SaaS 型セキュリティ対策

ウイルスバスタービジネスセキュリティサービス

ユーザーズガイド

Version 2.36

日本事務器株式会社

改版履歴

Version	日付	変更内容
2.36	2023/07/31	Android エージェントアプリ(新バージョン:2.0.0)インストール手順追加
2.35	2022/10/19	iOS インストール手順の修正
2.34	2021/02/25	仮想パッチ機能追加
2.33	2020/01/10	Ver6.7 対応 Mac セキュリティ機能強化
2.32	2019/06/25	Ver6.6 対応 セキュリティ機能強化
2.31	2018/10/26	注意事項修正(除外していただく URL 情報)
2.30	2018/09/14	Ver6.5 対応(Web 管理コンソールの UI 変更)
2.20	2018/03/07	Ver6.3 対応(情報漏えい対策、ランサムウェアの概要、アグレッシブ検索)
2.12	2017/10/20	Ver6.2 対応 アプリケーションコントロール修正
2.11	2017/07/12	注意事項 運用に必要な URL 情報更新。ログ保存期間 30 日から 60 日へ
2.10	2017/04/28	Ver6.1 対応(機械学習機能、アプリケーションコントロール)
2.00	2016/12/27	Ver6.0 対応
1.80	2016/02/19	Ver5.8 対応(ランサムウェア対応)
1.72	2016/01/07	iOS インストールの準備注意事項追加
1.71	2015/11/10	予約検索、手動検索結果確認および制限事項追加。ログ閲覧注意事項追加。
1.70	2015/02/05	Ver5.7 対応
1.60	2014/07/18	新規作成

目次

1. はじめにお読みください ＜重要＞

本ユーザーズガイドは、**ウイルスバスタービジネスセキュリティサービス（以下 VBBSS と表記します）**のインストールおよび、管理運用設定について記載いたします。詳細な設定内容についてはオンラインヘルプをご確認ください。

1.1. 注意事項

（1）ウイルス対策製品を利用中の場合
すでにウイルス対策製品がインストールされているデバイスに、VBBSS をインストールする場合は、必ず利用されているウイルス対策製品をアンインストールしてから VBBSS をインストールしてください。

（2）既存ウイルス対策製品の自動アンインストール機能について
Windows クライアントに VBBSS を導入する場合、自動アンインストール対応製品であれば、事前にアンインストールを行わなくても VBBSS インストール時に自動的にアンインストールされます。
※対応製品でバージョンが異なると自動アンインストールできないこともございます。
展開前に自動アンインストールが行えるか、必ず確認を行ってください。

・クライアントインストール時に自動アンインストールされるウイルス対策製品
https://success.trendmicro.com/jp/solution/1311309

（3）VBBSS のアンインストールパスワード設定
初期設定では VBBSS クライアントのアンインストールやアンロード（停止）のパスワードが設定されていません。利用者の不用意なアンインストールや停止を行わせないために、アンインストールパスワード設定をおすすめします。パスワードを設定するには「ポリシー設定（グローバル）」をご確認ください。

（4）除外フォルダ、ファイル設定
データベース領域やアーカイブログデータなど、ディスク I/O が頻繁に発生するフォルダやファイルはリアルタイム検索から除外が必要になる場合があります。例）データベースフォルダ
リアルタイム検索の除外フォルダやファイルを設定するには「ポリシー設定のグローバル除外リスト、検索除外」をご確認ください。

（5）クライアントへのポップアップ通知設定
デバイス画面へのポップアップ通知（ウイルス検知など）により、利用者への不安と混乱を招く可能性を考慮し、初期設定でポップアップ通知は無効になっています。クライアントでのポップアップ通知を有効にするには「ポリシー設定の権限およびその他の設定のアラート」をご確認ください。

（6）挙動監視設定
システム要件を満たしていても旧マシンの場合動作が重くなる場合があります。

新しい脅威に対応するため、システムの改変を監視する挙動監視機能が初期設定で有効になっています。
動作が遅くなり業務に支障を与える場合は、挙動監視機能の承認済みプログラムリスト（除外）に登録するか挙動監視機能を無効に設定してください。※無効化は推奨されません。
挙動監視を無効にするには「ポリシー設定の挙動監視＜ランサムウェア＞」をご確認ください。
※ラインサムウェア対策を行うには挙動監視機能を有効にする必要があります。

（7）Web レピュテーションおよび、URL フィルタの除外設定
Web レピュテーション（不正 Web サイト接続ブロック）および、URL フィルタ（Web 閲覧規制機能）共に初期設定で有効になっています。イントラサイトや業務システムで http、https 接続を頻繁に使用している場合、レスポンスが悪くなる場合があります。そのような場合は URL サイトを除外します。
URL サイトを除外するには「ポリシー設定のグローバル除外リスト、承認済み/ブロックする URL」をご確認ください。

（8）ウイルス検索方式設定（Windows）
ウイルス検索方式がスマートスキャン方式の場合（初期設定）、各デバイスから頻繁にクラウド（インターネット）への問合せセッションが発生します。
・スマートスキャンサーバへの問合せ ⇒ リアルタイム検索ファイル数の約 7%
・スマートスキャンフィルタパターンチェック ⇒ 5 分に 1 回
問い合わせデータは 1KB 以下のためネットワーク帯域は心配ありませんが、同時セッション数を考慮する必要があります。

VBBSS での利用、最大 10 セッション／1 デバイス。
100 デバイスの場合、同時 1,000 セッション程度必要です。
ファイアウォールやルーターの同時セッション数にご注意ください。

（9）VBBSS を運用するために必要な通信ポート
以下サイトをご確認ください。
https://success.trendmicro.com/jp/solution/1310552

（10）URL フィルタなどを使っていて接続先を限定している場合に除外していただく URL 情報
※ファイアウォールやプロキシサーバでアンチウイルス機能を使っている場合にも、除外が必要となる場合があります。
プログラムアップデート時などサイズの大きいファイルをダウンロードする場合に、通信がタイムアウトしアップデートできないケースなど。

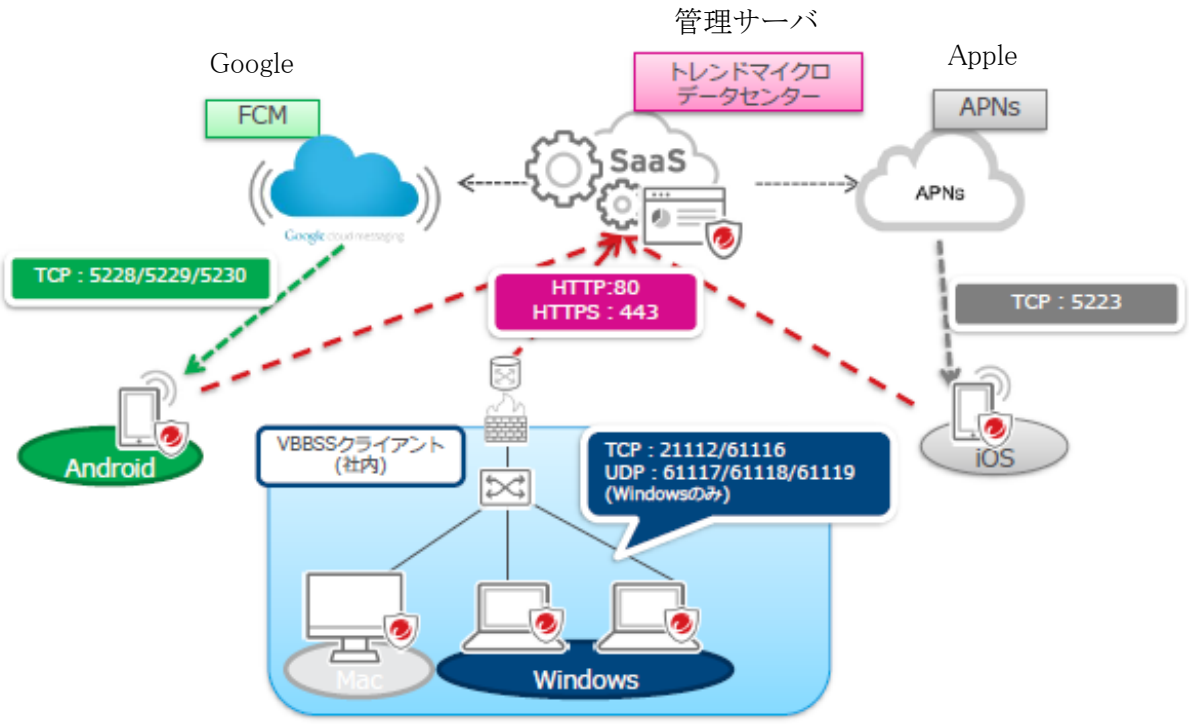
VBBSS の運用に必要な URL や通信ポートは以下サイトの
https://usersguide.anshinplus.jp/
「ウイルスバスタービジネスセキュリティサービス通信概要」をご確認ください。

1.2. プラットフォームごとの提供機能

導入されるプラットフォームにより提供される機能が異なります。

	機能	Windows	Mac OS	Android	iOS
セキュリティ対策	ウイルス対策	○	○	○	
	スパイウェア対策	○	○	○	
	Web レピュテーション	○	○	○	
	ファイアウォール	○			
	挙動監視	○			
	デバイスコントロール	○	○		
	URL フィルタリング	○	○		
	機械学習型検索	○	○		
	情報漏えい対策	○			
	仮想パッチ	○			
	アプリケーションコントロール	○			
集中管理	ポリシー管理	○	○	○	○
	管理ログ	○	○	○	○
	管理者への通知	○	○	○	○
	レポート	○	○	○	
	モバイルデバイス管理			○	○

1.3. 通信ポート概要図


管理サーバ
Google
Apple
トレンドマイクロ
データセンター
FCM
APNs
SaaS
APNs
TCP : 5228/5229/5230
HTTP:80
HTTPS : 443
TCP : 5223
Android
VBBSSクライアント
(社内)
TCP : 21112/61116
UDP : 61117/61118/61119
(Windowsのみ)
iOS
Mac
Windows

1.4. 導入について

導入手順を確認いただきクライアントにインストールするだけで基本的なウイルス対策は初期設定により施されています。
※iOS や Android で MDM 機能を使う場合はポリシー設定が必要です。
何から始めたら良いか分からない場合は以下優先順序を参考にしてみてください。

優先項目

1.「導入手順」によるクライアントへのインストール。
2.「管理コンソール」のダッシュボードやインストールしたクライアントの確認。
3. 注意事項にある検索除外などを行う必要があり場合は「ポリシー設定」の除外を設定。
4. 定期的（スケジュールを設定し）にクライアントの検索を行う場合「ポリシー設定」の検索方式＜予約検索＞。
5. 脅威を検出した場合に管理者に通知メールを行わせたい場合は「管理」の通知。
6. どのような検出があるかの履歴を確認したい場合「ダッシュボード」、「ログ」。
7. Android、iOS でパスワードポリシーを設定する場合は「ポリシー設定」Android、iOS。

8. その他の URL フィルタ、デバイスコントロール、アプリケーションコントロールなどの機能をご利用の場合は、「ポリシー設定」をご確認ください。

1.5. セキュリティ機能について

VBBSS6.6 より実装されました Windows のファイルレス攻撃対策（ハードディクスに保存されないメモリ上のみに存在するマルウェアを検索）機能を有効にするには下記 5 項目を設定する必要があります。

1.「リアルタイム検索」 オン
2.「リアルタイム検索」「設定」「対象」 タブ
　☑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
3.「挙動監視」 オン
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］ オン
5. 機械学習型検索 オン

2. 導入手順

本サービス利用開始 ～ インストールについて説明いたします。

2.1. インストール時の注意事項(システム要件)

■システム要件

以下 URL リンクのシステム要件をご確認ください。

VBBSS システム要件

◆Windows

ファイアウォール機能について

Windows クライアントはインストール中にファイアフォールドライバがインストールされるため、ネットワークが一時的に切断される場合があります。初期設定のままインストールする場合はファイアウォール機能無効のため通信断はありませんが、ファイアウォール機能を有効にしてインストールする場合は、影響の無いときにインストールを行ってください。

・初期設定

サーバ(初期設定)　ファイアウォール機能無効

デバイス(初期設定)　ファイアウォール機能無効

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

◆iOS

iOS 端末を管理するための APNs 証明書を作成・登録時に apple ID が必要です。

2.2. インストール時の便利な機能

(1)グループ指定インストール

デバイスの追加を行う時にグループを指定してインストールできます。

※初期設定ではサーバ(初期設定)とデバイス(初期設定)グループのみが設定されており、異なるポリシーを設定する場合はグループを追加することができます。また、インストール後に(初期設定)グループから他のグループへ移動することもできます。

サーバ(初期設定):Windows サーバ OS

デバイス(初期設定)Windows クライアント OS、Mac、Android、iOS

例)インストール直後に「営業部」配下へデバイスを登録したい場合

デバイスの追加時にグループ指定します。グループを指定したインストーラを使ってインストールしたデバイスはグループ「営業部」に配置されます。

(2)ラベル付け

デバイスの追加を行う時に、利用者の名前などをラベルとして入力させることができます。

(インストール URL によるインストール時のみ)

インストール時に入力したラベル情報はデバイスの一覧情報のラベルに表示されます。

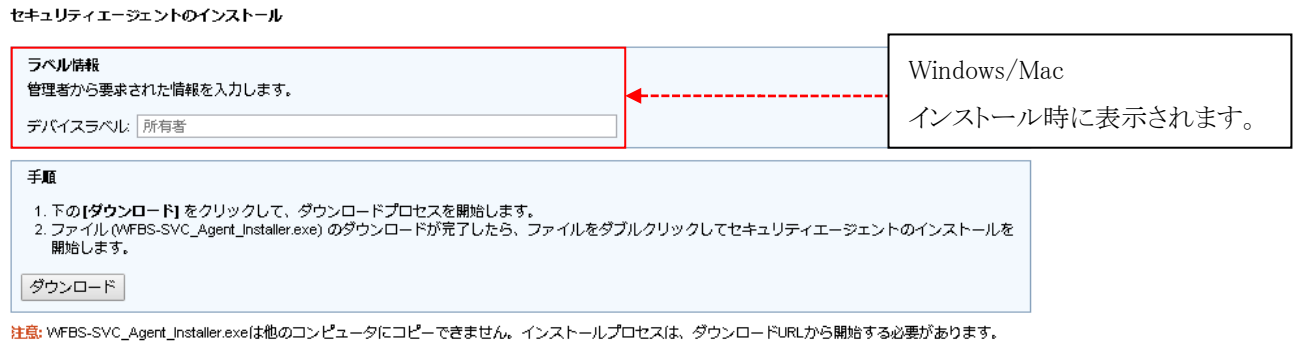
ラベルは画面から直接入力も可能です。

ラベル付け機能を有効にするためには、管理コンソールの「管理」より一般設定を選択します。

デバイス管理タブを開き「エンドポイントのラベル付けを有効にする」のチェックをつけラベル形式を入力(例では所有者)して「保存」をクリックしてください。

ラベル付けを有効にした後にインストーラリンク(URL)を使用してインストールを行うとインストール開始時にラベル情報(ラベル)入力を促すことができます。

※入力必須にはできません。



2.3. 管理コンソール ＜最初のログイン＞

本サービス契約、または評価版のお申込み完了後、2 通の登録完了メールがお客様へ送付されます。
[通知] あんしんプラス アカウント登録完了のお知らせ
[通知] あんしんプラス ライセンス登録完了のお知らせ
管理コンソールに接続するためには、アカウント登録完了メールに記載されているログイン ID とパスワードが必要になります。

アカウント登録完了メール

このメールには重要な情報が記載されています。大切に保管してください。
また、このメッセージは登録システムによって自動的に作成されたメールです。
本メールに対するメッセージの返信は受け付けておりませんので、あらかじめご了承ください。
==========
プラス株式会社 様

アカウントの登録が完了しました。すぐにサービスをご利用できます。

【ログイン ID】
pfsl-zzz00001
【パスワード】
はじめに次の URL をクリックし、パスワード発行の手続きを行ってください。

https://Forgetpwd.trendmicro.com/ForgetPassword/ResetPassword?T=29560842&v=883c2474-6bb5-485c-a3f1-3c79000
※この URL は 7 日間のみ有効です。

サービスを利用するには、下記の URL からログインしてください。
＊ ログイン URL：https://clp.trendmicro.com/Dashboard?T=295608453

※上記 URL はサンプルです。お客様へ送信されたアカウント登録完了メールに記載されている URL からログインしてください。

まず初めに管理コンソールへログインするためのパスワードを設定します。
「はじめに次の URL をクリックし、パスワード発行の手続きを行ってください。」の URL をクリックするとパスワードのリセット画面が表示されます。パスワードを入力後「送信」をクリックしてください。

以上でパスワードの設定は完了です。

「OK」をクリックすると管理コンソールへのログイン画面を表示します。

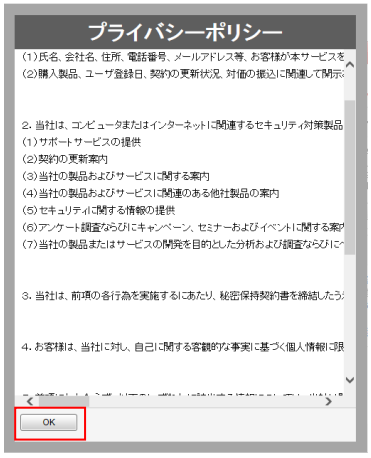
2.4. インストールの準備

※管理コンソールでの作業

(1)アカウント登録完了メールのログイン URL のリンクをクリックすると管理コンソール画面が開きます。
メールに記載されているアカウント及び最初に設定したパスワードを入力してログインをクリックしてください。

サポートブラウザで管理コンソールにログインしてください。
サポートブラウザのバージョン等の詳細は、システム要件を確認してください。

(2)プライバシーポリシーの確認画面が表示されます。
個人情報の取り扱いに同意した上で先に進んでください。
※最初のログイン時のみ表示されます。

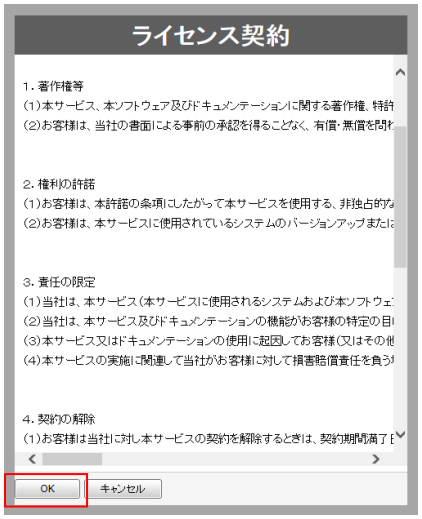


(3)ご契約中のサービス一覧が表示されます。
先に進む場合は、VBBSS の「コンソールを開く」をクリックします。
※「キーを入力」は本サービスで使用しません

(4)ライセンス契約の確認画面が表示されます。

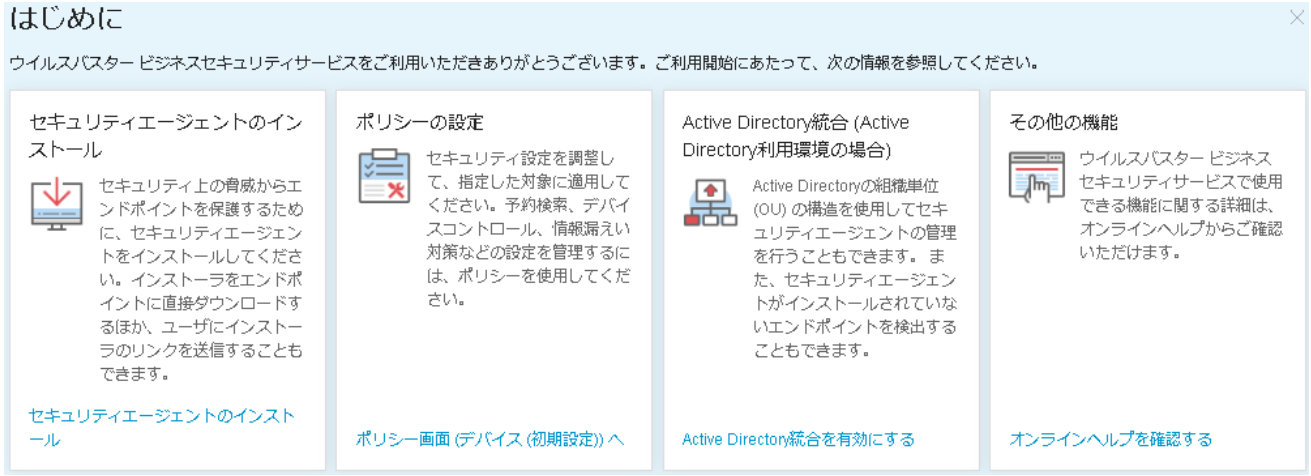
使用許諾の取り扱いに同意した上で先に進んでください。

※最初のログイン時のみ表示されます。

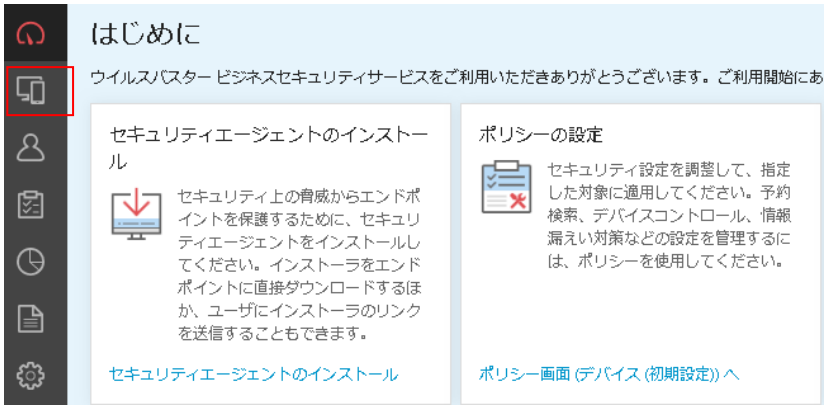


(5)管理コンソールのダッシュボードが開き、「はじめに」や「新機能」などの情報が表示されます。

必要が無い場合は×で閉じてください。再度表示させる場合はオンラインヘルプアイコン「？」より「はじめに」や「新機能」を選択すると表示させることができます。



「セキュリティエージェント」をクリックしてください。



(6)「セキュリティエージェントの追加」をクリックします。

セキュリティエージェントはすべてのクライアント一覧表示やグローバル設定「共通設定」を行う画面です。

(7)インストール方法を選択します。

インストール方法は 3 つあります。

①インストーラリンクの送信(Windows、Mac、Android、iOS)　他のユーザにインストール用の URL リンクを共有。

②インストーラのダウンロード(Windows、Mac)　インストール用のファイルをダウンロードします。

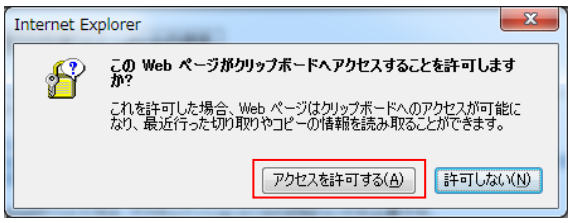
③このエンドポイントにインストール(Windows、Mac)　管理コンソールにログインしている端末にインストール。

2.5. ①他のユーザにインストール用のリンクをメールで送信

(1)インストール用 URL のリンクをメールなどで各クライアント(使用ユーザ)へ送信し、各クライアントで URL をクリックして、インストールを行います。「メールコンテンツ表示」をクリックするとインストール用 URL のリンクが表示されます。「コンテンツをコピー」をクリックするとクリップボードに内容がコピーされます。

※Firefox を利用の場合、「テキストのコピー」の表示に Flash 用プラグイン(application/x-shockwave-flash) の追加が求められる場合があります。

(2)クリップボードへのアクセス許可確認が表示された場合は「アクセスを許可する」をクリックします。



コピーされた情報をインストールが必要なユーザへメールで送付、掲示板などで共有してURLリンクより、インストールを行ってください。

◆テキストのコピー内容

次のリンクをクリックし、手順に従ってセキュリティエージェントをインストールしてください。

http://wfbs-svc-nabu.trendmicro.com/wfbs-svc/download/ja/view/activation_mgclink?id=YqMksdABGy0sQiS6XY7Yc2zuC68SuFPdtYvJLhdEMWetXE1ejkpk1oXT

認証コード (iOS 登録用):xxxxxxx

リンクおよびコードの有効期限:

2018 年 xx 月 xx 日 x 曜日 xx:xx

インストール用 URL は Windows、Mac、Android、iOS 共通で使用できます。※URL はお客様毎に異なります。

2.6. ②インストーラのダウンロード

インストール用ファイルを共有ディスクに保存して各コンピュータでインストール、または CD-ROM 等で配布してインストールする場合はインストーラをダウンロードします。

※インストールパッケージは最新の物を使うようにしてください。適時アップデートやバージョンアップが行われるため、古い物を使うとインストール後にアップデートが行われインストールに時間がかかります。また、バージョンの世代が異なると不具合を起こす可能性もあります。アップデートやバージョンアップが行われた後は、インストールパッケージをダウンロードしなおしてください。

(1)Windows、Mac を選択後「ダウンロード」をクリックします。

Windows 用

ダウンロードユーティリティ（WFBS-SVC_Downloader.exe）をダウンロードして実行し、セキュリティエージェントのインストーラ（WFBS-SVC_Agent_Installer.msi）を取得します。

Mac 用

ZIP ファイルをダウンロードして展開し、セキュリティエージェントのインストーラパッケージを取得します。セキュリティエージェントをインストールする前に、「WFBS-SVC_Agent_Installer.pkg」ファイルと「Identifier.plist」ファイルが同じフォルダにあることを確認してください。

(2)クライアントのインストール方法は、(Windows)インストールパッケージを使用したインストール手順、Mac の場合は(Mac)URL リンクを用いたインストール手順の(3)～をご確認ください。

2.7. ③このエンドポイントにインストール

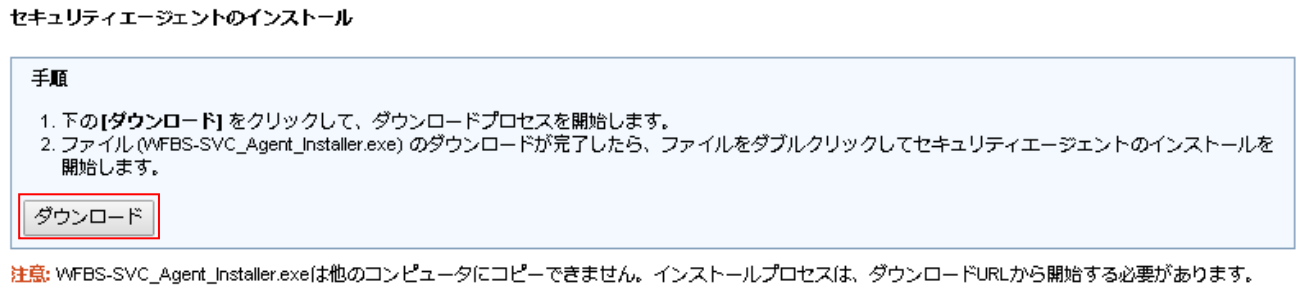
管理コンソールを開いているクライアントに直接インストールする場合は「このエンドポイントにインストール」をクリックします。

「インストール」をクリックしたあとは（Windows）、（Mac）URL リンクを用いたインストール手順へ進んでください。

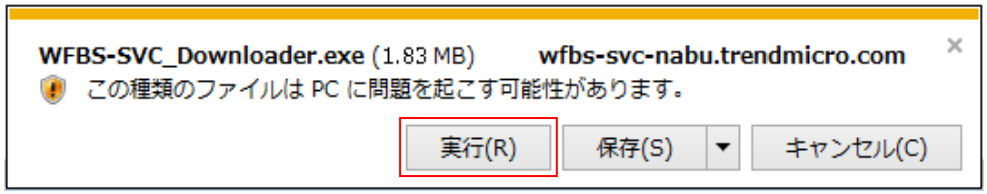
2.8. (Windows) URL リンクを用いたインストール手順

※クライアントでの作業

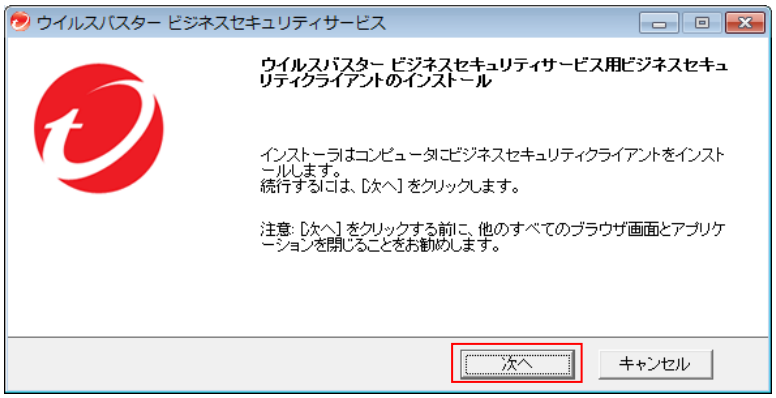
(1) インストール用 URL を使ってインストールを開始します。※メール等でインストール URL 情報を取得してください。
URL リンクをクリックすると、インストールプログラムダウンロード画面が開きます。
「ダウンロード」をクリックしてください。



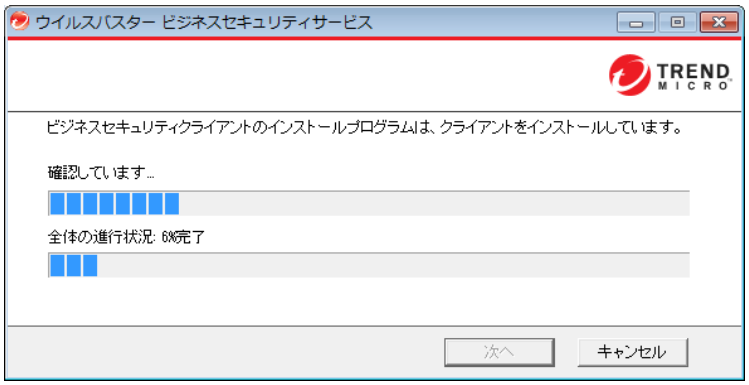
(2)「実行」をクリックしてください。または保存されたファイル「WFBS-SVC_Agent_Installer.exe」を実行します。



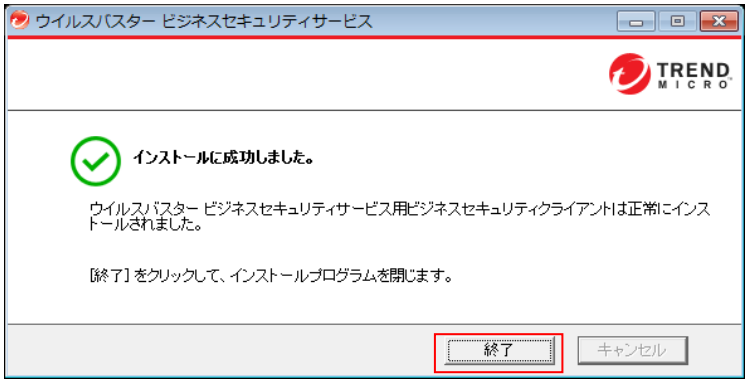
(3) インストールウィザードが開始されます。
インストールを続ける場合は、「次へ」をクリックしてください。



(4)プログラムのダウンロードへ進みます。※プログラムサイズは約 100MB。
ダウンロード後、自動的にインストールを開始します。



(5)インストールが完了すると「インストールに成功しました。」と表示します。
「終了」をクリックしてください。



※再起動を促すポップアップが表示された場合は、再起動を実行してください。

(6)インストール完了後、タスクトレイに「セキュリティエージェント」アイコンが表示されます。
インストール完了後は、最新プログラムへのアップデート、パターンファイルのアップデートを行いますので、マウスカーソルをアイコンに当てると表示がオフラインになる場合がありますが、しばらくそのままにしてください。

オンライン表示（正常）

オフライン表示

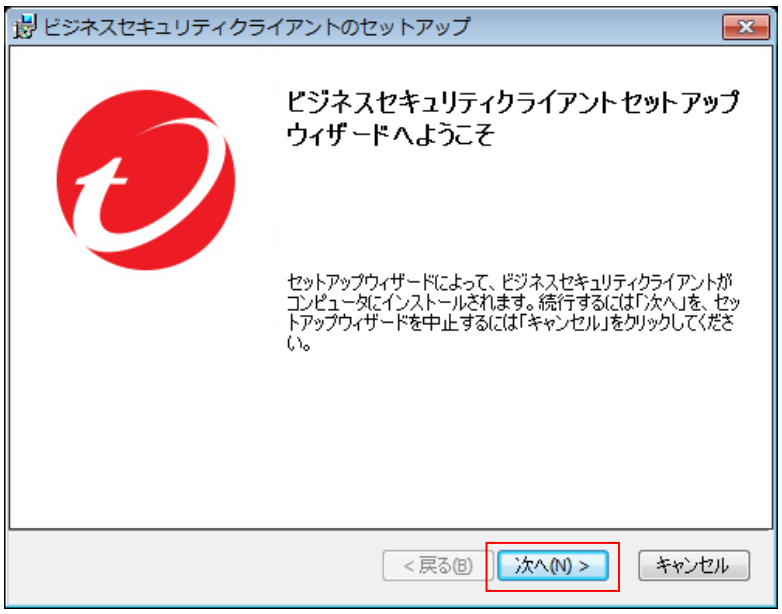
以上で Windows クライアントのインストールは完了となります。

2.9. (Windows)インストールパッケージを使用したインストール手順

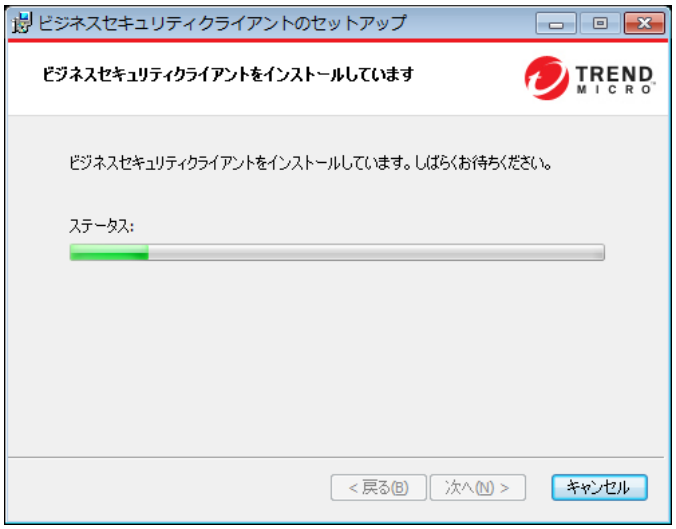
※クライアントでの作業

(1)ダウンロードしたインストールプログラム【WFBS-SVC_Agent_Installer.msi】を使ってインストールを行います。
インストールするクライアントでインストールパッケージファイルを実行します。

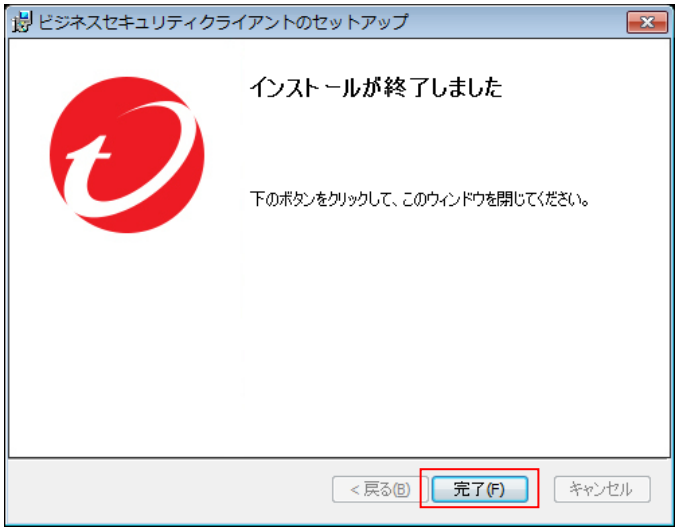
(2)インストールプログラムを実行すると、インストールウィザードが開始されます。
インストールを続ける場合は「次へ」をクリックします。



(3)インストールを開始します。



(4)インストールが完了したら「終了」をクリックします。



※再起動を促すポップアップが表示された場合は、再起動を実行してください。
(最新版でないインストールパッケージを使用してインストールした場合、インストール後に最新バージョンへのアップデートが行われ数分後に再起動要求メッセージが表示される場合があります。)

(5)インストール完了後、タスクトレイに「セキュリティエージェント」アイコンが表示されます。
インストール完了後は、最新プログラムへのアップデート、パターンファイルのアップデートを行いますので、マウスカーソルをアイコンに当てると表示がオフラインになる場合がありますが、しばらくそのままにしてください。

オンライン表示(正常)

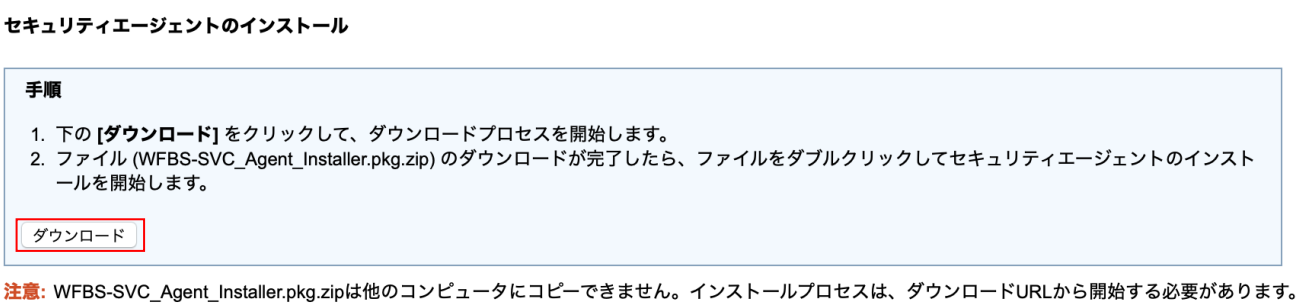
オフライン表示

以上で Windows クライアントのインストールは完了となります。

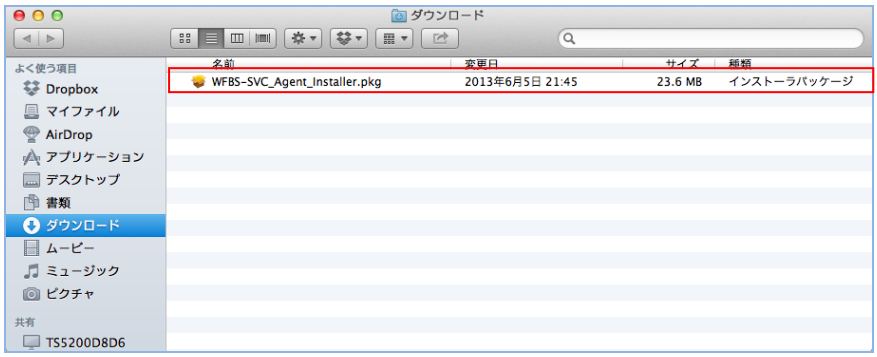
2.10. (Mac)URL リンクを用いたインストール手順

※クライアントでの作業

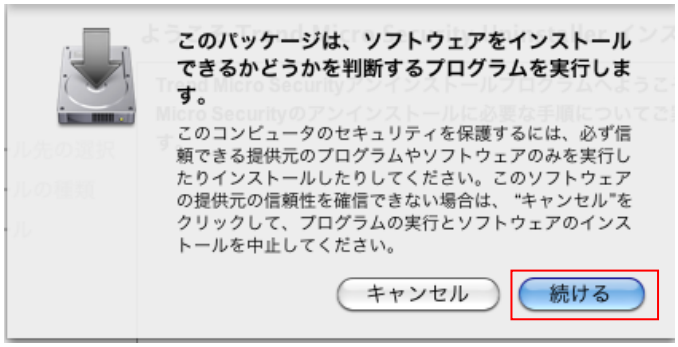
(1)インストール用 URL を使ってインストールを開始します。※メール等でインストール URL 情報を取得してください。
URL リンクをクリックすると、インストールプログラムダウンロード画面が開きます。
「ダウンロード」をクリックしてください。



(2)インストールプログラムがダウンロードされます。



(3)ダウンロードした「WFBS-SVC_Agent_Installer.pkg」をクリックします。
インストールを続ける場合は「続ける」をクリックしてください。



(4)インストールプログラムが起動します。

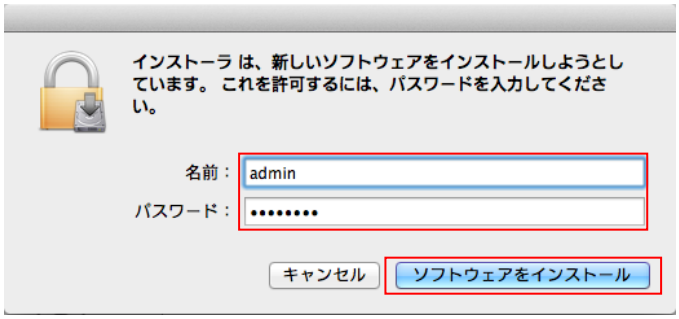
インストールを続ける場合には「続ける」をクリックしてください。

(5)インストールディスクを選択後「続ける」をクリックしてください。

(6)サーバへの接続テストを行います。続ける場合は「続ける」をクリックしてください。

(7)選択したディスクへインストールします。「インストール」をクリックしてください。

(8)インストール許可の確認が表示された場合には、管理者の名前とパスワードを入力後「ソフトウェアをインストール」をクリックします。



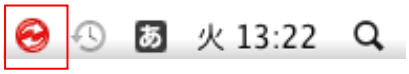
(9)インストールを開始します。しばらくお待ちください。

(10)インストールが完了しました。「閉じる」をクリックします。

(11)インストール完了後、メニューバーに Trend Micro Security のアイコンが表示されます。

通常

インストール完了後は最新プログラムへのアップデート、パターンファイルのアップデートを行いますので
アイコン表示が一時的に変わりますが、そのままにしてください。



アップデート中

以上で Mac クライアントのインストールは完了となります。

2.11. (Android)URL リンクを用いたインストール手順

※クライアントでの作業

(1)インストール用 URL を使ってインストールを開始します。※メール等でインストール URL 情報または QR コードを取得してください。
URL または QR コードから Google Play へアクセスします。

(2)Android デバイスへのインストール手順は下記サイトの「Step 2 Android デバイスへのインストール」をご確認ください。
Android デバイスへのビジネスセキュリティサービス(新バージョン 2.0.0)の クライアントプログラムのインストール手順
https://success.trendmicro.com/jp/solution/000294188
※2023 年 7 月 31 日メンテナンス後より(新バージョン 2.0.0)がリリースされます。

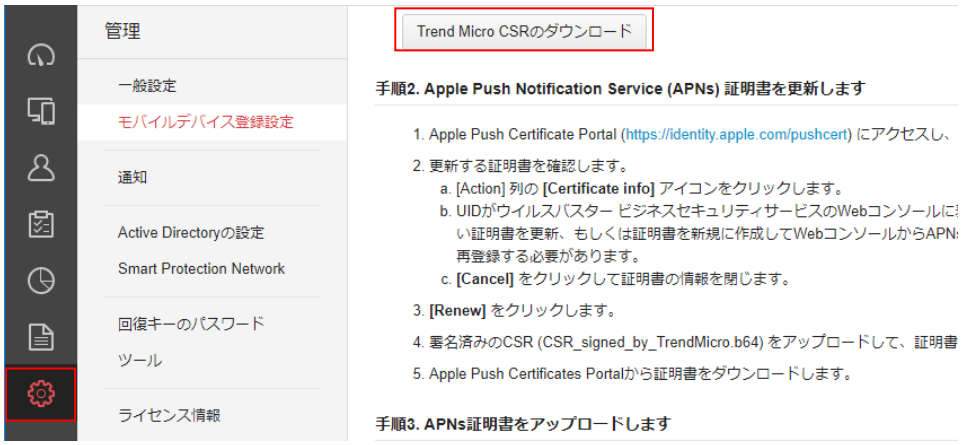
2.12. (iOS)インストールの準備

※管理コンソールでの作業

iOS 端末に VBBSS をインストールし各種機能をご利用いただくには、事前に APNs 証明書を作成・登録する必要があります。また、APNs 証明書の有効期限は 1 年間であるため、必ず更新期限内に更新してください。期限が過ぎるとクライアントの再インストールが必要になります。
APNs 証明書の作成・更新のために Apple ID が 1 つ必要です。個人の Apple ID でも作業できますが、会社用で 1 つ Apple ID を取得することをお勧めします。

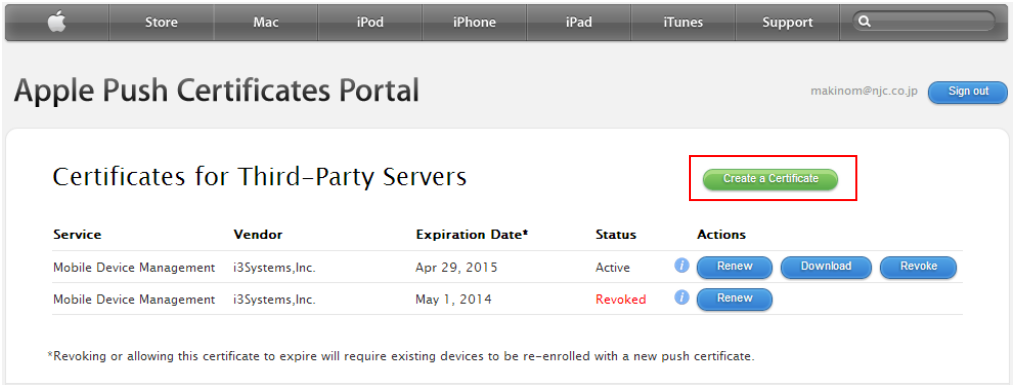
■APNs(Apple Push Notification)とは
iPhone/iPad アプリに Push 通知を行うために利用する Apple の仕組みです。

(1) 手順 1. 管理よりモバイルデバイス登録設定を選択し「Trend Micro CSR のダウンロード」をクリックして CSR ファイルをダウンロードします。

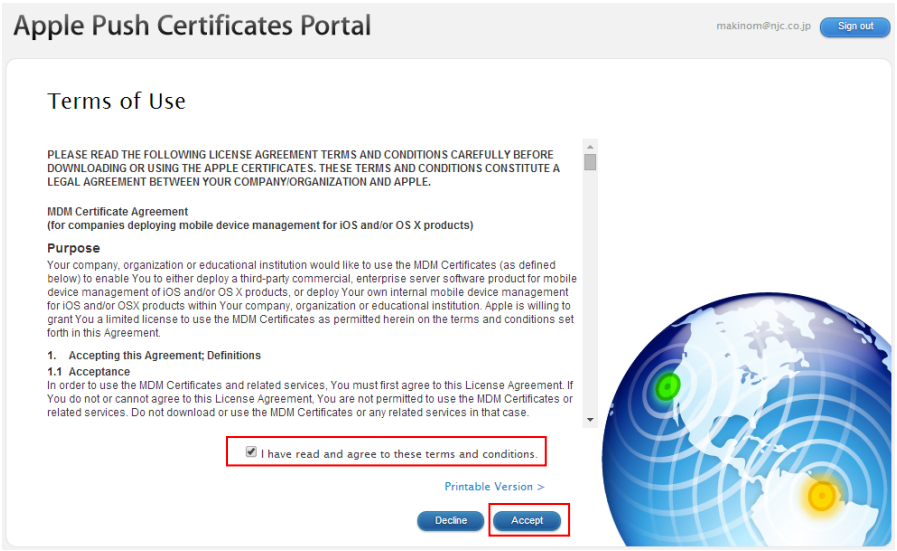


(2) 手順 2. Apple Safari または Google Chrome を使って Apple Push Certificate Portal (https://identity.apple.com/pushcert)にアクセスし、Apple ID でサインインしてください。
※Apple ID は証明書の更新時にも必要です会社で所有している Apple ID の使用をお勧めします。

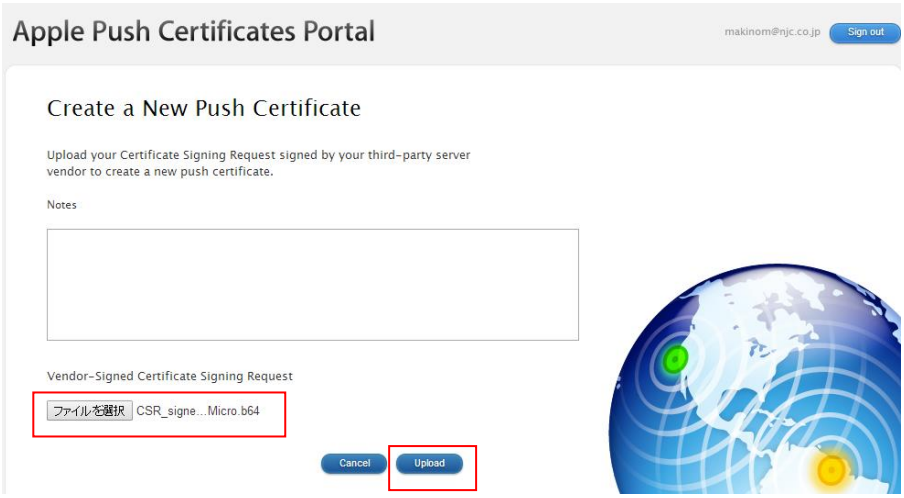
サインイン後、「Create a Certificate」をクリックします。



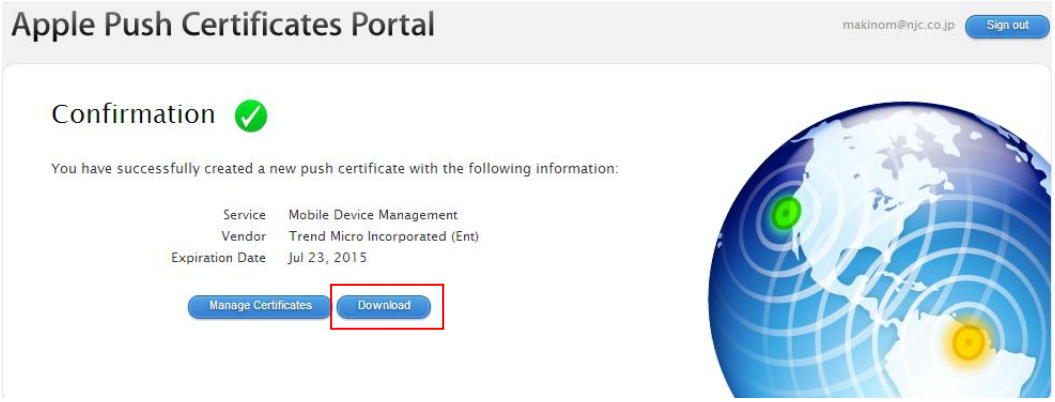
(3)使用許諾が表示された場合は「I have read and agree to these terms and conditions.」にチェックを入れ「Accept」をクリックします。



(4)ダウンロードした CSR ファイルを選択し、「Upload」をクリックします。



(5)APNs 証明書が作成されました。「Download」をクリックし、cer ファイルをダウンロードしてください。



(6) 手順 3. 管理コンソールにてダウンロードした cer ファイルをアップロードします。
証明書を作成するために使用した Apple ID を指定します。
ファイルを選択後、「APNs 証明書のアップロード」をクリックします。

(7) APNs 証明書登録が完了し、iOS 管理の準備が整いました。
登録後は、管理＞デバイス登録設定より、登録されている APNs 証明書のシリアル番号、UID、有効期限などを確認できます。

※Android/iOS へのインストール時に「使用許諾契約書」が表示されますが、「Android および iOS デバイス向けの使用許諾契約書」のカスタマイズより、文面を修正することも可能です。

■APNs 証明書に関する通知
APNs 証明書の関する通知は、以下の場合に行われます。
・APNs 証明書の有効期限が近付いている時（30 日前、14 日前、7 日前、3 日前）
・APNs 証明書の有効期限が切れた時
・APNs 証明書が削除された時
・APNs 証明書が無効化された時
※通知は管理＞通知＞受信者で設定しているメールアドレスへ送信されます。

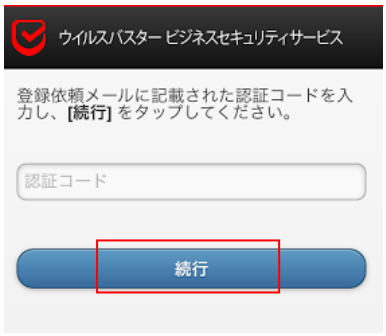
2.13. (iOS) URL リンクを用いたインストール手順

※クライアントでの作業

(1) メール等でインストール URL 情報を取得してください。

(2) iOS 標準のブラウザでインストール URL リンクを開きます。(iOS へのインストールは認証コードが必要です。)

(3) 認証コードを入力し「続行」をタップします。

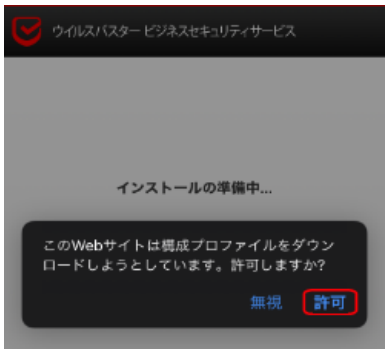


(4) 使用許諾の確認を表示します。続けるには、「同意する」をタップします。

(5) 「続行」をタップしてください。

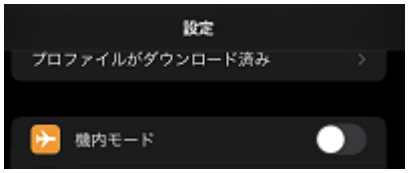
構成プロファイル表示の許可確認が表示された場合は許可してください。

(6) 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



(7) 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］を開きます。

(8)「プロファイルがダウンロード済み」をタップします。



(9)プロファイルのインストール画面が表示されたら、「インストール」をタップします。

(10)iOS のパスコードを入力します。

(11)警告画面が表示されたら内容を確認の上、「インストール」をタップします。

(12)リモート管理画面が表示されたら、「信頼」をタップします。

(13)インストール完了画面が表示されたら、「完了」をタップします。

以上で iOS クライアントのインストールは完了となります。

※ブラウザにインストール画面が残っている場合は閉じてください。

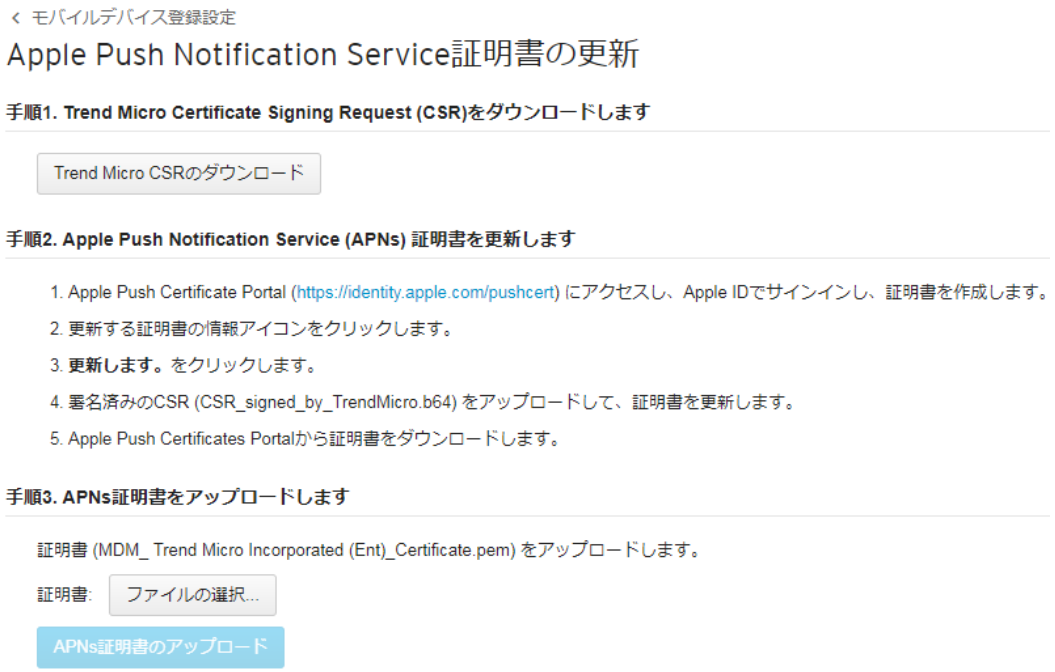
2.14. (iOS) APNs 証明書の更新手順

APNs 証明書の更新は、Web 管理コンソールから下記の手順で行うことができます。

(1) 管理コンソールにアクセスします。

(2) [管理]>[モバイルデバイス登録設定]>[APNs 証明書更新]をクリックします。

手順に従って証明書更新作業を行ってください。



※必ず既存の証明書を更新してください。[Create a Certificate] で新規に作成した証明書をアップロードした場合、登録済みのすべての iOS デバイスでプロファイルの再インストールが必要になります。

2.15. (iOS)APNs 証明書の削除／無効化

APNs 証明書の削除/無効のいずれかの操作を行うと、サーバからクライアントへの通知/リモート操作は行われなくなります。証明書の削除は管理コンソールから、無効化は Apple Push Certificate Portal から行うことができます。

APNs 証明書の削除は下記の手順で行うことができます。

・管理コンソールにアクセスします。

・[管理]＞[モバイルデバイス登録設定]＞[証明書の削除]をクリックします。

APNs 証明書の無効化は下記の手順で行うことができます。

・Apple Push Certificate Portal にアクセスし、ログインします。

・該当の証明書を特定し、[Revoke]をクリックします。

※証明書が無効化されるまでに 24 時間程度要します。

3. アンインストール手順

アンインストールについて説明いたします。

3.1. Windows のアンインストール手順

(1) 管理コンソールから強制アンインストールする場合

管理コンソールからアンインストールを実施する場合は、以下の手順で行います。

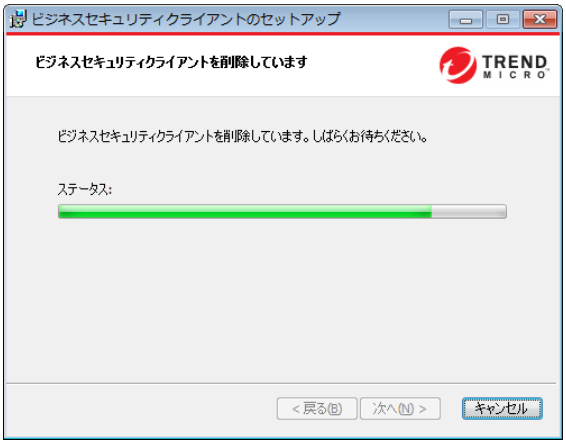
①管理コンソールの「セキュリティエージェント」一覧から対象の Windows クライアントを選択します。
②タスク＞「セキュリティエージェントのアンインストール」を選択後、「アンインストール」をクリックします。

③アンインストール実施タイミングについて
アンインストールは管理コンソールからアンインストール後すぐに行われません。管理コンソールからアンインストール後、該当クライアントが管理サーバに接続したタイミングでサイレントアンインストールが行われます。
※数分から数十分

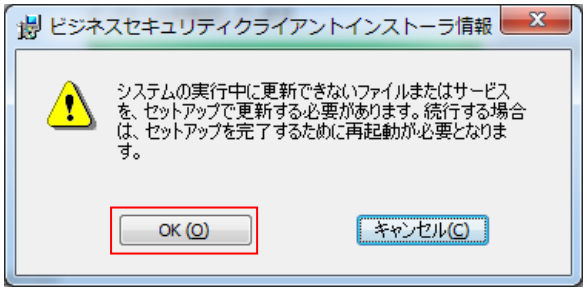
(2)クライアント側でアンインストールする場合

①Windows の[プログラムと機能]を起動します。

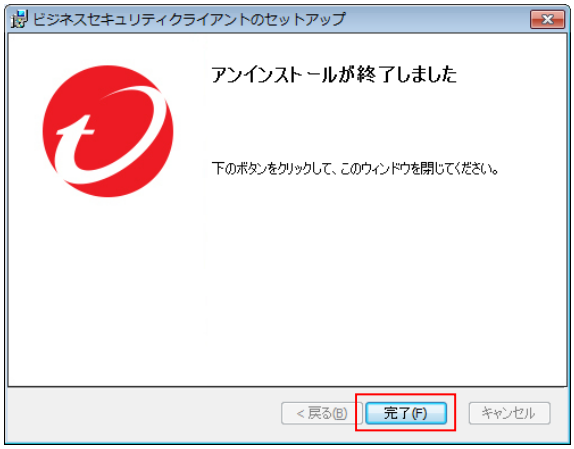
②「Trend Micro Security Agent」を選択しアンインストールを選択するとアンインストールが始まります。



③再起動の警告が表示された場合は、「OK」をクリックしアンインストール完了後、必ず再起動してください。



④アンインストールが終了しましたと表示されたら「完了」をクリックして終了します。



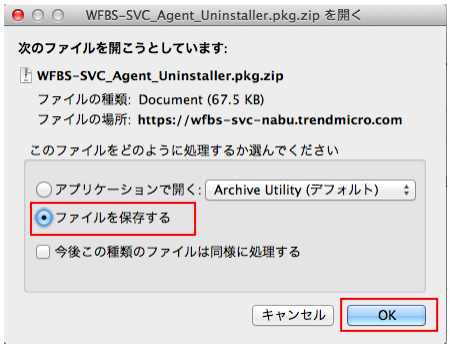
以上で Windows クライアントのアンインストールは完了となります。

3.2. Mac のアンインストール手順

(1) 管理コンソールの管理よりツールを選択します。

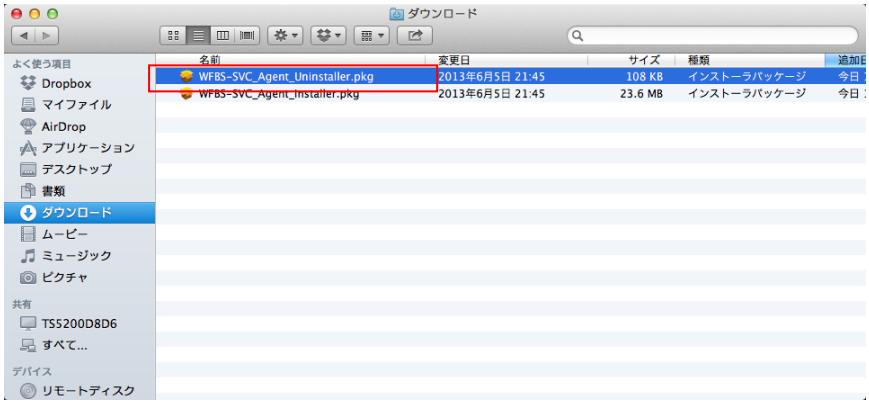
ツールのページが開きますのでアンインストーラ(Mac)の「ダウンロード」をクリックします。

(2) ファイルを開く確認が表示された場合は「ファイルを保存する」をチェックし「OK」をクリックしてください。



(3) アンインストールプログラムがダウンロードされます。

ダウンロードしたアンインストールパッケージファイル(WFRM-SVC_Agent_Uninstaller.pkg)をクリックしてアンインストールを行います。他の Mac でアンインストールを行う場合は、コピーして対象 Mac 上でプログラムを実行してください。



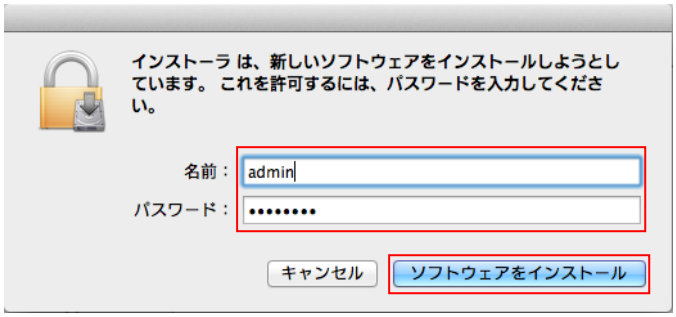
(4)アンインストールを続ける場合には「続ける」をクリックしてください。

(5)アンインストールプログラムが起動します。

「続ける」をクリックしてください。

(6)「インストール」をクリックしてください。

(7)インストール許可の確認が表示された場合には、管理者の名前とパスワードを入力後「ソフトウェアをインストール」をクリックします。



(8)アンインストールを開始します。しばらくお待ちください。

(9)アンインストールに成功しましたと表示されたら「閉じる」をクリックします。

(10)管理コンソールより該当 Mac クライアントを削除します。

①管理コンソールの「セキュリティエージェント」一覧から対象の Mac クライアントを選択します。

②タスク＞「セキュリティエージェントのアンインストール」を選択後、「アンインストール」をクリックします。

※Windows と異なり Mac はアンインストールしても管理コンソールより削除されないため

以上で Mac クライアントのアンインストールは完了となります。

3.3. Android のアンインストール手順

※機種やバージョンにより画面とは異なる場合があります。

アンインストール手順は以下サイトをご確認ください。

セキュリティエージェントのアンインストール手順（Android デバイス）

https://success.trendmicro.com/jp/solution/1116342

3.4. iOS のアンインストール手順

(1) 管理コンソールから強制アンインストールする場合

管理コンソールからアンインストールを実施する場合は、以下の手順で行います。

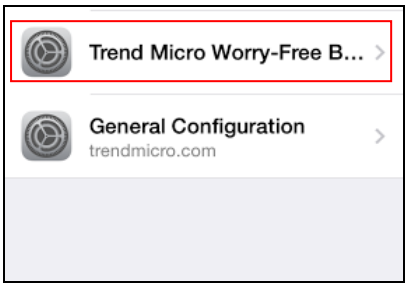
①管理コンソールの「セキュリティエージェント」一覧から対象のiOS クライアントを選択します。
②タスク＞「セキュリティエージェントのアンインストール」を選択後、「アンインストール」をクリックします。

※アンインストールを行うと iOS 端末から即時プロファイルが削除されます。

以上で iOS クライアントのアンインストールは完了となります。

(2)クライアント側でアンインストールする場合

(1)iOS 端末の設定＞一般＞プロファイルを開き、
Trend Micro Worry-Free をクリックします。



(2)アンインストールする場合は
「削除」をクリックします。

(3)「削除」をクリックします。

(4)iOS 端末のパスコード入力を求められた場合は
パスコードを入力してください。

以上で iOS クライアントのアンインストールは完了となります。

4. クライアントイメージ展開

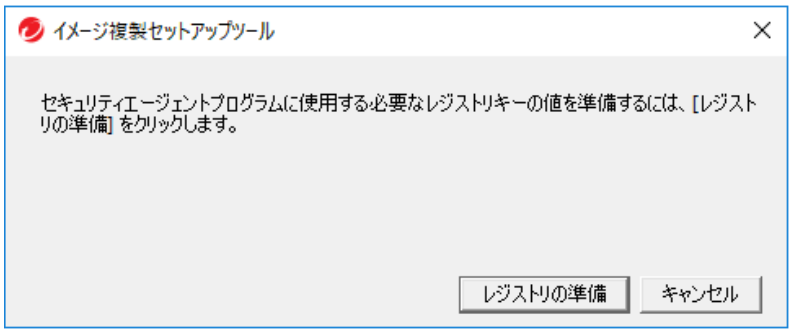
クライアントイメージ展開について説明いたします。

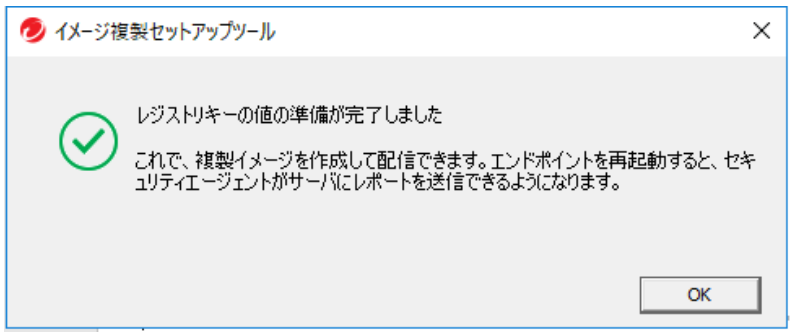
4.1. (Windows)クライアントをイメージ展開する場合の手順

※クライアントでの作業

イメージ展開(ディスクコピーやバックアップ)を行う前に VBBSS 固有情報クリアを行います。
展開用のマスタ PC で Windows シャットダウンを行う前に実行してください。
※展開前に固有情報をクリアしないと管理コンソール上でコピーマシンを正しく認識できず、正常に動作しません。
固有情報クリアツール(ImageCloningSetupTool)は管理コンソールの管理＞ツール＞イメージ複製セットアップツール よりダウンロードします。

(1) マスタ PC にて ImageCloningSetupTool.exe を実行し、画面に表示される指示に従います。





(2)マスタ PC をシャットダウン後、展開作業を行ってください。(コピーマシン上で固有情報が再生成されます。)
※VBBSS 固有情報をクリアする前に展開してしまった場合は、コピーマシン上で ImageCloningSetupTool を実行してください。固有情報がクリアされ、OS 再起動後に固有情報が再生成されます。

5. 管理コンソール概要

管理コンソールについて説明いたします。

5.1. 管理コンソール

詳しい機能説明は、管理コンソールのヘルプ(？アイコン)よりオンラインヘルプをご確認ください。

オンラインヘルプ

現在開いているページに関するオンラインヘルプ

管理コンソールではエンドポイントの状態やウイルスパターン情報などを閲覧、ポリシー設定を行うなどエンドポイントのセキュリティ状態を一元的に管理できます。社内ネットワークに接続されていないWindows、クライアントやMac、Android端末もインターネットに接続されていれば、状態を把握することができます。いつも管理コンソールを見なくてもメールによる通知設定を行っておけば、セキュリティ違反やウイルス駆除失敗などの事態が発生した場合に管理者へメールを通知することができます。

アカウント登録完了メールのログイン URL リンクをクリックすると管理コンソール画面が開きます。
アカウント登録完了メールに記載されているアカウント及びパスワードを入力してログインをクリックしてください。
※初めてログインする場合は最初にパスワード設定を行います。

5.2. ログイン後の画面

ログインするとダッシュボードの画面になります。

左側にアイコンメニューが配置されており、一番上の横 3 本線をクリックするとアイコンのメニュー名が表示されます。

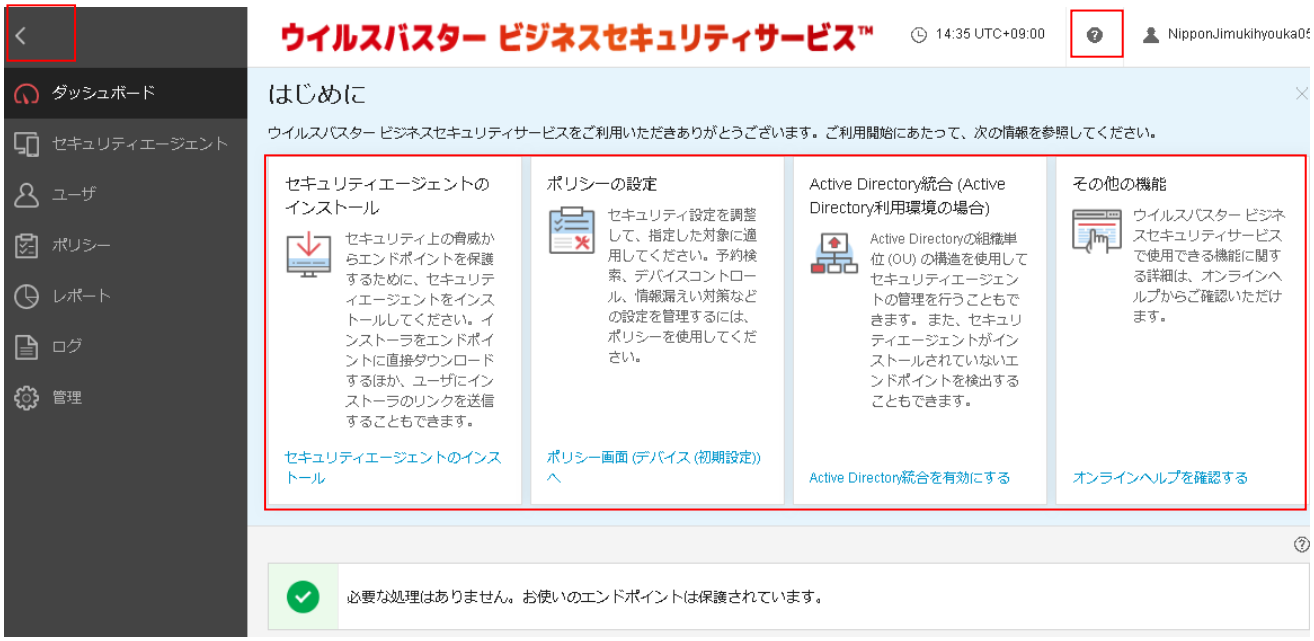
＜で閉じることができます。

上部に情報ウインドウが表示されます。

新規にログインすると「はじめに」メッセージを表示します。

機能アップデートがあると「新機能」メッセージを表示します。

それぞれ×で閉じることができ、ヘルプ（？）から再表示させることもできます。



◆左メニュー概要

ダッシュボード	管理しているエンドポイントのセキュリティ状態が一目で分かります
セキュリティエージェント	エンドポイントの追加、削除、一覧表示、グループごとのポリシー設定など
ユーザ	エンドポイントにログインしているユーザ名から状況を確認できます
ポリシー	すべてのセキュリティエージェントに適用されるグローバル設定や除外設定
レポート	検出された脅威の概要と詳細を確認できる PDF レポートを作成します
ログ	セキュリティリスクの検出状況やアップデート状況の確認
管理	通知設定やラベル付などの一般設定、ツールのダウンロードなど

6. ダッシュボード

ダッシュボードについて説明します。

6.1. ダッシュボードウィジェット概要

■アクションセンター

管理者に問題解決のための措置を求めるイベントが表示されます。問題のないときは「必要な処理はありません。お使いのエンドポイントは保護されています。」となり、異常が発生すると警告メッセージが表示されます。

■セキュリティリスクの検出数

検出された脅威の概要を知り、特定期間中(最大 60 日間)にどの脅威が影響を与えたのかを表示します。

■感染経路別の検出数

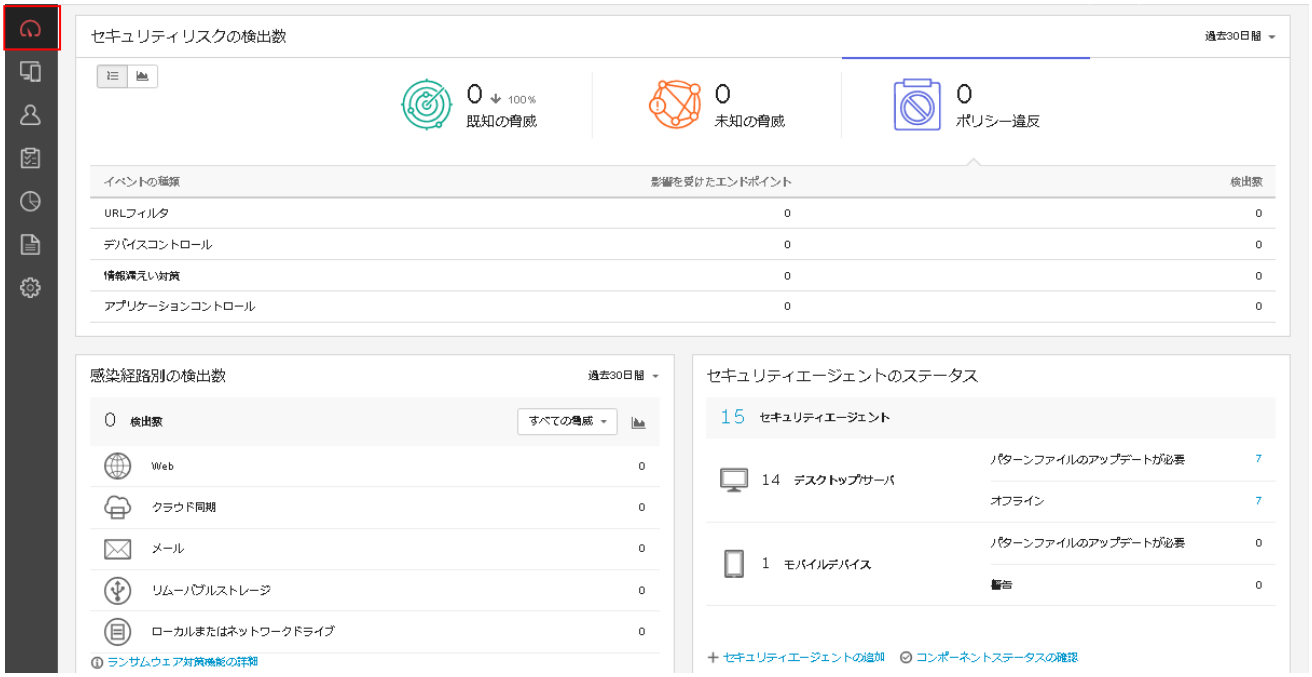
このウィジェットは、脅威の検出の概要を提供し、感染チャネルに基づいて検出を分類します。

■セキュリティエージェントのステータス

ネットワーク上のセキュリティエージェントの接続とアップデート状況の概要が提供されます。

■ライセンスステータス

最新のライセンス情報とシートの使用率を確認することができます。



[ダッシュボード] 画面に表示される情報の更新間隔は、セクションごとに異なります。一般的には、1 分～10 分間隔です。画面の情報を手動で更新するには、ブラウザで表示更新をします。

6.2. セキュリティリスクの検出数

脅威やポリシー違反ごとに検出した脅威の数、影響を受けたデバイスを確認できます。

統計表示／グラフ表示

◆既知の脅威

ウイルス/不正プログラム、スパイウェア/グレーウェア、Web レピュテーション、ネットワークウイルス

◆未知の脅威

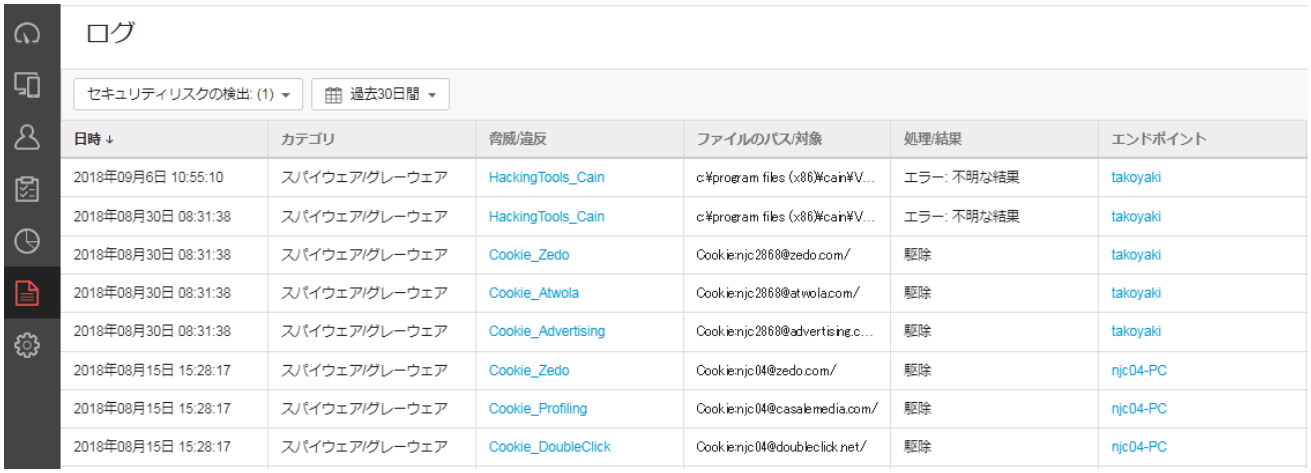
挙動監視、機械学習

◆ポリシー違反

URL フィルタ、デバイスコントロール、情報漏えい対策、アプリケーションコントロール

(1) 脅威の詳細を確認するには検出した脅威をクリックします。

(2) エンドポイントで検出された脅威の一覧および詳細を確認することができます。



6.3. 感染経路別の検出数

(1)感染経路別の検出数の内容を確認するには検出経路ごとに表示されるカウント数をクリックします。

詳細は以下サイトをご覧ください。

https://success.trendmicro.com/jp/solution/1114304

(2)検出した内容を表示します。

6.4. セキュリティエージェントのステータス

(1)パターンのアップデートおよびエンドポイントのオフライン状況を確認できます。

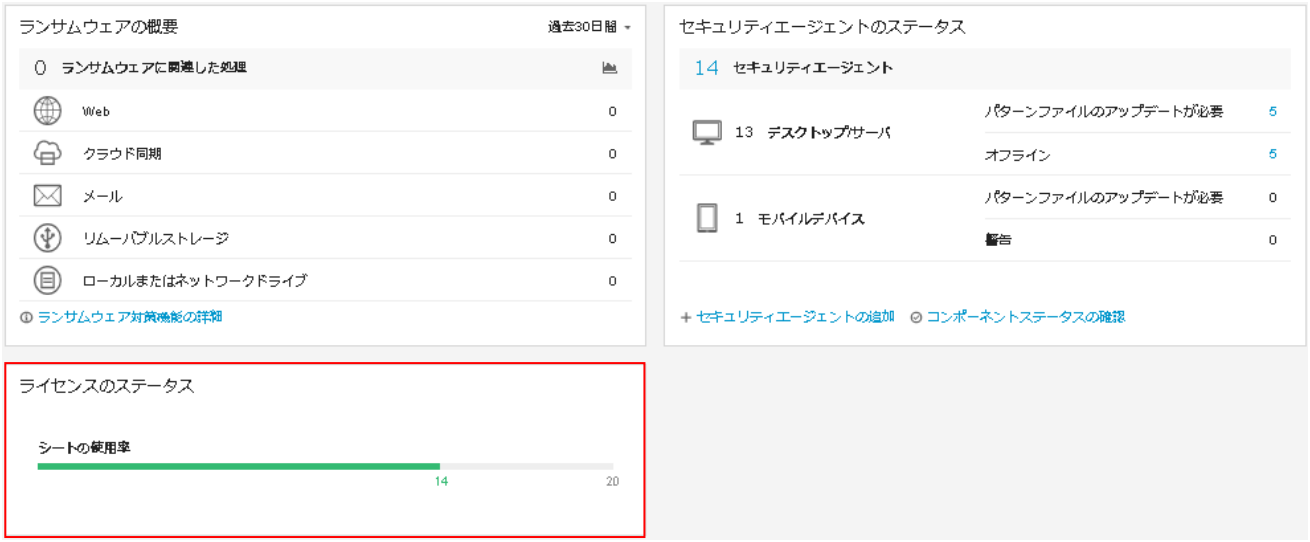
(2)「セキュリティエージェントの追加」をクリックすると、「インストール方法の選択」画面に推移します。

(3)「コンポーネントステータスの確認」をクリックすると、パターンファイルや検索エンジン等のバージョンを確認できます。

6.5. ライセンスのステータス

(1)保有ライセンス数とインストールされている使用数を確認できます。

保有ライセンス以上にインストールをすると正常に動作しない場合があります。



7. セキュリティエージェント

セキュリティエージェントについて説明します。

7.1. セキュリティエージェントの主な機能

・セキュリティエージェントの追加（インストール URL の取得やインストールパッケージのダウンロード）
・VBBSS のインストールされているエンドポイントの一覧表示
・グループの追加、グループごとのポリシー設定など

■画面構成

(1)列のカスタマイズ

列のカスタマイズをクリックして一覧表示させたい項目を選択し、「保存」をクリックしてください。

(2)セキュリティエージェント一覧表示

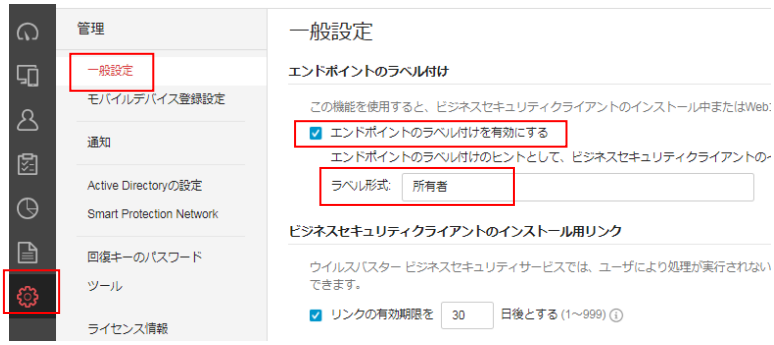
一覧表示にラベル情報を追記することができます。

※この機能を使うには「デバイスでのラベル付け」を有効に設定します。

◆ラベル付け機能を有効化

①ラベル付け機能を有効にするためには、管理コンソールの「管理」より一般設定を選択します。

「エンドポイントのラベル付けを有効にする」のチェックをつけラベル形式を入力(例では所有者)して「保存」をクリックしてください。



②ラベル付けを有効にした後にインストール URL を表示する「インストーラリンク」を使用して Web インストールを行うとインストール開始時にラベル情報（所有者）入力を促すことができます。※入力必須ではありません。

7.2. セキュリティエージェント一覧の主な項目の見方

	エンドポイント	ラベル	種類	前回の接続日時	IPv4アドレス	IPv6アドレス	オペレーティングシステム	ステータス	アーキテクチャ	暗号化ステータ
	njc01-PC	vbbss01	Windows	たった今	192.168.1.108	-	Win 7 Service Pack 1	オンライン	x86	暗号化できませ
	njc02-PC	vbbss02	Windows	29日前	192.168.1.107	-	Win 7 Service Pack 1	オフライン	x86	暗号化できませ
	njc03-PC	vbbss03	Windows	29日前	192.168.1.105	-	Win 7 Service Pack 1	オフライン	x86	暗号化できませ
	njc04-PC	vbbss04	Windows	たった今	192.168.1.250	-	Win 7 Service Pack 1	オンライン	x86	暗号化できませ

エンドポイント:コンピュータ名を表示します。

種類:Windows／Mac／Android／iOS

ユーザ:ログインユーザを表示します。

IPv4 アドレス:優先ネットワークの IPv4 アドレスを表示します。

IPv6 アドレス:優先ネットワークの IPv6 アドレスを表示します。

オペレーティングシステム:オペレーションシステムを表示します。

ステータス:オンライン／オフライン

オンライン→エンドポイントが VBBSS 管理コンソールに接続できている状態。

オフライン→エンドポイントが VBBSS 管理コンソールに接続できない状態。

5 分毎にオンライン／オフラインの確認を行います。エンドポイントがインターネットに接続されていない場合や、電源を切っている場合はオフラインになります。

5 分間の通信が 3 回(15 分)無くなるとオフラインと判断します。

暗号化ステータス:暗号化ステータスの状態を表示します。

暗号化ステータス	説明
-	デバイスで実行されているオペレーティングシステムでは暗号化がサポートされていません。
復号されました (ユーザ)	少なくとも1つのディスクがウイルスバスタービジネスセキュリティサービスにより暗号化され、ユーザにより復号されました。 暗号化コマンドをもう一度送信し、デバイスを管理してください。
復号しています...	BitLockerは、デバイスを復号しています。
復号しています...(一時停止)	復号プロセスがユーザによって一時停止されました。デバイスから復号を再開してください。
復号しています...(ユーザ)	少なくとも1つのディスクがウイルスバスタービジネスセキュリティサービスにより暗号化され、ユーザにより復号されました。 暗号化コマンドをもう一度送信し、デバイスを管理してください。
暗号化されました	デバイスが暗号化されました。
暗号化されています (ユーザ)	少なくとも1つのディスクがユーザにより暗号化されましたが、ウイルスバスタービジネスセキュリティサービスにより管理されていません。 暗号化コマンドを送信し、デバイスを管理してください。
暗号化しています...	BitLockerは、デバイスを暗号化しています。
暗号化しています...(一時停止)	暗号化プロセスがユーザによって一時停止されました。デバイスから暗号化を再開してください。

ロックされています	デバイスを暗号化または復号できません。デバイスがBitLockerによりロックされています。先にデバイスのロックを解除してください。
暗号化されていません	考えられるシナリオは、次の通りです。 ▪ デバイスが一度も暗号化されていません。 ▪ デバイスがウイルスバスタービジネスセキュリティサービスによって復号されました。 ▪ デバイスがユーザによって暗号化され、その後、復号されました。
一部が暗号化されています	新しいディスクがデバイスに追加されました。新しいディスクを暗号化するには、暗号化コマンドを再び送信してください。
保留中	デバイスが属するドメインが変更されています。ウイルスバスタービジネスセキュリティサービスは、次回、ビジネスセキュリティクライアントがサーバに報告するとき、自動的に暗号化コマンドを送信します。
中断しました	BitLocker保護がユーザにより保留にされています。暗号化または復号を行うにはデバイスで保護を再開してください。
暗号化できません	ウイルスバスタービジネスセキュリティサービスによってデバイスを暗号化できません。 詳細については、暗号化ステータスの問題を解決するを参照してください。
不明	ウイルスバスタービジネスセキュリティサービスで暗号化ステータスを取得できません。暗号化に対応していないバージョンのビジネスセキュリティクライアントがデバイスで実行されている可能性があります。暗号化コマンドを送信して、状態を更新してください。
失敗しました	暗号化または復号に失敗しました。下記のWebサイト (英語) でエラーコードを検索し、問題をトラブルシューティングしてください。 https://msdn.microsoft.com/en-us/library/windows/desktop/dd542648(v=vs.85).aspx

前回の接続日時:5 分以内の接続は「たった今」と表示します。オフラインになってからの経過時間や日数を表示します。

スマートスキャンサーバ:スマートスキャンサーバへの接続状態。

スマートスキャンを利用している場合はオンライン／オフラインに限らず接続となります。

スマートスキャンエージェントパターンファイル:定期的に更新されるパターンファイルのバージョンを表示します。

ウイルスパターン:従来型パターンファイルのバージョンを表示します。スマートスキャン利用時は-

検索方法:スマート／従来型

スマート:スマートスキャン利用時

従来型:従来型検索利用時

7.3. モバイル(Android、iOS)管理

管理コンソールより以下の操作を行えます。

■Android

リモート検索(位置情報)、リモートロック、パスワードリセット、リモート消去を行えます。

■iOS

リモートロック、パスコードクリア、リモート消去

Android、iOS 端末はアイコンより識別できます。

エンドポイント名をクリックした際に表示できる「デバイス詳細」情報

項目	説明	備考
デバイス名	エンドポイントがインストールされた端末のデバイス名	
グループ	Web 管理コンソール上で属するグループ名	
前回の接続日時	エンドポイントが最後に VBBSS サーバに接続した時間	
電話電話	電話番号	
機種	機種名	
システム	プラットフォーム情報	Android/iOS
バージョン (ビルド)	Android/iOS のバージョン情報	
容量		
使用可能	使用可能な容量	
IMEI	端末識別番号	取得可能な場合のみ表示
MEID	端末識別番号	取得可能な場合のみ表示
シリアル番号	シリアル番号	取得可能な場合のみ表示
モデルのファーム ウェア		取得可能な場合のみ表示
Wi-Fi MAC	Wi-Fi 接続時の MAC アドレス	機能が有効化され取得可能な場合のみ表示
Bluetooth MAC	Bluetooth 接続時の MAC アドレス	機能が有効化され取得可能な場合のみ表示

Android

リモート検索（位置情報）、リモートロック、パスワードをリセット、リモート消去を実行します。

※リモート消去は情報をクリアして初期状態にしますので、十分に注意してください。

イベントは最新のコマンド（実行した履歴）、既存の場所（取得した位置情報）を確認できます。

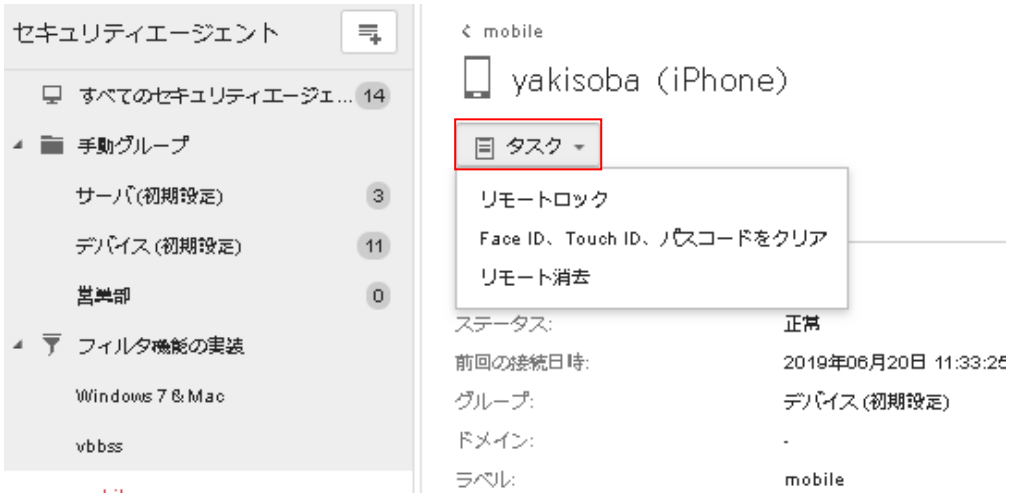
iOS

リモートロック、パスコードをクリア、リモート消去を実行します。

※リモート消去は情報をクリアして初期状態にしますので、十分に注意してください。

イベントは最新のコマンド（実行した履歴）を確認できます。

モバイルデバイス選択後、タスクより機能を選択することで実行されます。



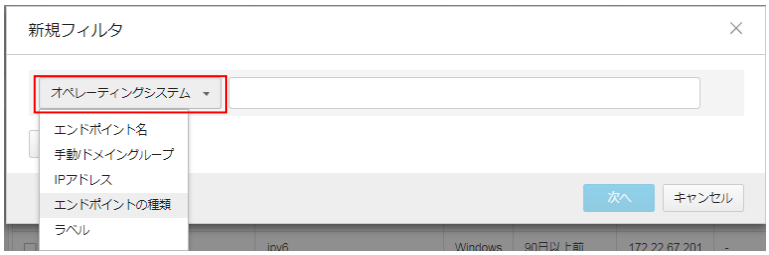
7.4. フィルタ機能

さまざまな条件でエンドポイント表示にフィルタをかけ表示させることができます。

「最新のパターンファイルを使用していないクライアント」など標準で用意されているフィルタ機能もあります。

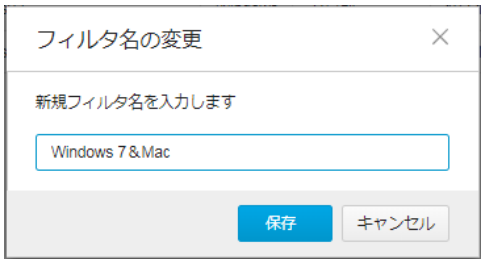
①フィルタルールを作成するにはセキュリティエージェント＋のアイコンより「新規フィルタ」を選択します。

②項目を選択します。(例ではエンドポイントの種類) OS やラベル名でフィルタできます。



③条件を選択します。複数選択、条件の追加も可能です。(例では Windows7、Mac)

④フィルタ設定に名前を付けて保存します。



⑤作成したフィルタを選択すると条件に一致するエンドポイントだけが表示されます。

削除するまでこのフィルタルールはいつでも使うことができます。

7.5. グループ機能

グループを分けることでグループごとに異なるポリシー設定や手動検索の実行などを行うことができます。

(1)グループの追加

例えば、システム部と営業部で異なる URL フィルタ設定を行うなど。

①グループを作成するにはセキュリティエージェント＋のアイコンより「新規グループ」を選択します。

②グループの名前を入力します。(例では営業部)

グループを追加する場合、その他のグループから設定をインポートすることもできます。

「ポリシー設定をインポートする」にチェックを入れソース(コピー元)となるグループを選択して「保存」をクリックしてください。

(2)ポリシー設定の複製

グループからグループへポリシー設定を複製することができます。

①ポリシー設定複製元グループのアイコンをクリックし、設定の複製を選択します。

②設定の複製先を選択します。(例ではデバイス(初期設定)→営業部)

③複製をクリックします。

(3)エンドポイントのグループを移動する

現在のグループを選択します。下記図ではデバイス(初期設定)

対象デバイスのチェックボックスにチェックを入れ、行の表示が水色反転してからドラッグ＆ドロップで移動先グループへ移動させます。(例では 2 台のエンドポイントを営業部へ移動)

エンドポイント検索やフィルタ機能で検索後にグループ移動することもできます。

※Windows クライアント移動時の注意

ファイアウォール機能を無効に設定しているグループから、ファイアウォール機能を有効に設定しているグループへエンドポイントを移動またはその逆を行う場合、ファイアウォールドライバが有効／無効に切り替わるためネットワークが一時的に切断される場合があります。このような場合、通信アプリケーションや業務を終了してから移動を行ってください。

7.6. 脅威の手動検索

エンドポイントすべてや選択単位で脅威の手動検索を行うことができます。(Windows、Mac のみ)
オフライン端末は実行されません。
通常は「通常検索の開始」を選択してください。

アグレッシブ検索の使用
アグレッシブ検索は、検出率の高いパターンを使用した、通常よりアグレッシブな手動検索です。通常検索実行後に不審な挙動が見られる場合などに実行してください。
※アグレッシブ検索では、通常検索に比べデバイスのパフォーマンスに影響する場合や、誤検出が発生する場合があります。

エンドポイントを選択して手動検索を実行する場合。
セキュリティエージェント一覧よりエンドポイントを選択して「検索」より通常検索の開始を選択します。

グループ単位で手動検索を実行する場合。
グループのアイコンをクリックし「通常検索の開始」を選択します。

検索の実行結果はエンドポイントごとに確認できます。

エンドポイント	予約検索の開始	予約検索の完了	通常検索の開始	通常検索の完了
njc01-PC	2018年9月11日 火曜日 10:00	2018年9月11日 火曜日 10:05	2018年9月12日 水曜日 08:48	2018年9月12日 水曜日 08:52
njc02-PC	2018年8月14日 火曜日 10:00	2018年8月14日 火曜日 10:09	2018年8月6日 月曜日 16:09	2018年8月6日 月曜日 16:18
njc03-PC	2018年8月14日 火曜日 10:00	2018年8月14日 火曜日 10:09	2018年8月6日 月曜日 16:10	2018年8月6日 月曜日 16:19
njc04-PC	2018年9月11日 火曜日 10:00	2018年9月11日 火曜日 10:05	2018年8月15日 水曜日 15:26	2018年8月15日 水曜日 15:26

脅威の検出があった場合にはダッシュボードやログにも記録されます。
隔離や削除ができていれば基本的には問題ありません。

7.7. パターンの手動アップデート

パターンのアップデートは 1 時間ごとに最新パターンを確認し、トレンドマイクロのアップデートサーバに最新パターンが配置されると自動的にアップデートが行われますが、脅威の対応時に即時アップデートさせたい場合や、パターンが上がっていないオンラインエンドポイントがある場合に手動アップデート指示を行うことができます。

エンドポイントを選択して今すぐアップデートを実行する場合。
セキュリティエージェント一覧よりエンドポイントを選択して「タスク」より今すぐアップデート選択します。

グループ単位で今すぐアップデートを実行する場合。
グループのアイコンをクリックし「今すぐアップデート」を選択します。

エンドポイントのパターン一覧はセキュリティエージェント一覧から確認できます。

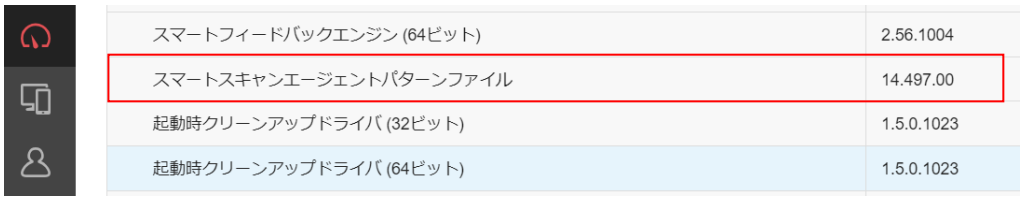
エンドポイント	ラベル	種類	ステータス	前回の接続日時	スマートスキャンエージェントパターンファイル
njc03-PC	vbbss03	Windows	オンライン	13分前	15.185.00
njc01-PC	vbbss01	Windows	オンライン	9分前	15.185.00
njc02-PC	vbbss02	Windows	オンライン	8分前	15.181.00
njc04-PC	vbbss04	Windows	オンライン	10分前	15.185.00

最新パターンの確認

ダッシュボードのセキュリティエージェントのステータスより「コンポーネントステータスの確認」をクリックすると現在の最新パターンやエンジン情報を確認することができます。

通常はスマートスキャンエージェントパターンファイル

検索方式が従来型の場合はウイルスパターンファイルになります。



パターンが上がっていないエンドポイントの確認。

ダッシュボードのセキュリティエージェントのステータスや「最新のパターンファイルを使用していないクライアント」からも確認できます。

※エンドポイントがオフラインの場合はパターンをアップデートできません。

7.8. クライアント一覧のエクスポート

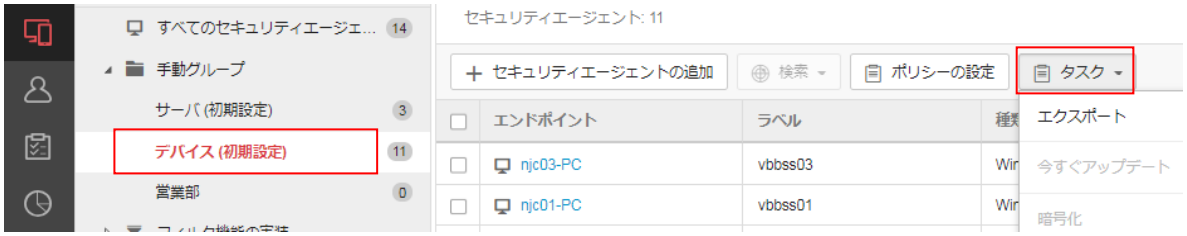
クライアント一覧を csv ファイルでエクスポートすることができます。

すべての一覧をエクスポートする場合。

すべてのセキュリティエージェントより「タスク」のエクスポートを選択します。

グループ単位でエクスポートする場合。

グループを選択後、「タスク」のエクスポートを選択します。



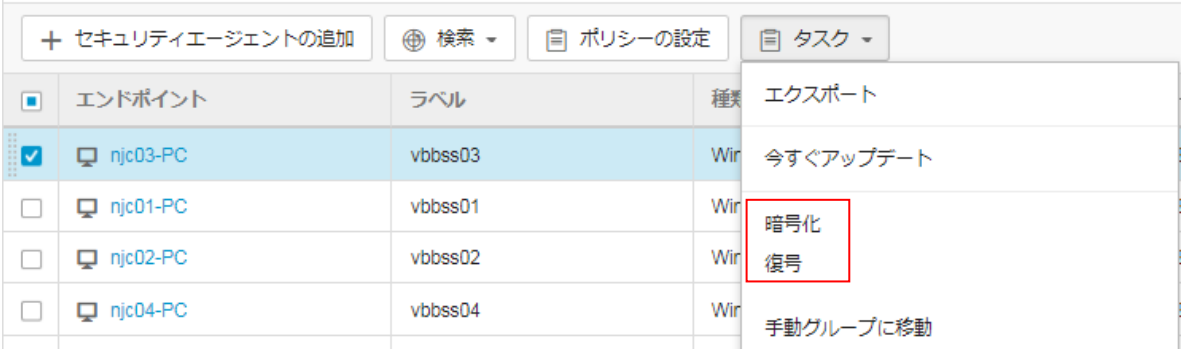
7.9. ディスク暗号化、復号

Windows の BitLocker 機能で Windows10 以降のディスク暗号化を行えます。
システム要件や暗号化ステータスについてはオンラインヘルプをご確認ください。

暗号化関連のヘルプ
https://success.trendmicro.com/jp/solution/1117023

VBBSS で暗号化ができない場合、または既に暗号化済みのステータスが正しく表示されない場合はオンラインヘルプをご確認ください。
暗号化ステータスの問題を解決する

暗号化、復号はセキュリティエージェントのエンドポイントを選択後、タスクより実行します。



暗号化ステータスもクライアント一覧より確認します。

エンドポイント	アーキテクチャ	暗号化ステータス	クライアントのバージョン
njc01-PC	x86	暗号化できません	6.3.1297/13.1.2079
njc02-PC	x86	暗号化できません	6.3.1297/13.1.2079

8. ポリシー設定

ポリシー設定について説明します。

8.1. ポリシー設定概要

初期設定でも推奨される設定が施されていますが、より強固な設定や URL フィルタリングを個別に設定したい場合などにポリシー設定を行うことで設定をカスタマイズできます。
ポリシーにはすべてのセキュリティエージェントに適用されるグローバル設定とグループごとに設定するポリシー設定があります。

8.2. ポリシー設定(グローバル)

グローバルセキュリティエージェント設定

◆セキュリティ設定一覧。
機能右側の！マークにマウスカーソルを合わせると詳細を確認できます。

◆クライアントコントロール一覧

＜重要＞

利用者がセキュリティエージェントをアンインストール／停止することを防止するために「アンインストールパスワードと終了/ロック解除パスワードを設定することを推奨します。

※Windows のみ

グローバル除外リスト

グローバル除外リスト設定一覧

◆Web レピュテーション ／ URL フィルタ

Web 閲覧や接続に関する承認済み(許可)およびブロックに関する設定を行えます。

イントラサイトや URL フィルタでブロックするカテゴリに含まれていても許可したい URL がある場合は、承認済み URL として登録します。閲覧させたくない URL をブロックするブロックする URL も登録できます。

ブロックする URL のリストよりも承認済み URL のリストが優先されます。

・承認済み URL リスト

・ブロックする URL リスト

・承認済み IP アドレスリスト

・許可されたプロセスのリスト

◆不正プログラム検索除外

特定のプログラムおよび関連プロセスを挙動監視、デバイスコントロール、およびリアルタイム検索から除外します

・信頼済み Windows プログラムリスト

・信頼済み Mac プログラムリスト

・機械学習型検索除外リスト

◆デバイスコントロール

指定された外部ストレージデバイスへのアクセスを許可します。

・許可された USB デバイスのリスト

8.3. ポリシー設定(グループ)

セキュリティエージェントより設定を行うグループのポリシーの設定を選択します。

アイコンをクリックすることでクライアント(プラットフォーム)OS の種類を切替ます。

ポリシー設定はプラットフォーム（Windows、Mac、Android、iOS）ごとに設定できる項目や詳細内容が異なります。

	Windows	Mac	Android	iOS
検索設定＜予約検索＞	○	○	○	
挙動監視＜ランサムウェア対策＞	○			
機械学習型検索	○	○		
仮想パッチ	○			
Web レピュテーション	○	○	○	
ファイアウォール設定	○			
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	○			
検索除外	○	○		
承認済み/ブロックする URL のリスト	○	△承認済みのみ	○	
権限およびその他の設定	○	○	○	
パスワード			○	
パスコード				○

(Windows)ポリシーの設定

検索方式＜予約検索＞

検索方法、リアルタイム検索、予約検索、手動検索に関する設定を行えます。
予約検索はリアルタイム検索で検知できなかった不正プログラム(新種)を後から検知できる可能性があるため、定期的に実施することを推奨します。
予約検索、手動検索の設定では検索時の CPU 使用率を設定できますが、低にするとクライアント使用状況によって検索が終わらなくなる可能性があるためご注意ください。

挙動監視＜ランサムウェア対策＞

初期設定はオンです。
挙動監視は、オペレーティングシステム、レジストリエントリ、その他のソフトウェア、ファイルやフォルダへの不正な変更からエンドポイントを保護します。
一般的なプログラムではない場合、挙動監視によってブロックされる場合があります。
そのような場合はプログラムの除外設定が必要になる場合があります。

機械学習型検索

初期設定はオフです。
機械学習型検索は、高度な機械学習テクノロジを使用して、リムーバブルストレージ、Web、メールを経由する不審なプロセスやファイルに含まれる蔓延前の未知のセキュリティリスクを検出します。
一般的なプログラムではない場合、機械学習型検索によってブロックまたは検知される場合があります。
そのような場合はプログラムの除外設定が必要になる場合があります。

仮想パッチ

初期設定はオフです
侵入防御ルールを使用してエンドポイントを保護できるようになりました。仮想パッチ機能では、ホストベースの侵入防御システム（HIPS）を使用して仮想パッチを既知の脆弱性に適用します。この機能は、挙動監視、ファイアウォール、機械学習型検索を含む包括的な保護機能の一部です。
仮想パッチルール約 150
※機能のオン／オフしかできません。ルールを個別で除外したりできないため、問題が起きた場合には仮想パッチ機能をオフにしてください。

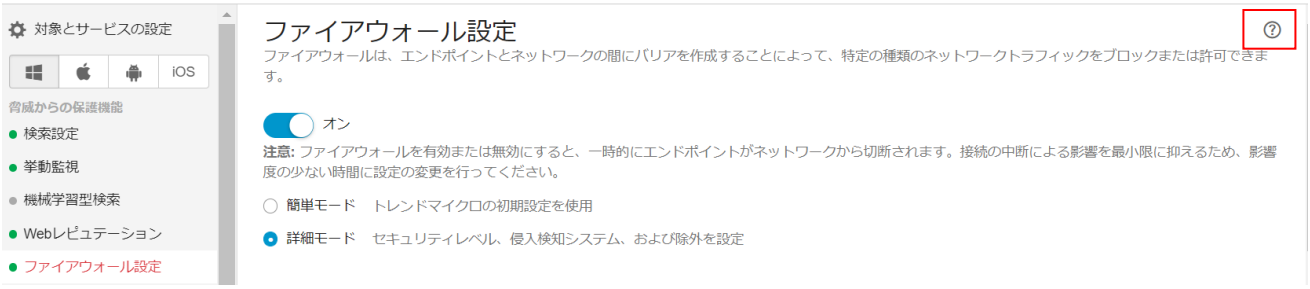
Web レピュテーション

不正 Web サイトの脅威からの保護を強化します。
2018 年 9 月 2 日以降に新規サービス利用を開始されたお客様および新しくグループを作成した場合は、セキュリティレベルの初期設定が中になっています。今までは初期設定が低でした。
セキュリティレベル中以上での利用を推奨しますが、中、高にすることによって業務に必要な Web サイトもブロックされてしまう可能性があります。業務で必要なサイトを除外設定に登録するか、セキュリティレベルを 1 つ下げるなどの変更が必要になる場合もあります。

ブラウザ脆弱性対策
Web ブラウザの脆弱性と不正スクリプトを特定し、これらの脅威の使用によって Web ブラウザが悪用されないようにします。

ファイアウォール設定

初期設定はオフです。
ネットワークウイルス検索機能を有効にする場合は、「オン」に設定します。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。
※設定を有効または、無効にする場合、一時的にネットワークが切断される場合があります。
このような場合、通信アプリケーションや業務を終了してから設定変更を行ってください。
オンにした場合は「簡単モード　トレンドマイクロの初期設定を使用」を推奨しますが、詳細モードでルールを作成することもできます。



デバイスコントロール

初期設定はオフです。

周辺デバイスへのアクセスを制御します。

デバイスコントロールを有効にする場合は、「オン」に設定します。

詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

情報漏えい対策

初期設定はオフです。
情報漏えい対策は、ネットワーク全体の機密データの転送を監視またはブロックします。
情報漏えい対策を有効にする場合は、「オン」に設定します。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

管理者は次のことを実行できます。

・メールや外部デバイスなどの一般的な転送チャネルを通したデジタル資産の転送を制限または阻止
・制定されたプライバシー標準へのコンプライアンスの実施

機密情報の漏えいの危険性を監視するには、まず次の点について確認する必要があります。
・どのデータを無許可のユーザから保護する必要があるか。
・機密データはどこにあるか。
・機密データはどのような方法で送受信されるか。
・どのユーザが機密データへのアクセスや機密データの送信を許可されているか。

◆情報漏えい対策ポリシー
VBBSS は、情報漏えい対策ポリシーで定義された一連のルールに照らしてファイルまたはデータを評価します。ポリシーによって、不正な転送から保護する必要があるファイルやデータが判別され、転送の検出時に VBBSS で実行する処理が決定されます。

DLP ポリシーを定義する設定

設定	説明
ルール	DLP ルールには複数のテンプレート、チャネル、処理を含むことができます。各ルールは、ルールを包含する DLP ポリシーのサブセットです。 注: 情報漏えい対策では、優先順位に従ってルールとテンプレートが処理されます。ルールが ″[許可]″ に設定されている場合、リスト内の次のルールが処理されます。ルールが ″[ブロック]″ に設定されている場合、ユーザの処理がブロックされ、そのルール/テンプレートはそれ以上処理されません。
テンプレート	DLP テンプレートは、データ ID と論理演算子（And、Or、Except）を組み合わせて条件文を形成します。特定の条件文を満たすファイルまたはデータだけに、DLP ルールが適用されます。 DLP ルールには、1 つまたは複数のテンプレートを含めることができます。情報漏えい対策では、テンプレートのチェック時に初回一致ルールが使用されます。これは、特定のファイルまたはデータがテンプレート内のデータ ID に一致すると、それ以上他のテンプレートがチェックされないことを意味します。
チャネル	チャネルは、機密情報を送信するエンティティです。情報漏えい対策では、メール、リムーバブルストレージデバイス、インスタントメッセンジャーアプリケーションなど、一般的な送信チャネルがサポートされます。
処理	情報漏えい対策は、いずれかのチャネルを通じて機密情報を送信する試みを検出したときに、指定された処理を実行します。
除外設定	除外設定は、設定されている DLP ルールよりも優先して機能します。除外設定により、監視対象外と圧縮ファイルの検索を管理できます。

事前定義済みの情報漏えい対策テンプレート

情報漏えい対策には、次のように、さまざまな規制基準に準拠するために使用可能な事前定義済みのテンプレートが付属しています。これらのテンプレートは、変更や削除ができません。

・GLBA:Gramm-Leach-Billey Act

・HIPAA:Health Insurance Portability and Accountability Act（医療保険の相互運用性と説明責任に関する法律）

・PCI-DSS:Payment Card Industry Data Security Standard（PCI-DSS: カード会員データや取引情報を保護することを目的に作成されたクレジット業界のセキュリティ基準）

・SB-1386:US Senate Bill 1386

・US PII:United States Personally Identifiable Information（米国で個人を特定できる情報）

すべての事前定義済みのテンプレートの目的の一覧、および保護されるデータの例については、次の情報漏えい対策に関する Web サイトをご確認ください。

https://success.trendmicro.com/jp/solution/1312344

URL フィルタ

初期設定はオンです。

Web 閲覧規制を行うことができます。初期設定では危険のあるフィッシングサイトなどをブロックする設定となります。

掲示板への書き込みのみを規制するなど、高度な制御はできません。

フィルタ強度を中、高にすると業務に関係のないサイトを選択してくれますが、カスタムルールでブロックするカテゴリを任意に設定できます。

また時間帯を指定することも可能です。

アプリケーションコントロール

初期設定はオフです。

以下の照合方法でアプリケーションをブロック／許可指定できます。

・アプリケーションレピュテーションリスト

・ファイルまたはフォルダのパス

・ハッシュ値(SHA-256) ※手動入力またはファイルのインポート

・悪用されるリスクのあるソフトウェアリスト

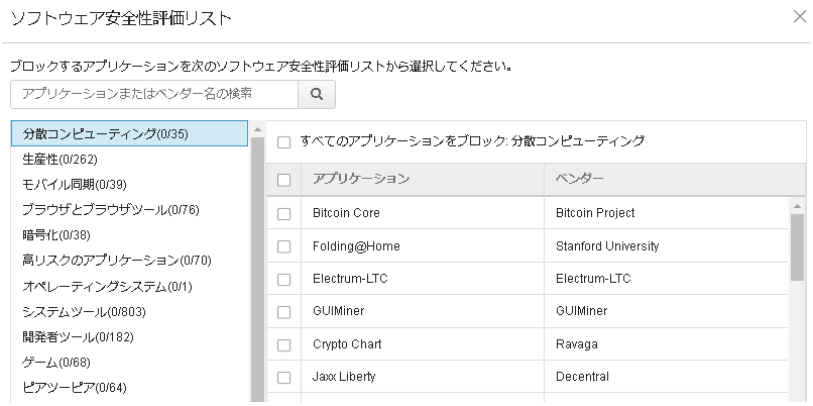
アプリケーションリストでブロック／許可されない場合は、ファイルパスやハッシュ値で指定してください。

アプリケーションコントロールを有効にする場合は、「オン」に設定します。

※ロックダウンモードはインストールや変更が禁止されているような環境可でのご利用を想定しています。

詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

例えばルールの追加で照合方法:アプリケーションレピュテーションリストを使用する場合はアプリケーションの管理(アプリケーションリスト)よりブロックや許可するアプリケーションを選択することができます。



検索除外

検索対象からフォルダ、ファイルおよびファイル拡張子単位で除外できます。
ファイルの読み書きが非常に多いアプリケーションの場合、リアルタイム検索の影響で業務に支障が出る可能性もあります。アプリケーションの仕様やナレッジで検索除外が必要な場合がありますので必ず確認してください。
例えばデータベースフォルダなど

除外対象機能
・リアルタイム検索/予約検索/手動検索（フォルダ、ファイル、ファイル拡張子）
・スパイウェア/グレーウェア（スパイウェアリストから選択）
・挙動監視（承認済みプログラムリスト、ブロックするプログラムリスト）

d:¥sqlserver と e:¥log フォルダをリアルタイム検索から除外する例です。
＋追加をクリックしてフォルダパスを追加します。

追加したフォルダがリストに表示されます。

フォルダパスを削除する場合は行の一番右にマウスカーソルを合わせます。ゴミ箱アイコンが表示されますのでクリックすると行が削除されます。

承認済み/ブロックする URL

グループごとの承認済み/ブロックする URL をカスタマイズできます。
初期値はグローバル承認済みおよびブロックする URL のリストです。
※「除外の指定」を選択するとグループ用にカスタマイズできます。
ブロックする URL のリストよりも承認済み URL のリストが優先されます。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

URL の安全性の評価を確認するには、次の Web サイトにアクセスしてください。
https://global.sitesafety.trendmicro.com/
通常の Web サイトが誤って不正な Web サイトと評価された疑いがある場合の変更リクエストや、
Web サイトがどのカテゴリに割り当てられているかの確認を行えます。

権限およびその他の設定

設定項目

・権限（クライアントへ与える権限）

・アラート（クライアントに表示させるアラート項目）

・その他の設定（セキュリティエージェントセルフプロテクション）

権限

指定した設定をセキュリティエージェント上で変更することをユーザに許可します。

※設定に関する項目はクライアント側で設定するか管理コンソール側で設定するかの択一です。可能な限りクライアントには権限を与えず、管理コンソール側で設定することを推奨します。（初期設定）

権限一覧

アラート

指定したイベントが発生すると、セキュリティエージェントアイコン上部にアラートが表示されます。

アラート設定一覧

その他設定

セキュリティエージェントセルフプロテクション

（Mac）ポリシーの設定

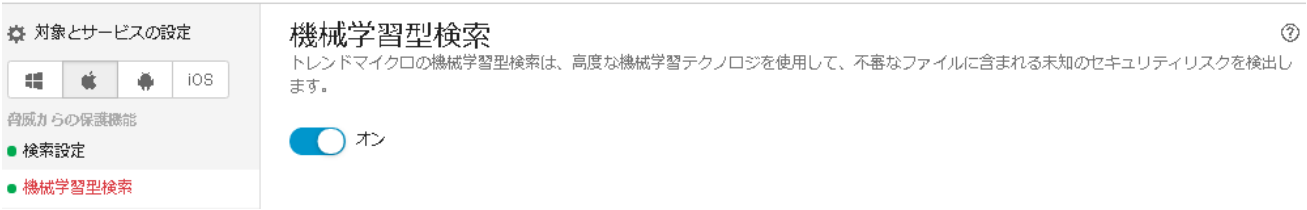
検索方式＜予約検索＞

検索方法、リアルタイム検索、予約検索、手動検索に関する設定を行えます。
予約検索はリアルタイム検索で検知できなかった不正プログラム（新種）を後から検知できる可能性があるため、定期的に実施することを推奨します。
予約検索、手動検索の設定では検索時の CPU 使用率を設定できますが、低にするとクライアント使用状況によって検索が終わらなくなる可能性があるためご注意ください。

検索設定一覧

機械学習型検索

初期値はオンです。
※機械型学習検索により検出されたログは、ウイルス/不正プログラムログに記載されます。



Web レピュテーション

不正 Web サイトの脅威からの保護を強化します。
2018 年 9 月 2 日以降に新規サービス利用を開始されたお客様および新しくグループを作成した場合は、セキュリティレベルの初期設定が中になっています。今までは初期設定が低でした。
セキュリティレベル中以上での利用を推奨しますが、中、高にすることによって業務に必要な Web サイトもブロックされてしまう可能性があります。業務で必要なサイトを除外設定に登録するか、セキュリティレベルを 1 つ下げるなどの変更が必要になる場合もあります。

デバイスコントロール

初期設定はオフです。
周辺デバイスへのアクセスを制御します。
デバイスコントロールを有効にする場合は、「オン」に設定します。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

URL フィルタ

初期設定はオンです。
Web 閲覧規制を行うことができます。初期設定では危険のあるフィッシングサイトなどをブロックする設定となります。
掲示板への書き込みのみを規制するなど、高度な制御はできません。
フィルタ強度を中、高にすると業務に関係のないサイトを選択してくれますが、カスタムルールでブロックするカテゴリを任意に設定できます。
また時間帯を指定することも可能です。

承認済み URL

グループごとの承認済み/ブロックする URL をカスタマイズできます。
初期値はグローバル承認済み URL のリストです。
※「除外の指定」を選択するとグループ用にカスタマイズできます。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

検索除外

指定した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。

権限およびその他の設定

権限

指定した設定をセキュリティエージェント上で変更することをユーザに許可します。

アラート

指定したイベントが発生すると、セキュリティエージェントアイコンの下にアラートが表示されます。

アップデート設定

VBBSS のプログラムアップデートやバージョンアップを一時的に無効に設定にする場合は、「セキュリティエージェントのアップグレードと Hotfix の配信を無効にする」を有効にします。

（Android）ポリシーの設定

検索設定

Web レピュテーション

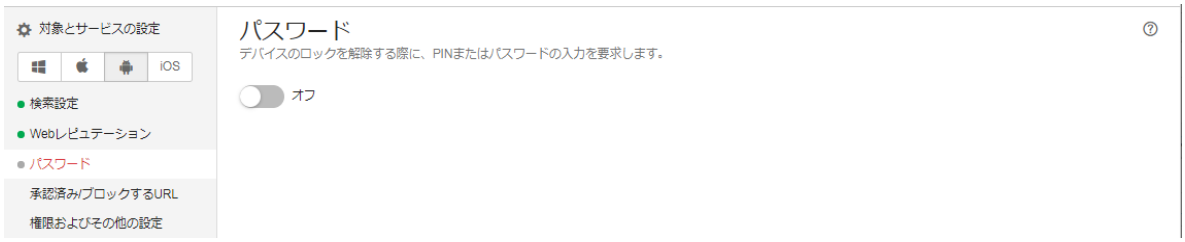
不正 Web サイトの脅威からの保護を強化します。

2018 年 9 月 2 日以降に新規サービス利用を開始されたお客様および新しくグループを作成した場合は、セキュリティレベルの初期設定が中になっています。今までは初期設定が低でした。

セキュリティレベル中以上での利用を推奨しますが、中、高にすることによって業務に必要な Web サイトもブロックされてしまう可能性があります。業務で必要なサイトを除外設定に登録するか、セキュリティレベルを 1 つ下げるなどの変更が必要になる場合もあります。

パスワード

デバイスのロックを解除する際に、PIN またはパスワードの入力を要求します。

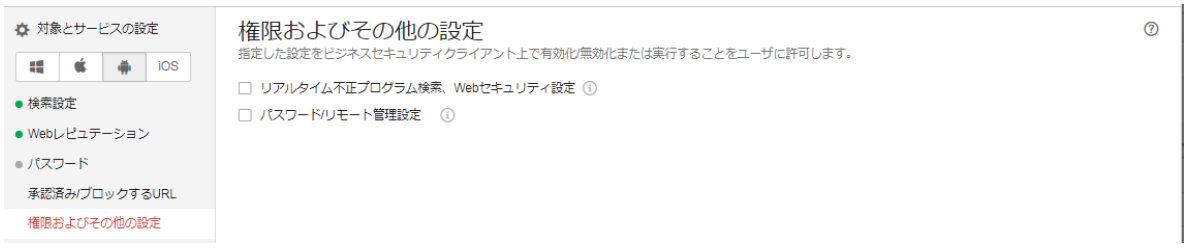


承認済み/ブロックする URL

グループごとの承認済み/ブロックする URL をカスタマイズできます。
※有効にすると、グローバル設定の［除外/ブロック設定］は、このグループには適用されません。
ブロックする URL のリストよりも承認済み URL のリストが優先されます。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

権限およびその他の設定

指定した設定をセキュリティエージェント上で有効化/無効化または実行することをユーザに許可します。



(iOS)ポリシーの設定

パスコード

パスワード関連のポリシーを強制させることができます。

有効にするにはオンにします。

60 分以内にパスコードを設定するようユーザに通知が届きます。

※60 分を超えると、パスワード設定するまで通知が繰り返され操作できません。

パスワードは「複雑さ」、「セキュリティ」パスワード変更頻度、「自動ロック」などが設定できます。

9. ユーザ

ユーザについて説明します。

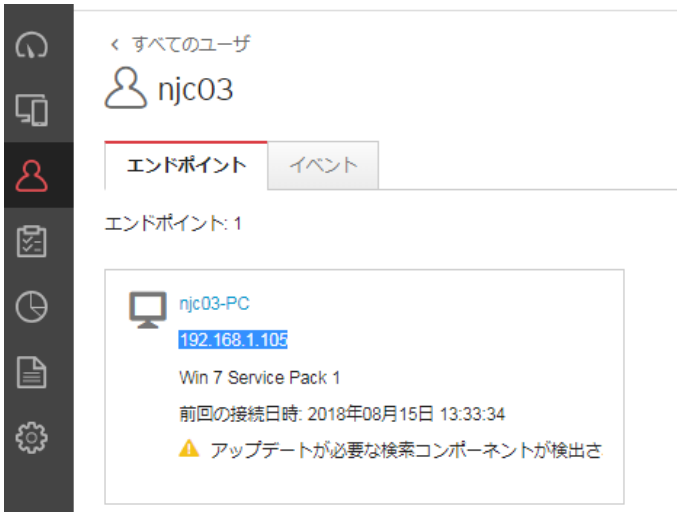
9.1. ユーザの概要

[ユーザ] 画面には、ログオンアカウント情報と、アクティブなユーザに関連付けられているエンドポイントが表示されます。保護対象のエンドポイントにユーザがログオンするたびに、VBBSS はエンドポイントをユーザカウントに関連付けて、特定のユーザの活動を監視および評価できるようにします。

エンドポイントを最後にログオンしたユーザカウントに関連付けます。たとえば、ユーザ A がエンドポイント X にログオンすると、VBBSS はリスト内でエンドポイント X をユーザ A に関連付けます。次に、ユーザ B がエンドポイント X にログオンすると、VBBSS はリスト内でエンドポイント X をユーザ B に移動します。

ユーザをクリックするとユーザに関連付けられているエンドポイント情報が表示されます。

1 ユーザが複数台使用している場合はエンドポイントが複数台表示されます。



10. レポート

レポートについて説明します。

10.1. レポートの主な機能

レポート生成やログ閲覧を行えます。「レポートの予約」により、1 回限り、週 1 回、月 1 回の予約を設定し定期的にメール送信することもできます。
レポートの送信先を指定した場合は、メールの添付として PDF 形式で送付されます。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

レポート設定一覧

レポート内容(抜粋)

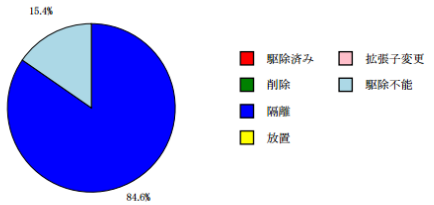
NJC | ウイルスバスター ビジネスセキュリティサービス™あんしんプラス

VBBSSレポート

開始:2017年4月13日 00:00:00JST
終了:2017年4月21日 00:00:00JST
生成日時:2017年4月20日 11:11:18JST
含まれるグループ:評価

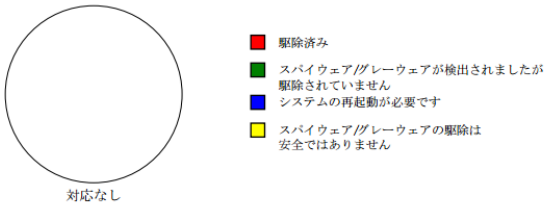
目次

ウイルス概要



処理	検出頻度	%
駆除済み	0	0.0%
削除	0	0.0%
隔離	11	84.6%
放置	0	0.0%
拡張子変更	0	0.0%
駆除不能	2	15.4%
ウイルス合計	13	
上位のウイルス名	検出頻度	%
Eicar_test_1	12	92.3%
Eicar_test_file	1	7.7%

スパイウェア/グレーウェア概要



処理	検出頻度	%
駆除済み	0	0.0%
スパイウェア/グレーウェアが検出されましたが 駆除されていません	0	0.0%
システムの再起動が必要です	0	0.0%
スパイウェア/グレーウェアの駆除は 安全ではありません	0	0.0%
スパイウェア/グレーウェア合計	0	
上位のスパイウェア名	検出頻度	%
対応なし	対応なし	対応なし

ウイルスが検出されたデバイス (サーバを除く) 上位5件

デバイス名	検出数	%
JOSHO-PC	12	92.3%
[削除されたクライアント]	1	7.7%

11. ログ

レポートについて説明します。

11.1. ログの主な機能

ウイルスログや Web レピュテーションログ、URL フィルタログなどを閲覧または csv 形式でエクスポートできます。
※ログの保存期間は 60 日間です。
詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

画面で行うことができるタスク

◆セキュリティリスクの検出:

既知または未知の脅威検出、ポリシー違反などのセキュリティイベントに関するログ

◆Web コンソールイベント:

アカウントとエンドポイントの管理、管理設定など、VBBSS のコンソールでの活動に関するログ

◆コンポーネントのアップデート:

セキュリティエージェントのコンポーネントのアップデートに関するログ

◆セキュリティエージェントイベント:

手動アップデート、パスワードのリセット、リモート消去など、セキュリティエージェントプログラムに対して行われた処理に関するログ

タスクおよびログ表示期間の選択

閲覧期間は今日・過去 7 日間・過去 14 日間・過去 30 日間・過去 60 日間・カスタム範囲の設定ができます。

セキュリティリスクログの検出表示例

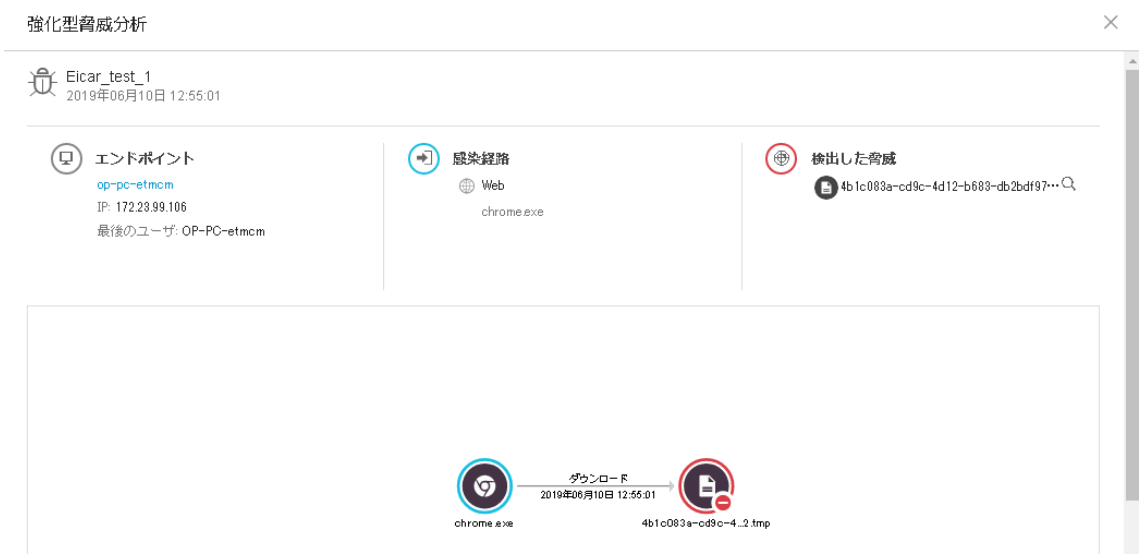
エクスポートより csv ファイルとしてダウンロードすることもできます。

※Web レピュテーションや URL フィルタログは、利用者が閲覧した回数より多い数のログが表示されることがあります。1ページ内に複数の URL が埋め込まれている場合、複数回のチェックがかかるためです。

感染経路の可視化

ログの詳細の◎をクリックすると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の確認を行えます。

簡易的な経路の確認画面



感染経路が確認可能な脅威ログのカテゴリ

・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

経路の可視化を行うには以下の設定を有効にします。

「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」タブの下記項目で設定します。

[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]:

※機能有効時は、無効の場合と比べてエージェント側のリソースを多く使用します。

検索除外の設定

ログの詳細より検索除外リストに追加することができます。

※業務上どうしても必要な場合や誤検知が疑われる場合のみ除外してください。

12. 管理

管理について説明します。

12.1. 管理の主な機能

エラー通知先のメールアドレス設定や、通知が発せられる閾値の変更などを行えます。

詳細はオンラインヘルプをご覧ください。「？」をクリックすると表示されます。

設定項目一覧

・一般設定

・モバイルデバイス登録設定

・通知

・Active Directory の設定

・Smart Protection Network

・回復キーのパスワード

・ツール

・ライセンス

・Web コンソール設定

一般設定

◆エンドポイントのラベル付け

「セキュリティエージェント」画面でエンドポイントをラベル付けすることができます

◆セキュリティエージェントのインストール用リンク

インストールパッケージの有効期限およびインストール用の URL リンクの有効期限を設定します。

※有効期限を設けることを推奨いたします。

◆クライアントツリーのクリーンナップ

セキュリティエージェントがサーバに一定期間接続されていない場合に、クライアントツリーからセキュリティエージェントを自動的に削除できます。接続が再度確立されると、サーバは削除された Windows および Mac セキュリティエージェントを自動的に復元します。

※アンインストールを忘れて撤去してしまったクライアントなどはセキュリティエージェント一覧に残り、ライセンスを消費してしまうため、設定日数経過後に自動的に削除させたい場合に設定します。

◆トラブルシューティング

サポートで必要な場合に設定を有効にしていただく場合があります。

通知設定

要確認および警告イベントのメールメッセージを送信するように VBBSS を設定します。通知の閾値を超えた場合に警告、要確認メールが送付されます。

◆設定タブ

通知先メールアドレスを登録できます。

「件名の先頭の文字列」も設定できます。

◆要確認タブ

脅威イベント・システムイベント・ライセンスイベントに関する通知をカスタマイズできます。

◆警告タブ

各脅威のイベントに対して時間に対しての検出件数を設定できます。

例えば 1 件でも検出した場合に通知させるときは「0」件の検出と設定します。

時間内に同じアラートを

13. クライアント画面

クライアント画面について説明します。

13.1. Windows クライアントのアイコン表示

クライアントのアイコン表示の意味は以下の URL を確認ください。

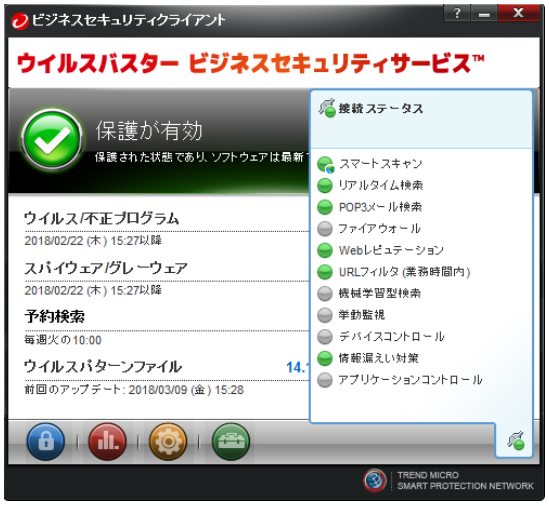
https://success.trendmicro.com/jp/solution/1310558

13.2. Windows の画面構成

タスク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」を選択するとクライアント画面が起動します。
管理コンソールからデバイスへ権限を与えられていれば、手動検索設定、検索除外設定、ファイアウォール設定などをクライアント側で設定することもできます。
※ポリシーが把握できなくなるためクライアント個々で設定を変更することは推奨しません。

(1) セキュリティエージェント画面
ウイルス／不正プログラムの検出数やパターンファイルのアップデート状況を確認できます。
緑色の場合、ソフトウェアは最新であり適切に実行されていることを示します。

右下の緑点にマウスカーソルを合わせると有効になっている機能が確認できます。



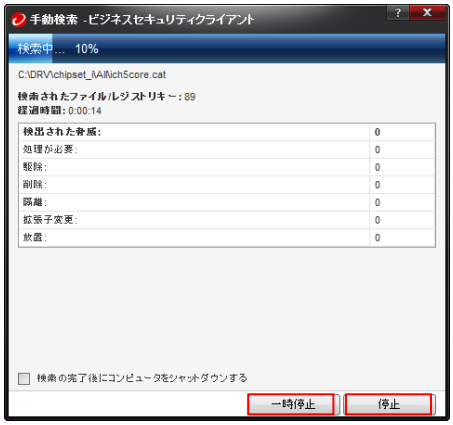
(2)検索

①手動検索を行えます。

ドライブやフォルダにチェックを入れ「検索」をクリックすると選択したディスク、フォルダのウイルスチェックを開始します。

②検索実行中の画面を表示します。

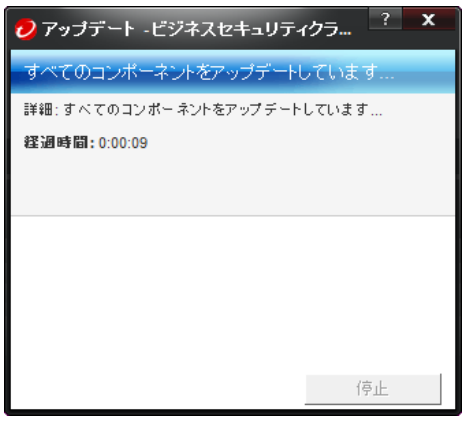
検索をやめる場合は「一時停止」か「中止」をクリックしてください。



(3)アップデート

「アップデート」をクリックするとインターネットの最新パターンを確認し、今すぐにパターンのアップデートを行うことができます。

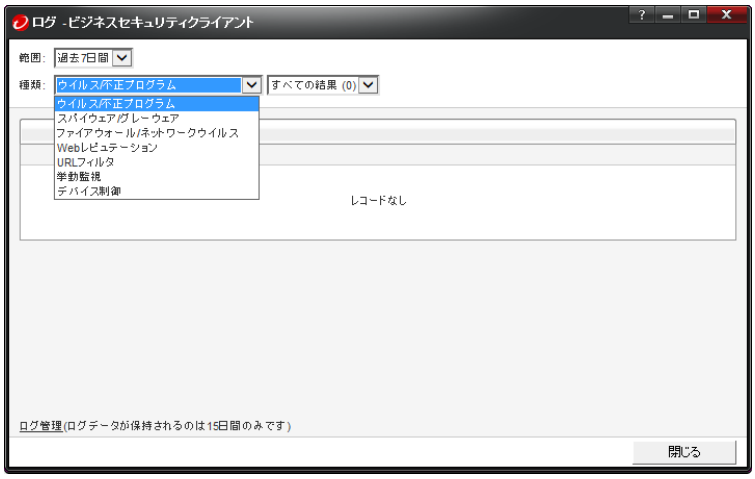
※1 時間ごとに自動で確認しています。



(4)ログ

赤いボタンをクリックするとログを確認することができます。

ウイルス、スパイウェア、ファイアウォール、Web レピュテーション、URL フィルタ、挙動監視、デバイス制御のログが閲覧できます。※クライアント側に保存されるログデータは 15 日間(初期設定)となります。



(5)設定

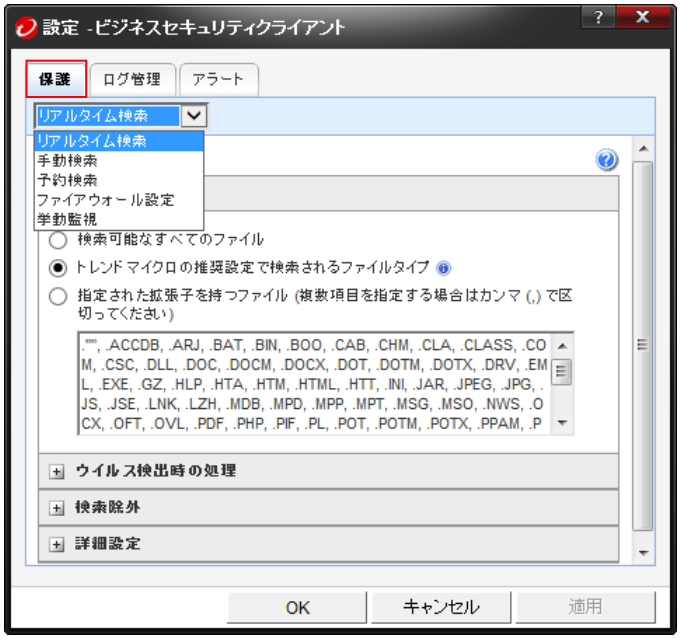
黄色いボタンをクリックすると、クライアントへ権限が与えられている場合のみ、各機能の設定変更を行うことができます。

※設定に関する項目はクライアント側で設定するか管理コンソール側で設定するかの択一です。可能な限りクライアントには権限を与えず、管理コンソール側で設定することを推奨します。(初期設定)

①保護

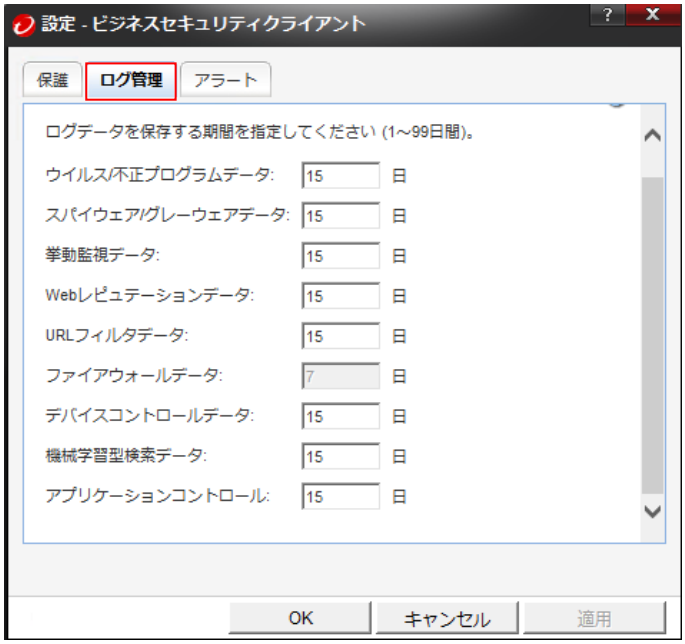
リアルタイム検索、手動検索、予約検索、ファイアウォール設定、挙動監視の設定を変更できます。

※管理コンソールのデバイス＞各グループのポリシー設定＞クライアントの権限＞セキュリティ設定タブで許可が与えられている場合のみ



②ログ管理

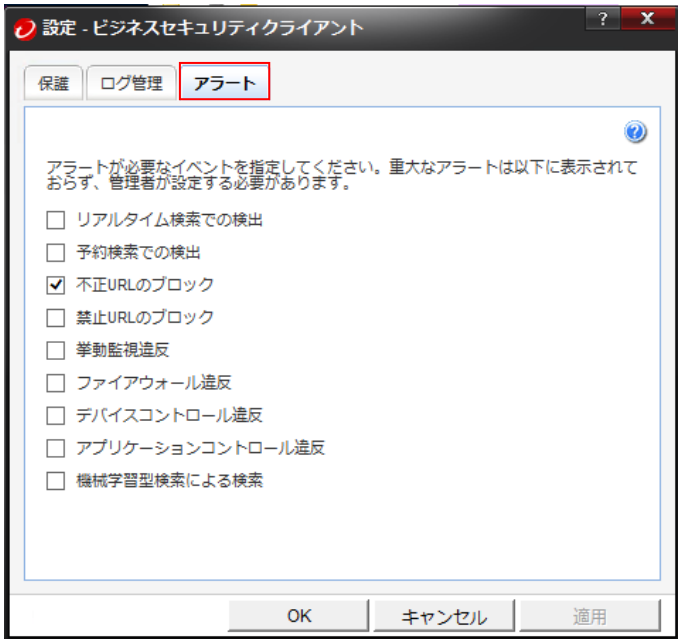
クライアントに残されるログ保存期間を 1～99 日間で設定できます。※ファイアウォールログ保存期間は除く



③アラート

クライアントに表示されるアラート表示（ポップアップ）項目を設定できます。

※クライアントでアラート表示が無効（チェックなし）の場合でも管理コンソールにはログが記録され、管理者は状況を把握することができます。



④ロック解除

管理コンソールの管理＞グローバル設定＞クライアントコントロール＞

セキュリティエージェントのロック解除と終了で「パスワード入力を要求する」を設定している場合のみ青いボタンが表示されます。設定変更の権限を与えられていないクライアントでも管理者は設定したパスワードを入力することで権限を与えられている場合と同等の設定をクライアント側で行えます。

13.3. Mac の画面構成

(1)保護状態

メニューバーのアイコンをクリックすると保護状態、エージェントやパターンファイルのバージョンを確認できます。

また、「Trend Micro セキュリティエージェントを開く」から手動アップデートや検索実行、ログの確認を行うことができます。

(2)アップデート

Trend Micro セキュリティエージェントを開きます。

「アップデート」をクリックするとインターネットへ最新パターンファイルを確認します。

※1 時間ごとに自動で確認しています。

(2) 検索

ウイルスの手動検索を行えます。

①クイック検索、カスタム検索、コンピュータ全体の検索から選択して「検索開始」クリックします、

コンピュータ全体の検索は一番時間がかかります。

②検索実行中の画面を表示します。

検索をやめる場合は「検索の停止」を一時的に止める場合は「一時停止」クリックしてください。

(3)ログ

ウイルス検知ログなどを表示できます。

①ログの種類

・セキュリティリスク

・ブロックされた Web サイト

・検索

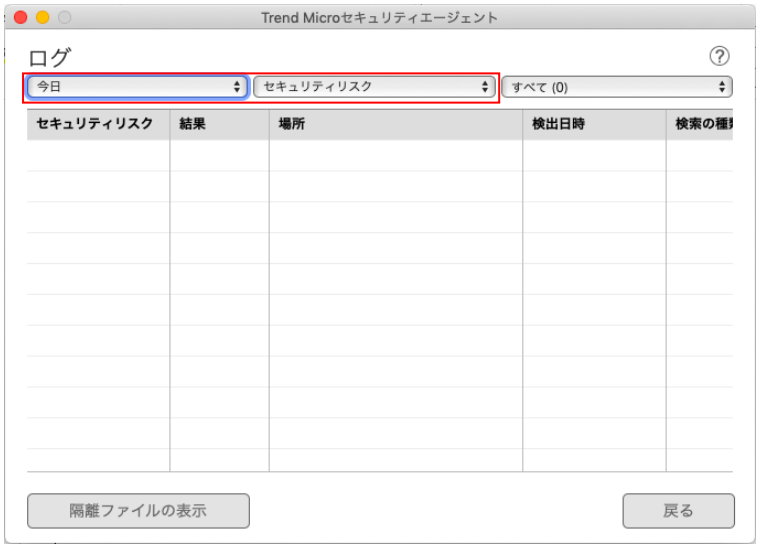
・デバイスコントロール

②期間

・今日、24 時間以内、7 日間、30 日間、カスタマイズ(期間指定)

ログを確認するにはノートアイコンをクリックします。

期間とログの種類を選択します。



13.4. Android の画面構成

※機種やバージョンにより画面とは異なる場合があります。

VBBSS アイコンをクリックします。

(1)ステータス

管理コンソールで「ユーザによるクライアント設定を許可する」に設定していると設定変更を行えます。

保護されています(緑色)になっていれば正常です。

(2)セキュリティ

不正プログラム検索と不正アプリ対策のチェックを行えます。

①不正プログラム検索

「検索開始」をクリックすると検索を開始します。

検索中画面

②「パターンファイルのアップデート」をクリックするとインターネットへ最新パターンファイルを確認します。

③不正アプリ対策

「検索開始」をクリックすると検索を開始します。

結果表示

情報を送信するようなアプリケーションが見つかった場合には表示されます。

正常なアプリケーションと認識できる場合は信頼することで以後、警告されなくなります。

不正なアプリケーションの場合はアンインストールすることを推奨します。

(3)ポリシー

ポリシー設定状況を確認できます。

管理コンソールより「許可」を与えられている場合は設定変更可能です。

・不正プログラム対策の有効/無効の切り替えや設定変更をユーザに許可する

　対象機能:ウイルス/スパイウェア対策、Web レピュテーション

・データセキュリティ対策の有効/無効の切り替えをユーザに許可する

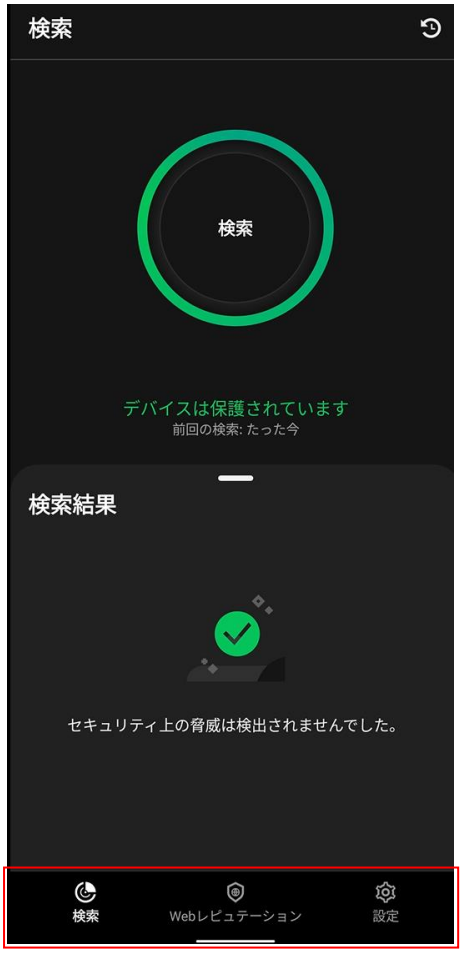
　対象機能: パスワード管理、リモート管理

13.5. Android の画面構成 バージョン 2.0.0

※機種やバージョンにより画面とは異なる場合があります。

2023 年 7 月 31 日メンテナンス後より(新バージョン 2.0.0)がリリースされます。

VBBSS アイコンをクリックすると下記画面が表示されます。



「検索」タブ

・手動検索の実行や検索履歴を確認できます。

・従来エージェントの「セキュリティ」タブに該当します。

「Web レピュテーション」タブ

・Web レピュテーション対応のブラウザを確認、検出履歴を確認できます。

・検出履歴については従来エージェントのホーム画面上部の「履歴」に該当します。

「設定」タブ

・各種設定やバージョン情報などが確認できます。

・従来エージェントの「ポリシー」タブおよびホーム画面上部の「設定」や「バージョン情報」に該当します。

SaaS 型セキュリティ対策

ウイルスバスタービジネスセキュリティサービス

ユーザーズガイド Version 2.36

発行日 : 2023 年 7 月 31 日
発行元 : 日本事務器株式会社