おまかせデータレスPC
ウイルス対策機能
初期設定簡易マニュアル

Ver.1.1

２０２１．１

ＮＴＴ東日本

機能一覧

■セキュリティ機能一覧

機能		詳細
検索設定 (ウイルス、スパイウェア対策)	検索方法	ウイルスの侵入を検知し、アクセス拒否、削除、名前変更、隔離、駆除を行います。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。リアルタイム検索、予約検索、手動検索を設定することができます。
	POP3 メール検索	POP3メール検索により、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。
	ファイルレス 攻撃対応	ハードディスクに保存されず、メモリ上にのみ存在するウイルスを検知・隔離します。
挙動監視	全般	OS、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に対する不正変更を監視・ブロックします。
	ランサムウェア 対応	ランサムウェア（身代金要求ウイルス）に対し、各種セキュリティ機能を複合的に実施して防ぐと共に、ランサムウェア独自の挙動に対して有効な対処やファイルの復元を行います。
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。
仮想パッチ		仮想パッチとは、脆弱性そのものを修正する正規パッチとは異なり、脆弱性を突く攻撃をネットワークレイヤで検知およびブロックするものです。脆弱性発覚後、各ベンダーから正規パッチがリリースされるまでの間、仮想パッチにより、本脆弱性を衝く攻撃のリスクを軽減することができます。
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。
ファイアウォール設定		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。
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。
情報漏えい対策		機密データの転送を監視・ブロックします。
URLフィルタ		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
アプリケーションコントロール		カテゴリ、ベンダー、アプリケーション名を指定してアプリケーションの利用を制限できます。

機能一覧

■管理機能一覧

機能		詳細
エージェントコントロール	エージェントアンインストール防止	指定のパスワードを入力しないとビジネスセキュリティクライアントツールのアンインストールができないようにします。
	エージェント終了防止	指定のパスワードを入力しないとツールの終了/ロック解除ができないようにします。
ラベル表示		管理者が各デバイスの名称を管理コンソール上で判別しやすいようにラベル登録することができます。
通知		ウイルス感染時やソフトウェアの勝手な変更を行った際に、管理者へメール通知がされるように設定することが可能です。
除外設定		指定したフォルダ、ファイル、ファイル拡張子を検索しないようにします。 （過検知により正常なファイルが隔離されてしまうなどの場合に有効）
承認済み/ブロックするURL		指定したURLを常に許可/ブロックします。
感染経路の可視化		セキュリティイベント（脅威）が検出されるまでの簡易的な経路を確認できるようにします。

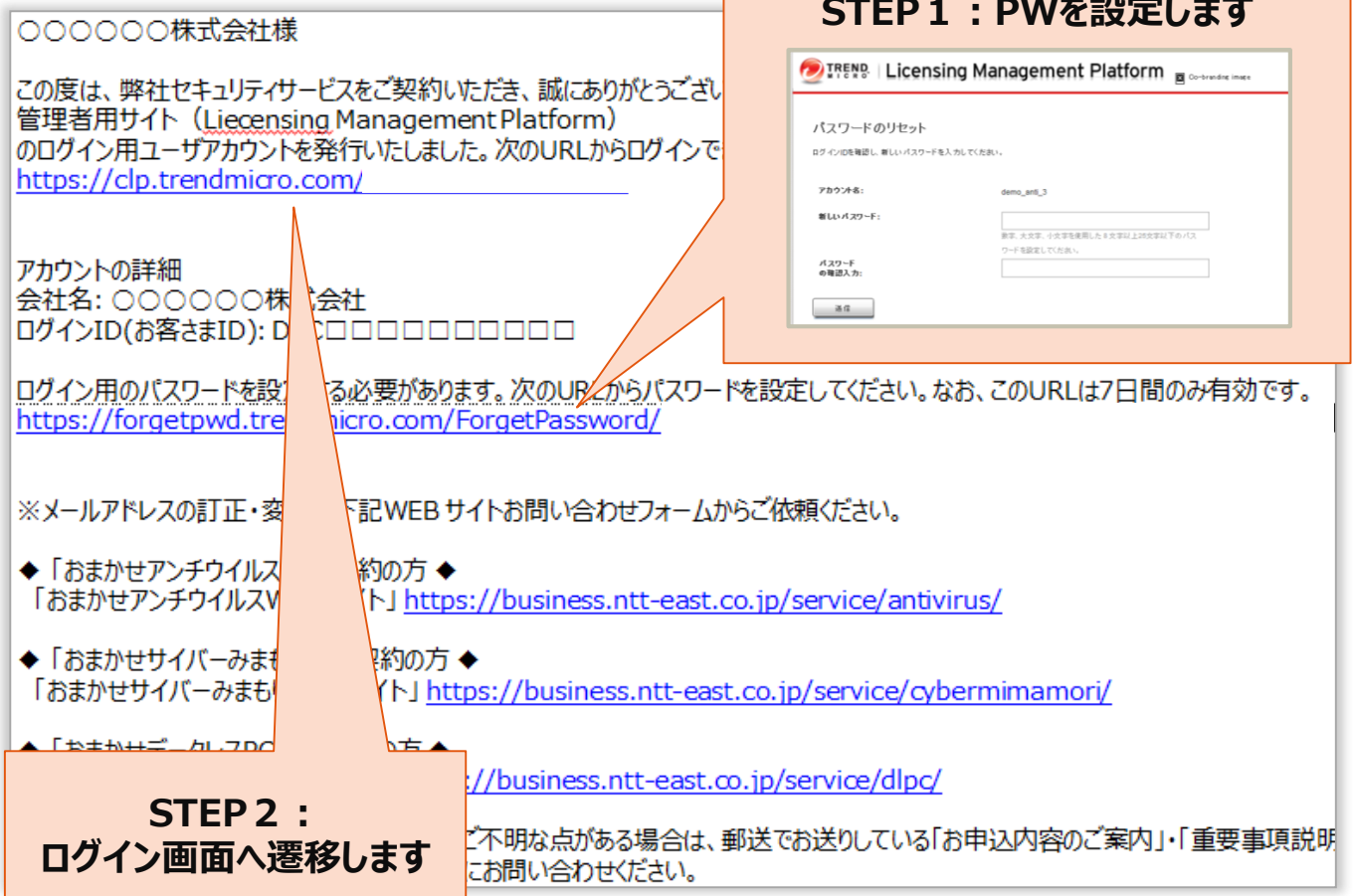
■その他機能一覧

機能	詳細
グループ管理	ライセンス数が多い場合など、グループを作成し管理を容易にすることができます。
フィルタ管理	特定の条件に該当するエンドポイントを確認したい場合などは、フィルタを作成し管理を容易にすることができます。
予約検索	金曜日のお昼にウイルスチェックするなど、デバイスの脅威を定期的に検索することができます。
手動アップデート	ビジネスセキュリティクライアントを最新のコンポーネントに手動でアップデートできます。

サービスへのログイン

おまかせデータレスPCのウイルス対策機能をより便利にご活用いただくため、必要なPWを設定し、管理コンソールにログインします。

件名：【NTT東日本】おまかせアンチウイルス・おまかせサイバーみまもり・おまかせデータレスPC新規アカウント発行のお知らせ　のメールを使います。



STEP１：PWを設定します

STEP２：
ログイン画面へ遷移します

STEP３：
『アカウントID（ログインID）』
『設定したPW』を投入し、ログイン

サービスへのログイン

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

二要素認証とは…

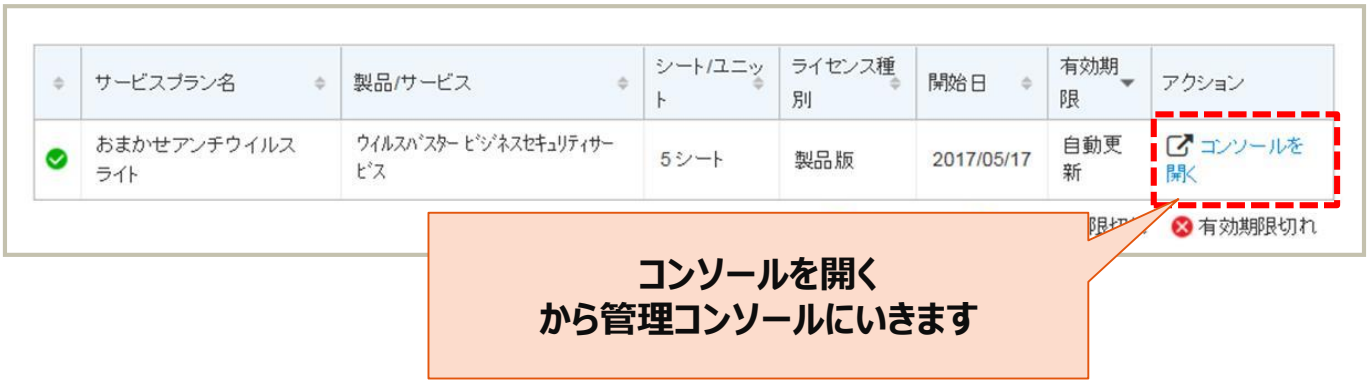
- 管理コンソールのログインにあたり、従来の ID ・パスワードに加えて“ワンタイムパスワード”を用いて認証を行うことで、セキュリティをさらに強化（第三者からの管理コンソールへの不正にログインを防止）することができます。
- ご利用の場合には、お手持ちの PC やスマートフォンに、第三者の提供するトークンアプリをインストール・設定する必要があります。
- トークンアプリは NTT 東日本およびトレンドマイクロ社の提供するものではなく、これをご利用になったことにより何らかの損害が発生した場合でも NTT 東日本およびトレンドマイクロ社では責任を負いかねますので、ご了承ください。

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

設定する場合はココをクリック

設定しない場合はココをクリック

サービスへのログイン

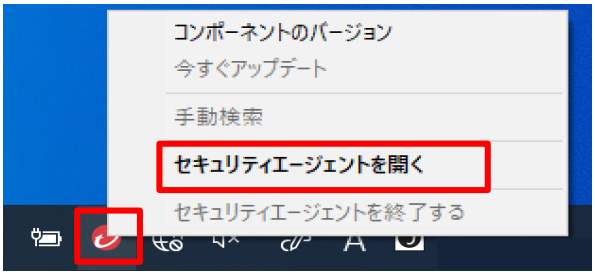


コンソールを開く
から管理コンソールにいきます

ダッシュボードが表示されたら
ログイン完了です

エージェントアイコン表示

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



番号	機能	詳細
1	ステータス	セキュリティエージェントのメイン画面に表示されるアイコンやその意味と対処内容を示しています。
		保護が有効
		コンピュータの再起動が必要/危険な状態
		今すぐアップデートが必要/Chromeの再起動が必要
		スマートスキャン使用不可/コンピュータの再起動が必要/アップデートが必要
2	ログ	関連するログ情報が表示されます。
3	設定	ビジネスセキュリティクライアントの各設定の表示および設定に使用されます。
4	ユーザツール	トレンドマイクロが提供するその他のツールに関する情報が示されます。

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

機能を設定する

デフォルトで以下の機能が設定されています。必要に応じ、設定変更をお願いします。

※NTT東日本の「セキュリティサポートデスク」にて代行設定が可能です。

機能			設定内容（デフォルト）	ページ番号
セキュリティ機能	検索設定	検索方法	スマートスキャン	12
		POP3メール検索	無効	13
		ファイルレス攻撃対応	無効	15
	挙動監視	全般	有効	18
		ランサムウェア対応	有効	19
	機械学習型検索		無効	20
	仮想パッチ		無効	21
	Webレピュテーション		有効（中）	22
	ファイアウォール設定		無効	23
	デバイスコントロール		一部機能のみ有効 ※「USBストレージデバイスでの自動実行機能をブロック」機能のみ有効	24
	情報漏えい対策		無効	28
	URLフィルタ		有効（低）	30
	アプリケーションコントロール		無効	32
	除外設定 ※グループごとに設定する場合		未設定	34
	承認済み/ブロックするURL		トレンドマイクロURLを許可	36
	感染経路の可視化		未設定	37

機能を設定する

デフォルトで以下の機能が設定されています。必要に応じ、設定変更をお願いします。

※NTT東日本の「セキュリティサポートデスク」にて代行設定が可能です。

機能			設定内容（デフォルト）	ページ番号
管理機能	エージェントコントロール	エージェント アンインストール防止	未設定	39
		エージェント 終了防止	未設定	40
	ラベル表示		未設定	41
	通知		未設定	43
	除外設定 ※全端末に適用する場合		未設定	44
その他	グループ管理		未設定	45
	フィルタ管理		未設定	46
	予約検索		未設定	47
	手動アップデート		-	48

機能を設定する（画面構成）

ポリシー設定方法には大きく２つの方法があります。

１．グループごとにポリシーを定める方法

⇒ P.8のセキュリティ機能はグループごとに設定します。

２．全端末に適用されるポリシーを定める方法

⇒ P.9の管理機能は、全端末に適用されるポリシーで設定します。

《 グループごとにセキュリティポリシーを定める場合 》

①「セキュリティエージェント」タブを押下します。

②「手動グループ」が表示されるため、設定したいグループを選択します。

※「すべてのセキュリティエージェント」には全端末情報が一覧で表示されます。
グループとは異なりますのでご注意ください。

③「ポリシーの設定」を押下します。

④設定するOSを選択します。

機能を設定する（画面構成）

ポリシー設定方法には大きく２つの方法があります。

１．グループごとにポリシーを定める方法

⇒ P.8のセキュリティ機能はグループごとに設定します。

２．全端末に適用されるポリシーを定める方法

⇒ P.9の管理機能は、全端末に適用されるポリシーで設定します。

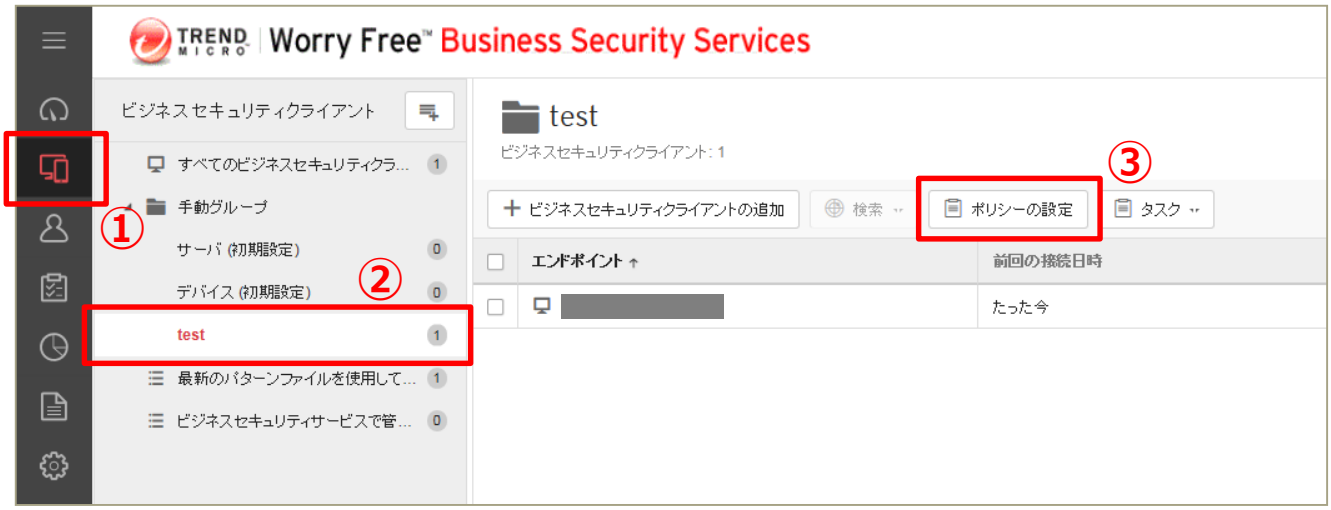
《 全端末に適用されるポリシー/ルールを定める場合 》

①「ポリシー」タブまたは「管理」タブを押下。

※設定する内容により、タブが異なりますのでご注意ください。

機能を設定する（検索設定）

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

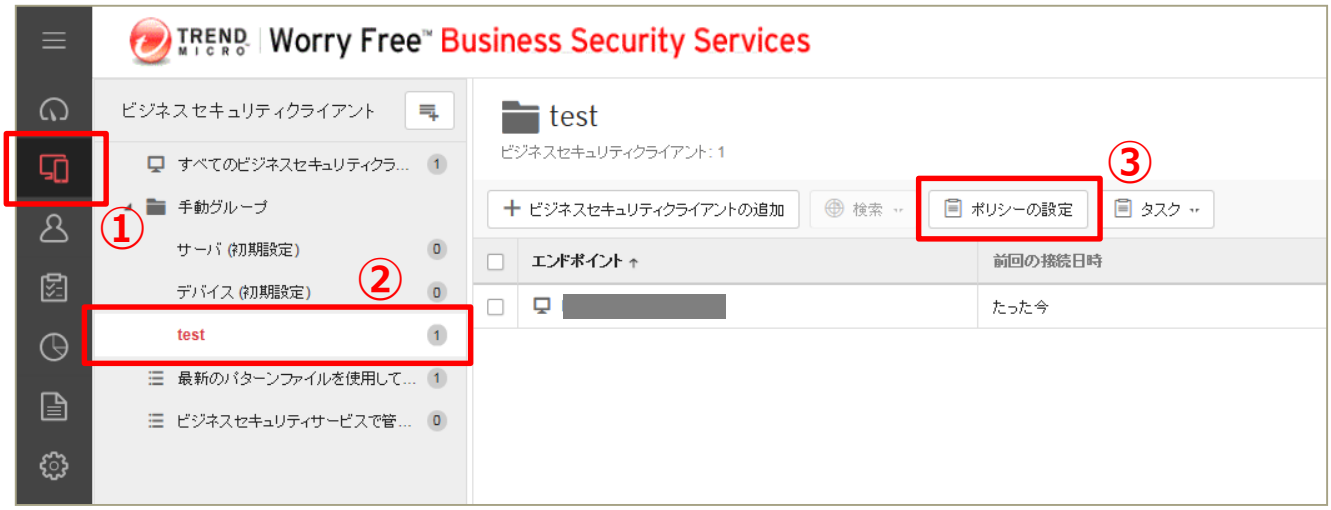


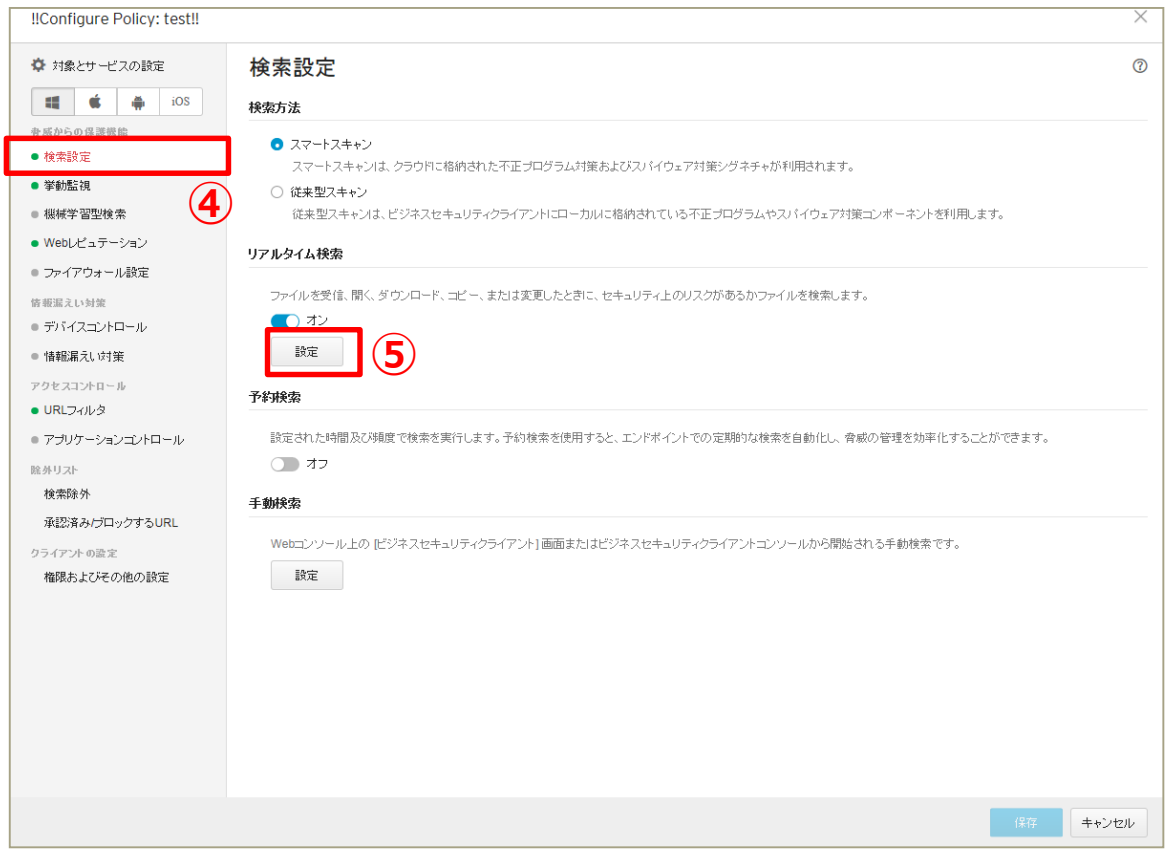
「保存」を押して終了です。

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

機能を設定する（検索設定 – POP3メール検索）

POP3メール検索機能を有効にします。
→メールの受信時にウイルス検索を実施することができます。





機能を設定する（検索設定 – POP3メール検索）

POP3メール検索機能を有効にします。
→メールの受信時にウイルス検索を実施することができます。

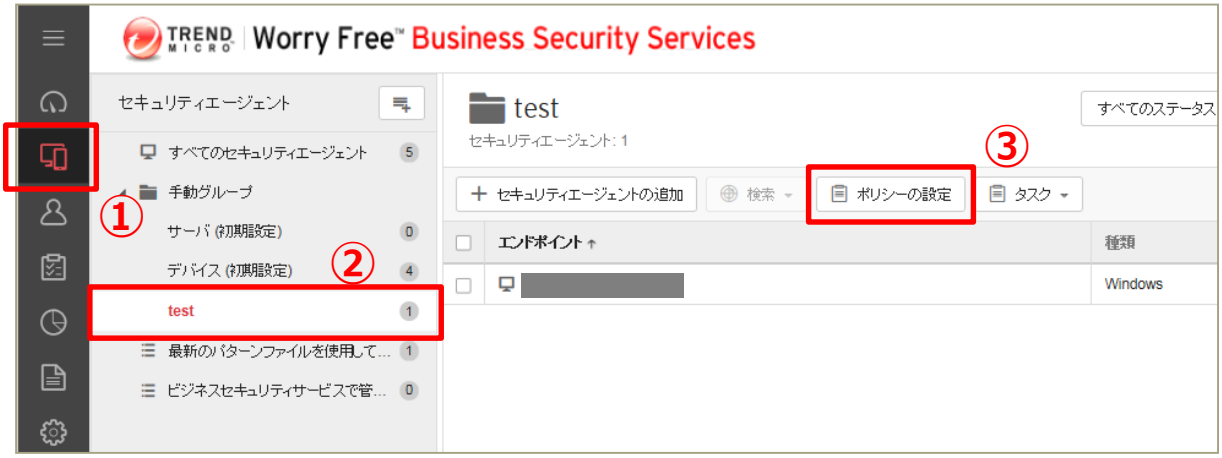
「保存」を押して終了です。

機能を設定する（ファイルレス攻撃対応）

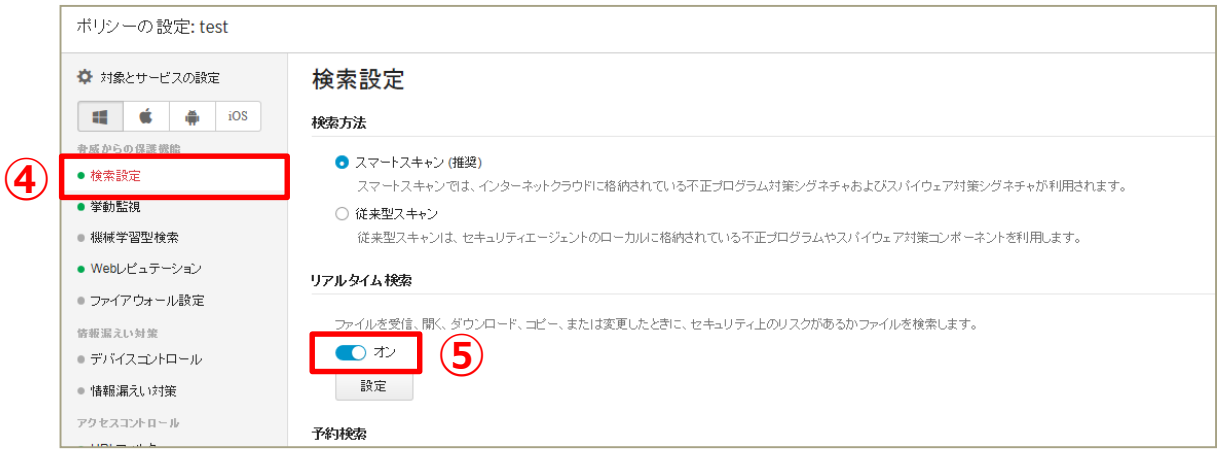
ファイルレス攻撃対応機能を有効にします。
→ハードディスクに保存されない(メモリ上にのみ存在)ウイルスを検出できます。

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

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



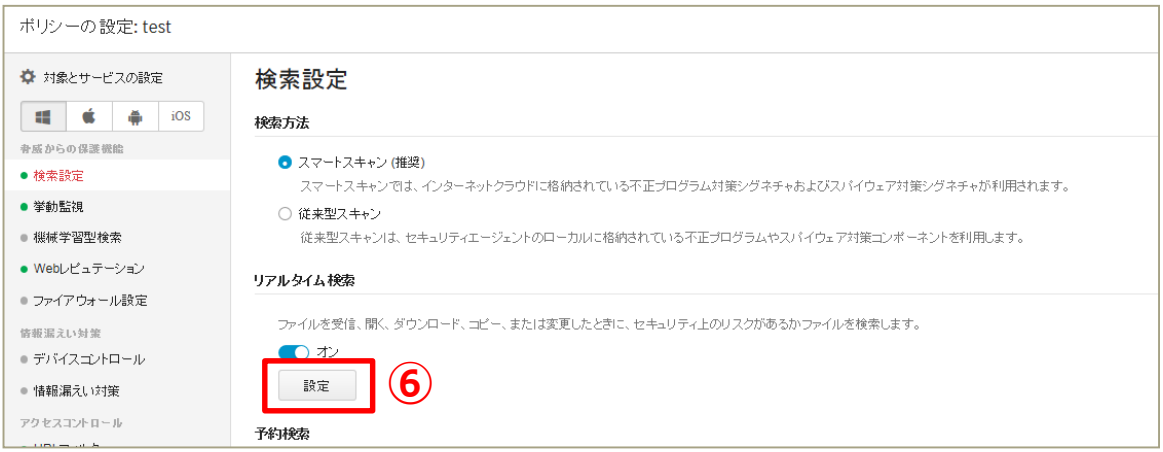
《 項目１ 》 ※項目番号は上記表を参照



機能を設定する（ファイルレス攻撃対応）

ファイルレス攻撃対応機能を有効にします。
→ハードディスクに保存されない(メモリ上にのみ存在)ウイルスを検出できます。

《 項目２ 》



機能を設定する（ファイルレス攻撃対応）

ファイルレス攻撃対応機能を有効にします。
→ハードディスクに保存されない(メモリ上にのみ存在)ウイルスを検出できます。

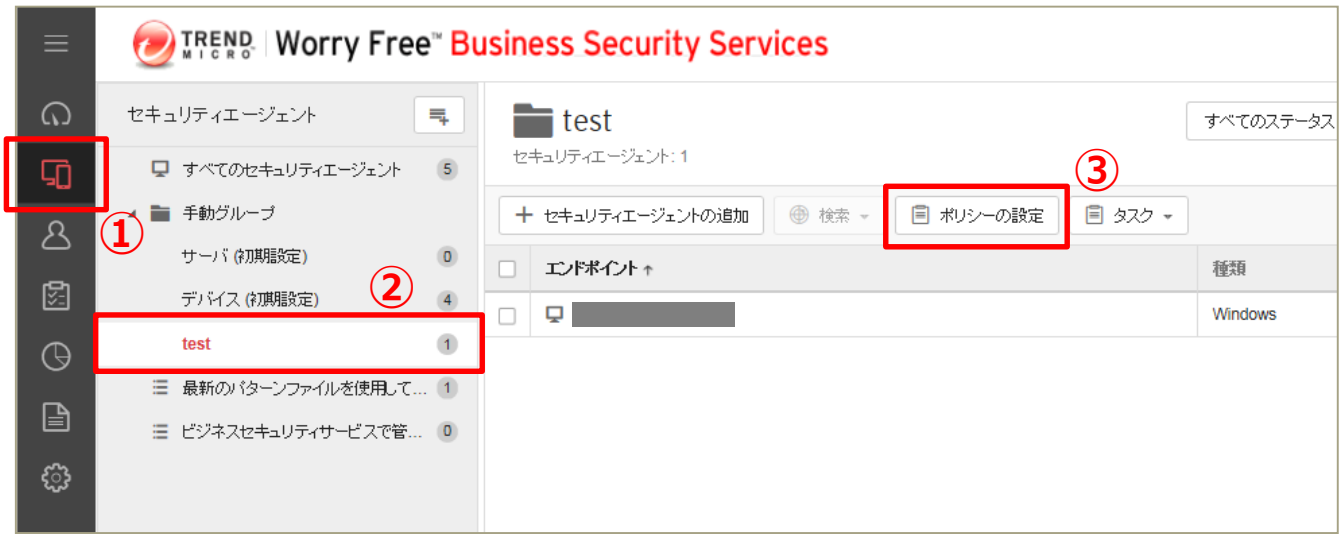
《 項目３,４ 》

《 項目５ 》

項目１～５を全て設定し、「保存」を押して終了です。

機能を設定する（挙動監視）

挙動監視機能を有効にします。
→プログラムやOS、レジストなどを不正に変更されないように
エンドポイントを保護します。



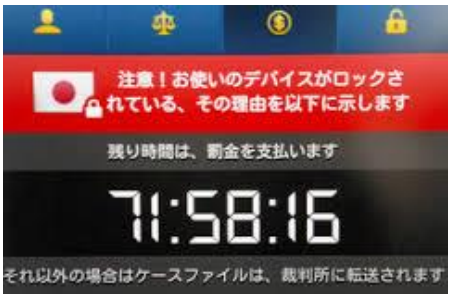
⑦ランサムウェア対策
※詳細は次ページに記載

「保存」を押して終了です。

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

機能を設定する（挙動監視－ランサムウェア対策）

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



◆ウイルス対策機能のランサムウェア対応機能

Ⅰ：不正なファイル暗号化や変更から文書を保護

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

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

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

Ⅲ：ランサムウェアに関連付けられていることの多いプロセスをブロック

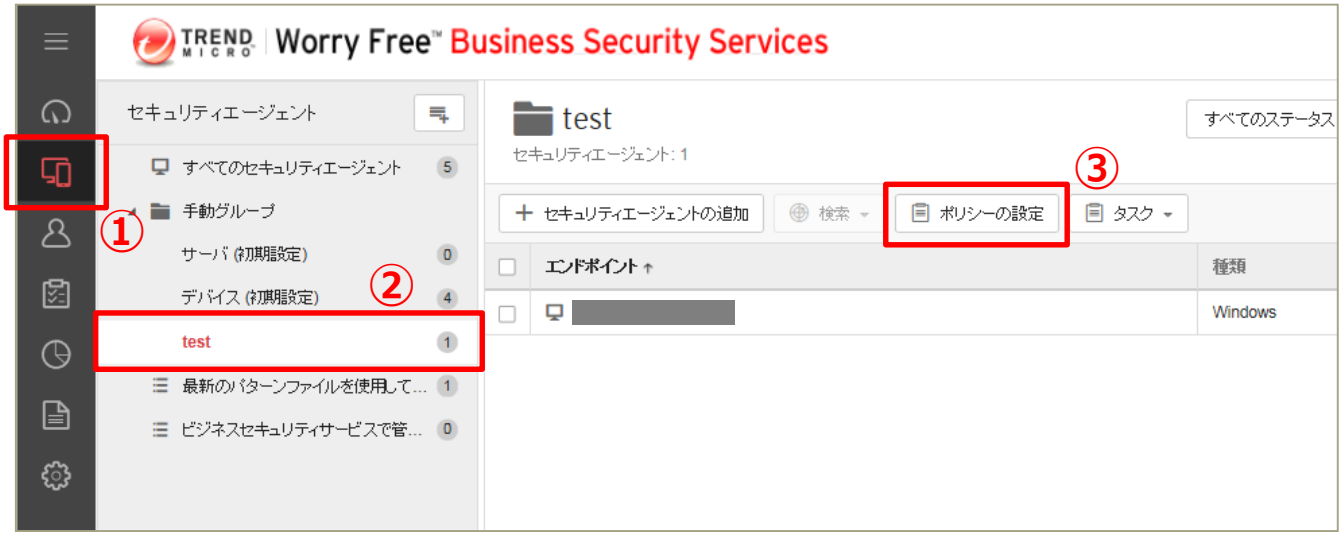
OSで利用されている実行ファイル等にインジェクションされるようなランサムウェアの挙動を監視し、不審な動作をブロックします。

Ⅳ：プログラム検査を有効にして不正な実行可能ファイルを検出ブロック

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

機能を設定する（機械学習型検索）

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

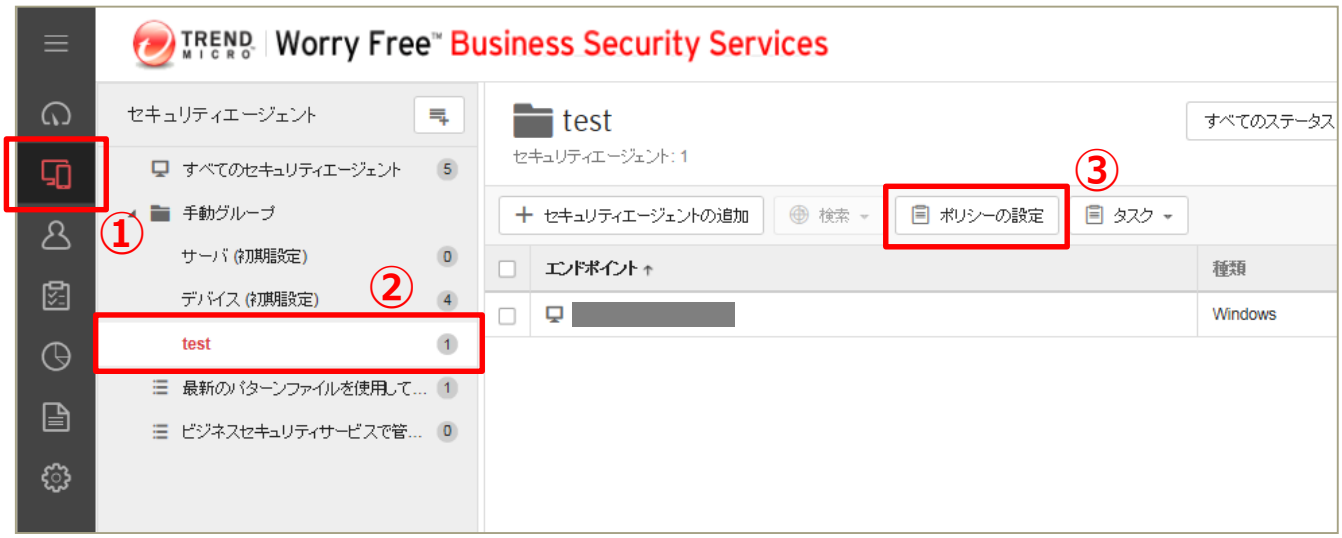


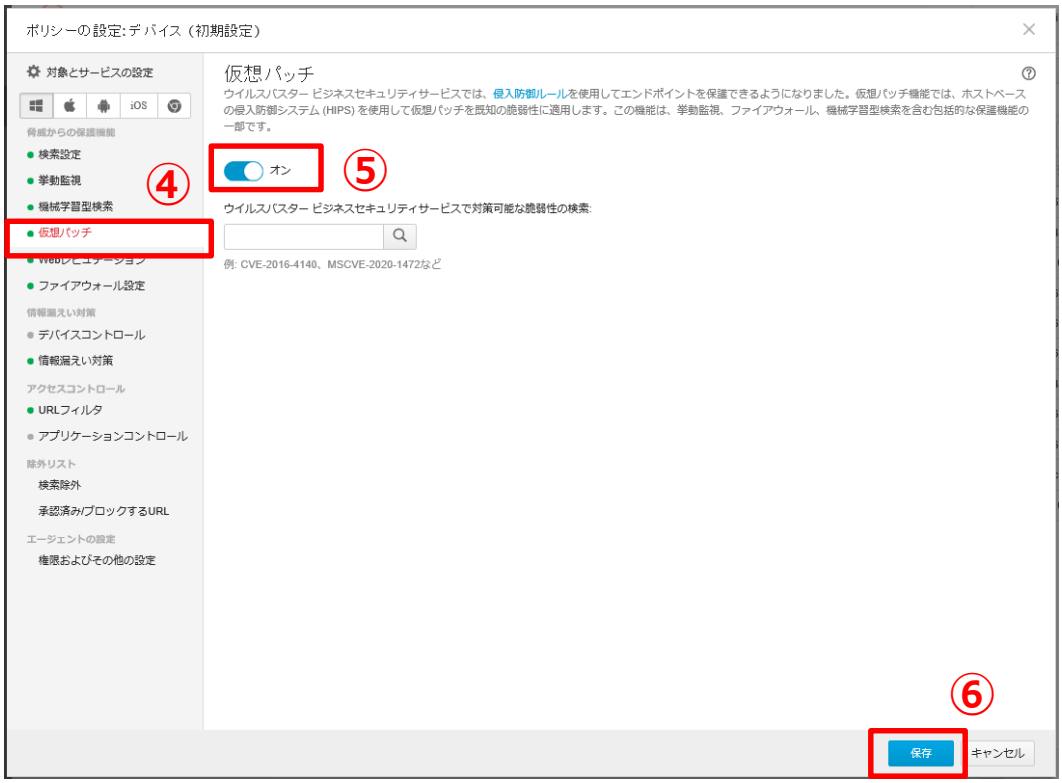
「保存」を押して終了です。

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

機能を設定する（仮想パッチ）

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



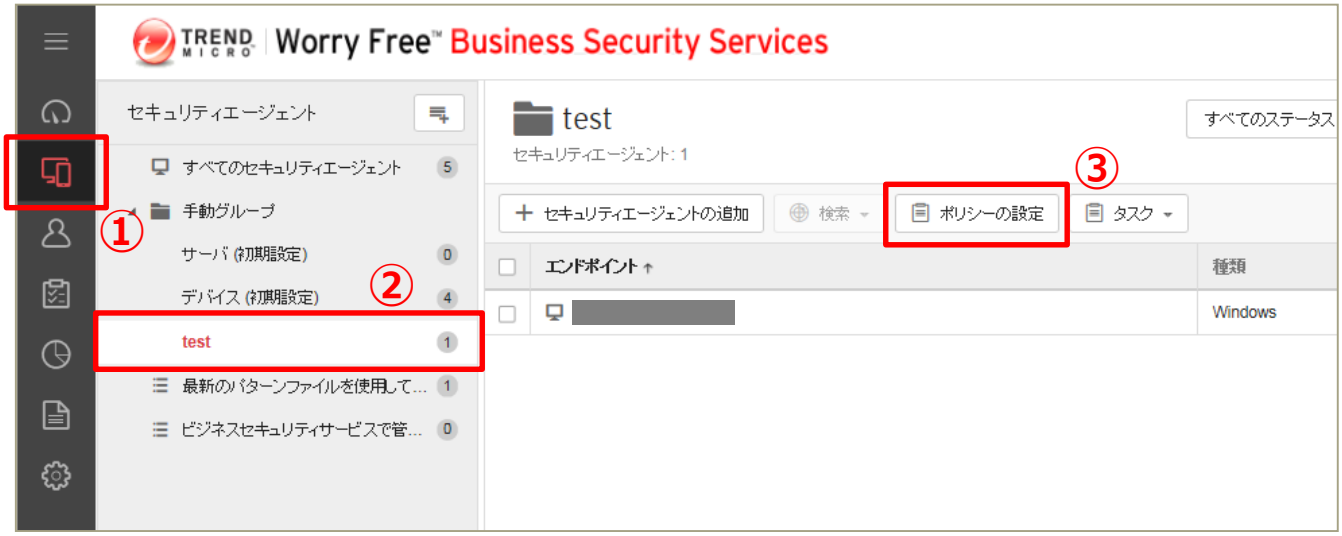


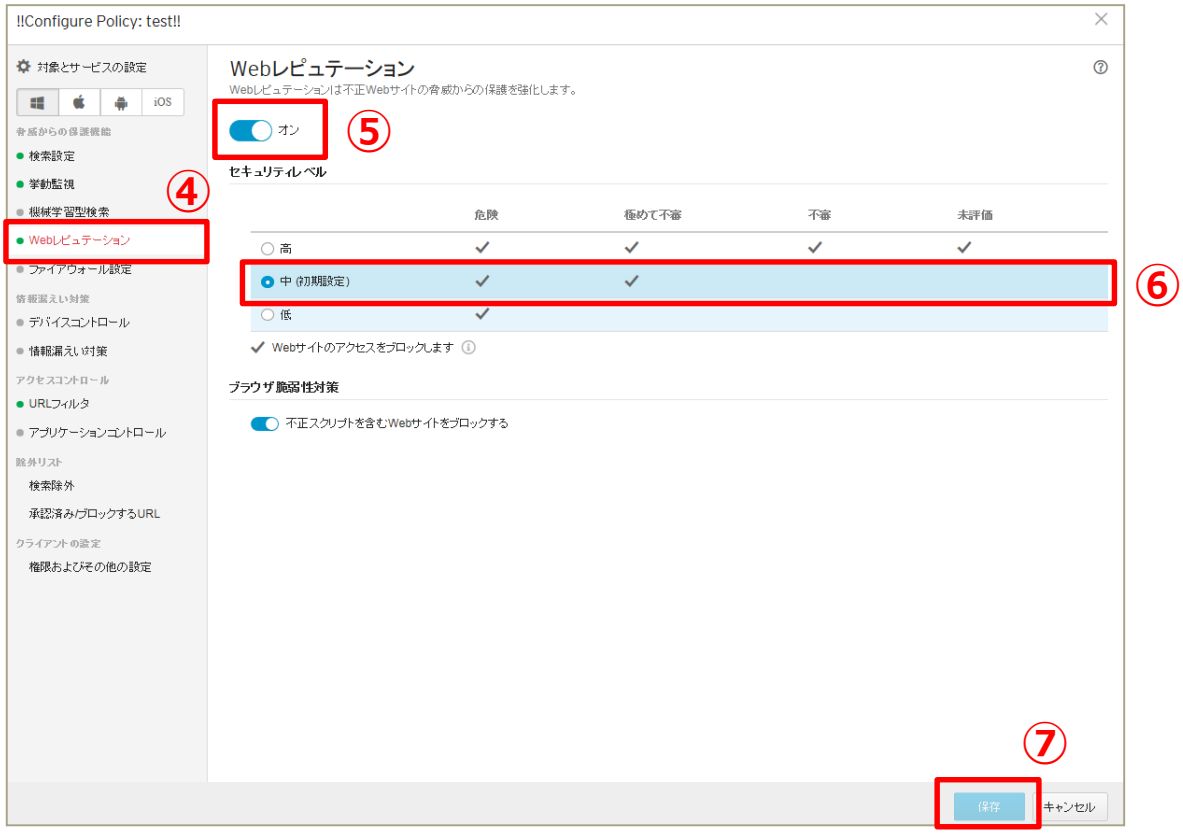
「保存」を押して終了です。

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

機能を設定する（Webレピュテーション）

Webレピュテーション機能を有効にします。
**　→危険なWebサイトへのアクセスを制限します。**
※ここではセキュリティレベル（中）を選択しています。



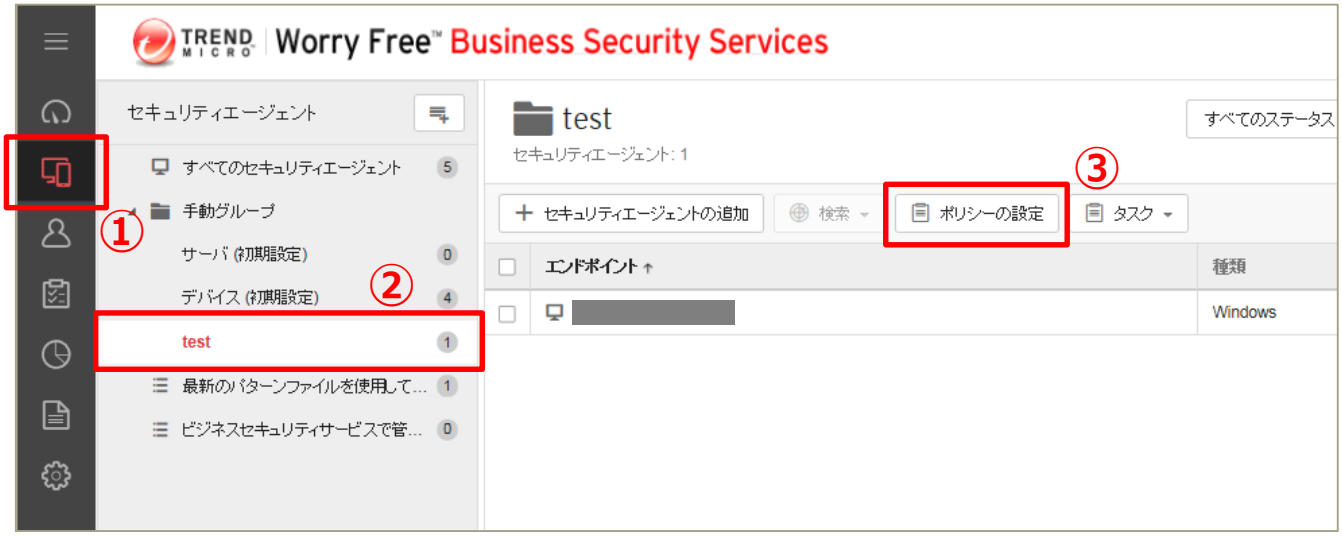


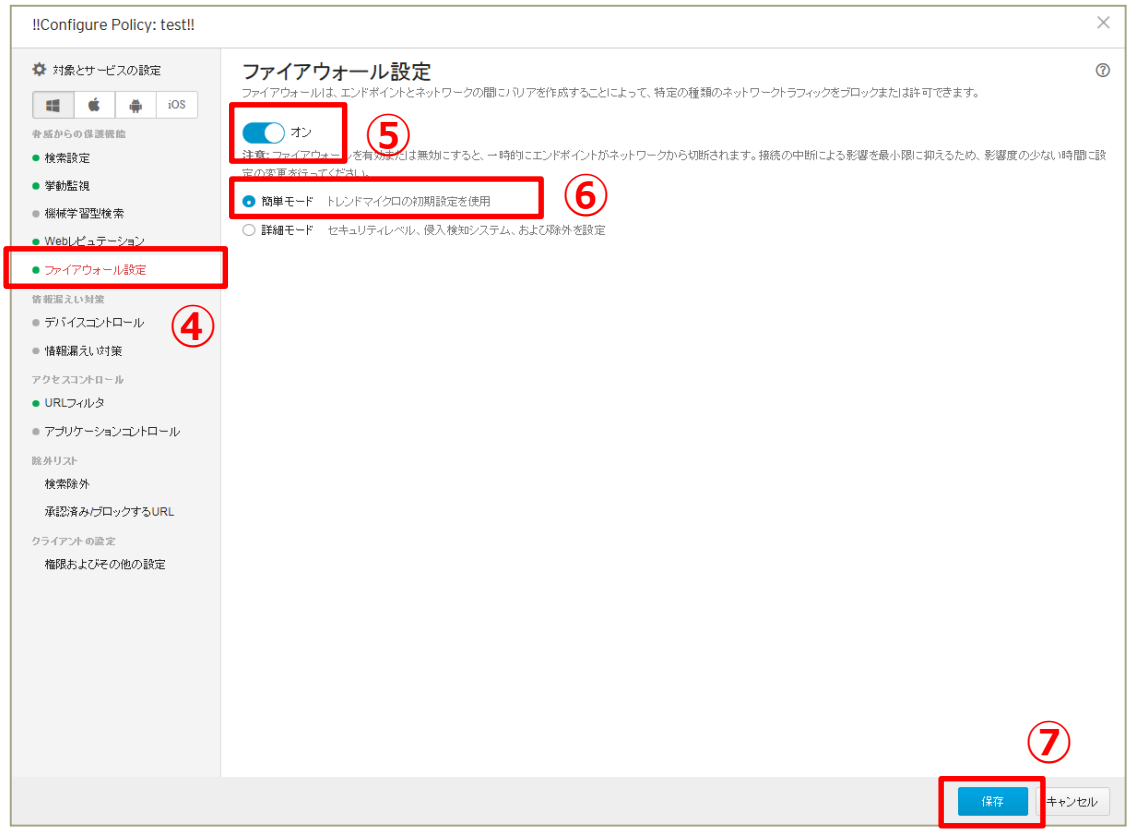
「保存」を押して終了です。

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

機能を設定する（ファイアウォール設定）

ファイアウォール機能を有効にします。
**　→インターネットからの攻撃をブロックします。**
※ここでは簡易モードで設定をしています。

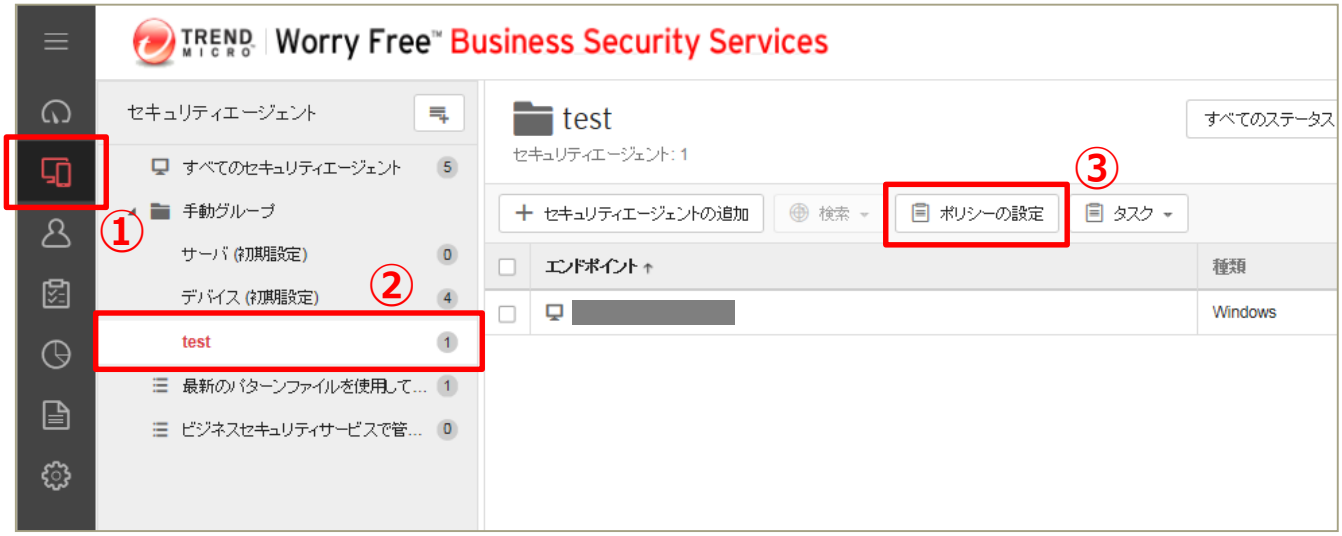


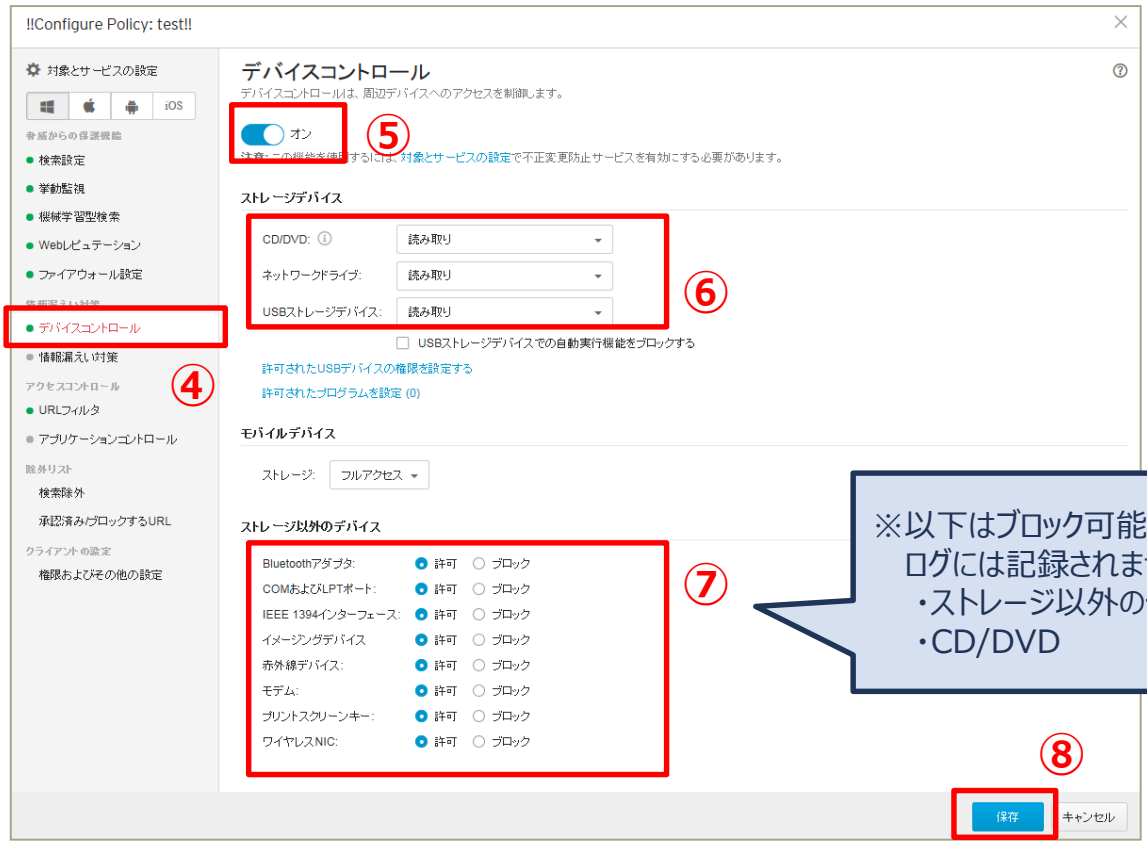


「保存」を押して終了です。

機能を設定する（デバイスコントロール）

USBインターフェースで接続するストレージ(USBメモリ等)の利用をコントロールします。
※ここでは、USBデバイスを読み取り専用にし、情報の持ち出しを禁止する設定を行います。





※以下はブロック可能ですが、
ログには記録されません。
・ストレージ以外のデバイス
・CD/DVD

「保存」を押して終了です。

機能を設定する（デバイスコントロール）

USBインターフェースで接続するストレージ(USBメモリ等)の利用をコントロールします。
※ここでは、USBデバイスを読み取り専用にし、情報の持ち出しを禁止する設定を行います。

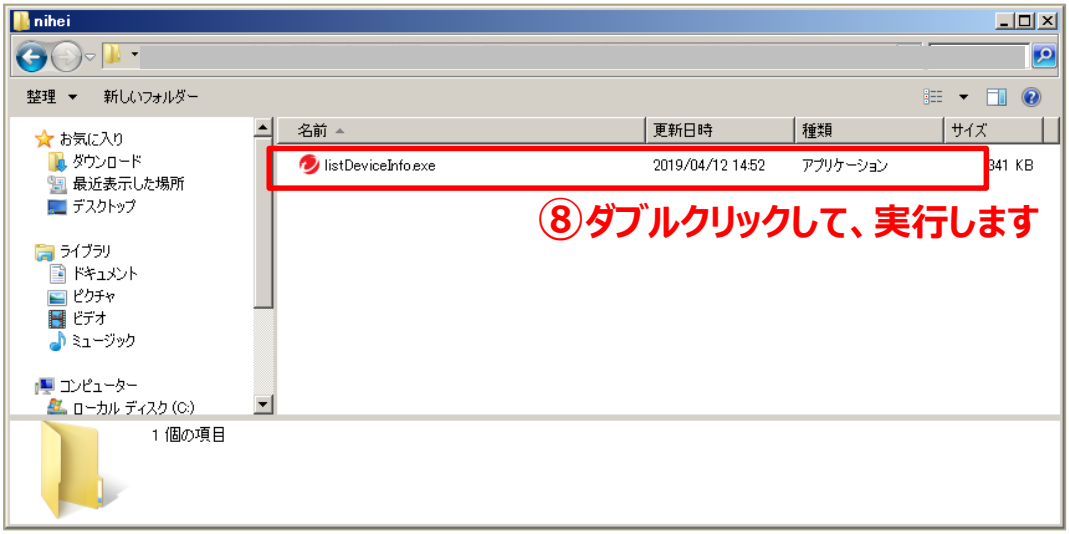
《 特定のUSBのみ常に許可する場合 》

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

機能を設定する（デバイスコントロール）

USBインターフェースで接続するストレージ(USBメモリ等)の利用をコントロールします。
※ここでは、USBデバイスを読み取り専用にし、情報の持ち出しを禁止する設定を行います。

⑧「名前をつけて保存」をクリックし、任意のフォルダに保存します

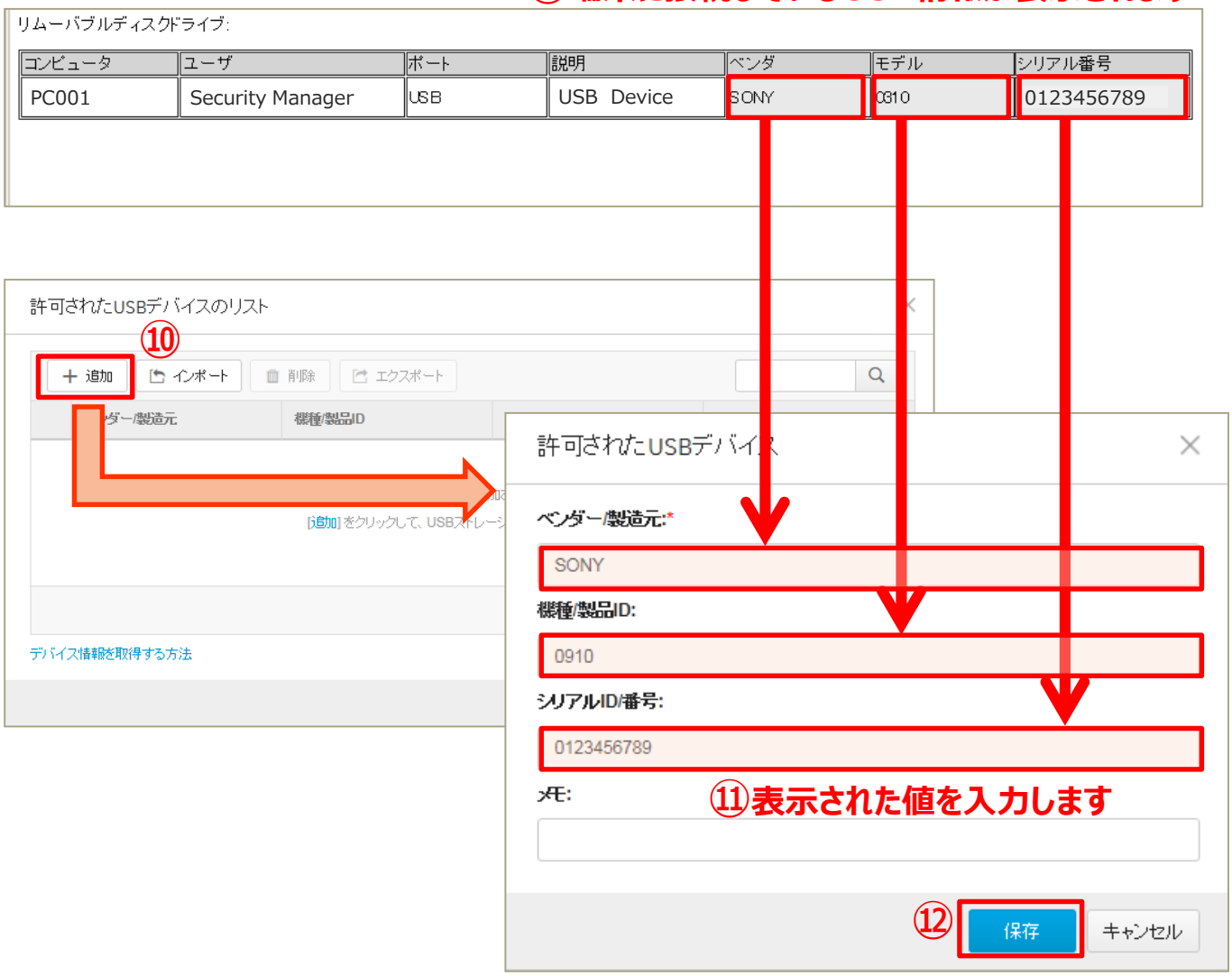


⑧ダブルクリックして、実行します

機能を設定する（デバイスコントロール）

USBインターフェースで接続するストレージ(USBメモリ等)の利用をコントロールします。
※ここでは、USBデバイスを読み取り専用にし、情報の持ち出しを禁止する設定を行います。

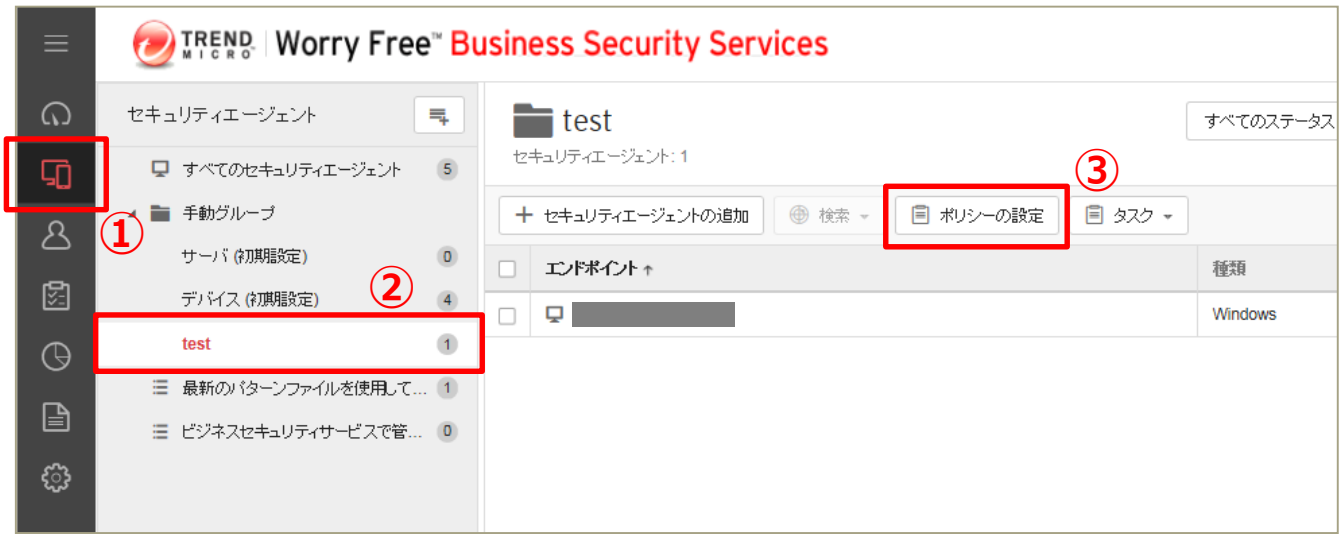
⑧端末に接続しているUSB情報が表示されます



「保存」を押して終了です。

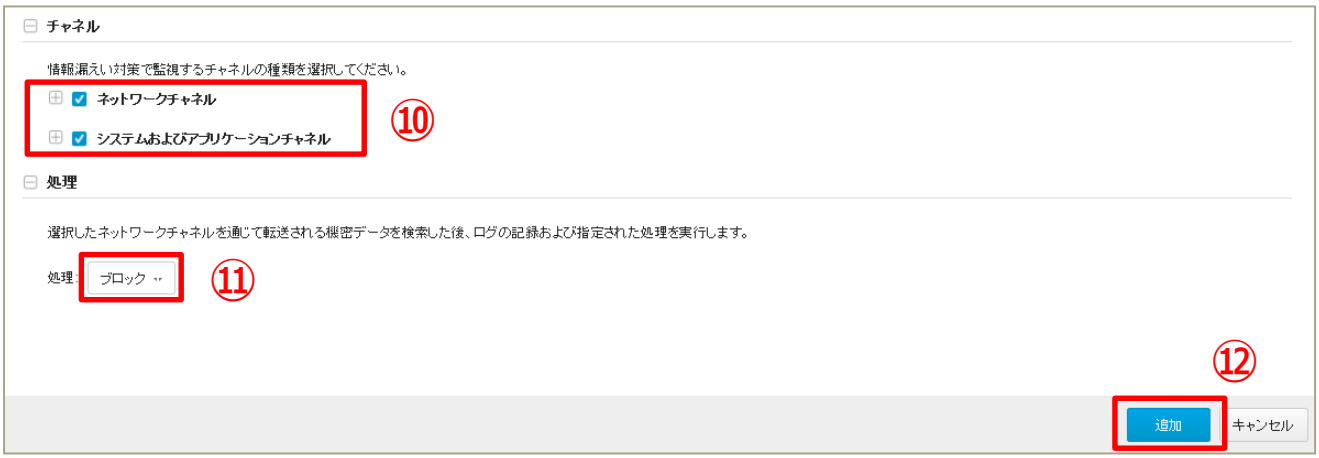
機能を設定する（情報漏えい対策）

情報漏えい対策機能を有効にします。
→機密データの転送を監視またはブロックします。
※ここでは「日本：パスポート番号」の転送ブロックの設定をしています。



機能を設定する（情報漏えい対策）

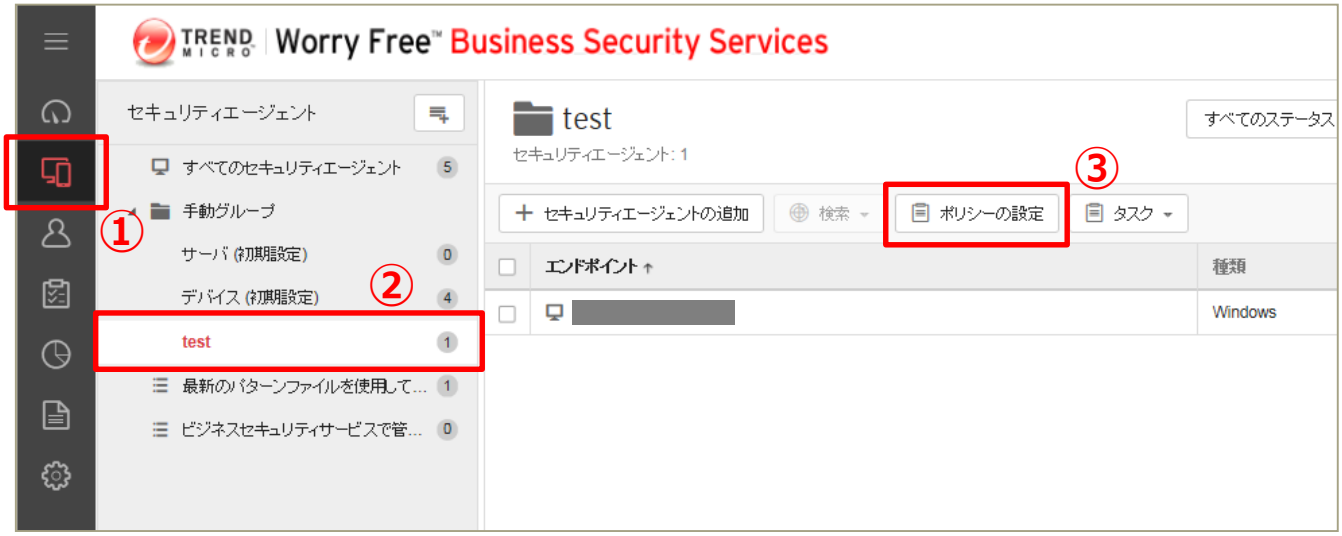
情報漏えい対策機能を有効にします。
→機密データの転送を監視またはブロックします。
※ここでは「日本：パスポート番号」の転送ブロックの設定をしています。

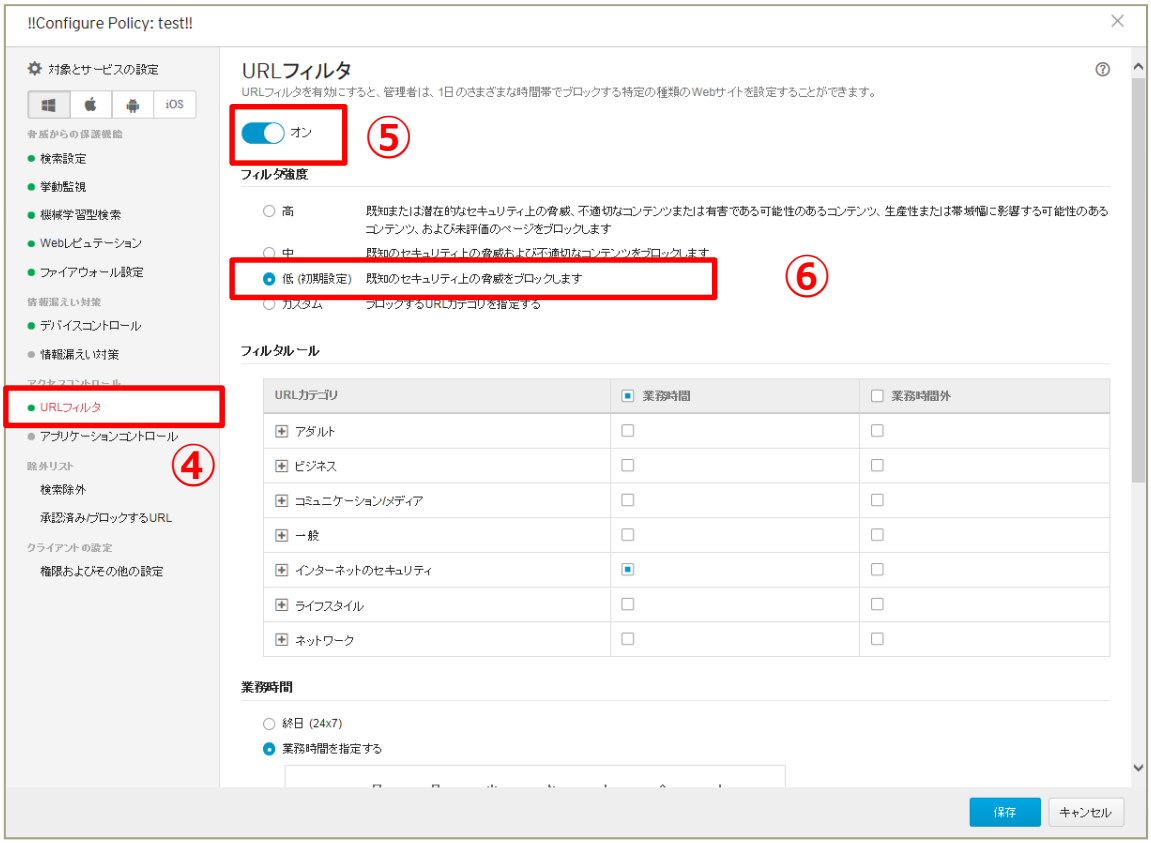


「保存」を押して終了です。

機能を設定する（URLフィルタ）

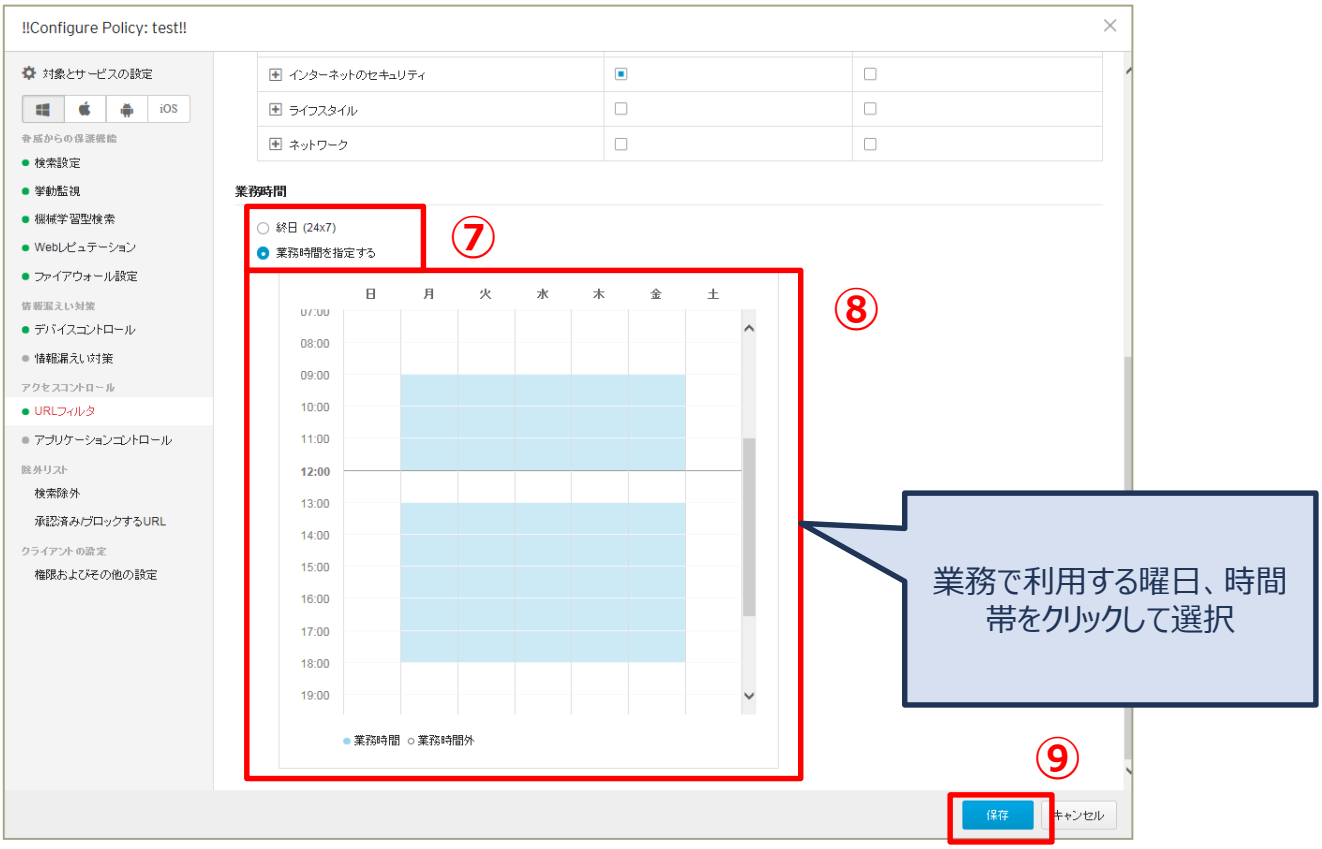
URLフィルタリングを設定します。
→カテゴリ別に閲覧するWebサイトを設定できます。
※ここではセキュリティレベル（低）を選択しています。





機能を設定する（URLフィルタ）

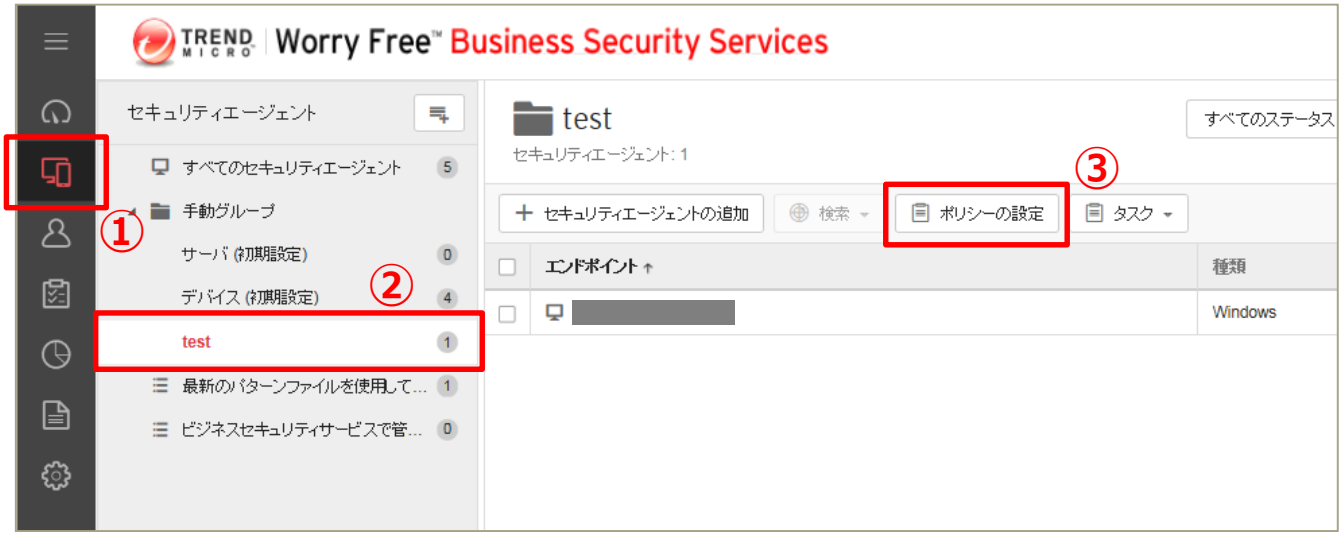
URLフィルタリングを設定します。
→カテゴリ別に閲覧するWebサイトを設定できます。
※ここではセキュリティレベル（低）を選択しています。

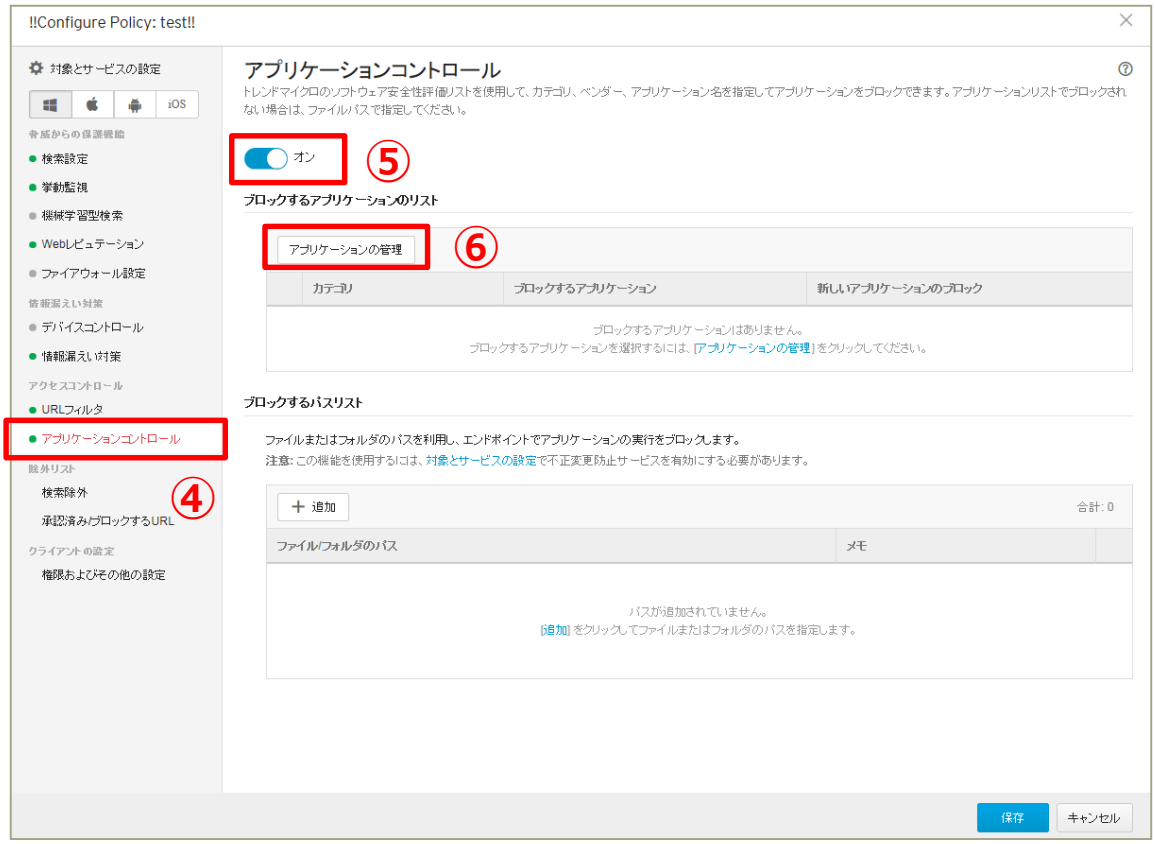


「保存」を押して終了です。

機能を設定する（アプリケーションコントロール）

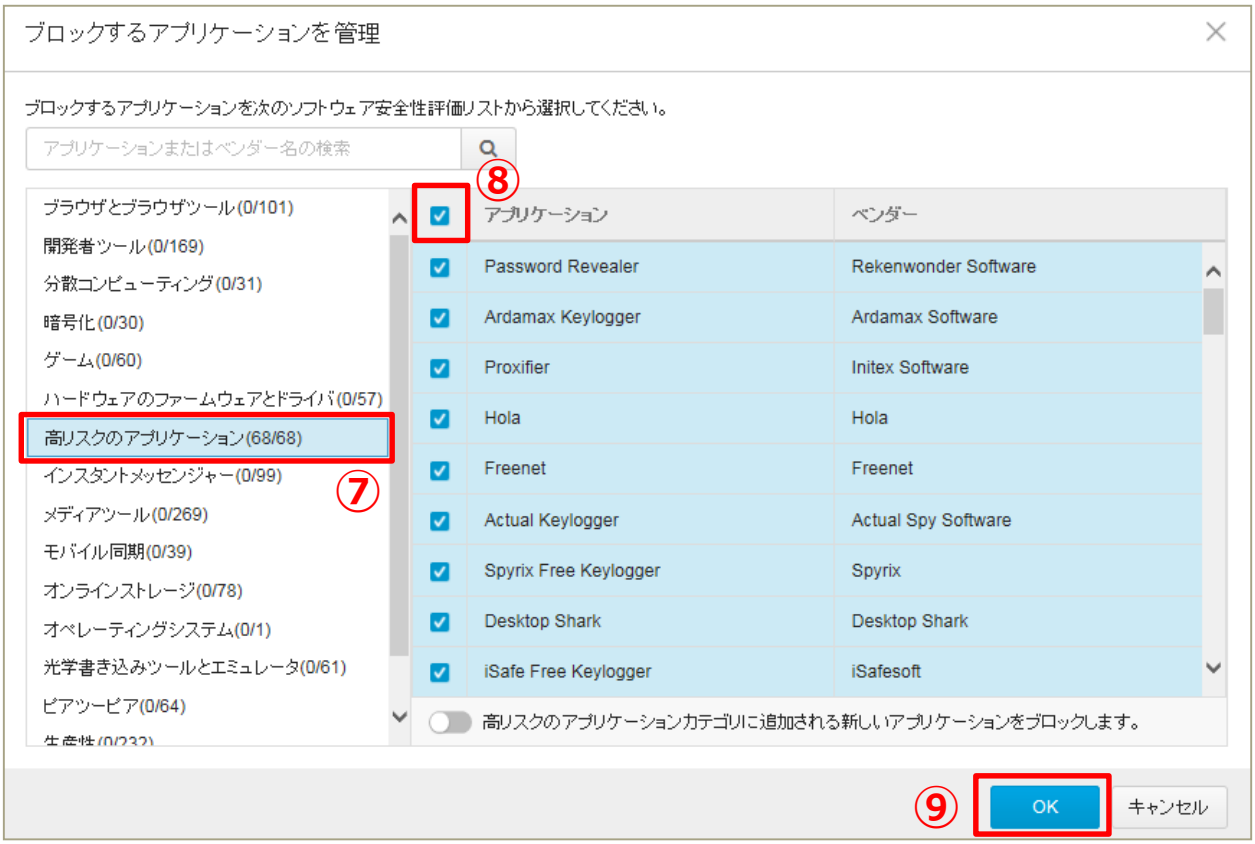
アプリケーションコントロール機能を有効にします。
→指定したアプリケーションの利用を制限します。
※ここでは簡易モードで設定をしています。





機能を設定する（アプリケーションコントロール）

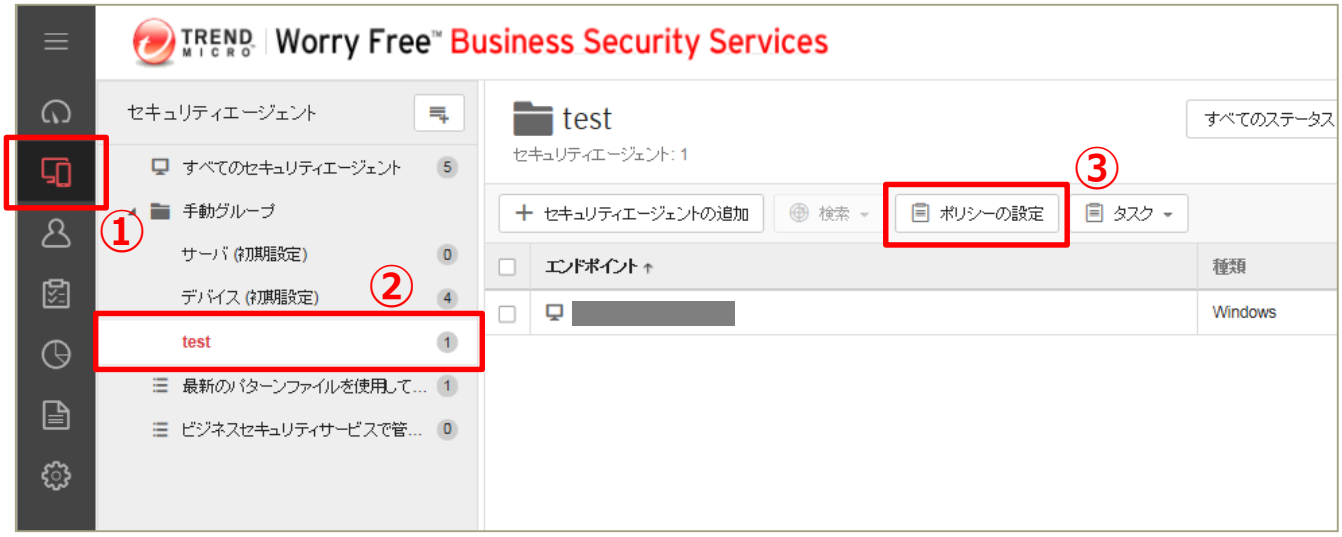
アプリケーションコントロール機能を有効にします。
→指定したアプリケーションの利用を制限します。
※ここでは簡易モードで設定をしています。



「保存」を押して終了です。

機能を設定する（除外設定）

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

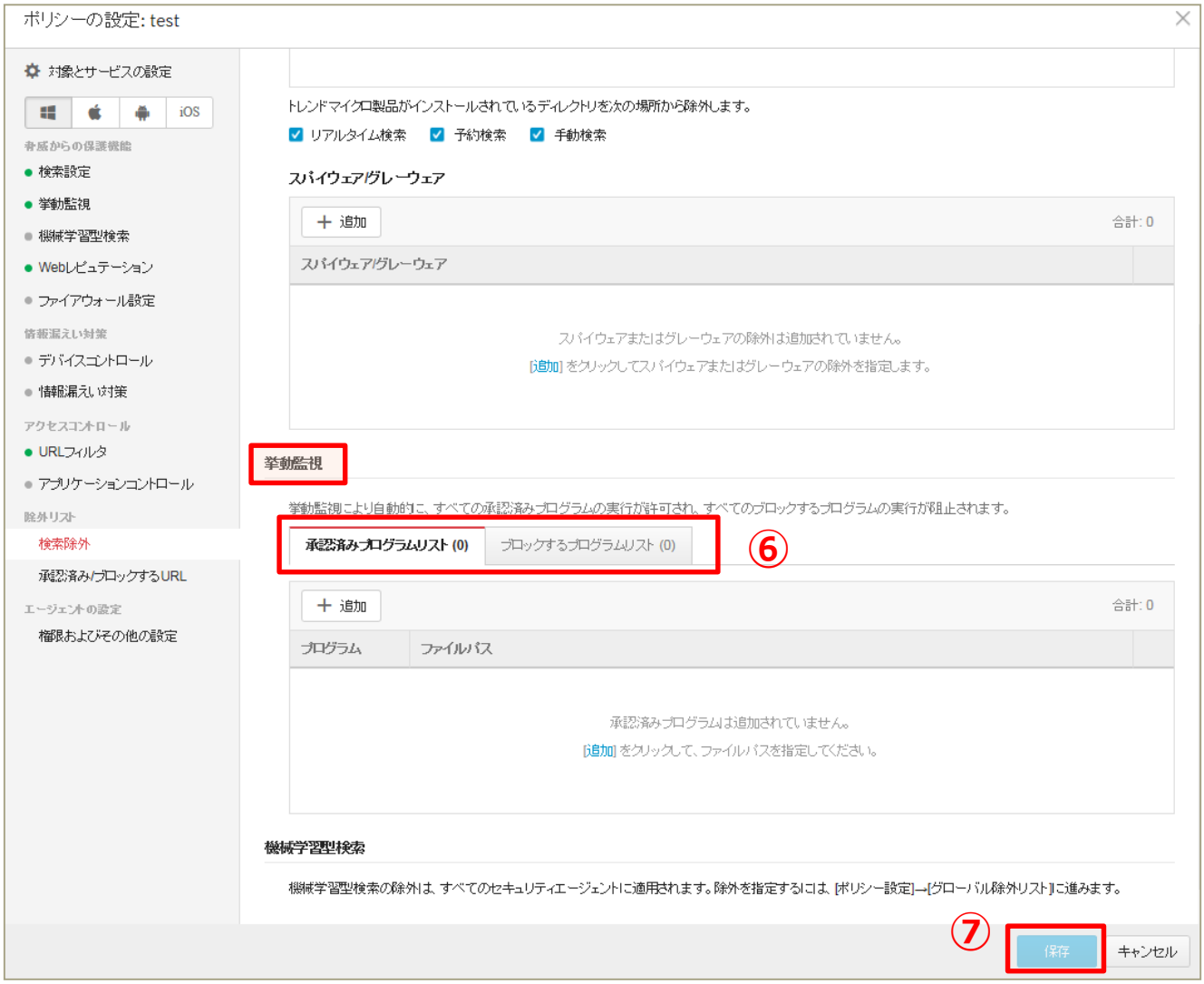


《 リアルタイム検索/予約検索/手動検索から除外する場合 》

機能を設定する（除外設定）

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

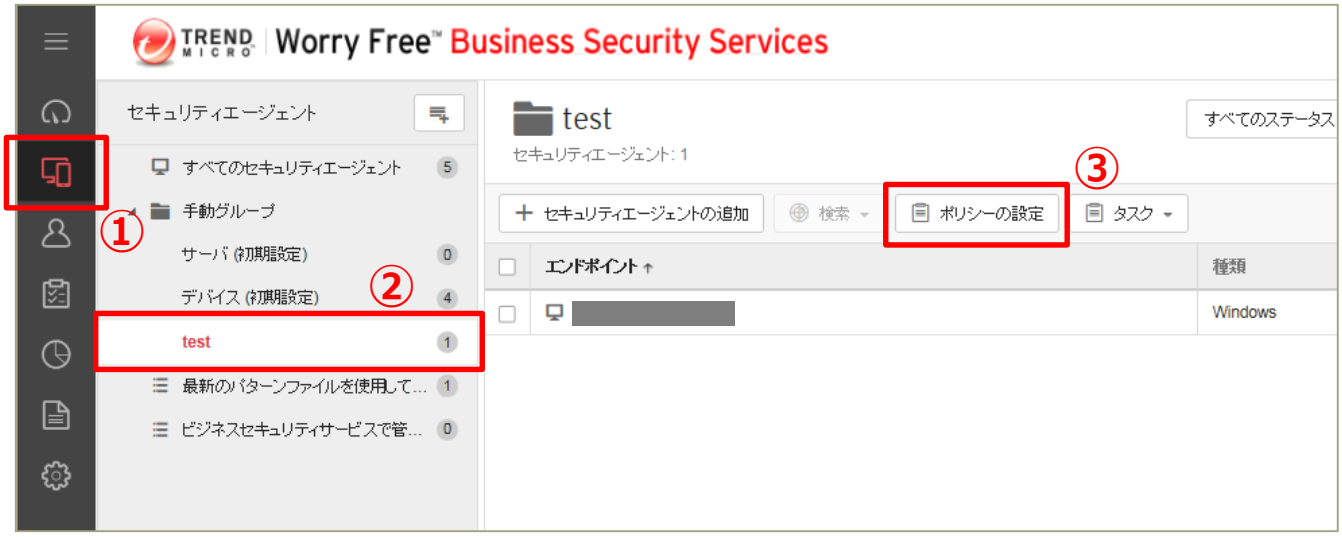
《 挙動監視から除外する場合 》

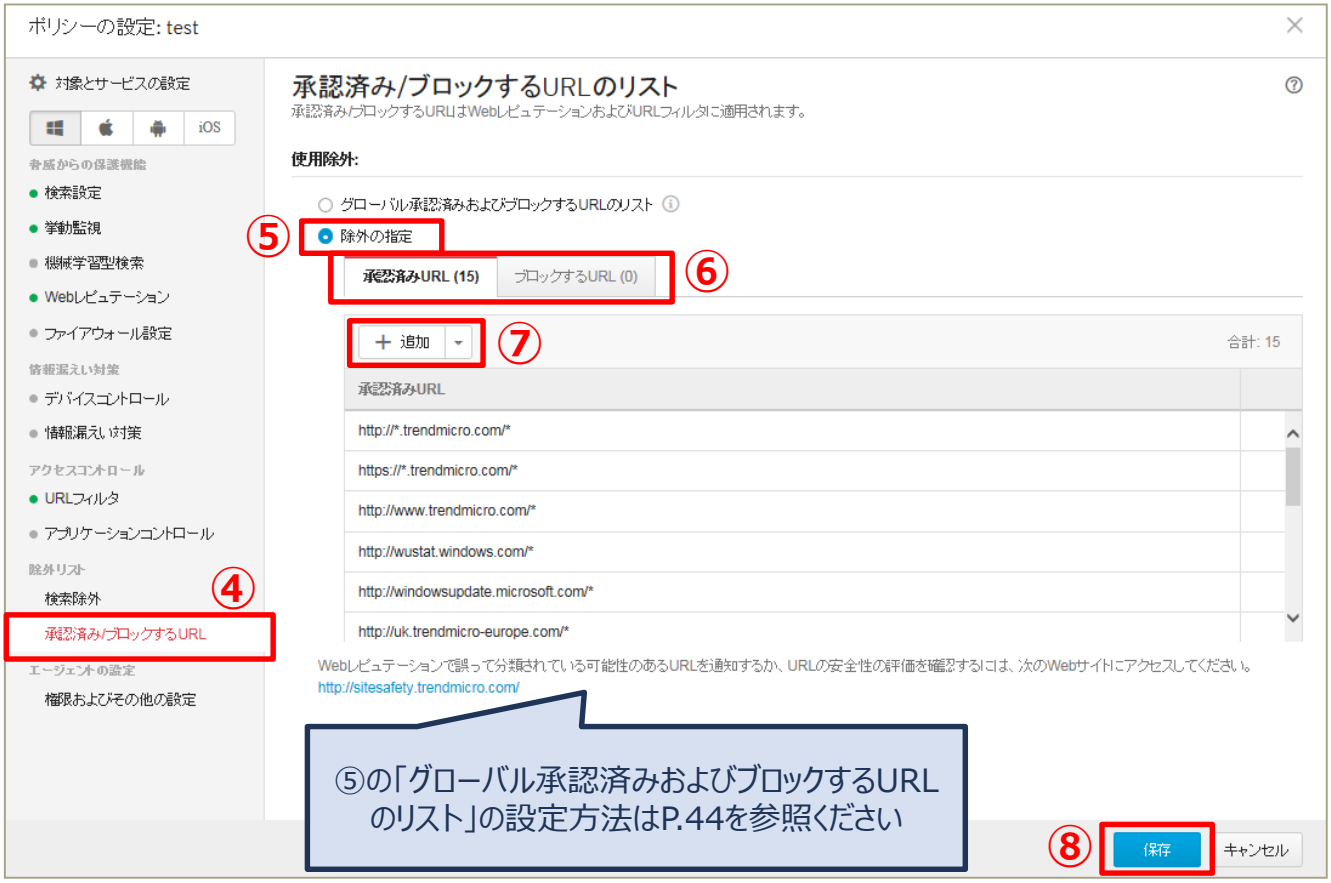


「保存」を押して終了です。

機能を設定する（承認済み/ブロックするURL）

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





「保存」を押して終了です。

機能を設定する（感染経路の可視化）

セキュリティイベントが検出されるまでの簡易的な経路が確認できます。

《 注意点 》

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

追加で必要なリソース

本機能が有効の場合、無効の場合に比べてクライアント端末のリソースを多く使用するため、パフォーマンスに影響が出る可能性があります。

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

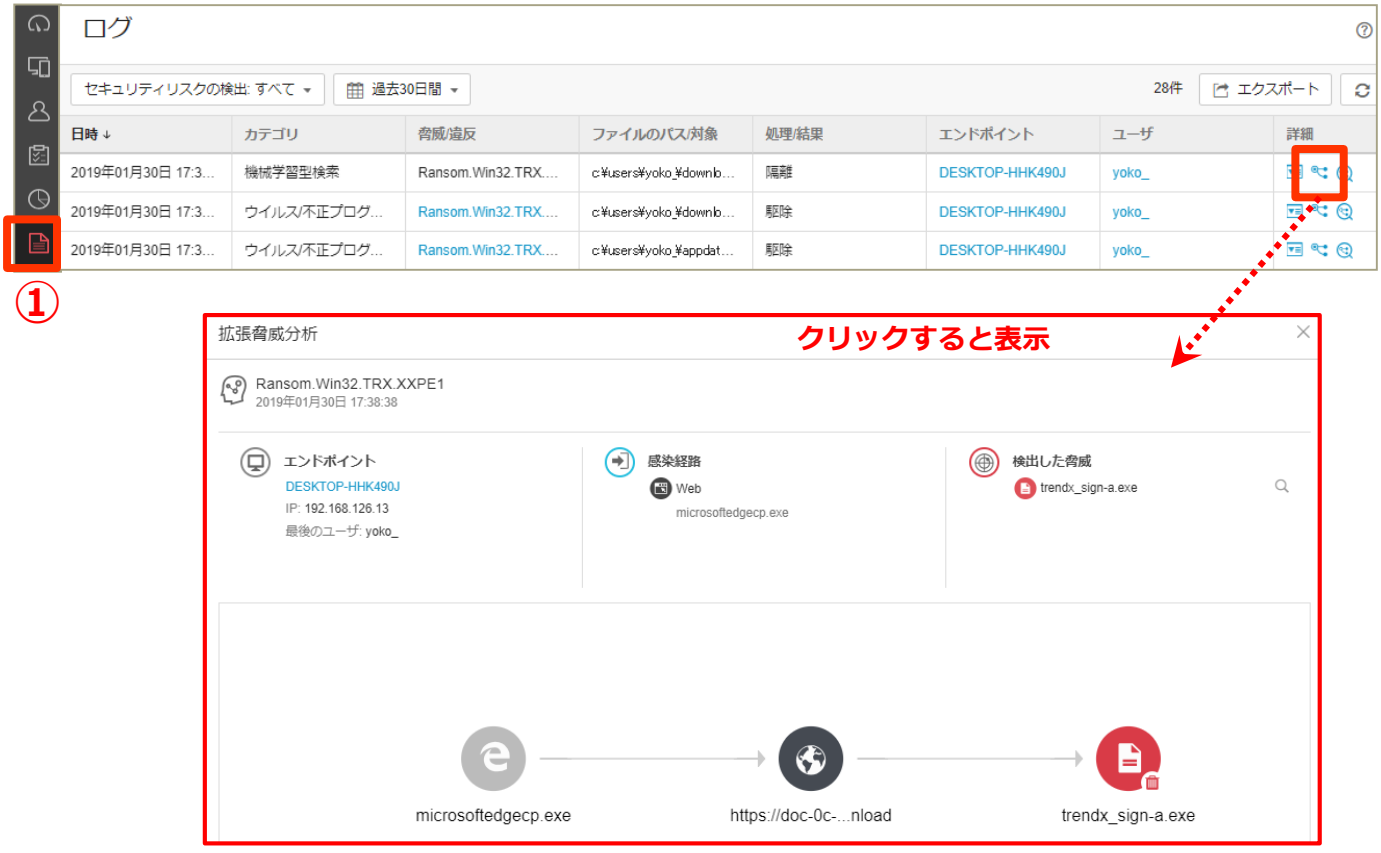
「保存」を押して終了です。

機能を設定する（感染経路の可視化）

セキュリティイベントが検出されるまでの簡易的な経路が確認できます。

《 感染経路の確認方法 》

・感染経路はログ画面で確認することができます。



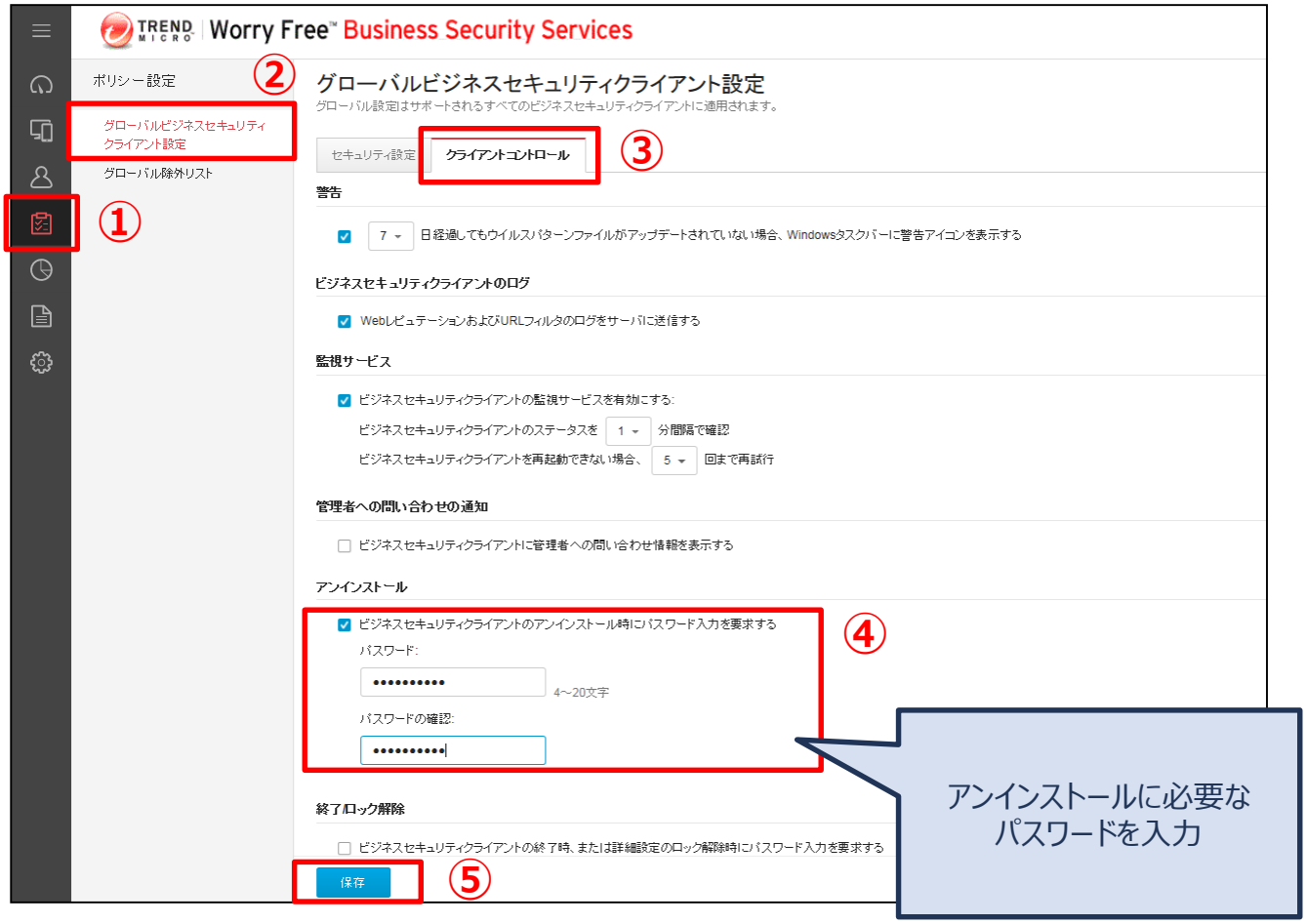
感染経路が確認可能な脅威ログのカテゴリ

下記４つで検知されたイベントについて、経路を確認することができます。

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

機能を設定する（エージェントアンインストール防止）

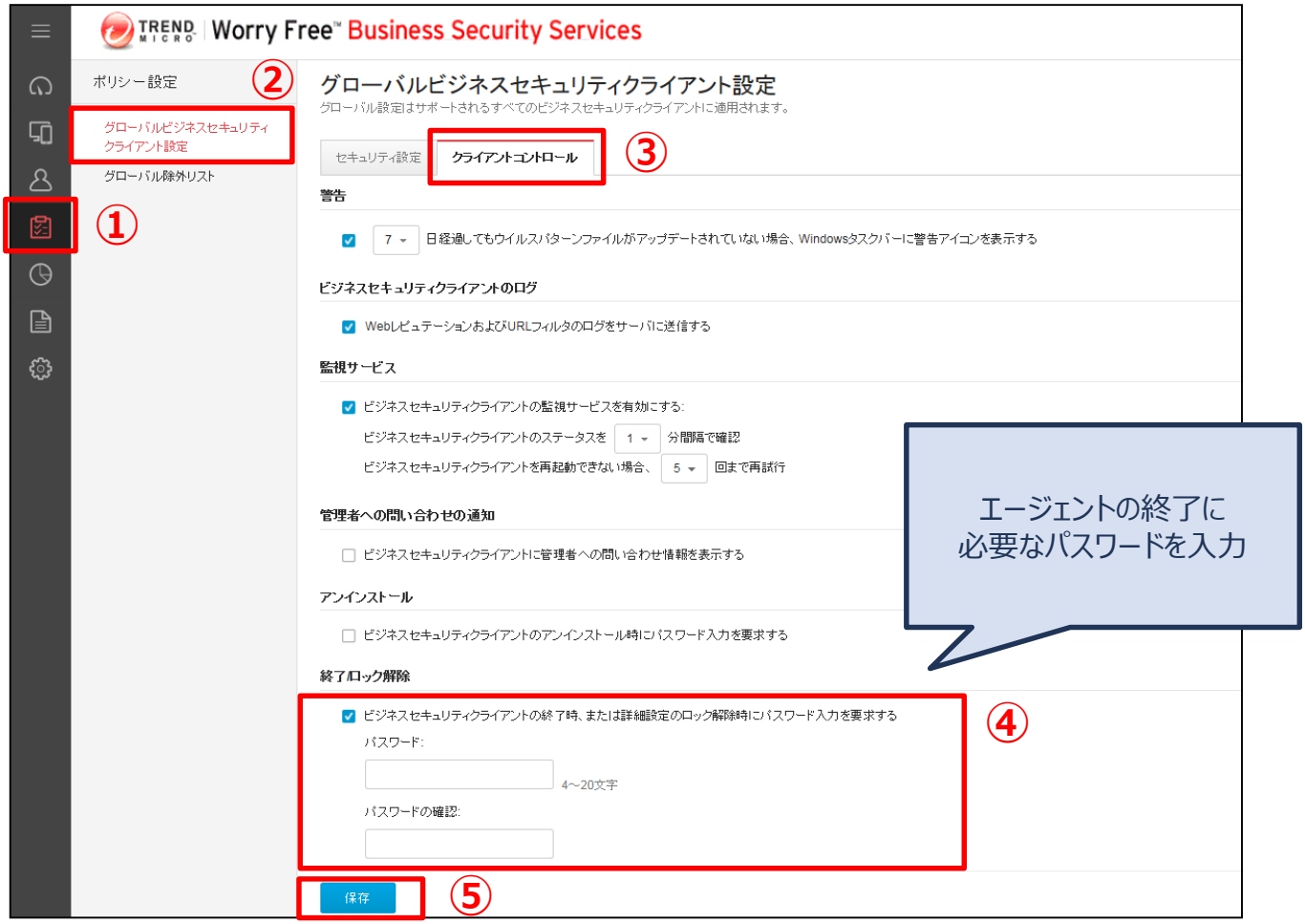
エージェントのアンインストール防止を設定します。
→指定のパスワードを入力しないとアンインストールができないようにします



「保存」を押して終了です。

機能を設定する（エージェント終了防止）

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



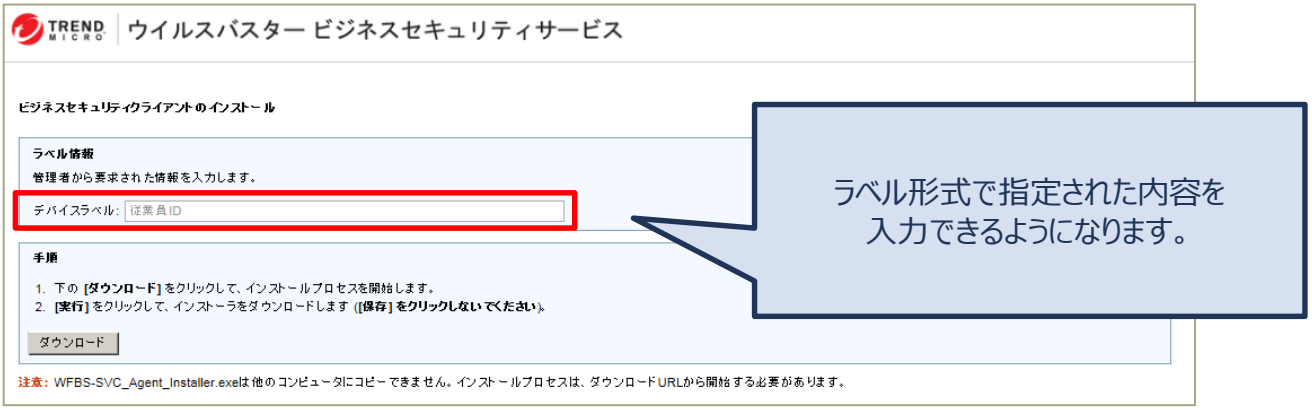
「保存」を押して終了です。

機能を設定する（ラベル表示）

管理者が各デバイスの名称を管理コンソール上で判別しやすいようにラベル登録することができます。
※ここではラベル形式に[従業員ID]を設定をしています。

「保存」を押して終了です。

【 参考 】エージェントインストール時の画面



機能を設定する（ラベル表示）

管理者が各デバイスの名称を管理コンソール上で判別しやすいようにラベル登録することができます。
※ここではラベル形式に[従業員ID]を設定をしています。

「セキュリティエージェント」タブでもラベルを入力することができます。

機能を設定する（通知）

ウイルス感染時等に、管理者へのメール通知を設定します。

「保存」を押して終了です。

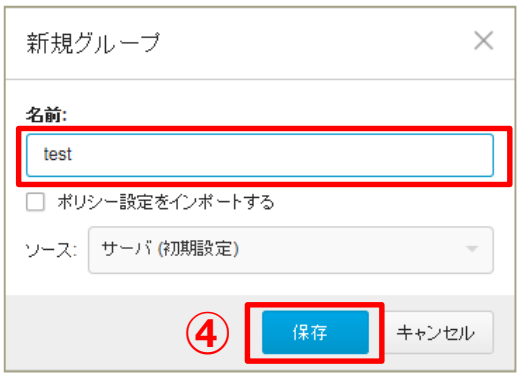
機能を設定する（除外設定）

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

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

機能を設定する（グループ追加）

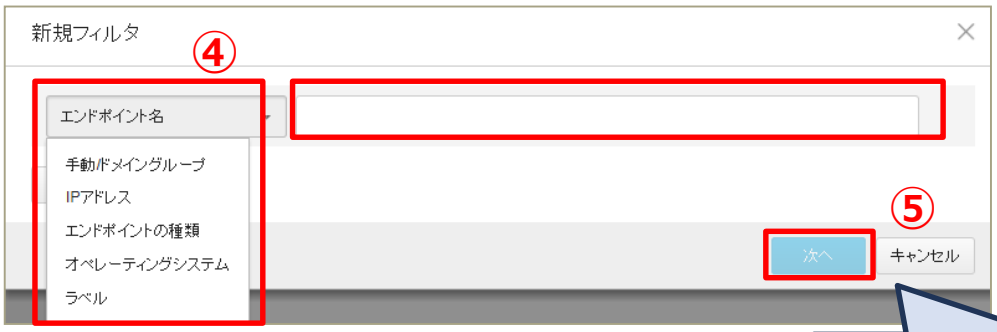
ライセンス数が多い場合など、グループを作成し管理を容易にすることができます。
※ここでは[test]グループを追加しています。



「手動グループ」の配下に新規グループが作成されます。

機能を設定する（フィルタ追加）

特定の条件に該当するエンドポイントを確認したい場合などは、フィルタを作成し管理を容易にすることができます。
※ここでは[test]フィルタを追加しています。



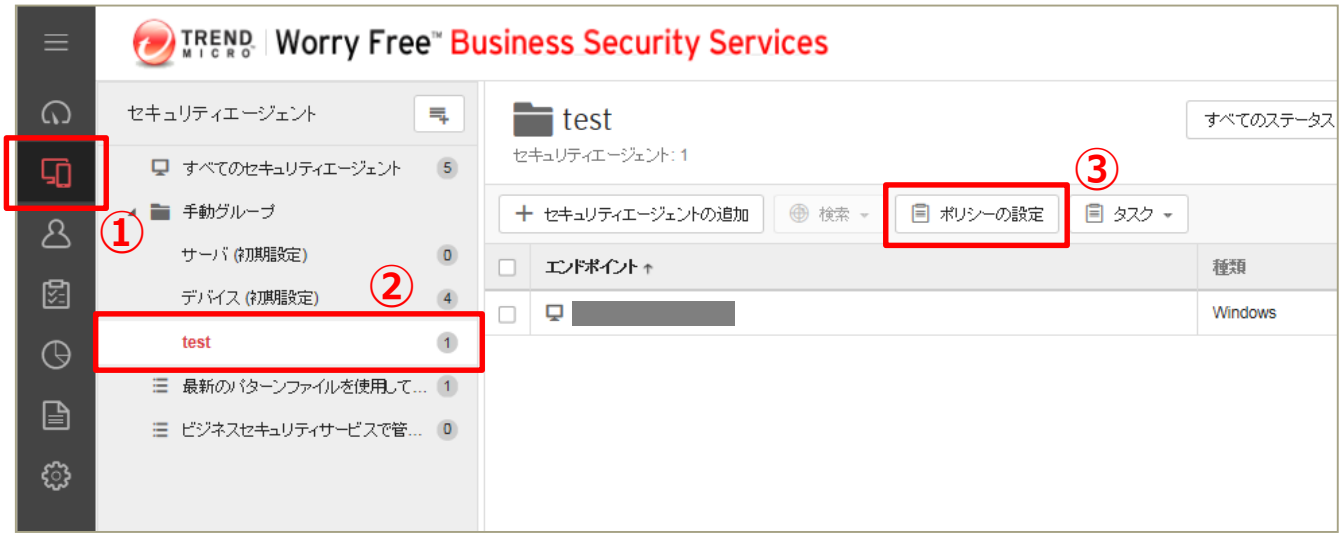
フィルタの条件を指定（AND条件）

フィルタ名を指定

「フィルタ機能の実装」の配下に新規フィルタが作成されます。

機能を設定する（予約検索）

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



「保存」を押して終了です。

機能を設定する（手動アップデート）

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

方法(1)：管理コンソールから手動でアップデートする

③でチェックしたエンドポイントのアップデートを行います。

「アップデート」を押して終了です。

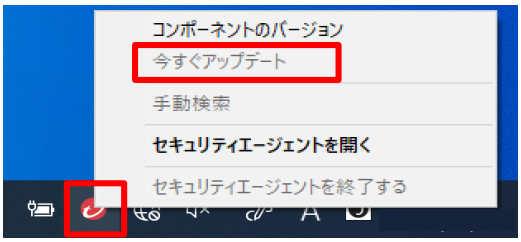
エージェントのアップデートが開始するまでに5～10分かかります。

機能を設定する（手動アップデート）

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

方法(2)：エージェントから手動でアップデートする

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



ファイルのダウンロードが始まります。

完了のメッセージが表示されますので
「閉じる」ボタンをクリックします。

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

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