中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料
（ウイルスバスター ビジネスセキュリティサービス）

Ver1.0（2023.07）

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）

総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、トレンドマイクロ社の中小企業向けセキュリティ対策製品を利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業や利用者が利用時に実施すべき作業の理解を助けることを目的としています。

(イ) 前提条件

トレンドマイクロ社の中小企業向けセキュリティ対策製品として、「ウイルスバスター ビジネスセキュリティ（有償）」「ウイルスバスター ビジネスセキュリティサービス（有償）」が存在します。（2022 年 11 月 1 日現在）利用する製品により使用可能な機能が異なります。**本資料では「ウイルスバスター ビジネスセキュリティサービス」の利用を前提としております。**

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに、第 4 章では利用者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。
4 利用者向け作業	対象のチェックリスト項目に対する利用者向けの設定手順や注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2022 年 11 月 1 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
2-1 マルウェア対策 **テレワーク端末にウイルス対策ソフトをインストールし、リアルタイムスキャンを有効にする。ウイルス対策ソフトの定義ファイルを自動更新する設定にするか、手動で更新するルールを作成する。**	・ポリシー設定 – Windows 端末の設定 ・ポリシー設定 – グローバルセキュリティエージェント設定 ・ポリシー設定 – macOS 端末の設定 ・ポリシー設定 – Android 端末の設定 3 - 1 - 1	P.6 P.6 P.19 P.25
7-3 インシデント対応・ログ管理 **テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集する。**	・ログの確認 ・レポート設定	P.27 P.29

表 3. チェックリスト項目と利用者向け作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
2-1 マルウェア対策 **テレワーク端末にウイルス対策ソフトをインストールし、リアルタイムスキャンを有効にする。ウイルス対策ソフトの定義ファイルを自動更新する設定にするか、手動で更新するルールを作成する。**	・リアルタイム検索と自動アップデート	P.31

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

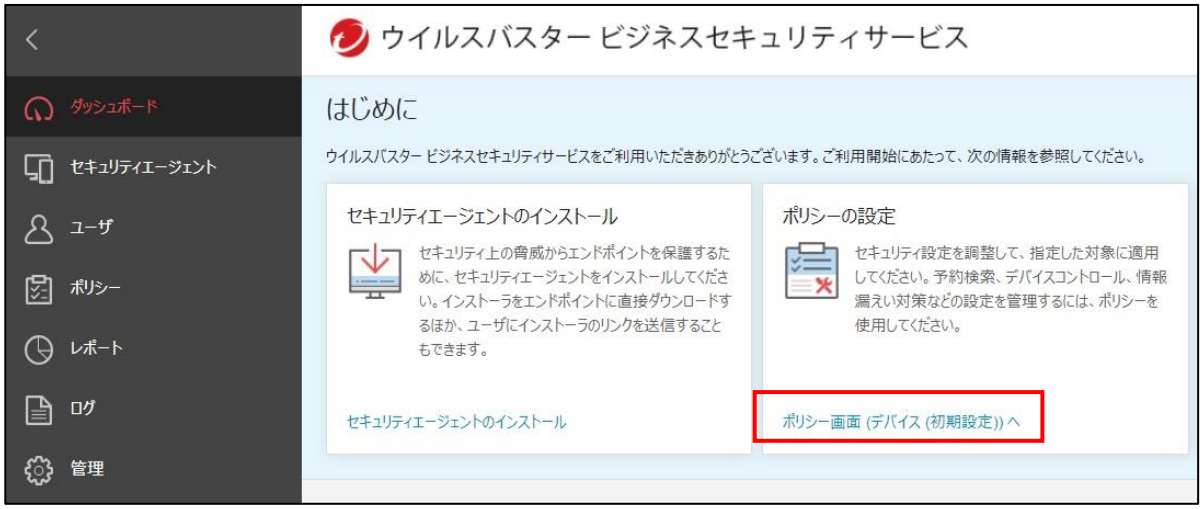
3-1 チェックリスト 2-1 への対応

3-1-1 ポリシー設定－Windows 端末の設定

ここでは、Windows 端末のマルウェア対策に関わるポリシーを設定します。

【手順①】

管理コンソール画面で「ポリシー画面（デバイス（初期設定））へ」をクリックします。



【手順②】

「ポリシーの設定：デバイス（初期設定）」画面が開くので、Windows のアイコンをクリックします。

脅威からの保護機能：検索設定

「検索設定」をクリックすると、「検索方法」「リアルタイム検索」「予約検索」「手動検索」の設定をすることができます。
（以下の記載例はデフォルトの設定）
「検索方法」は「スマートスキャン（推奨）」を選択します。

●「リアルタイム検索」の設定

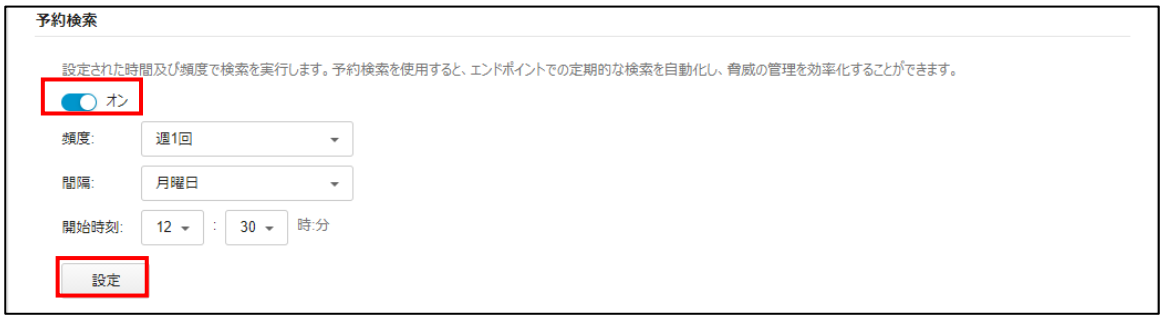
「リアルタイム検索」欄で「設定」をクリックし「リアルタイム検索設定」画面を開きます。

必要に応じて、リアルタイム検索の設定を変更します。

（以下の記載例はデフォルトの設定）

●「予約検索」の有効化と設定

「予約検索」欄で設定をオンにすると「頻度（月１回/週１回/毎日）」「間隔（日曜から土曜の曜日指定）」「開始時刻」を指定できます。「設定」をクリックすると「予約検索設定」画面が開きます。



必要に応じて、予約検索の設定を変更（※）します。

（以下の記載例はデフォルトの設定）

※　「グローバルセキュリティエージェント設定」の「セキュリティ設定」の「一般検索」の「行われなかった予約検索を翌日の同じ時刻に実行」にチェックしておくことで予約検索が実行できなかった場合、翌日に実行するように設定できます。この項目はデフォルトでチェックが入っています。

●手動検索の設定

「手動検索」欄で「設定」をクリックし、「手動検索設定」画面を開きます。

必要に応じて、手動検索の設定を変更します。

（以下の記載例はデフォルトの設定）

（参考）脅威からの保護機能：挙動監視

「挙動監視」を開くと「不正プログラム挙動ブロック」「ランサムウェア対策」「脆弱性対策」「イベント監視」の設定をすることができます。

（以下の記載例はデフォルトの設定）

●イベント監視の有効化と設定

「イベント監視」欄から、この設定をオンにすると、監視するシステムのイベントを指定することができます。
（以下の記載例はデフォルトの設定）

（参考）脅威からの保護機能：機械学習型検索

「機械学習型検索」を開くと、検出時の処理（ファイル：隔離/ログのみ、プロセス：終了/ログのみ）の設定ができます。
この機能は、デフォルトで ON になっています。（以下の記載例はデフォルトの設定）

（参考）脅威からの保護機能：Web レピュテーション

「Web レピュテーション」の設定により、不正な Web サイトをブロックし端末を保護することができます。
（以下の記載例はデフォルトの設定）

（参考）エージェントの設定：権限およびその他の設定

●権限の設定

テレワークをしているユーザ側で設定変更を行える項目を指定できます。

●アラートの設定

指定したイベントが発生した時に、各端末のセキュリティエージェントアイコンの上にアラートを表示させることができます。

●その他設定

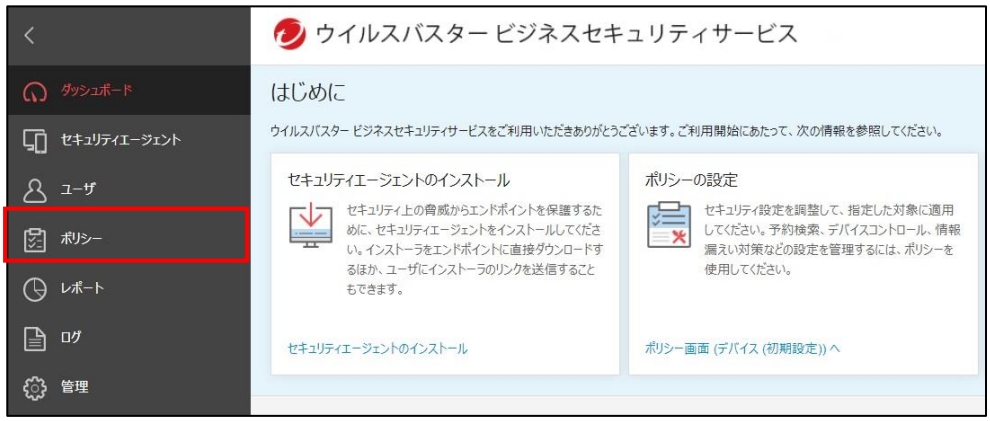
セルフプロテクションの設定ができます。これにより、不正なプログラムや実際のユーザがセキュリティエージェントを無効化することを防ぎます。

3-1-2　ポリシー設定－グローバルセキュリティエージェント設定

この項目では、すべてのセキュリティエージェントに適用される設定を行います。様々な設定を自社の環境に応じて設定することで、テレワーク端末がマルウェアに感染した場合に即座に検知、防御することができます。

【手順①】

管理コンソール画面で「ポリシー」を開きます。



【手順②】

「グローバルセキュリティエージェント設定」の「セキュリティ設定」から、「一般検索」「ウイルス検索」「スパイウェア/グレーウェア検索」「挙動監視」「HTTPS Web 評価」といった項目を必要に応じて設定・変更します。

（以下の記載例はデフォルトの設定）

【手順③】

「グローバルセキュリティエージェント設定」の「エージェントコントロール」から、「警告」「セキュリティエージェントのログ」「監視サービス」「管理者への問い合わせの通知」「アンインストール」「終了/ロック解除」 といった項目を必要に応じて設定します。

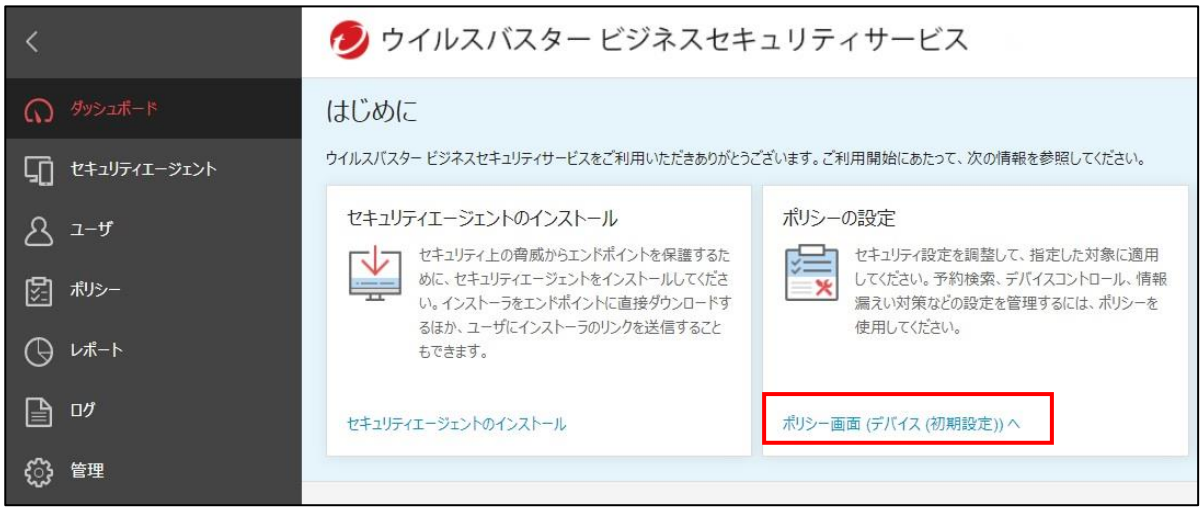
（以下の記載例はデフォルトの設定）

3-1-3　ポリシー設定－macOS 端末の設定

この項では、macOS 端末のマルウェア対策に関わるポリシーを設定します。

【手順①】

管理コンソール画面で「ポリシー画面（デバイス（初期設定））へ」をクリックします。



【手順②】

「ポリシーの設定：デバイス（初期設定）画面」が開くので、Apple のアイコンをクリックします。

脅威からの保護機能：検索設定

「検索設定」をクリックすると、「検索方法」「リアルタイム検索」「予約検索」「手動検索」の設定をすることができます。

（以下の記載例はデフォルトの設定）

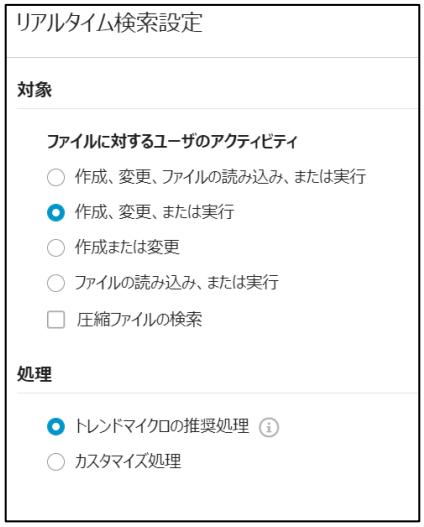
「検索方法」は「スマートスキャン（推奨）」を選択します。


ポリシーの設定: デバイス (初期設定)
対象とサービスの設定
iOS
脅威からの保護機能
検索設定
機械学習型検索
Webレピュテーション
情報漏えい対策
デバイスコントロール
アクセスコントロール
URLフィルタ
除外リスト
承認済みURL
検索除外
エージェントの設定
権限およびその他の設定
検索設定
検索方法
スマートスキャン (推奨)
スマートスキャンでは、インターネットクラウドに格納されている不正プログラム対策シグネチャおよびスパイウェア対策シグネチャが利用されます。
従来型スキャン
従来型スキャンは、セキュリティエージェントのローカルに格納されている不正プログラムやスパイウェア対策コンポーネントを利用します。
リアルタイム検索
ファイルを受信、開く、ダウンロード、コピー、または変更したときに、セキュリティ上のリスクがあるかファイルを検索します。
オン
設定
予約検索
設定された時間及び頻度で検索を実行します。予約検索を使用すると、エンドポイントでの定期的な検索を自動化し、脅威の管理を効率化することができます。
オフ
手動検索
Webコンソール上の [セキュリティエージェント] 画面またはセキュリティエージェントコンソールから開始される手動検索です。
設定
保存
キャンセル

●「リアルタイム検索」の設定

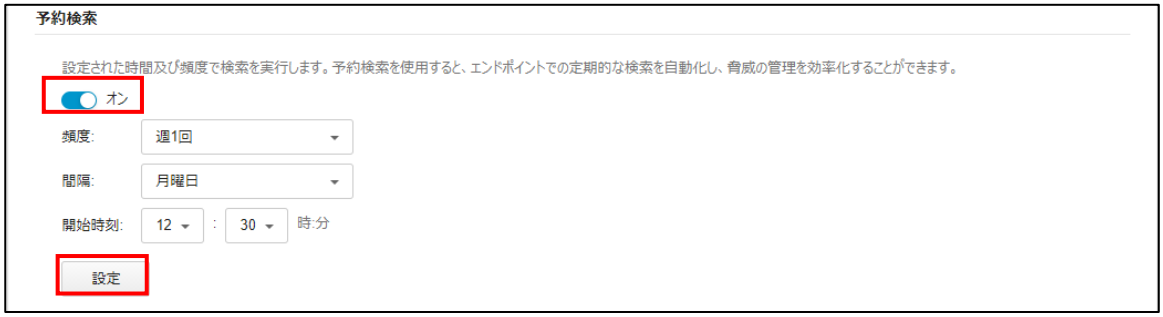
「リアルタイム検索」欄で「設定」をクリックし「リアルタイム検索設定」画面を開きます。

必要に応じて、リアルタイム検索の設定を変更します（。以下の記載例はデフォルトの設定）



●「予約検索」の有効化と設定

「予約検索」欄で設定をオンにすると「頻度（月１回/週１回/毎日）」「間隔（日曜から土曜の曜日指定）」「開始時刻」を指定できます。「設定」をクリックすると「予約検索設定」画面が開きます。



必要に応じて、予約検索における設定を変更（※）します。（以下の記載例はデフォルトの設定）

「グローバルセキュリティエージェント設定」の「セキュリティ設定」の「一般検索」の「行われなかった予約検索を翌日の同じ時刻に実行」にチェックしておくことで予約検索が実行できなかった場合、翌日に実行するように設定できます。デフォルトはチェックが入っています。

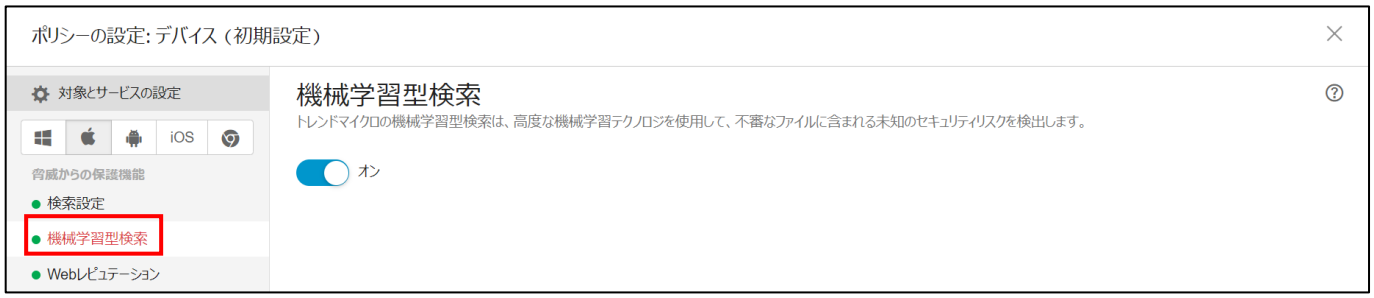
●「手動検索」の設定

「手動検索」欄で「設定」をクリックし「手動検索設定」画面を開きます。

必要に応じて、手動検索の設定を変更します。（以下の記載例はデフォルトの設定）

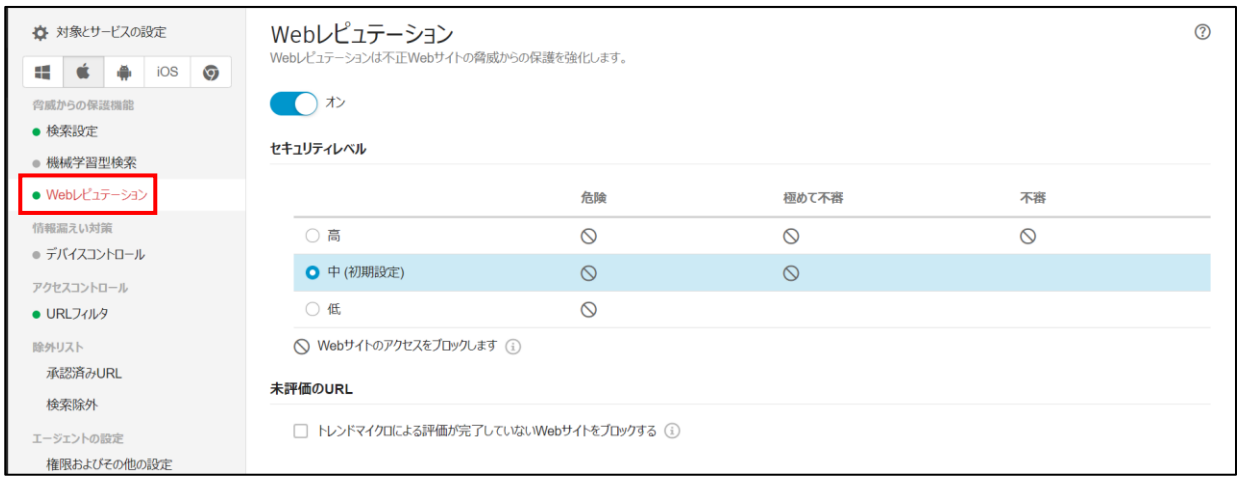
（参考）脅威からの保護機能：機械学習型検索

「機械学習型検索」をオンに設定することで、機械学習型検索を有効にできます。この機能は、デフォルトで ON になっています。（以下の記載例はデフォルトの設定）



（参考）脅威からの保護機能：Web レピュテーション

Web レピュテーションの設定により、不正な Web サイトをブロックし端末を保護することができます。
（以下の記載例はデフォルトの設定）



（参考）エージェントの設定：権限およびその他の設定

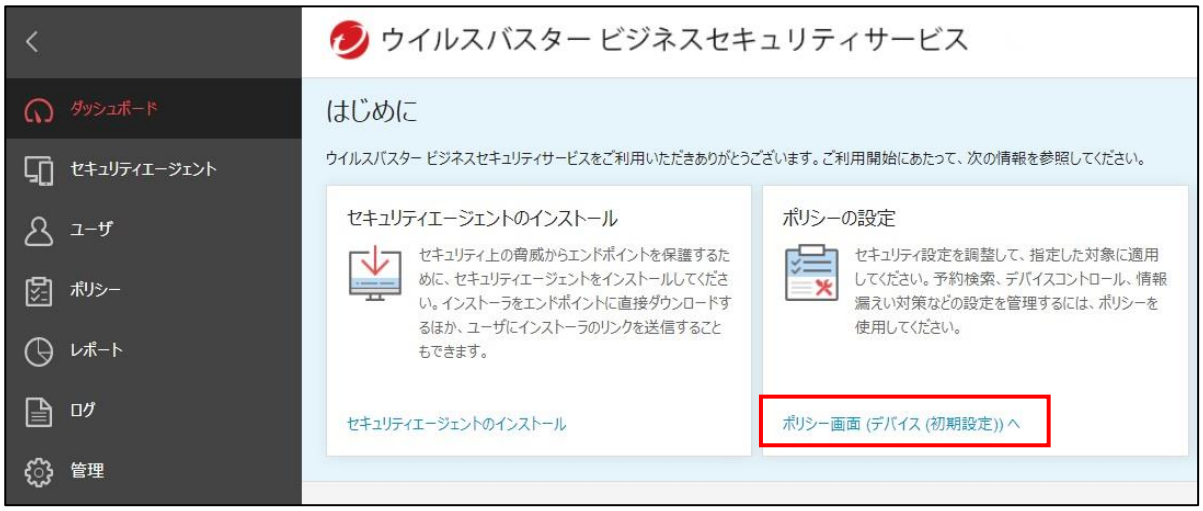
ユーザに許可する権限やエージェントへのアラートの表示、アップデート設定などを行うことができます。

3-1-4　ポリシー設定－Android 端末の設定

この項では、Android 端末のマルウェア対策に関わるポリシーを設定します。

【手順①】

管理コンソール画面で「ポリシー画面（デバイス（初期設定））へ」をクリックします。



【手順②】

「ポリシーの設定：デバイス（初期設定）画面」が開くので、Android のアイコンをクリックします。

検索設定

「リアルタイム不正プログラム検索」をオンにします。この設定はデフォルトでオンになっています。

（参考）Web レピュテーション

Web レピュテーションの機能により、不正な Web サイトをブロックし端末を保護することができます。
（以下の記載例はデフォルトの設定）

（参考）権限およびその他の設定

端末のセキュリティエージェント上で、ユーザ実行/設定変更できる項目を指定することができます。

3-2 チェックリスト 7-3 への対応

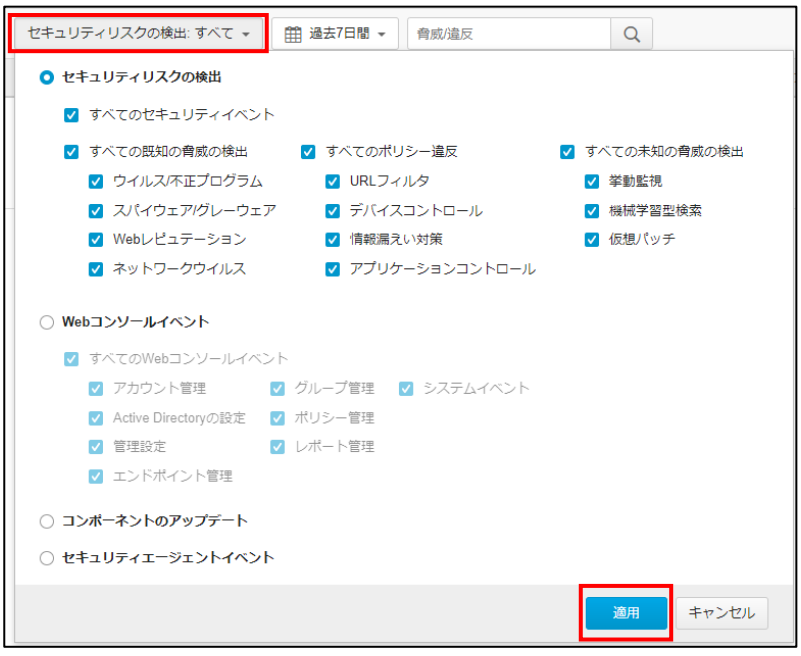
本製品では、セキュリティイベントのログの確認やセキュリティイベントのレポートを配信する設定を行うことができます。
セキュリティイベントのレポートを用いて、テレワーク環境で不審なイベントが発生していないか定期的に確認することで、**セキュリティインシデントの被害が拡大するリスクを低減することができます。**

3-2-1 ログの確認

管理コンソール上でセキュリティリスクの検出ログ、web コンソールのイベントログ、各端末のセキュリティエージェントのイベントログなどを確認することができます。

【手順①】
管理コンソールにログインして、「ログ」をクリックします。

【手順②】
「セキュリティリスクの検出:すべて」をクリックし、確認したいイベントにチェックを入れ、「適用」をクリックします。
このとき、ログの表示期間も同時に指定することができます。



【手順③】

詳細を確認したい端末をクリックすると、端末の「情報」と「イベント」を確認することができます。

「情報」タブからは、端末の詳細を確認することができます。

「イベント」タブからは、イベントの詳細を確認することができます。

3-2-2　レポート設定

この項では、管理コンソール上でセキュリティのイベントに関わるレポートを PDF 形式でメール受信できるように設定を行います。

【手順①】

管理コンソールにログインして、「レポート」を開き、「追加」をクリックします。

【手順②】

レポート設定画面が開くので、「一般設定」欄で任意のレポート名を入力し、「検索」欄でレポートの生成間隔を指定し、「対象」欄ですべての端末か特定のグループを対象にするか選択します。

「レポートの内容」欄で確認したいセキュリティイベントを選択して、レポートの受信メールアドレスを入力して「保存」をクリックします。


レポート設定
レポートの内容
すべてのセキュリティイベント
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
URLフィルタ
挙動監視
デバイスコントロール
ネットワークウイルス
受信者
メールアドレス:
例: user1@example.com; user2@example.com
注意: レポートは指定された受信者宛てにPDF形式の添付ファイルとして送信されます。
保存
キャンセル

４利用者向け作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の利用者が実施すべき対策の設定手順や注意事項を記載します。

４-１　チェックリスト２-１への対応

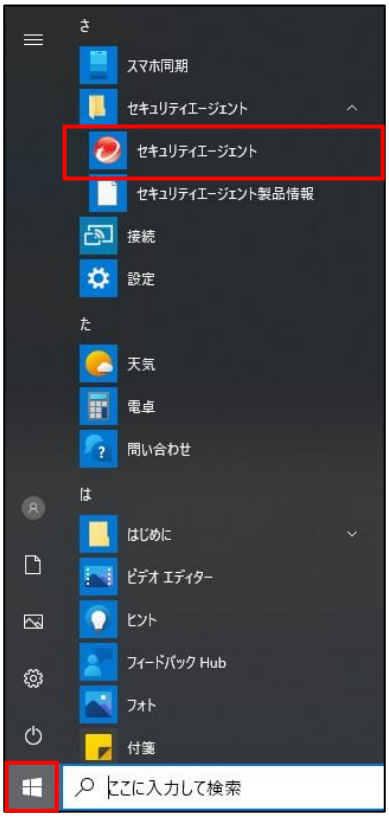
４-１-１　　リアルタイム検索と自動アップデート

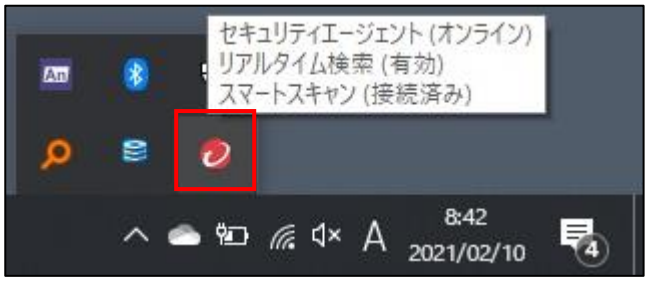
リアルタイムでの保護を有効にすることで、**テレワーク端末がマルウェアに感染した場合に即座に検知、防御することができます。**ウイルスバスタービジネスセキュリティサービスでは、リアルタイム検索はデフォルトで有効になっており、自動アップデートは１時間ごとに行われます。そのため、基本的に手動アップデートや手動検索は不要ですが、手動で実施する場合は、下記を参考に実施してください。

（参考）Windows 端末での手動アップデートと手動検索

【手順①】

スタートメニューの「セキュリティエージェント」からセキュリティエージェントを起動します。またタスクバーの通知領域の「セキュリティエージェント」アイコンから起動することもできます。





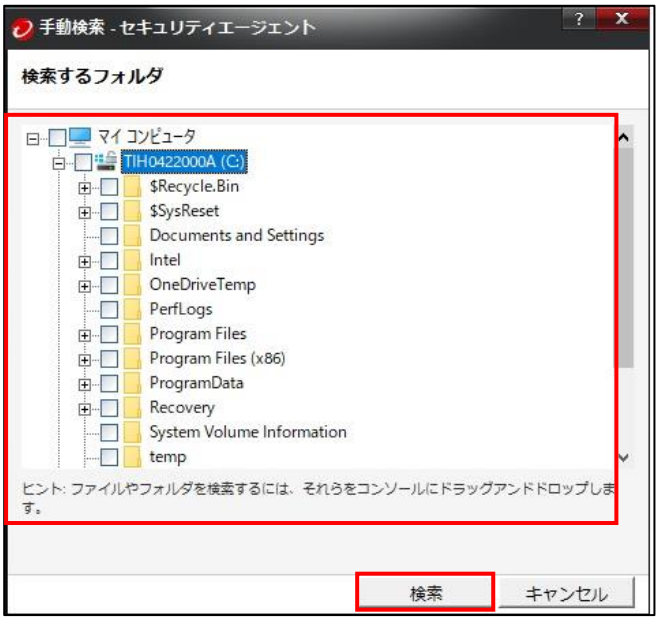
【手順②】

●手動アップデートの実行

セキュリティエージェントの「アップデート」をクリックすると、手動でマルウェアの定義ファイル等をアップデートできます。

●手動検索の実行

セキュリティエージェントの「検索」をクリックし、検索するフォルダを指定して「検索」をクリックすると手動で検索できます。



（参考）macOS 端末での手動アップデートと手動検索

【手順①】

Trend Micro セキュリティエージェントをクリックし、「セキュリティエージェントコンソールを開く」をクリックします。

【手順②】

●手動アップデートの実行

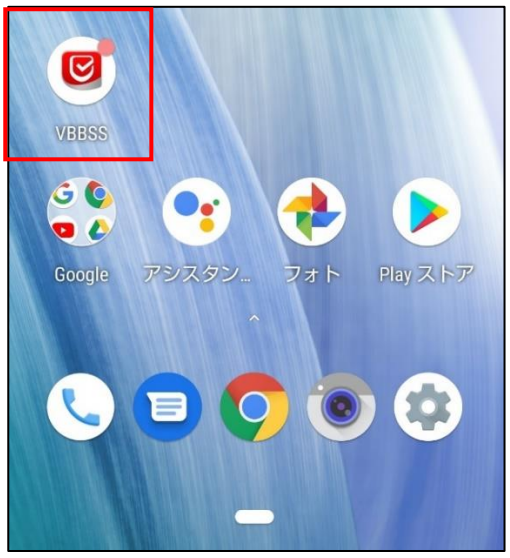
「アップデート」をクリックすると、手動でマルウェアの定義ファイル等をアップデートできます。

●手動検索の実行

「検索」をクリックすると端末内のファイルの検索方法として、「クイック検索」「カスタム検索」「コンピュータ全体の検索」が選択できます。必要に応じてそれぞれの検索方法で検索します。

（参考）Android 端末での手動アップデートと手動検索

ホーム画面から、「VBBSS」をタップし、アプリを起動します。



●不正プログラムの手動アップデートと手動検索の実行

【手順①】

「セキュリティ」をタップし、「不正プログラム検索」をタップします。

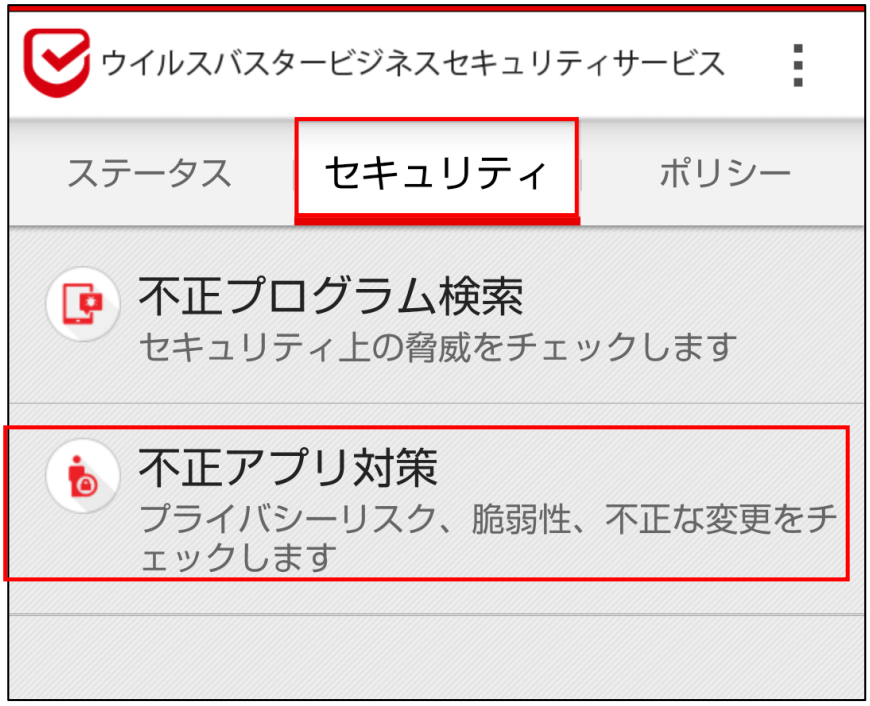
【手順②】

手動検索する場合は「検索開始」をタップし、手動アップデートする場合は「パターンファイルのアップデート」をタップします。

●不正アプリ対策の手動検索の実行

【手順①】

「セキュリティ」をタップし「不正アプリ対策」をタップします。



【手順②】

「検索開始」をタップします。