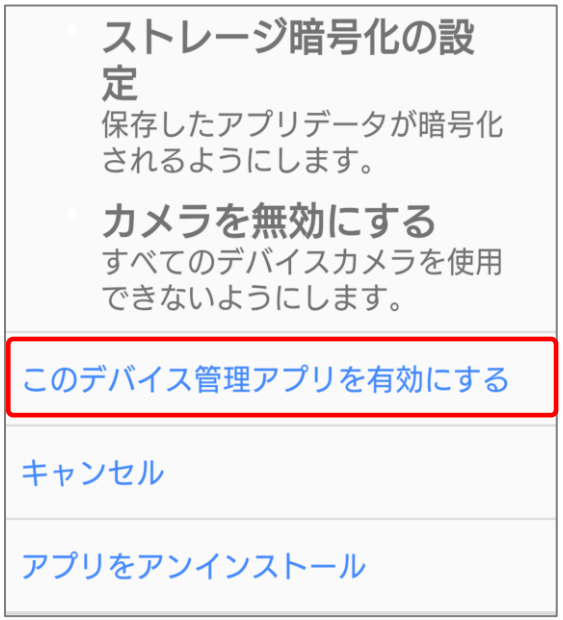


⑤デバイス管理者画面にて「許可」をタップします。

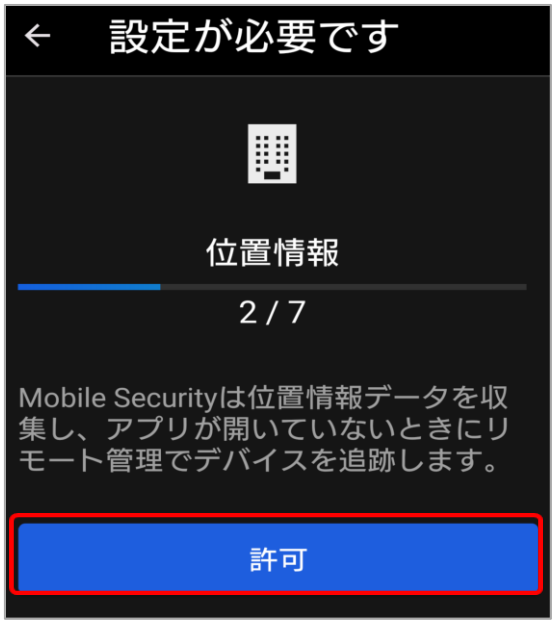


⑥「デバイス管理アプリの有効化」画面が表示されるため、下へスクロールします。

⑦「デバイス管理アプリの有効化」画面下部に表示されている、「このデバイス管理アプリを有効にする」をタップします。

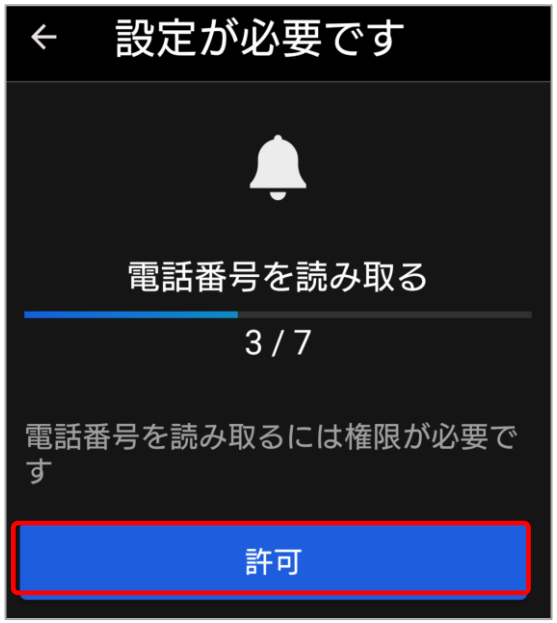


⑧位置情報画面にて「許可」をタップします。



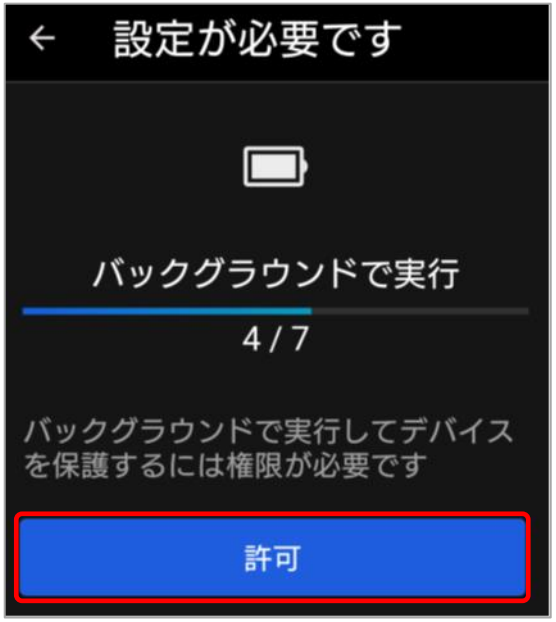
⑨位置情報へのアクセス許可を求められるため、
「アプリの使用時のみ」をタップします。

⑩「電話番号を読み取る」画面にて、「許可」をタップします。



⑪電話の発信と管理の許可を求められるため、「許可」をタップします。

⑫「バックグラウンドで実行」画面にて、「許可」をタップします。



⑬アプリにバックグラウンドでの実行について許可を求められるため、「許可」をタップします。

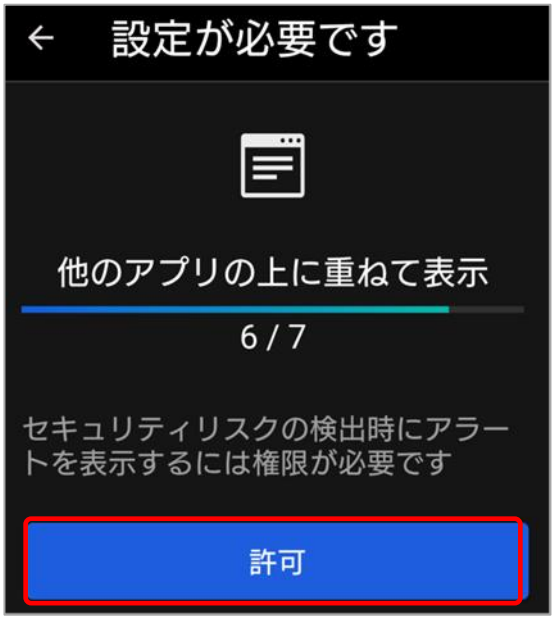
⑭「通知へのアクセス」画面にて「許可」をタップします。

⑮「通知へのアクセス」画面にて「Mobile Security」をタップします。
※一覧に「Mobile Security」のアプリが、
表示されていない場合は画面を下へスクロールし、
確認してください。

⑯「通知へのアクセス」画面にて、「通知へのアクセスを許可」のトグルボタンをタップし、ONにします。
※右図はOFF状態です。

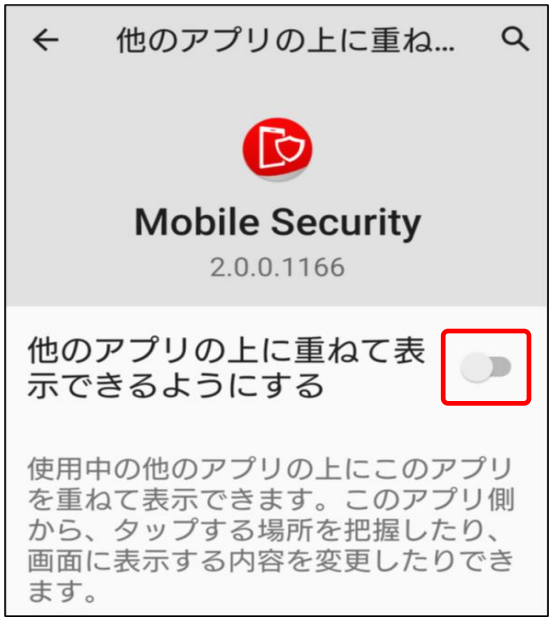
⑰トグルボタンをONにすると、右のような画面が表示されます。「許可」をタップし、通知へのアクセスを許可します。

⑱「他のアプリの上に重ねて表示」画面にて、「許可」をタップします。

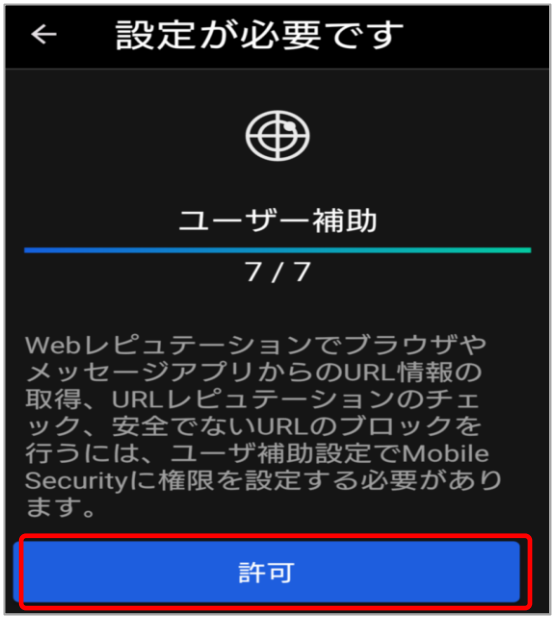


⑲「他のアプリの上に重ねて表示」設定画面にて、「Mobile Security」をタップします。
※一覧に「Mobile Security」のアプリが、表示されていない場合は画面を下へスクロールし、確認してください。

⑳「他のアプリの上に重ねて表示」画面で、トグルボタンをタップし、ONにします。
※右図はOFF状態です。



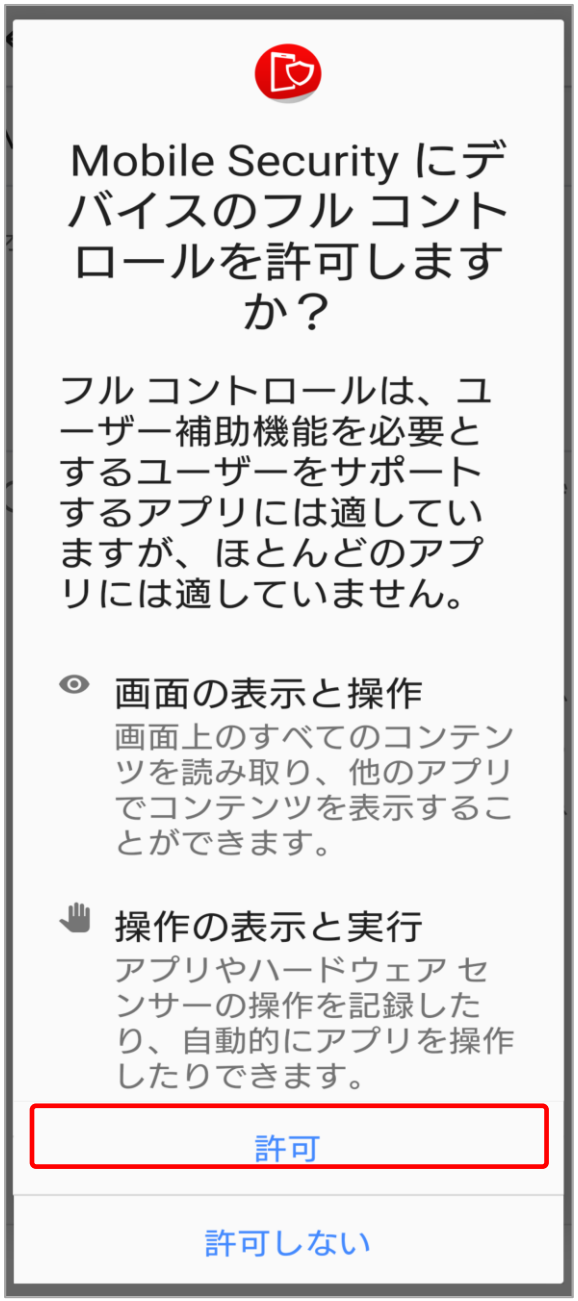
㉑トグルボタンをONにすると、「ユーザ補助」画面が表示されるため、「許可」をタップします。



㉒ユーザ補助画面にて「Mobile Security」をタップします。

㉓「Mobile Securityを使用」のトグルボタンをタップし、ONにします。
※右図はOFF状態です。

㉔右のような画面が表示されるため、「許可」をタップし、
デバイスのフルコントロールを許可します。



㉕仕事用メールアドレスを入力後、「続行」をタップします。

※入力したメールアドレスが管理コンソールのエンドポイント項目に表示されるアカウント名となります。

㉖インストール完了です。
※端末のホーム画面にて「Mobile Security」の
アイコンが表示されます。

■登録の確認

①管理コンソールにアクセスし、ログインします。
ユーザ登録時に設定した「ログインID」と「パスワード」を入力して、「ログイン」ボタンをクリックします。

②「セキュリティエージェント」タブをクリックし、表示された画面内にインストールを実施したAndroidデバイスが登録されていることを確認します。

14. 新エージェントへ移行（Android） 1 / 7

Android端末にてエンドポイントセキュリティの旧エージェントを使用している方は
新エージェントへの移行作業を必ず実施してください。
※ エンドポイントセキュリティは「ウイルスバスタービジネスセキュリティサービス」を指します。

■新エージェント概要
- Google Playにエージェントを掲載
- エージェントコンソールの全体デザインの変更

■移行対象者
Android端末にてエンドポイントセキュリティ バージョン 9. X をご利用中の方。
(2023/7/31 より前に公開されたバージョンをご利用中の方)

■移行対象期間
2023/8/29 ～ 2024/8/31
※2024年9月1日からエンドポイントセキュリティ バージョン（9. X）はサポート対象外となります。

■移行時の注意事項
移行完了後、ログ情報を含む旧エージェント情報はWeb管理コンソール上から削除されます。

【参考】バージョン確認方法
Android端末で下図を参考にご確認ください。

14. 新エージェントへ移行（Android） 2 / 7

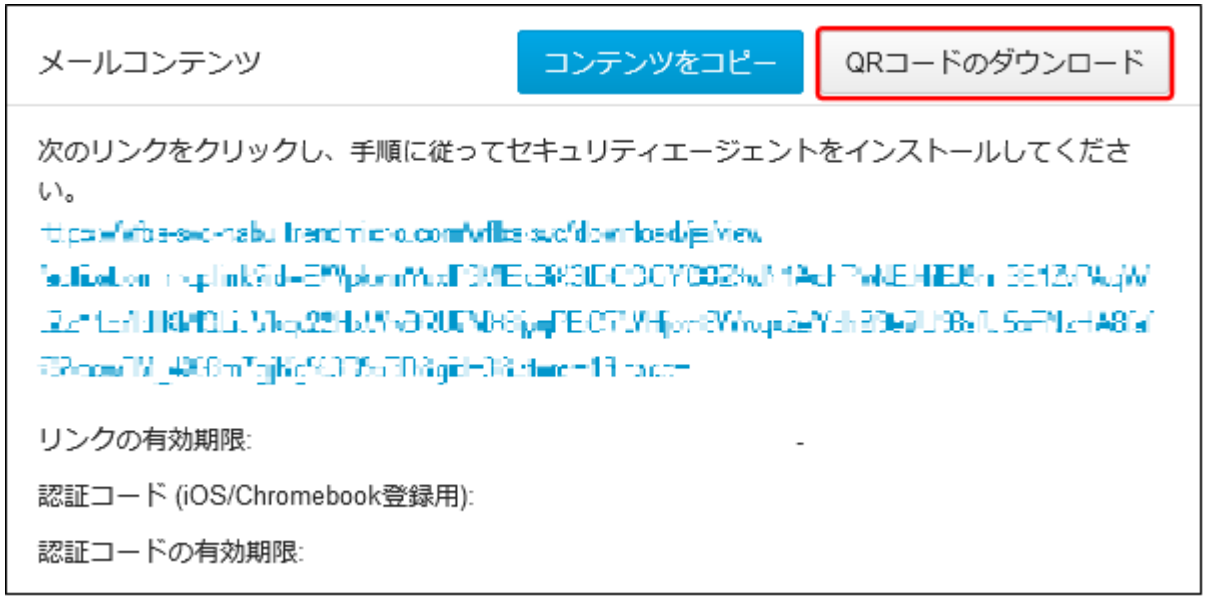
■移行手順

①PCにて管理コンソールへログインします。その後、「セキュリティエージェント」タブを選択し、
手動グループのデバイスにて「開通時初期設定」※を選択します。
その後、「セキュリティエージェントの追加」を選択します。

※「開通時初期設定」とは、お申込み時に
申請いただいた内容の設定情報を
反映させたポリシーグループになります。
新たなポリシーを作成している際は、
作成したポリシーグループをご指定ください。

「セキュリティエージェントのインストール方法」画面が表示されるため、
「メールコンテンツの表示」を選択します。

②メールコンテンツ画面が表示されるため、「QRコードのダウンロード」を選択しQRコードをダウンロードします。

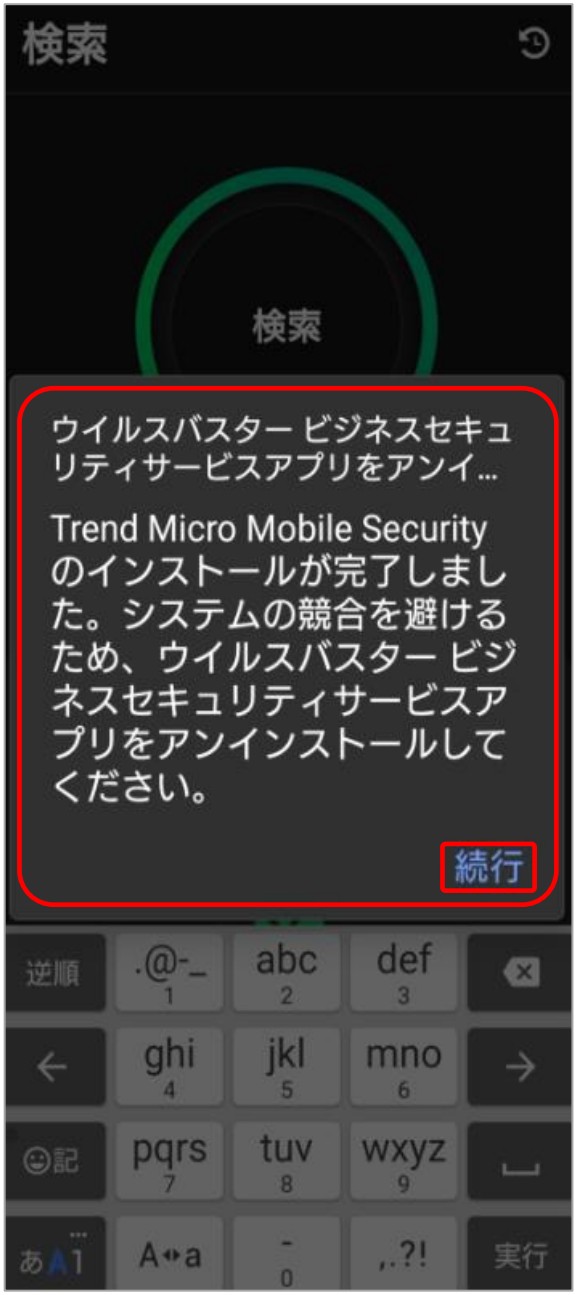


その後、ダウンロードしたQRコードをAndroid端末にて読み込みます。
インストール画面が表示されるため、本マニュアルの
「13.インストール（Android）1/17 ～15/17」を参照し、インストール作業を行います。

※「13.インストール（Android） 15/17」実施後は次ページの③へ進んでください。

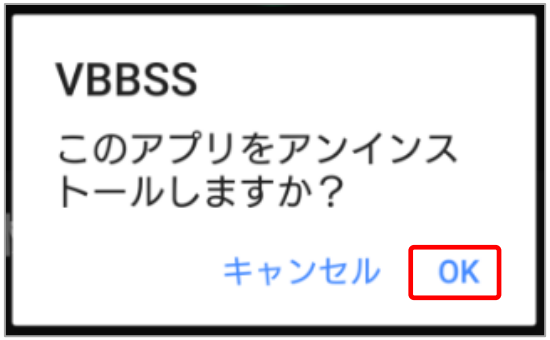
14. 新エージェントへ移行（Android） 4 / 7

③「13.インストール（Android）15/17」を実施後、
旧エージェントのアンインストールを促す通知が表示されるため、「続行」を選択します。



14. 新エージェントへ移行（Android） 5 / 7

④「このアプリをアンインストールしますか？」と
表示されるため、「OK」を選択します。



⑤アプリのホーム画面下に「VBBSSをアンインストール
しました」と表示されたことを確認します。
※通知は数秒で消えます。

Android端末のホーム画面にて旧バージョンのアプリアイコンが
削除され、新バージョンのアプリアイコンが追加されます。

旧バージョン

新バージョン

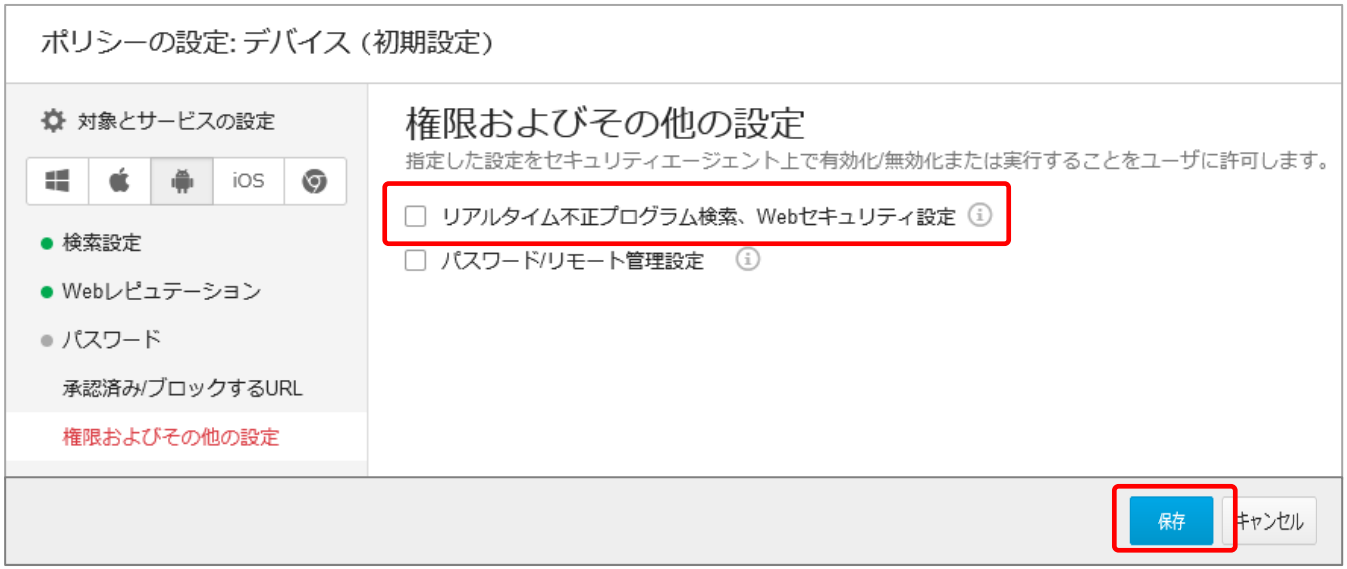
⑥初回スキャン後、移行完了となります。
⇒次ページの「移行後の確認事項」をご確認ください。

14. 新エージェントへ移行（Android） 6 / 7

■移行後の確認事項
旧エージェントにて下図の赤枠部分を有効にしていた場合、
設定は移行されないため、再度設定を行う必要があります。

①管理コンソール上にて「リアルタイム不正プログラム検索、Webセキュリティ設定」を
チェック後、設定を保存してください。

【管理コンソール > セキュリティエージェント > 任意のグループ > ポリシーの設定 > Androidのアイコン >
権限およびその他の設定 】

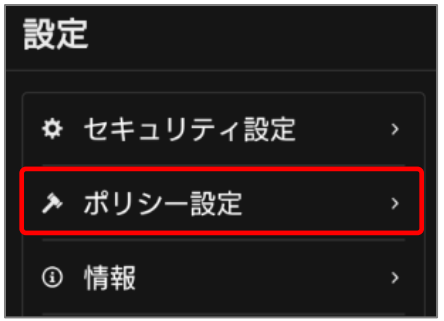


⇒次ページに進んでください

14. 新エージェントへ移行（Android） 7 / 7

②Android端末にて「Mobile Security」アプリを起動後、
画面下部の「設定」を選択します

③表示された一覧から「ポリシー設定」を選択します。



④ 「①」の手順にて設定権限を与えた、「リアルタイム不正プログラム検索、Webセキュリティ設定」について、任意の設定を行ってください。
※右図は「不正プログラムのリアルタイム検索」設定の例です。

15. 新エージェントへ移行（iOS） 1 /6

iOS端末にてエンドポイントセキュリティの旧エージェントを使用している方は、必ずアンインストールを実施してください。その後、新エージェントへの移行作業を実施してください。
※ エンドポイントセキュリティは「ウイルスバスタービジネスセキュリティサービス」を指します。
※ ご新規ユーザーの方は「17.インストール（iOS）事前準備 」へお進みください。

■エンドポイントセキュリティ 旧エージェント(Ver2.0未満)をご利用中の場合は、
下記手順の実施をお願いします。
- 16. 証明書の更新について
- 15. 新エージェントへ移行（iOS）
- 17. インストール（iOS）事前準備
- 18. インストール（iOS）

■新エージェント概要
①各機能の追加
- Webレピュテーション
- Wi-Fi保護
- 設定マネージャ
- モバイル検索
- 承認済み/ブロックするURLリスト

②アプリタイプのエージェントとして登場

■移行対象者
iOS端末にてエンドポイントセキュリティ バージョン(2.0未満)をご利用の方

■移行対象期間
2024年4月22日～2025年4月30日
※2025年5月1日からエンドポイントセキュリティ バージョン（2.0未満）はサポート対象外となります。

※旧エージェントのアンインストールを行います。
　下記いずれかの手順にてアンインストールを実施してください

- Web管理コンソールからアンインストールする場合
  該当ページ「15..新エージェントへ移行（iOS） 2/6 ～ 4/6」

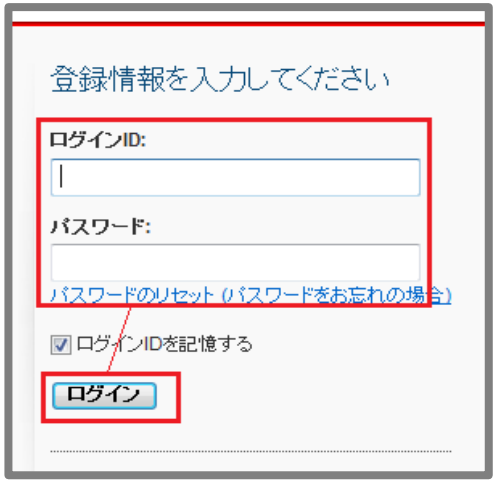
- iOSデバイスからアンインストールする場合
  該当ページ「15.新エージェントへ移行（iOS） 5/6 ～ 6/6」

■移行手順　Web管理コンソールからアンインストールする場合

管理者がWeb管理コンソールから操作します。

①パソコンのブラウザ（Google ChromeまたはSafari）にて、
　管理コンソールにアクセスします。

②ログインIDとパスワードを入力し、
　「ログイン」ボタンをクリックします



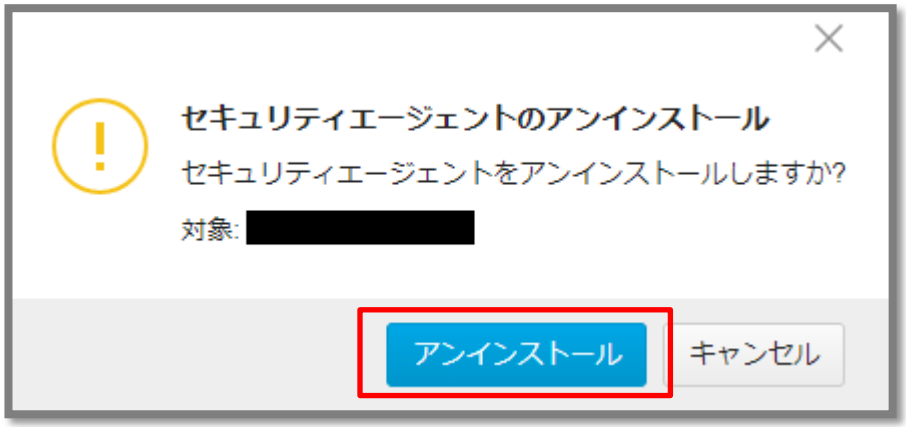
■移行手順　Web管理コンソールからアンインストールする場合

③登録済みの製品/サービスから「ウイルスバスター ビジネスセキュリティサービス」欄を確認し、「コンソールを開く」をクリックします。

④メニューから［セキュリティエージェント］をクリックし、表示された一覧からアンインストールを行いたいエンドポイント(iOS)のチェックボックスにチェックを入れ、［タスク］→［セキュリティエージェントのアンインストール］をクリックします。

■移行手順　Web管理コンソールからアンインストールする場合

⑤ポップアップが表示されますので［アンインストール］をクリックします。



⑥「コマンドが送信されました」のメッセージがコンソール上に表示されます。
クライアントツリーからも該当のクライアントが消えます。

Web管理コンソール上での作業は以上で終了です。iOS側での操作は必要ありません。

■移行手順　iOSデバイスからアンインストールする場合

iOSデバイス上で操作します。
①[設定] >　[一般]　> [プロファイルとデバイス管理]　を開き、「Trend Micro Worry-Free Business Security Service」をタップします。

②「削除」をタップし、パスコードを入力します。

■移行手順　iOSデバイスからアンインストールする場合

③［プロファイル] から削除されます。iOSデバイス上での操作は以上です。

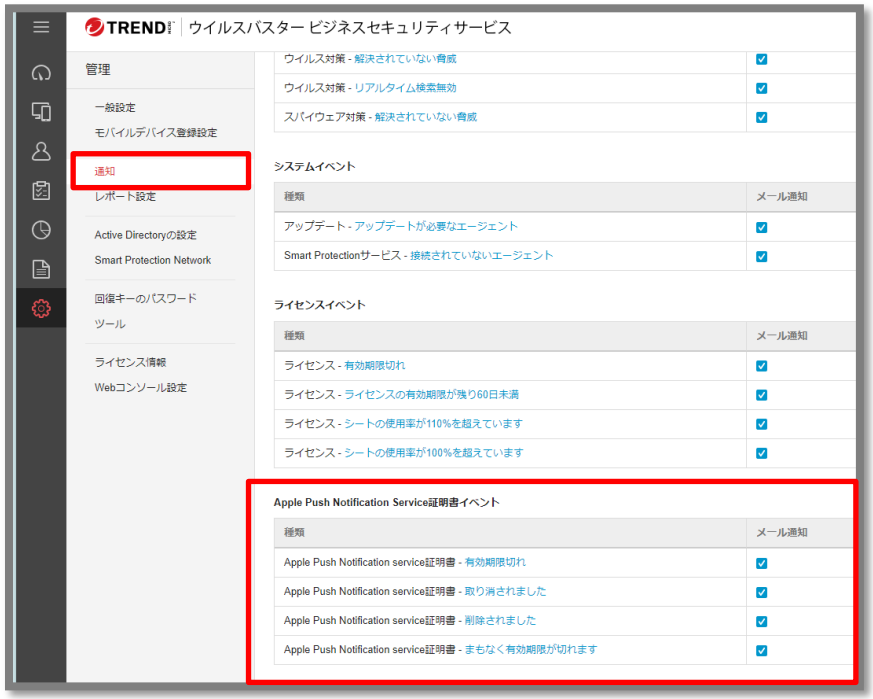
※iOSデバイス上のアンインストールをネットワークに未接続の状態で行った場合、
Web管理コンソールのクライアントツリーにデバイス情報が残ったままとなります。
別途削除してください。

16.証明書の更新について　1/4

iOSデバイスを管理するために、エージェントのインストールと有効なAPNs証明書が必要になります。
APNs証明書の有効期限は1年間有効となりますので、必ず期限が切れる前に更新いただきますよう
お願いいたします。

有効期限につきまして、Web管理コンソールの
以下設定により、証明書イベントを通知することもできます。（デフォルトは有効）
[管理] > [通知] > [要確認]タブ > 「Apple Push Notification Service証明書イベント

• 通知設定の確認画面



• 証明書の有効期限の確認画面

16.証明書の更新について　2/4

①パソコンのブラウザ（Google ChromeまたはSafari）にて、管理コンソールにアクセスし、ログインします。
ユーザ登録時に設定した「ログインID」と「パスワード」を入力して、「ログイン」ボタンをクリックします。

②「コンソールを開く」をクリックしてウイルスバスター ビジネスセキュリティサービスのコンソールを開きます。

③ 「管理」タブをクリックし、「モバイルデバイス登録設定」メニューをクリックします。

④登録されている証明書が表示されるため、「証明書の削除」をクリックします。

16.証明書の更新について 3/4

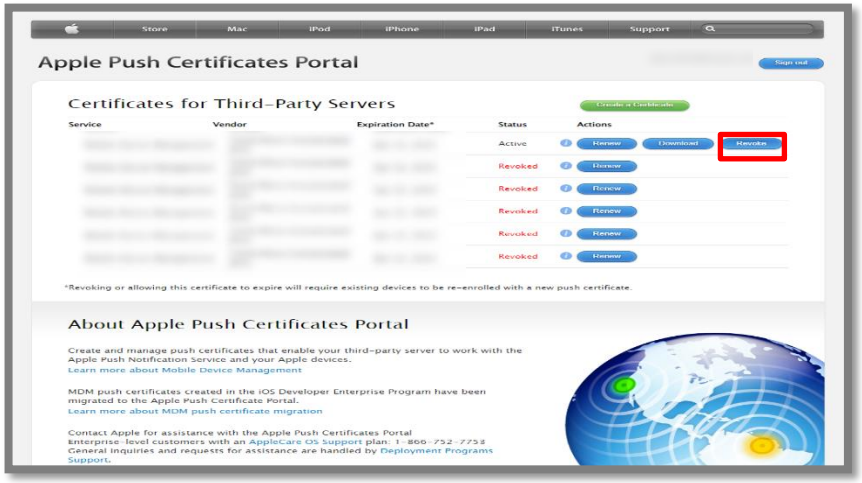
⑤Apple Push Nodification Service証明書を
削除の確認が表示されますので、
「削除」をクリックします。

⑥管理コンソール上で証明書が削除されたことを
確認します。

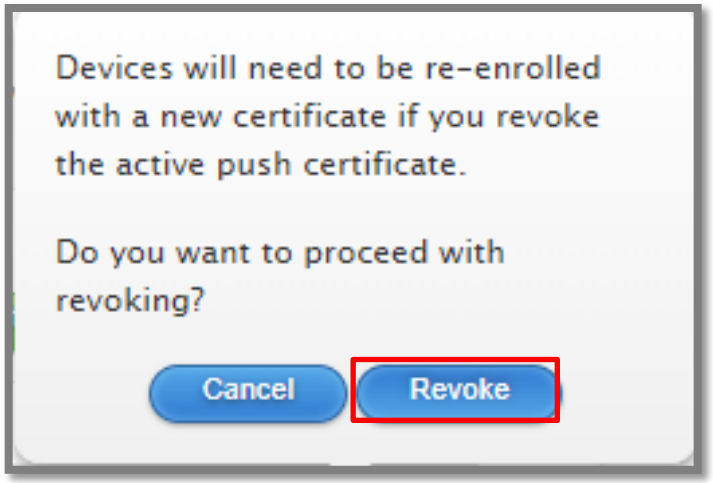
⑦Appleの
Apple Push Certificate Portal サイト
（ https://identity.apple.com/pushcert ）へ
アクセスし、Apple IDを使ってサインインします。
(SafariまたはGoogle Chromeを使用してアクセスしてください。
その他のブラウザの場合、表示が崩れたり正しい証明書が作成できないことがあります。)

16.証明書の更新について　4/4

⑧ Certificates for Third-Party Servers画面が表示されますので、該当証明書列の「Revoke」をクリックします。



⑨削除するかどうか確認の画面が表示されますので、「Revoke」をクリックします。



⑩15. 新エージェントへ移行（iOS）1/6を参照のうえアンインストールの手順を実施ください。

⑪18.インストールを参照のうえインストールの手順を実施ください。

証明書の更新（削除）については、以上になります。
後続の手順にて新規証明書のインストールを行ってください。

Step 1 ＞ APNs 証明書の作成および登録

①パソコンのブラウザ（Google ChromeまたはSafari）にて、管理コンソールにアクセスし、ログインします。
ユーザ登録時に設定した「ログインID」と「パスワード」を入力して、「ログイン」ボタンをクリックします。

②「コンソールを開く」をクリックしてウイルスバスター ビジネスセキュリティサービスのコンソールを開きます。

③「管理」タブをクリックし、「モバイルデバイス登録設定」メニューをクリックします。

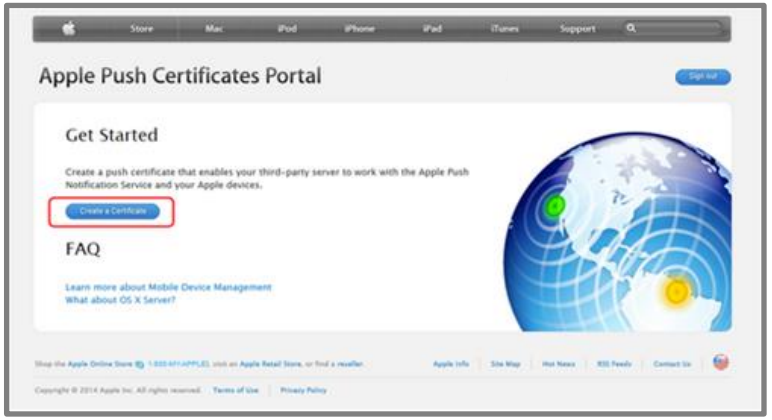
④「デバイス登録設定」画面が表示されます。「APNs証明書のアップロード」ボタンをクリックします。

⑤「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。

⑥ Appleのサイトで証明書を作成します。
Apple Push Certificate Portal サイト（ https://identity.apple.com/pushcert ）へアクセスし、Apple IDを使ってサインインします。
(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。)

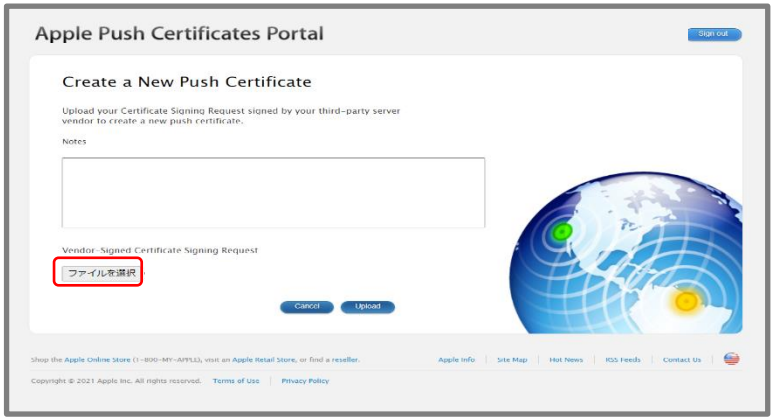
管理コンソール

⑦ Get Started画面が表示されます。
「Create a Certificate」ボタンをクリックします。

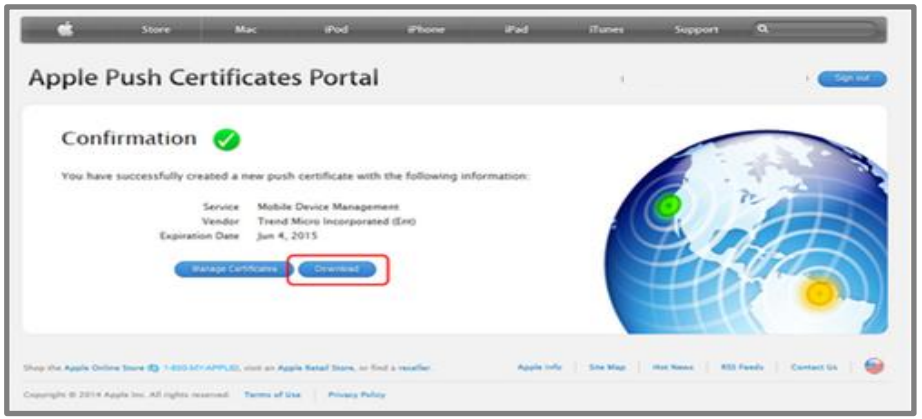


⑧ 「Terms of Use」画面が表示されます。内容を確認の上、「I have read and agree to these terms and conditions.」にチェックを入れ、「Accept」ボタンをクリックします。

⑨ 「Create a New Push Certificate」画面が表示されます。「参照」をクリックし、手順1.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。



⑩ 「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。



⑪管理コンソールへ戻り、6で使用したApple IDを入力します。その後、「ファイルの選択」をクリックし、10で作成したAPNs証明書をアップロードします。
アップロードした証明書が表示されます。

17. インストール（iOS）事前準備 4/5

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します。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保存します。
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面をご用意していますが、お客様のご利用環境にあ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。

iOSデバイスを管理するために、エージェントのインストールと有効なAPNs証明書が必要になります。
APNs証明書の有効期限は1年間有効となりますので、必ず期限が切れる前に更新いただきますようお願いいたします。

Step 2 ＞ インストール情報の取得

①「セキュリティエージェント」タブをクリックし、
表示された画面内の「＋セキュリティエージェントの追加」ボタンをクリックします。

②デバイスの追加画面が表示されます。

該当のデバイスをクリックし、１つ目の項目にある「メールコンテンツの表示」をクリックします。

③次の2つの情報を取得します。

- インストール用のリンク
- 認証コード

iOSデバイスへインストールの際、この2つの情報が必要となります。

「テキストのコピー」で内容をコピーしてメモ帳などに保存するか、もしくは「メールの送信」をクリックしてインストールを行う デバイスへ内容を送信します。

18. インストール（iOS）1/10

Step 3 ＞ iOSデバイスへのインストール
①iOS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認証コードを入力します。

[Step2-③] で確認した認証コードを入力し、
[続行] をタップします。

③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。

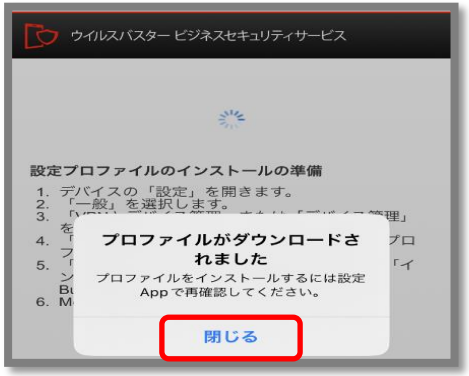
18. インストール（iOS）2/10

④プロファイルのダウンロードを実施します。
確認の上、「続行」をタップします。

⑤構成プロファイルのダウンロード許可を求める画面が
表示されますので、「許可」をタップします。

18. インストール（iOS）3/10

⑥ダウンロード完了画面が表示されますので、
「閉じる」をタップし、ホーム画面から［設定］→［一般］
を開きます。

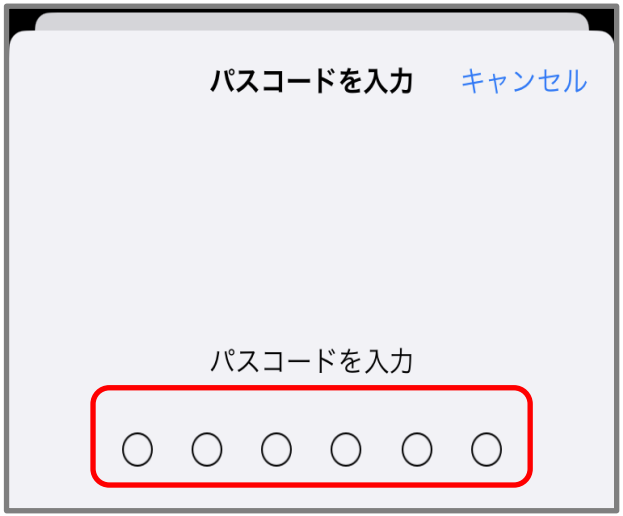


⑦[VPNとデバイス管理]を開き、
該当の「ダウンロード済みプロファイル」から
「Trend Micro Worry-Free Business Security
Services」をタップします。

18. インストール（iOS）4/10

⑧プロファイルのインストール画面が表示されましたら、
「インストール」をタップします。

⑨パスコードを入力します。



18. インストール（iOS）5/10

⑩警告画面が表示されましたら内容を確認の上、
「インストール」をタップします。

⑪リモート管理画面が表示されましたら、
「信頼」をタップします。

18. インストール（iOS）6/10

⑫インストール完了画面が表示されましたら、
「完了」をタップします。

⑬Appのインストールの画面が表示されましたら、
「インストール」をタップします。

18. インストール（iOS）7/10

Step 4 ＞ iOSデバイスへのインストール

①App storeの画面が表示されましたら、
「インストール」をタップします。

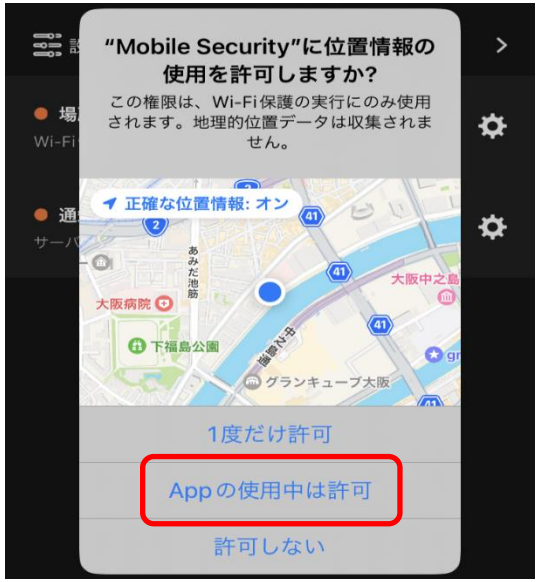
②Appleのサインイン・認証を完了後、
インストールが開始します。

③iOSのホーム画面にアプリが表示されていることを確認し、開きます。

18. インストール（iOS）8/10

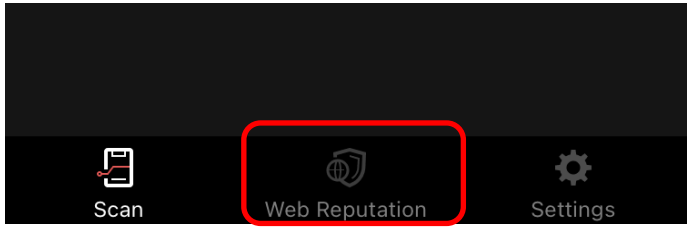
④通知方法の画面が表示されますので、「許可」を選択します。

⑤位置情報の使用を許可の画面が表示されますので、
「Appの使用中は許可」を選択します。

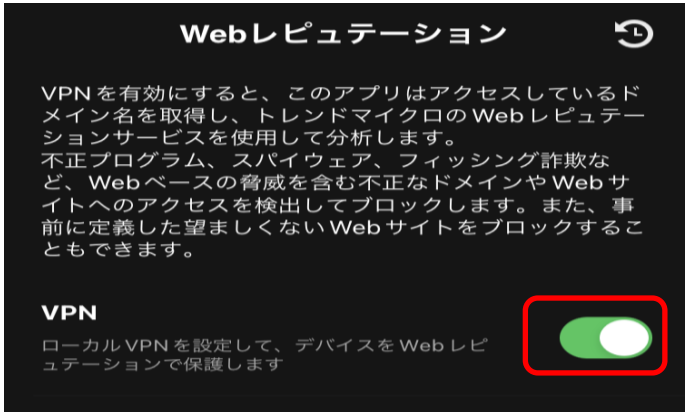


18. インストール（iOS）9/10

⑥アプリ画面内の下部にある
Web Reputationをタップします。



⑦Web Reputationで、VPNをオンにします。
VPN構成の追加の画面が表示された場合、「許可」をタップします。



18. インストール（iOS）10/10

■登録の確認

①管理コンソールにアクセスし、ログインします。
ユーザ登録時に設定した「ログインID」と「パスワード」を入力して、「ログイン」ボタンをクリックします。

②「セキュリティエージェント」タブをクリックし、表示された画面内にインストールを実施したiOSデバイスが登録されていることを確認します。

iOSのインストール手順につきましては、
以上になります。

19. 機能を設定する（Windows） 1/16

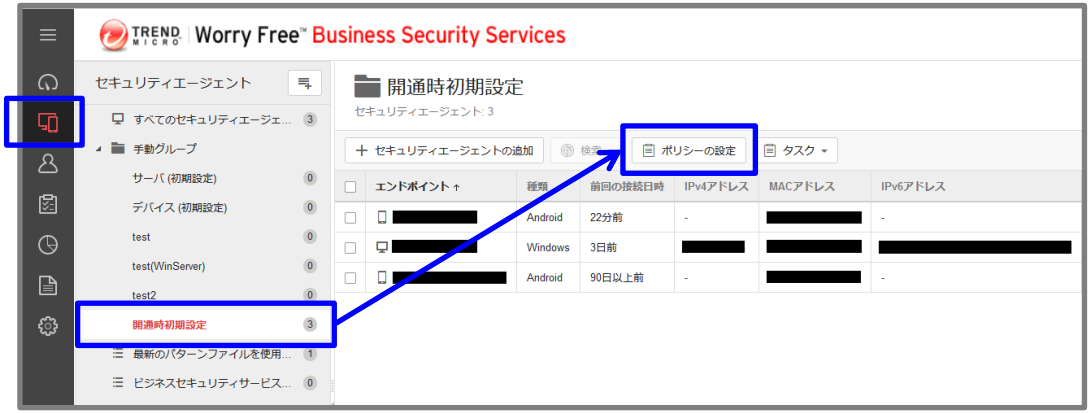
初期設定値として、以下の機能が設定されております。ご利用環境やセキュリティポリシーに応じて、設定の変更をお願いいたします。

機能	初期設定値	お客様にて設定可能な項目	ページ番号
ウイルス対策	スマートスキャン	スマートスキャン	
Webレピュテーション	有効（中）	低/中/高より選択	95
ファイアウォール	無効	有効/無効から選択	96
挙動監視	有効	有効/無効から選択	97
ランサムウェア対策機能	有効	有効/無効から選択	98
機械学習型検索	無効	有効/無効から選択	99
URLフィルタリング	有効（低）	低/中/高/カスタムより選択 業務時間設定が可能	100
承認済み/ブロックURL登録	無し	追加登録可	101
アプリケーションコントロール	無効	有効/無効から選択 （対象アプリケーションを指定可）	102
デバイスコントロール	無効	有効/無効から選択 （権限選択可）	104
エージェントアンインストール防止	無効	有効（パスワード設定）	108
アラート設定	有効	アラート受信者の変更・追加	109

※Mac、Android、iOSの設定方法については、トレンドマイクロ社のWEBページを参照下さい。
（https://docs.trendmicro.com/ja-jp/documentation/article/worry-free-business-security-services-67-server-help-policy-management_001 ）

19.機能を設定する（Webレピュテーション） 2/16

①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」



②「Webレピュテーション」を選択

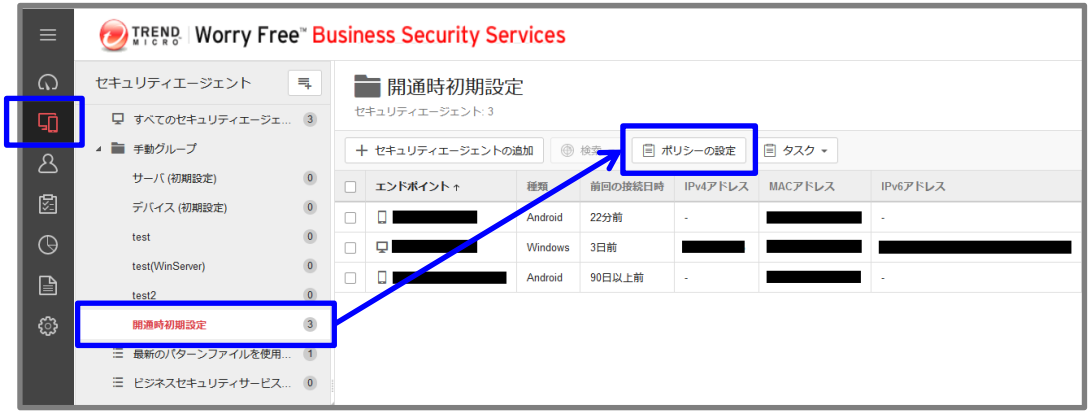
③セキュリティレベルを選択します。
（低・中・高）
※初期値は「中」となっております。

④ブラウザ脆弱性対策機能を有効にする
場合は、「不正スクリプトを含むページを
ブロックする」にチェックを入れます。

⑤「保存」をクリックします。

19.機能を設定する（ファイアウォール）　3/16

①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」

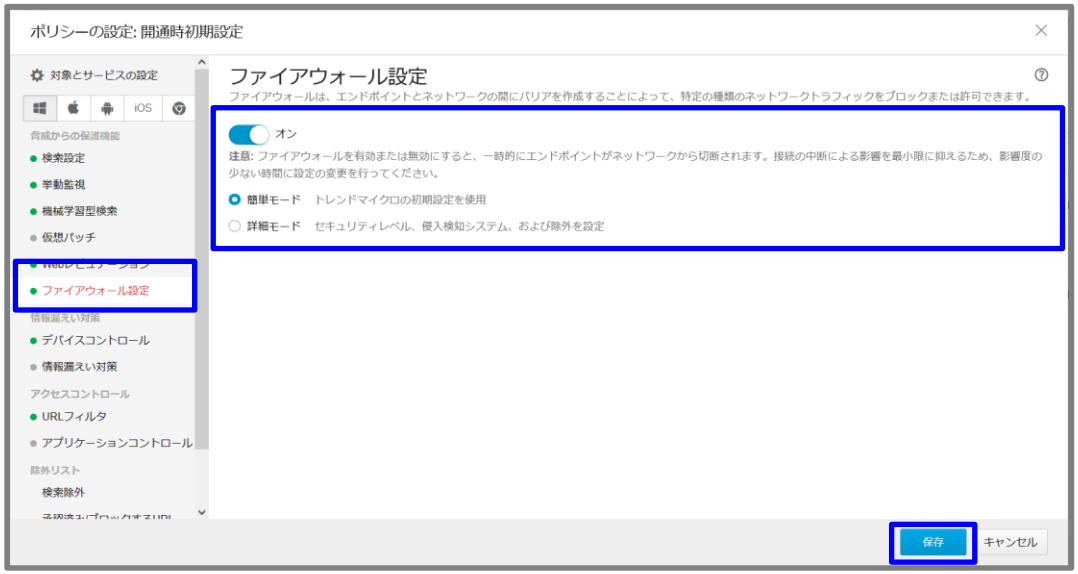


②「ファイアウォール」を選択

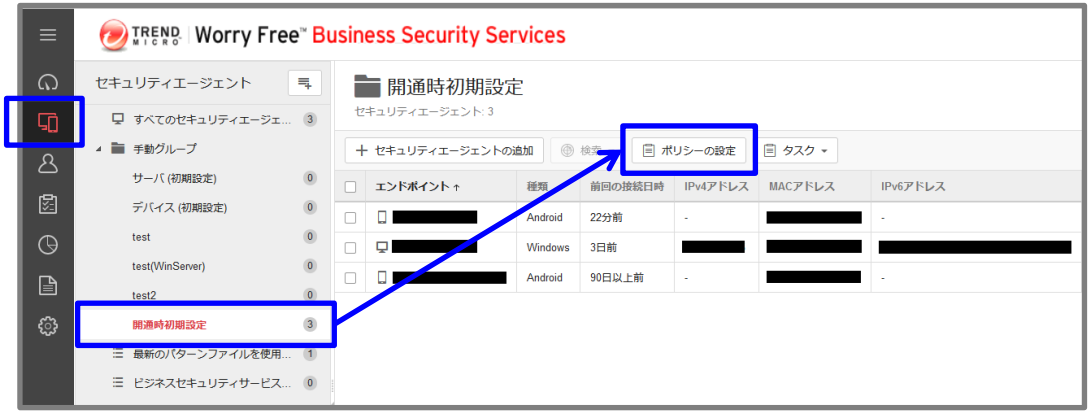
③有効にする場合、チェックを入れます。

④簡易モード/詳細モードを選択します。

⑤「保存」をクリックします。



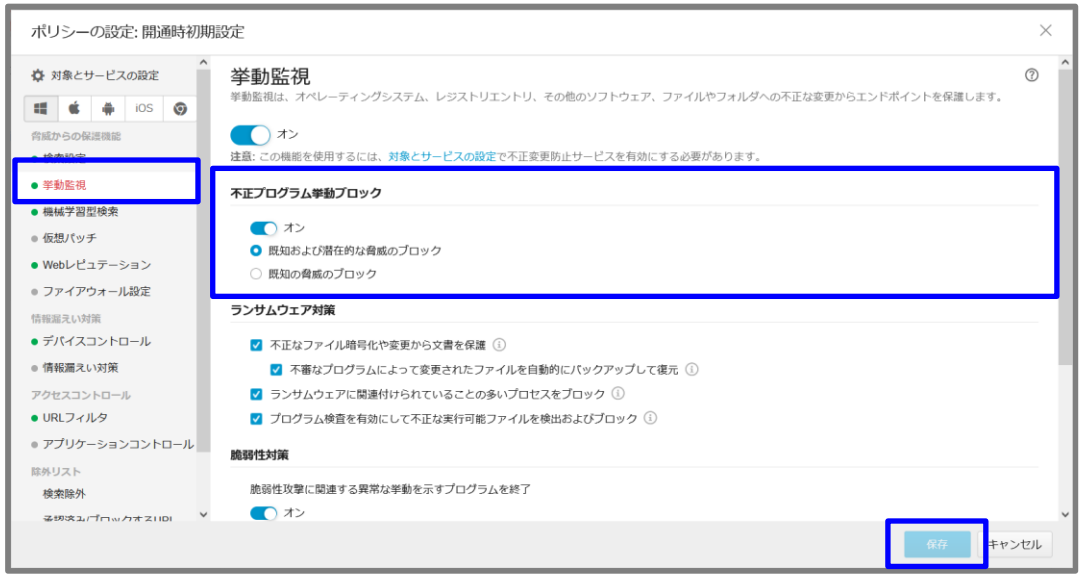
①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」



②「挙動監視」を選択

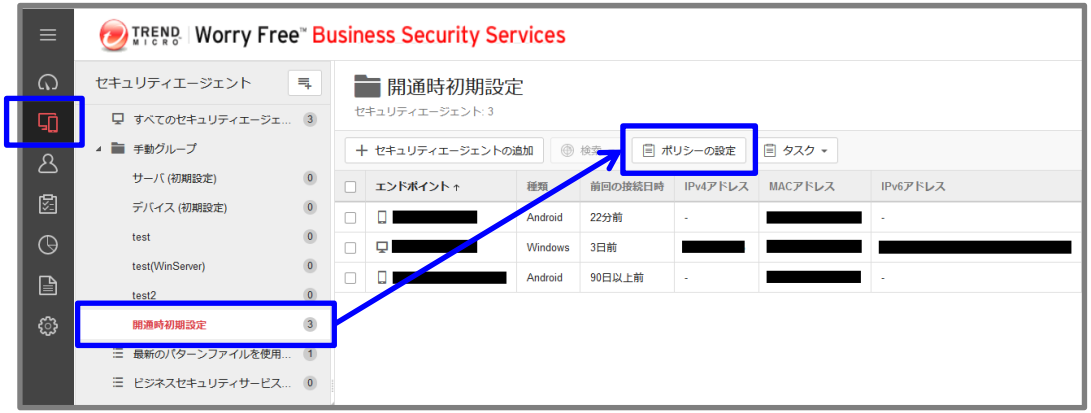
③不正プログラム挙動ブロックの内
有効にする項目にチェックを入れます。

④「保存」をクリックします。



19.機能を設定する（ランサムウェア対策）　5/16

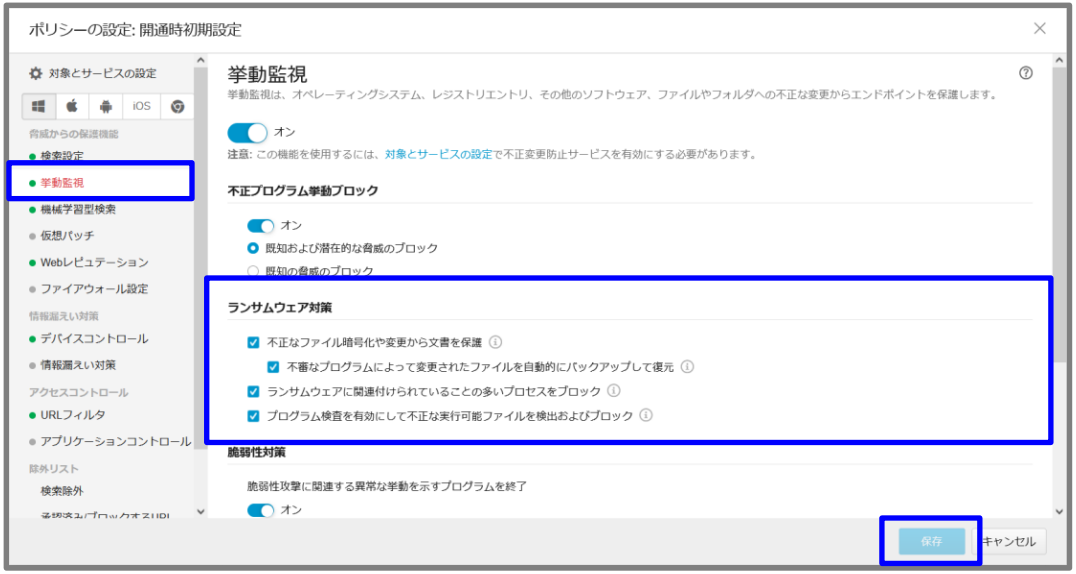
①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」



②「挙動監視」を選択

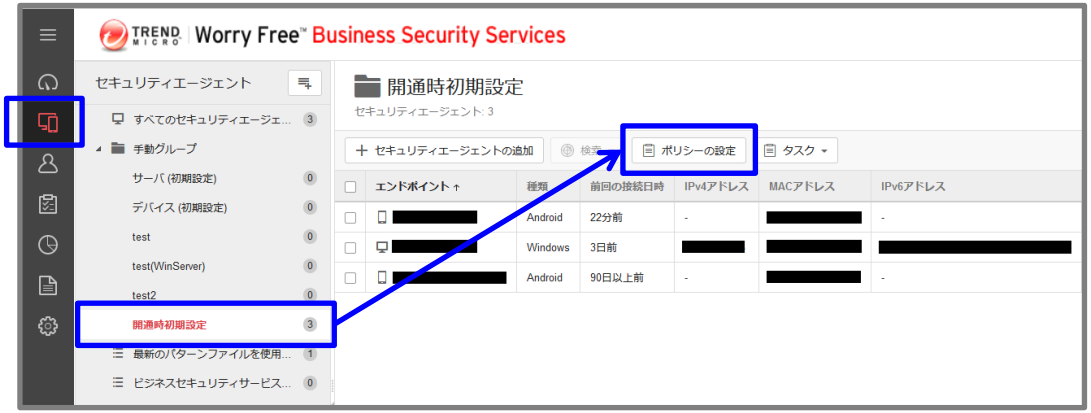
③「ランサムウェア対策」にて、
設定変更を行います。
※初期値はすべて「有効」と
なっています。

④「保存」をクリックします。



19.機能を設定する（機械学習型検索）　6/16

①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」



②「機械学習型検索」を選択

③機械学習型検索を有効化する場合は、
チェックを入れます。

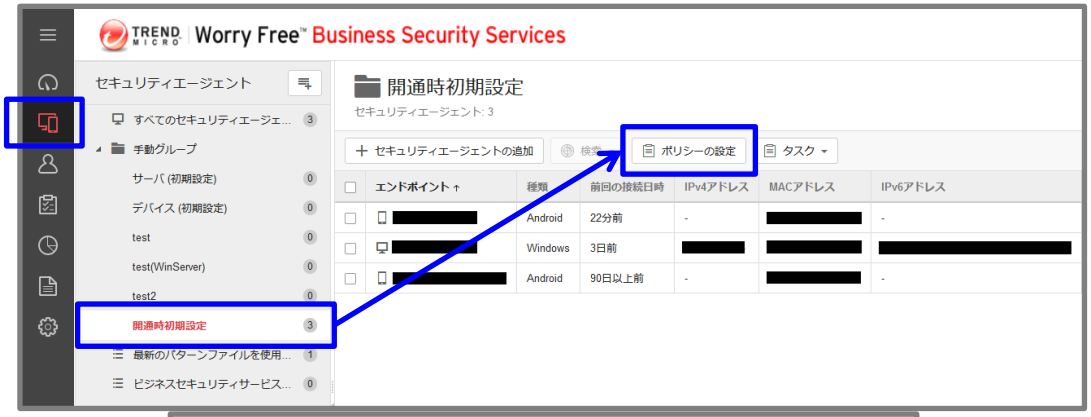
④ファイルに対する処理を選択します
⇒隔離 or ログのみ

⑤プロセスに対する処理を選択します
⇒終了 or ログのみ

⑥「保存」をクリックします。

19.機能を設定する（URLフィルタリング）　7/16

①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」



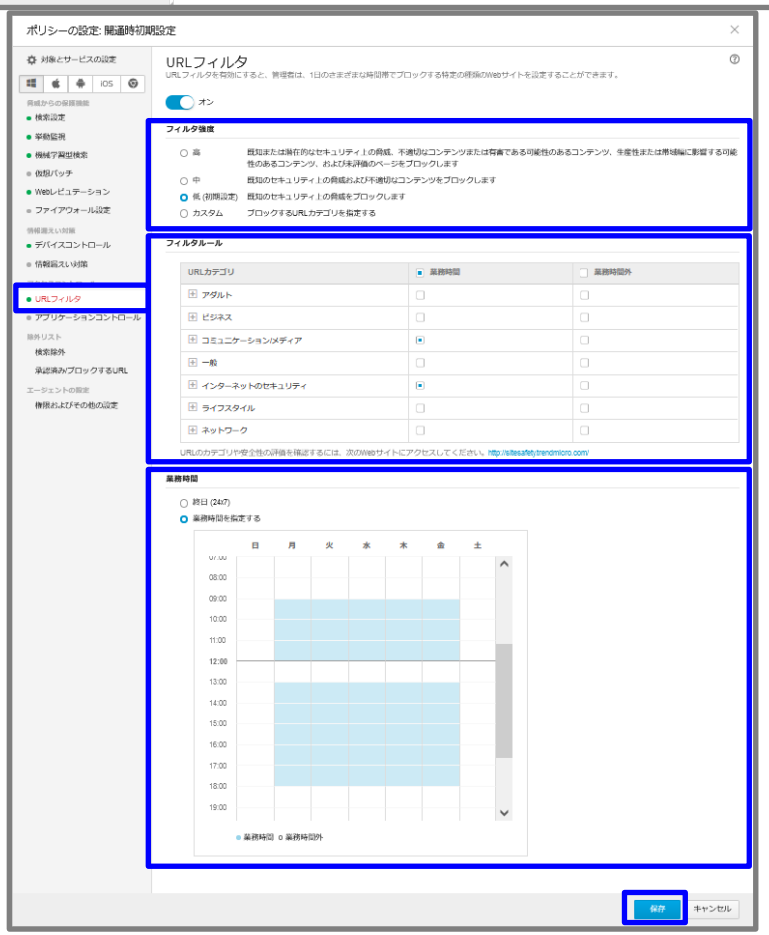
②「URLフィルタ」を選択

③フィルタ強度を選択
（低・中・高・カスタム）
※初期値は「低」となっております。

④フィルタルールにて、
ブロック対象のURLカテゴリを指定します。
※初期値は
「インターネットのセキュリティ」が
有効となっております。

⑤フィルタリングを適用する時間を指定する場合、
業務時間の設定を行います。
※初期値は、「終日（24x7）」となっております。

⑥「保存」をクリックします。



19.機能を設定する（承認済･ブロックURL登録）　8/16

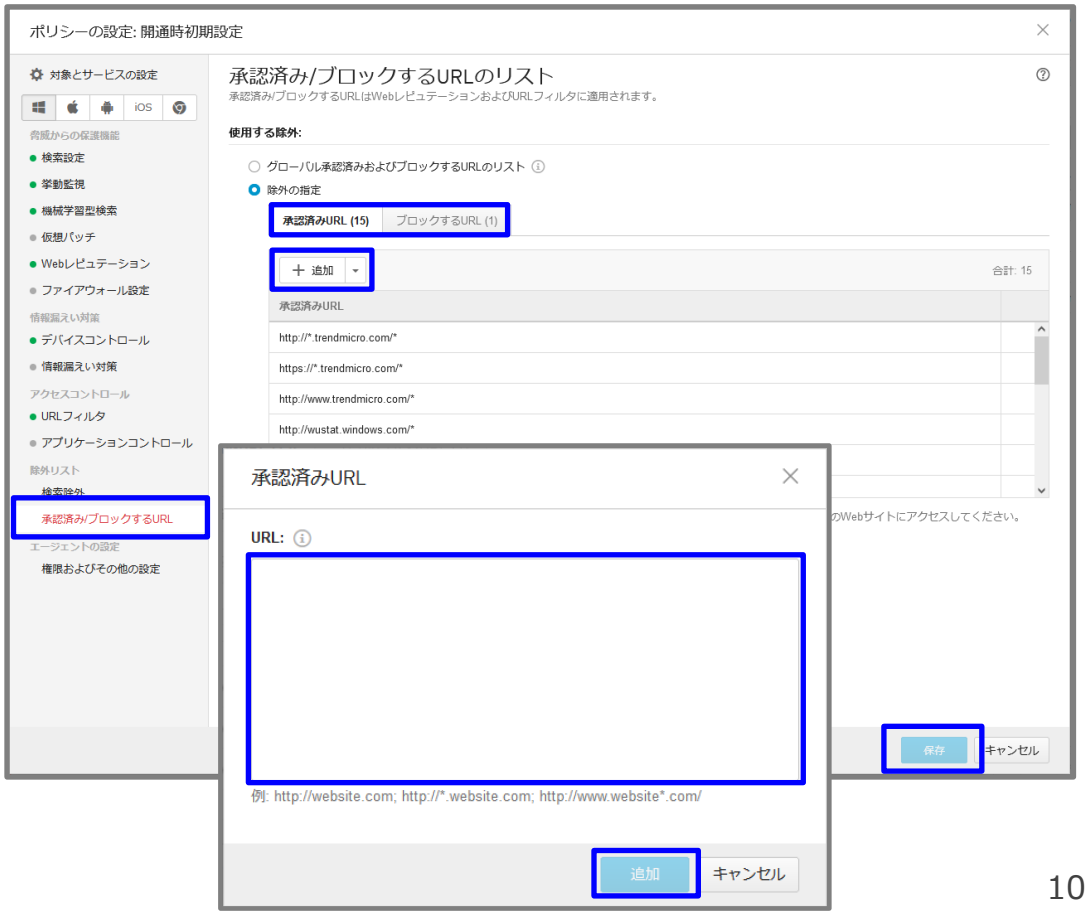
①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」

②除外登録を行う場合は、
「承認済みURL」タブを選択。
ブロック登録を行う場合は、
「ブロックするURL」タブを選択。
除外登録は③へ
ブロック登録は④へ

③除外登録を行う場合、「＋追加」を
クリックし、承認済みURL にURLを
入力し、「追加」をクリック。
※登録したURLはWebレピュテーション
およびURLフィルタ機能の除外対象に
なります。

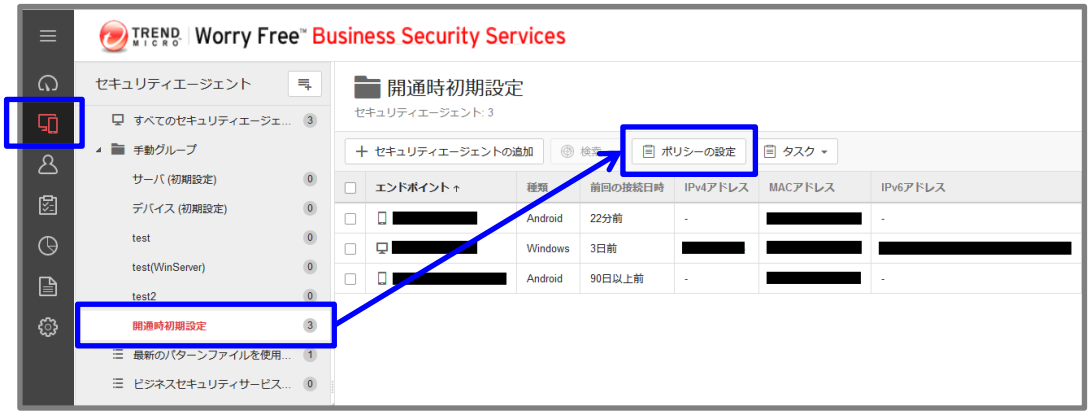
④ブロック登録を行う場合、「＋追加」を
クリックし、ブロックするURL に
URLを入力し、「追加」をクリック。

⑤「保存」をクリックします。



19.機能を設定する（アプリケーションコントロール）（1/2）9/16

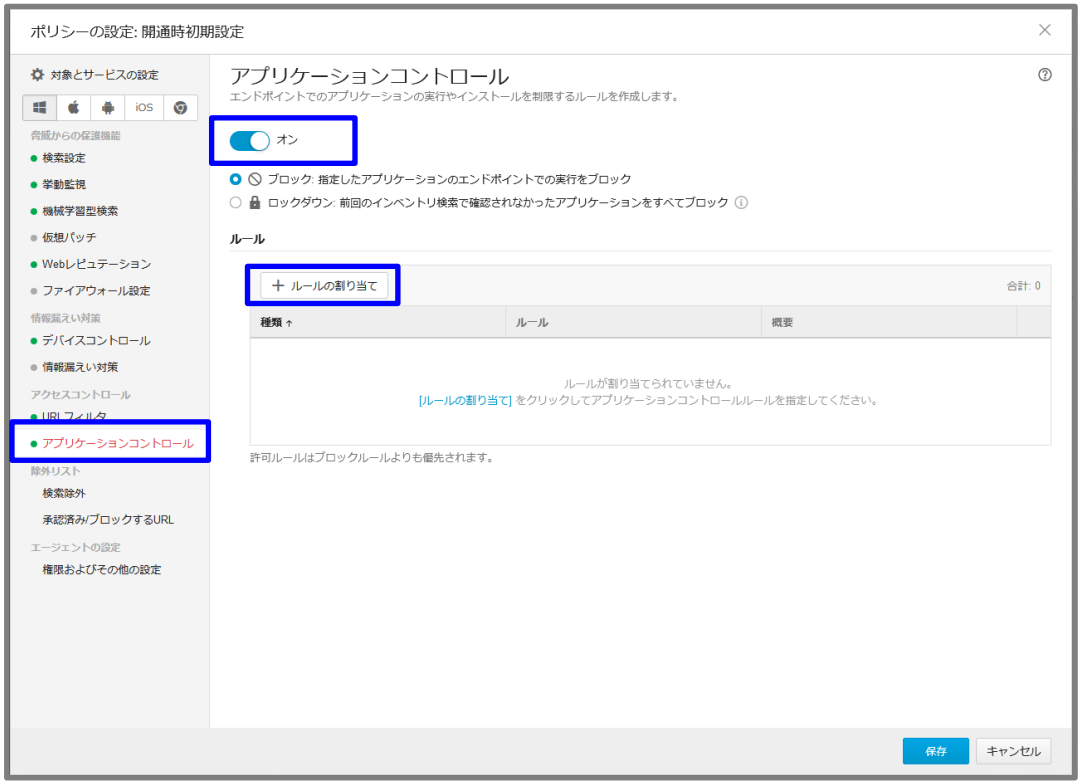
①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」



②「アプリケーションコントロール」を選択

③「アプリケーションコントロールのオンオフ」を「オン」にします。

④ ルールの「＋ルールの割り当て」をクリックしします。



19.機能を設定する（アプリケーションコントロール）（2/2）10/16

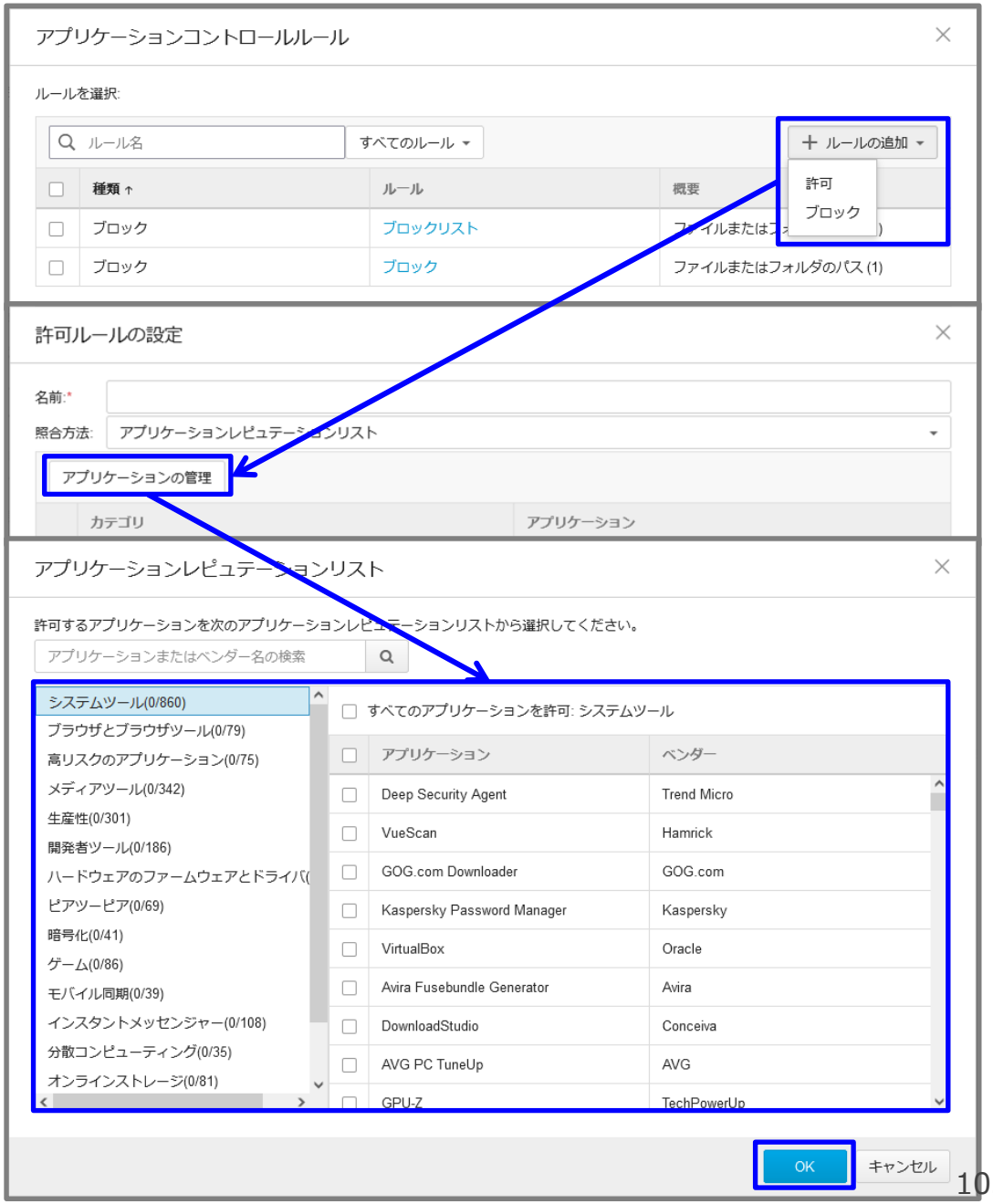
⑤「アプリケーションコントロール」にて、「＋ルールの追加」を選択。

⑥許可を行う場合は、「許可」をクリック。
ブロックを行う場合は、「ブロック」をクリック。
許可は⑦へ
ブロックは⑧へ

⑦許可を行う場合、
「アプリケーションの管理」をクリック。
許可するアプリケーションを☑とし、
「OK」をクリックします。

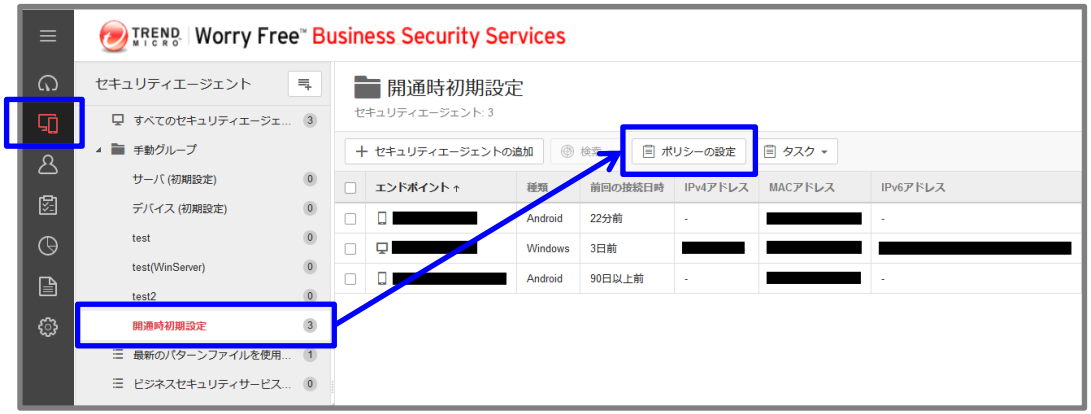
⑧ブロック登録を行う場合、
「アプリケーションの管理」をクリック。
ブロックするアプリケーションを☑とし、
「OK」をクリックします。

⑨「保存」をクリックします。



19.機能を設定する（デバイスコントロール）(1/4) 11/16

①管理コンソールにて、
「ビジネスセキュリティクライアント」
⇒グループを選択⇒「ポリシーの設定」



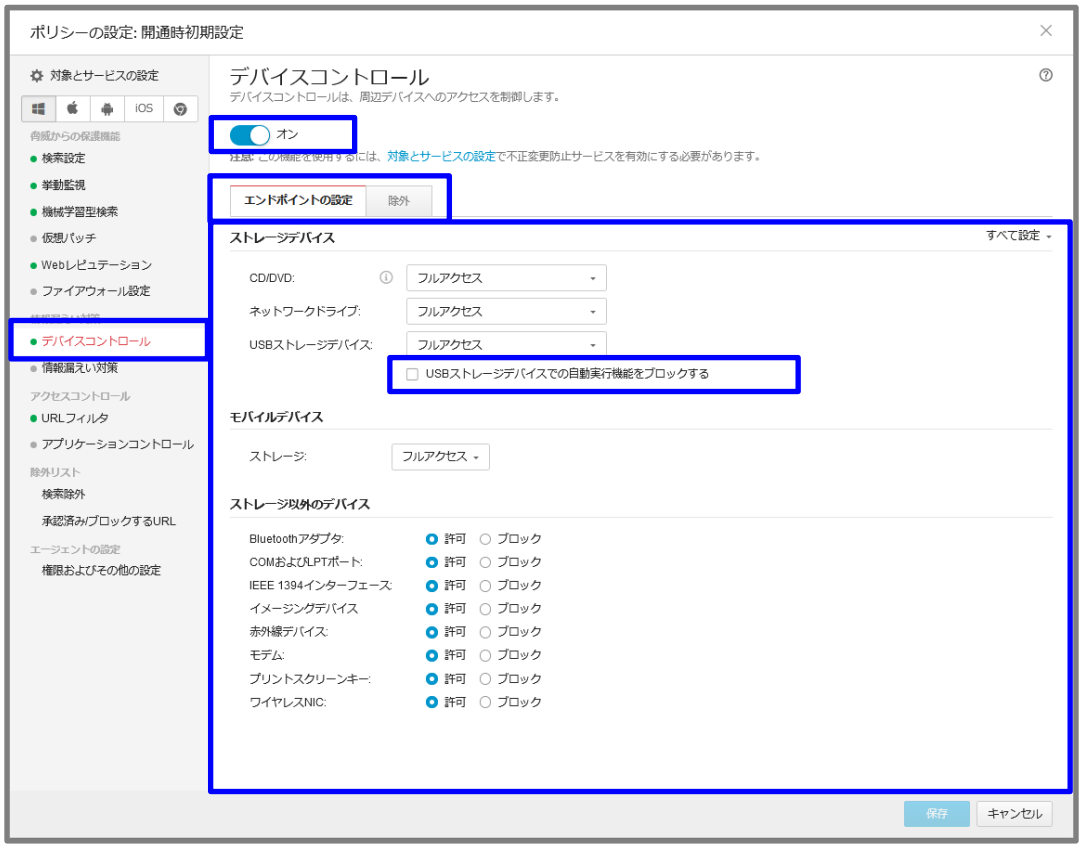
②「デバイスコントロール」を選択

③「デバイスコントロールオンオフ」を
「オン」にします。

④エンドポイントの設定を行う場合は、
「エンドポイントの設定」タブを選択。
除外を行う場合は、
「除外」タブを選択。
エンドポイントの設定は⑤へ
除外は⑥へ

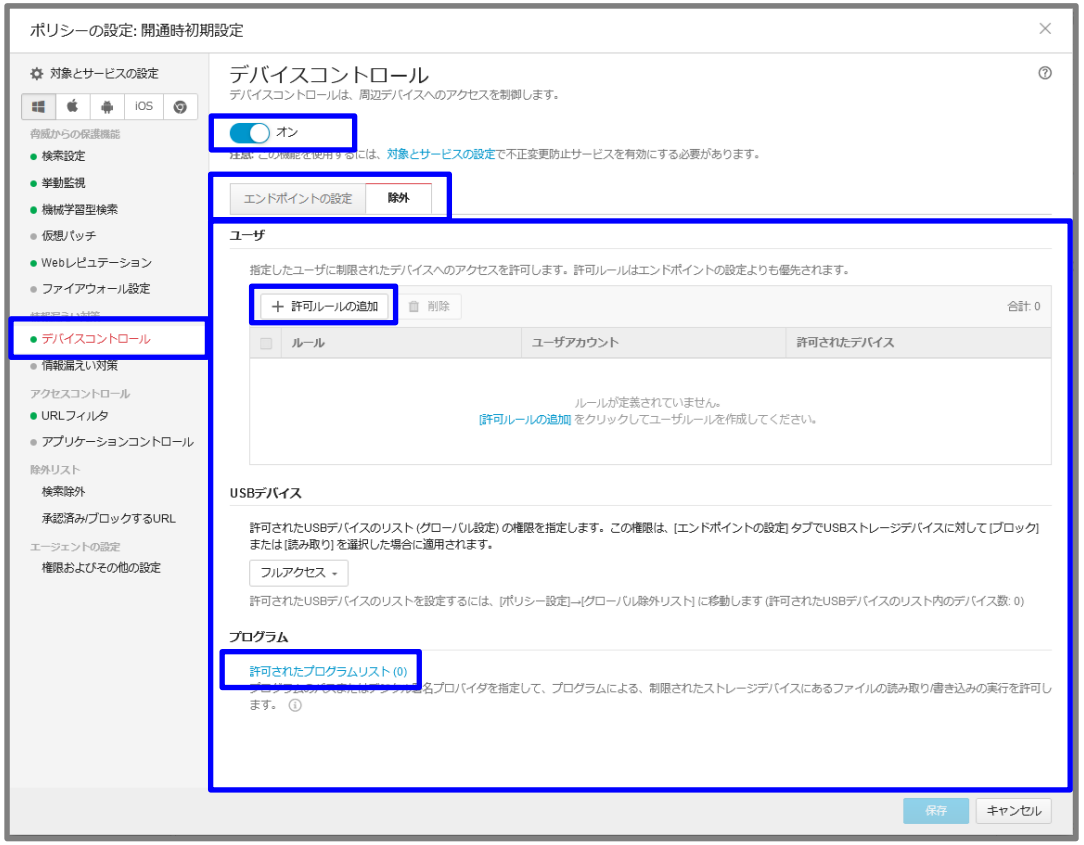
⑤対象のストレージデバイスの権限を
それぞれ選択します。

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場合、
チェックを入れます。



19.機能を設定する（デバイスコントロール）(2/4) 12/16

⑥除外を行う場合、「＋許可ルールの追加」をクリック。



19.機能を設定する（デバイスコントロール）(3/4) 13/16

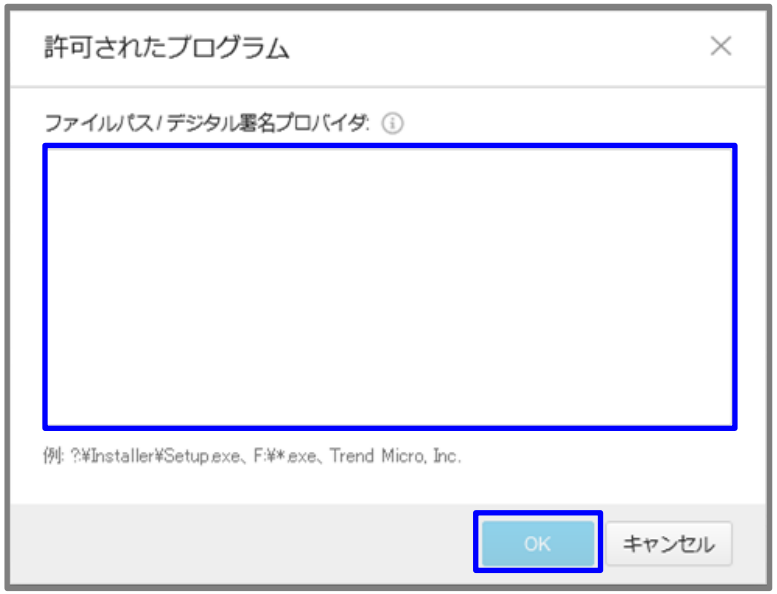
許可ルールにて、「ルール名」を入力。

除外するストレージデバイスを
それぞれ選択します。

19.機能を設定する（デバイスコントロール）(4/4) 14/16

許可されたプログラムリストのリンク先から
許可されたプログラムリストにて、
「＋追加」をクリック。

許可されたプログラムにて、
ファイルパス／デジタル署名プロバイダに
EXEを入力し、「OK」をクリック。



⑦「保存」をクリックします。

19.機能を設定する（アンインストール防止） 15/16

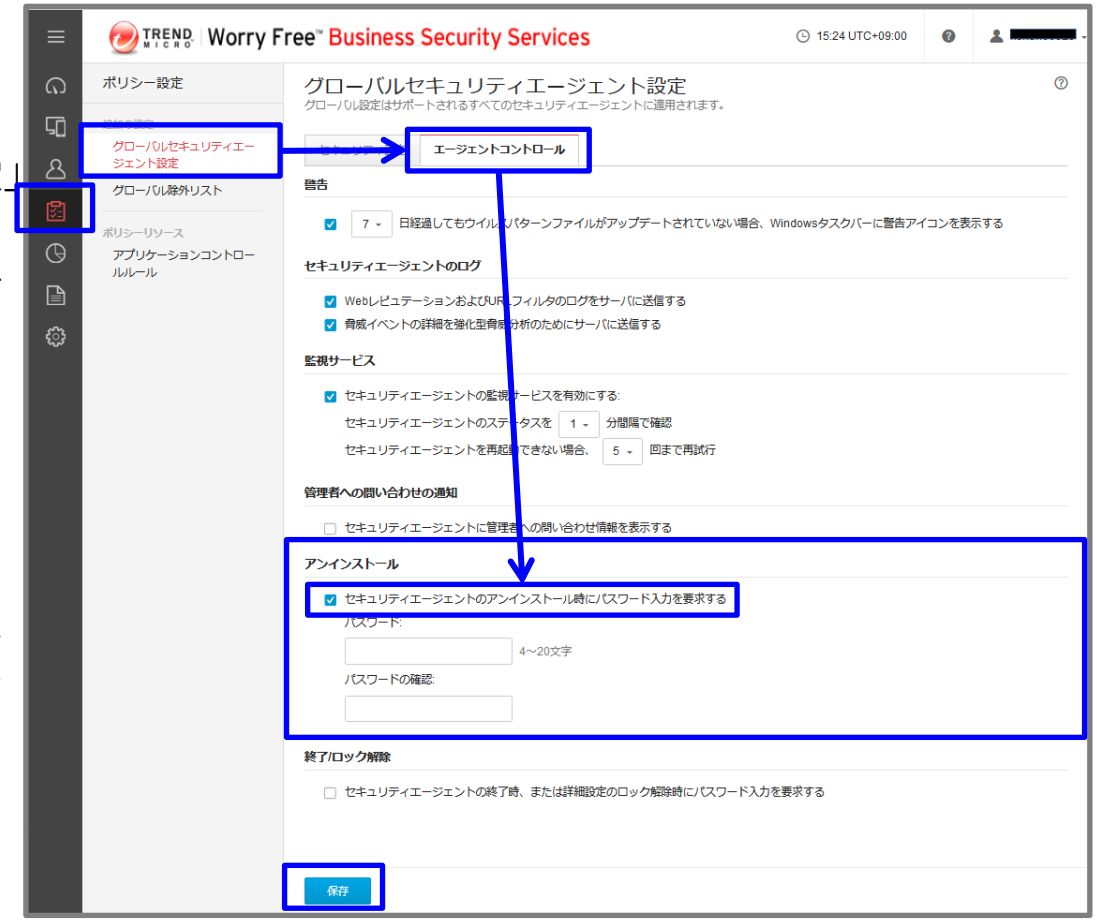
①管理コンソールにて、
「ポリシー」 ⇒
「グローバルセキュリティエージェント設定」

②「エージェントコントロール」タブを選択

③「アンインストール」にて、
「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」にチェックを入れます。

④パスワードを指定します。

⑤「保存」をクリックします。



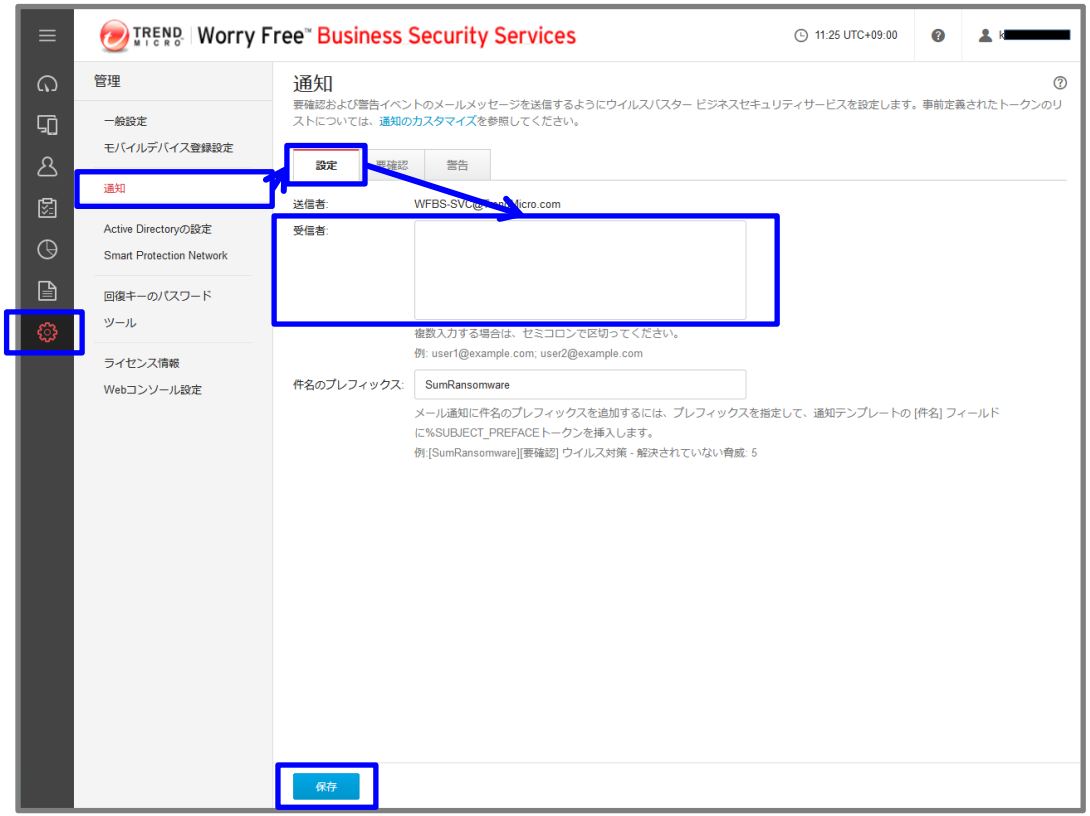
19.機能を設定する（アラート設定） 16/16

①管理コンソールにて、
「管理」⇒「通知」を選択

②「設定」タブを選択

③「受信者」に変更または追加となる
受信者メールアドレスを入力

④ページ下部の「保存」をクリックします。



※注意※
受信者を変更される場合は、サポートセンタにお電話ください。
重要アラートを通知するためのシステムに対し、メールアドレスの変更登録を実施する必要がございます。

20. EDRセキュリティご利用に伴う、既存設定に関する注意点 1/5

■EDRセキュリティご利用に伴う、既存設定に関する注意点

1.EDRセキュリティをご利用いただくにあたり、ご確認いただきたいこと

エンドポイントセキュリティをご利用いただいているお客様で、
下記「2.各種設定項目について」のいずれかの設定を「オフ」にしている場合は、
その設定に関連するEDR機能をご利用いただくことができません。
※デフォルト設定は全て「オン」となっておりますので、「オフ」に変更されている場合にご対応が必要となります。
※設定を「オン」にしていただくことで、関連するEDR機能の提供が可能となります。

2.各種設定項目について　※いずれかがオフの場合は設定変更（3.設定変更について）の対応が必要です。

①Chrome、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：オフ
影響：WebレピュテーションとURLフィルタリングのHTTPS通信検知ログを元とした注意が必要なイベントが
発生しなくなります。

②Web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]：オフ
影響：VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

③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]　：オフ
影響：VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

④Webレピュテーション：オフ
影響：Webレピュテーション検知を元とした、注意が必要なイベントが発生しなくなります。

3.設定確認・変更について
現在の設定の確認及び、各項目を「オン」に変更する手順は、次ページ以降をご参考ください。

20. EDRセキュリティご利用に伴う、既存設定に関する注意点 2/5

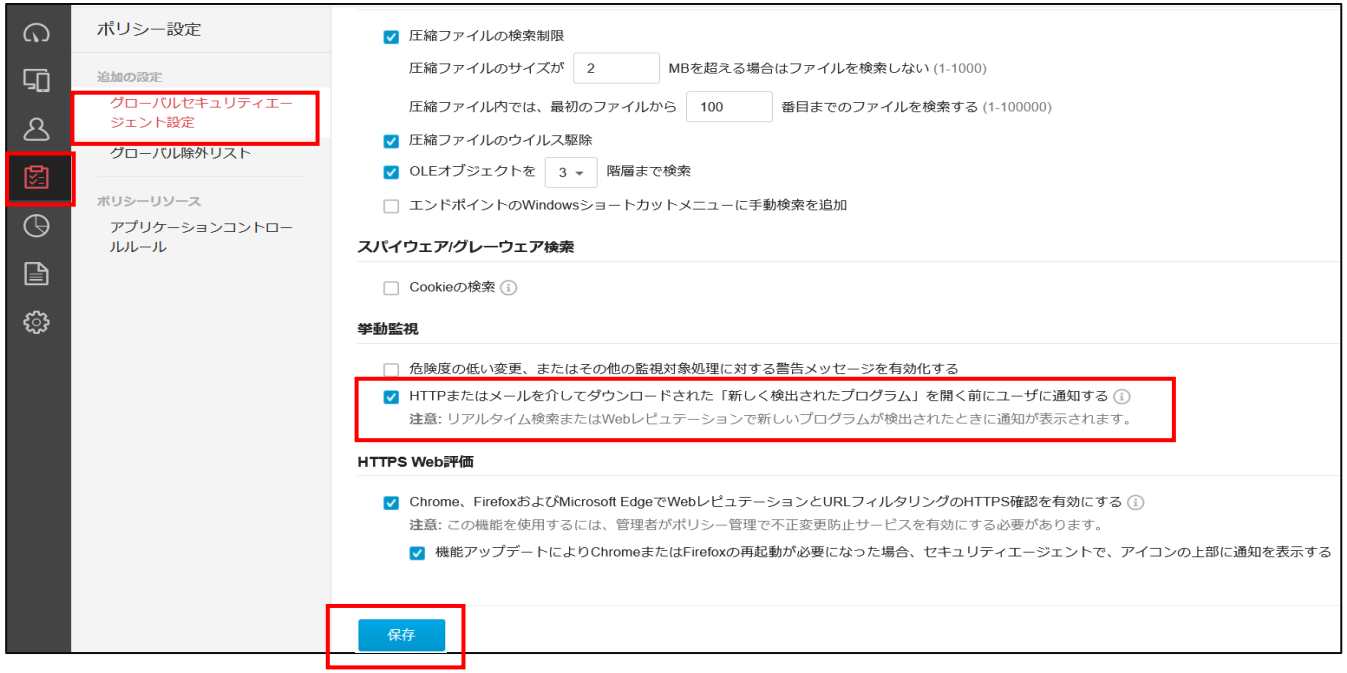
対象者：①[Chrome、FirefoxおよびMicrosoft EdgeでWebレピュテーションとURLフィルタリングのHTTPS確認を有効にする]がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒WebレピュテーションとURLフィルタリングのHTTPS通信検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールへログイン後、
「ポリシー」-「グローバルセキュリティエージェント設定」-「セキュリティ設定」タブにて下記を設定

「HTTPS Web評価」 の項目から
[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]をオン
（チェックを入れた状態）

②保存をクリック



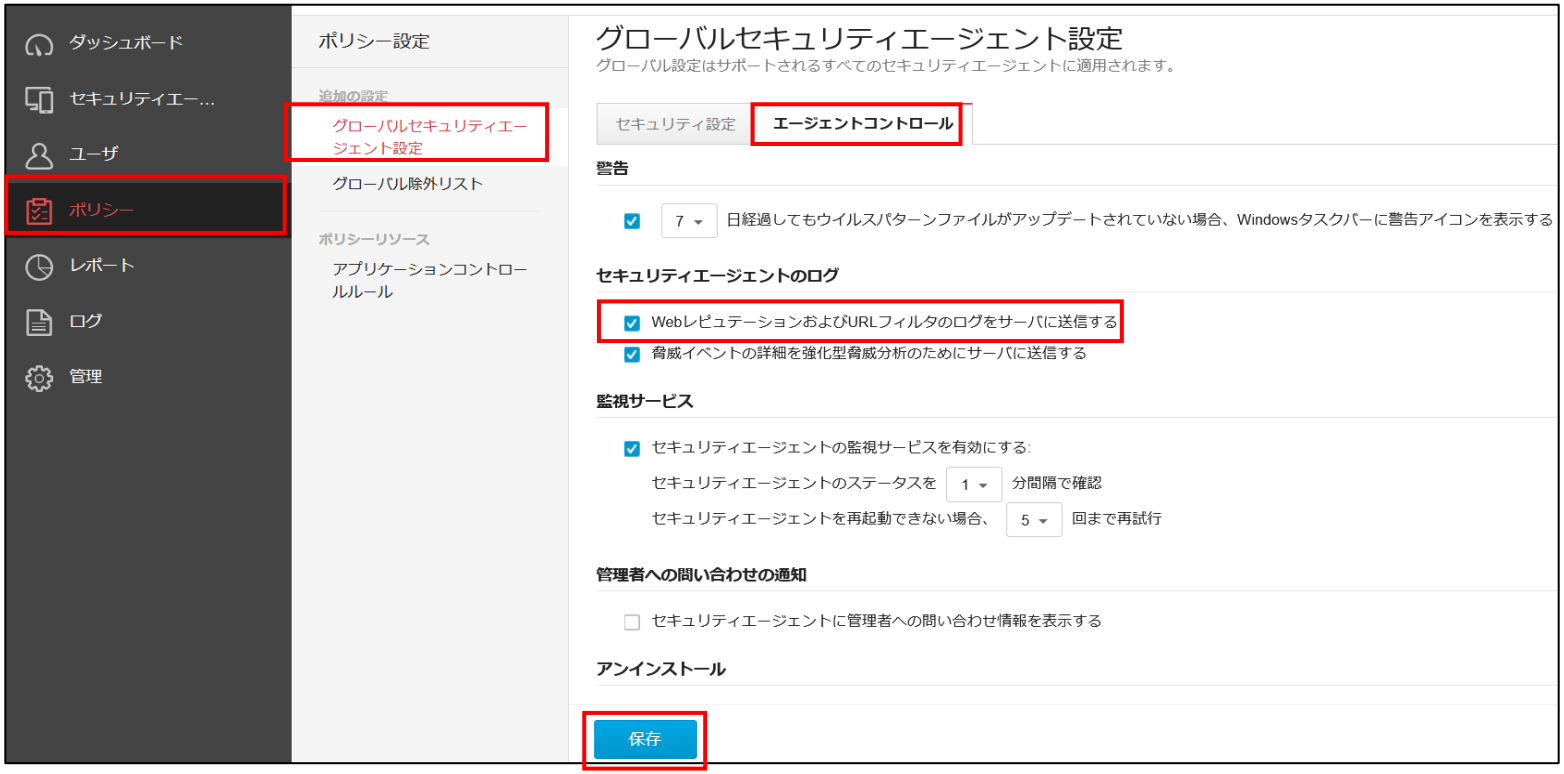
20. EDRセキュリティご利用に伴う、既存設定に関する注意点 3/5

対象者：② [Webレピュテーションおよびフィルタのログをサーバに送信する] がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒ VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールへログイン後、
「ポリシー」-「グローバルセキュリティエージェント設定」-「エージェントコントロール」タブにて下記を設定
[Webレピュテーションおよびフィルタのログをサーバに送信する] ：オン（チェックを入れた状態）

②保存をクリック



20. EDRセキュリティご利用に伴う、既存設定に関する注意点 4/5

対象者：③［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］ がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒ VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールへログイン後、
「ポリシー」-「グローバルセキュリティエージェント設定」-「エージェントコントロール」タブにて下記を設定
［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］ ：オン（チェックを入れた状態）

②保存をクリック

20. EDRセキュリティご利用に伴う、既存設定に関する注意点 5/5

対象者：④[webレピュテーション］がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒Webレピュテーション検知を元とした、注意が必要なイベントが発生しなくなります。

①管理コンソールへログイン後、
「セキュリティエージェント」-「開通時初期設定」※-「ポリシーの設定」 -対象のOSを選択し、
「webレピュテーション」タブにて下記を設定
[webレピュテーション］をオン

②保存をクリック

※「開通時初期設定」とは、お申込み時に申請いただいた内容の設定情報を反映させたポリシーグループになります。新たなポリシーを作成している際は、作成したポリシーグループをご指定ください。

21. Windows/Android/iOS　アンインストール

パソコンの買い替え時など、アンインストールを行う場合は下記手順にて実施します。
アンインストールが完了しますと、ライセンスは再利用可能となり、新デバイスへのインストールが可能になります。
アンインストール作業は管理コンソール側とクライアント側の両方から実施可能です。
※MacのEDRセキュリティのアンインストールにつきましては、117Pを参照ください。

管理コンソール側での実施方法

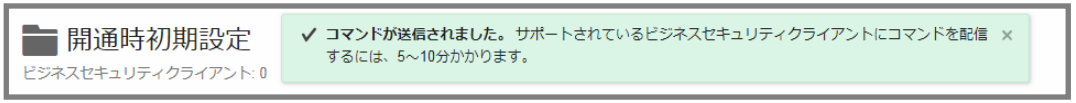
①管理コンソールにログインします。

②[セキュリティエージェント] タブを
クリックし、デバイスの登録情報を探し
チェックボックスにチェックを入れます。

③[タスク]から、
[セキュリティエージェントの
アンインストール] を選択します。

④管理コンソール上から、
該当のデバイスの登録が削除されます。

以上で、アンインストール作業の完了です。
クライアントコンピュータ側では、コンソールからの
削除通知を受信後、アンインストールが進められます。



22.Windowsアンインストール

クライアント側での実施方法（Windows10の場合）

※「ユーザー アカウント制御」により、許可、または管理者のパスワードを求められる場合があります。 操作を続行するためには、[続行]、または [はい] をクリックします。

① [スタート] ボタンから[コントロール パネル]を開きます。

② [プログラム]の項目にある[プログラムのアンインストール]をクリックします。

③表示された一覧の中から[セキュリティエージェント]をダブルクリックします。

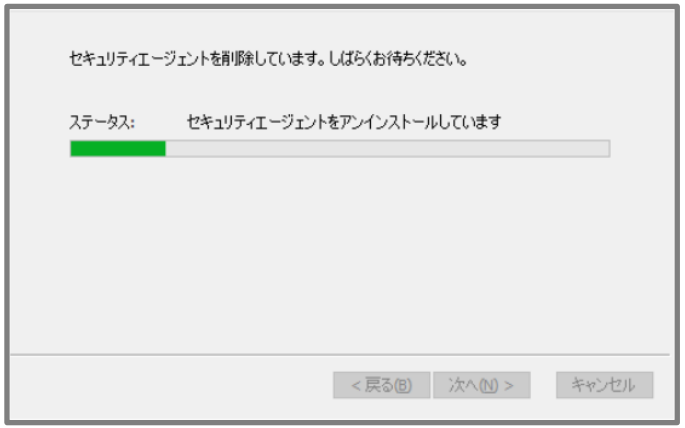
④アンインストール用パスワードを設定している場合は、下記の画面が表示されます。この場合はWeb管理コンソールで設定したパスワードを入力し、アンインストールを実行します。
本設定はWeb管理コンソールの［ポリシー］>［グローバルセキュリティエージェント設定］>［エージェントコントロール]タブ内の「アンインストール」での設定となります。アンインストールするためのウィザードが起動しますので、[次へ]をクリックします。

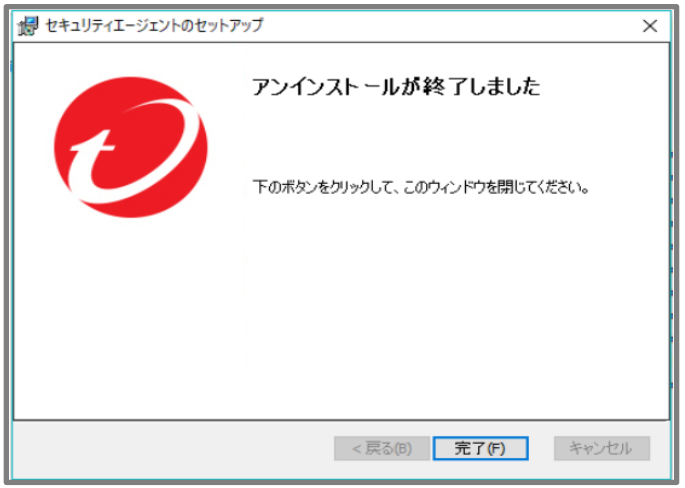
⑤途中で「ユーザ アカウント制御」の画面が表示される場合は、[はい]をクリックします。

⑥アンインストール処理が進んでいきます。

⑦しばらく待つと、アンインストール完了のメッセージが表示されます。[完了]をクリックし、Windows を再起動します。

操作は以上で終了です。





23. MacのEDRセキュリティのアンインストール

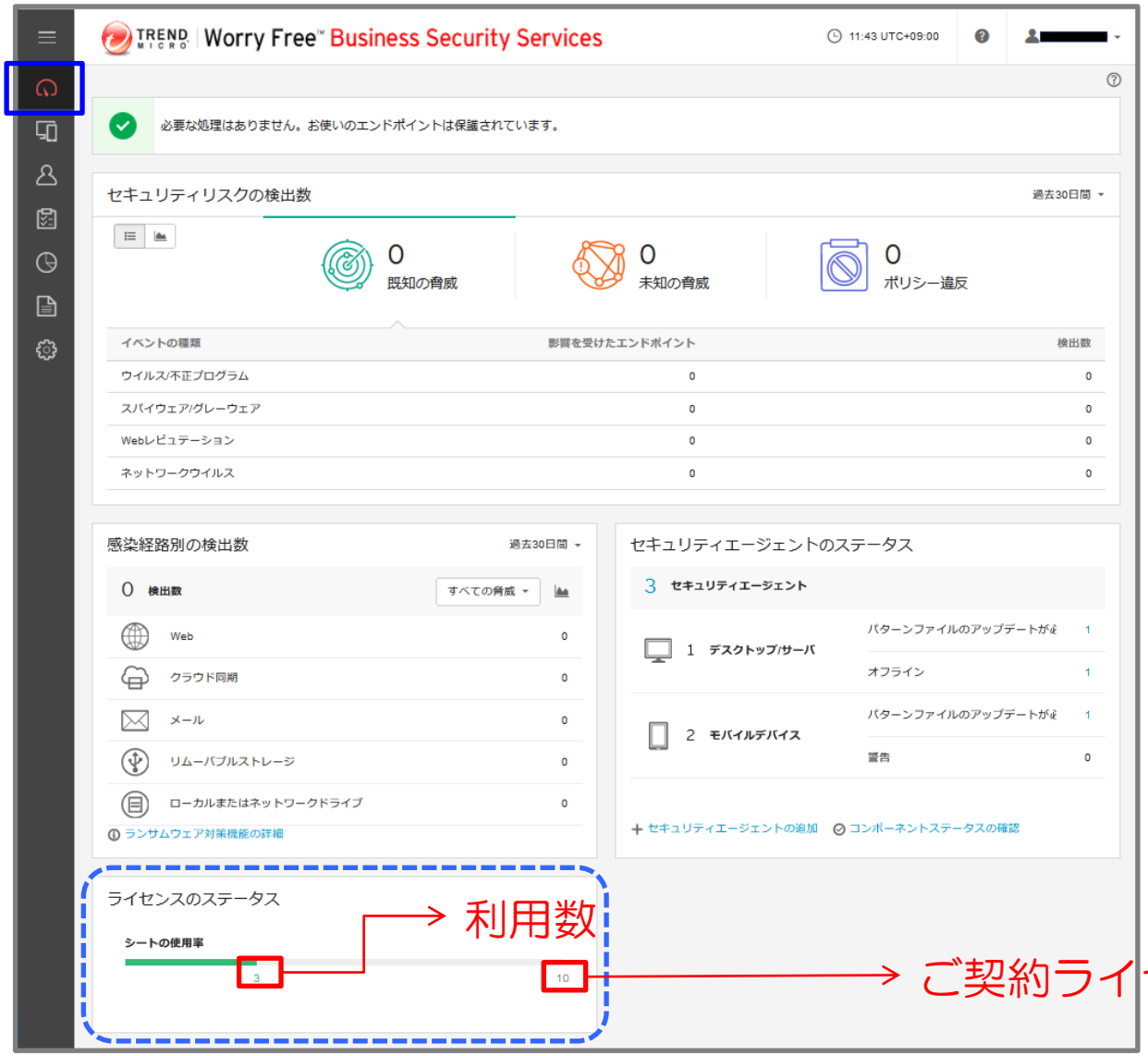
クライアント側での実施方法（Macの場合）

Macエンドポイントセキュリティのアンインストールにつきましては、115Pをご参照ください。

MacアプリのEDRセキュリティ アプリケーションのアンインストールにつきましては、
サポートセンター側での処理も必要となりますので、大変お手数をおかけしますが、
サポートセンターまでご連絡をお願い致します。

＜参考＞利用ライセンス数の確認方法

ご利用中のライセンス数、未利用ライセンス数の確認は、管理コンソールの「ダッシュボード」でご確認可能です。



24.レポート作成　1/2

セキュリティおまかせプランのご契約者さまには、毎月1度検出されたウイルスや不正コード等に関するレポートを登録されたメールアドレス宛に配信します。セキュリティの状況把握だけでなく、設定やポリシーの最適化検討を図る材料としても活用いただけます。月次レポートだけでなく、お客様任意の期間・対象を選択し、出力いただくことも可能です。

レポートの作成方法

①管理コンソールにて、「レポート」⇒「追加」

※【セキュリティおまかせプラン】月次レポート_エンドポイントセキュリティは、開通時に登録している月次レポートとなりますので、変更・削除しないようお願いいたします。（送付先メールアドレスは変更可）

24.レポート作成　2/2

②任意のレポート名を入力します。

③レポートの予約を「検索」で指定します。

③対象のデバイスを選択します。

④レポートの内容を選択します。

⑤レポートの受信者のアドレスを
　指定します。

⑥「保存」をクリックします。

25. 月次レポート確認方法　1 /2

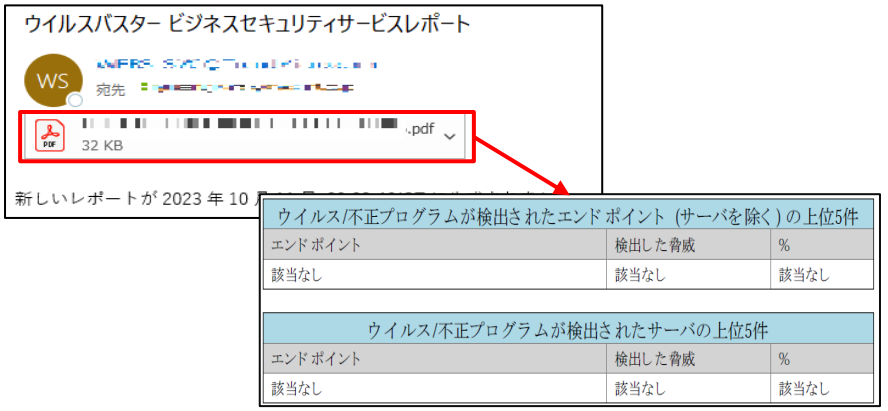
レポート通知メールの仕様変更に伴い2023年11月1日より、エンドポイントセキュリティの月次レポートの確認方法が変わります。

■変更概要

- レポートメールに添付しているファイルを削除し、管理コンソールへログイン後にレポートを確認いただくことでメール誤送信時の個人情報漏洩リスクを低減します。
- メール本文にて素早く検出概要を把握することが可能となります。

■変更内容

- 変更前
  レポート通知メールにPDFファイルを添付。
  添付ファイルの内容にてエンドポイント名・検出ファイルパス等を確認。



- 変更後
  レポート通知メールの本文にて、
  レポート概要・レポート名等を記載。
  PDFのレポートファイルについては
  管理コンソールへログイン後、確認。

メールイメージ

件名：ウイルスバスター ビジネスセキュリティサービスレポート
本文：
新しいレポート月次通知レポート1 がYYYY/MM/DDに生成されました。
（レポート概要）
ウイルス/不正プログラム検出：あり
スパイウェア/グレーウェア検出：なし
ネットワークウイルス検出：なし
Webレピュテーション違反：あり
挙動監視違反：なし
デバイスコントロール違反：なし
URLフィルタ違反：なし

Web コンソールにアクセスして、レポートを表示してください。

25. 月次レポート確認方法　2/2

■レポート確認方法

① レポート通知メールに記載しているリンク先「Webコンソールにアクセス」から管理コンソールへログインします。その後、左側メニューから「レポート」を選択し、
「【セキュリティおまかせプラン月次レポート】（エンドポイント）」※を確認します。
※開通時のレポート名です。レポート名を変更している場合は任意のレポートを確認してください。

② 「表示」欄から数字をクリックします。

③「レポート履歴」が表示されるため、対象のPDFをクリックし、レポートファイルをダウンロード後、レポートの内容を確認してください。

26. 管理コンソールログイン時のID･パスワードについて１/3

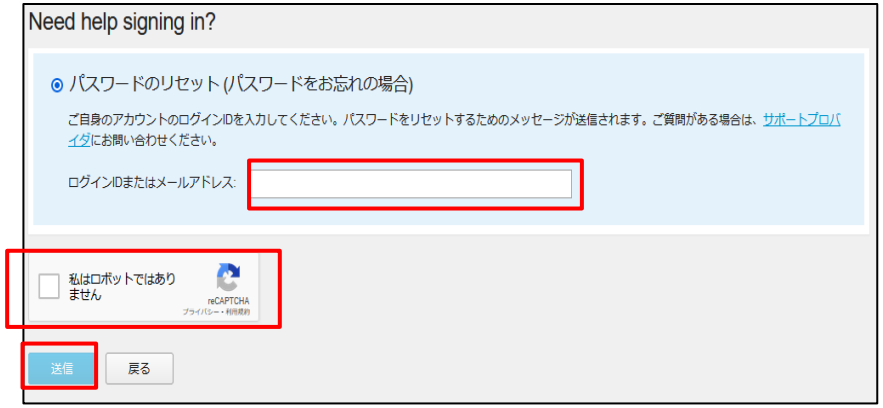
PCにて管理コンソールへログインする際のPWをお忘れの場合は、下記手順よりリセットすることが可能です。※IDを忘れた場合も下記の手順にて確認することが可能です。

■ログインIDの確認・パスワードリセット方法

① LMPログイン画面にて「パスワードのリセット（パスワードをお忘れの場合）」を選択します。

② パスワードリセット画面にてログインIDまたは、メールアドレスを入力します。
その後、認証をチェックし、「送信」ボタンをクリックします。

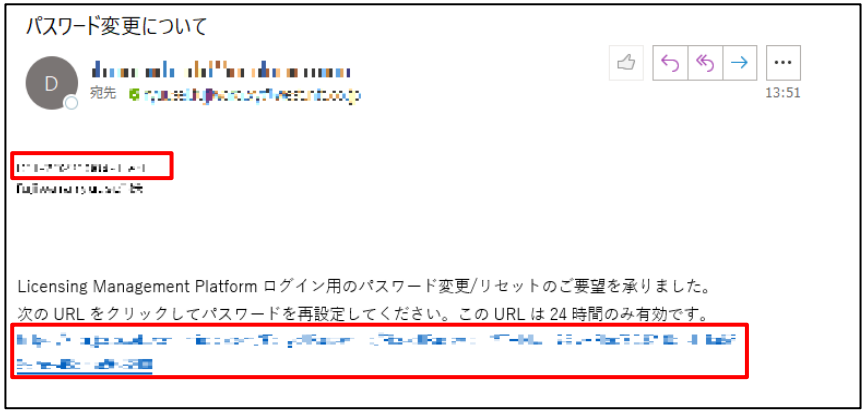
※ログインIDをお忘れの場合は、登録しているメールアドレスを入力してください。



26. 管理コンソールログイン時のID･パスワードについて 2/3

③数分後、パスワードリセットメールが届きます。
メール内のパスワードリセット用のURLへ
アクセスします。

※ログインIDをお忘れの場合はメール本文の
上部からID名を確認することが可能です。



④パスワードのリセット画面が開くため、
新しいパスワードを設定してください。
設定後、「送信」ボタンをクリックします。

※メールアドレスでリセットした場合
1つのメールアドレスで複数のアカウントを
登録している場合は、アカウント名の
プルダウンからパスワードをリセットしたい
アカウントを選択してください。

26. 管理コンソールログイン時のID･パスワードについて 3/3

⑤パスワード変更後、右図のような画面が表示されます。「OK」ボタンをクリックし、ログインしてください。