

# 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

2 0 2 1 . 1  
N T T 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、お客様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利用いただくため、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。**

○○○○○○株式会社様

この度は、弊社セキュリティサービスをご契約いただき、誠にありがとうございます。管理用サイト (Licensing Management Platform) のログイン用ユーザアカウントを発行いたしました。次のURLからログインで <https://clp.trendmicro.com/>

アカウントの詳細  
会社名: ○○○○○○株式会社  
ログインID(お客さまID): D○○○○○○○○○○○○○○

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

※メールアドレスの訂正・変更は下記WEBサイトお問い合わせフォームからご依頼ください。

◆「おまかせアンチウイルス」のご契約の方 ◆  
「おまかせアンチウイルス」お問い合わせサイト <https://business.ntt-east.co.jp/service/antivirus/>


◆「おまかせサイバーみまもり」のご契約の方 ◆  
「おまかせサイバーみまもり」お問い合わせサイト <https://business.ntt-east.co.jp/service/cybermimamori/>

▲「おまかせデータレスPC」のご契約の方 ▲  
<https://business.ntt-east.co.jp/service/dlpc/>

**STEP 1 : PWを設定します**




**STEP 2 : ログイン画面へ遷移します**



不明な点がある場合は、郵送でお送りしている「お申込内容のご案内」・「重要事項説明」をご覧ください。

**STEP 3 : 『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/>

### ▲ セキュリティをさらに強化

サイバー犯罪が高度化するにつれて、不正アクセスからインターネットアカウントを保護するにはパスワード保護だけでは不十分な場合があります。アカウントを適切に保護するために、2要素認証をただちに有効にすることを強く推奨します。



**2要素認証とは**  
2要素認証により、モバイルデバイスを使ってアカウントへのサインイン時に本人確認を行うことが可能になります。2要素認証によりセキュリティが強化され、パスワードが盗まれた場合でも、不正アクセスを防ぐことができます。  
[詳細](#)

**2要素認証が重要な理由**  
サイバー犯罪者によって本アカウントに不正アクセスされた場合、本コンソールからアクセス可能なトレンドマイクロ製品の保護をすべてオフにされる恐れがあります。それにより個人データ、企業機密、銀行情報への不正アクセスや、盗用、ランサムウェア、破損などの被害を受けやすくなる可能性があります。トレンドマイクロはアカウントを保護するために、2要素認証をただちに有効にすることを強く推奨します。

今後このメッセージを表示しない

危険性を理解したうえで、スキップします

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

サービスプラン名	製品/サービス	シート/ユニット	ライセンス種別	開始日	有効期限	アクション
おまかせアンチウイルス ライト	ウイルスバスター ビジネスセキュリティサ ビス	5シート	製品版	2017/05/17	自動更 新	<a href="#">コンソールを 開く</a>

有効期限切れ

コンソールを開く  
から管理コンソールにいきます

**TREND MICRO Worry Free™ Business Security Services** 15:49 UTC+09:00

セキュリティリスクの検出数 (過去30日間)

- 既知の脅威: 4 ↑
- 未知の脅威: 0
- ポリシー違反: 0 ↓ 100%

イベントの種類	影響を受けたエンドポイント	検出数
ウイルス/不正プログラム	1	2
スパイウェア/グレーウェア	0	0
Webレピュテーション	1	2
ネットワークウイルス	0	0

感染経路別の検出数 (過去30日間)

- 4 検出数 (すべての脅威)
- Web: 3
- クラウド同期: 0
- メール: 0
- リムーバブルストレージ: 0
- ローカルまたはネットワークドライブ: 1

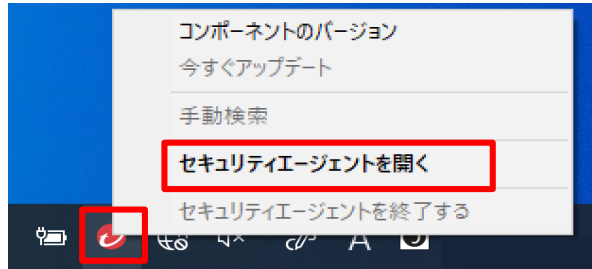
セキュリティエージェントのステータス




- 7 セキュリティエージェント
- 7 デスクトップサーバ: パターンファイルのアップデートが必要 (7), オフライン (7)
- 0 モバイルデバイス: パターンファイルのアップデートが必要 (0), 警告 (0)

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
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

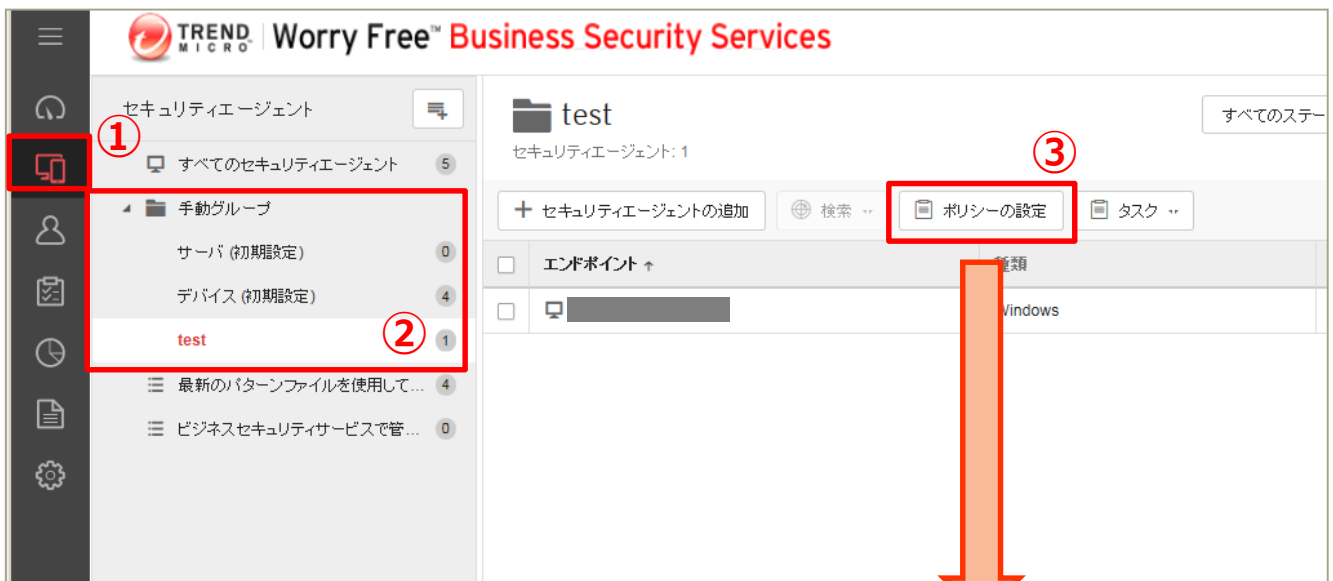
⇒ P.8のセキュリティ機能はグループごとに設定します。

## 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。

グローバルセキュリティエージェント設定  
グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール

一般検索

- 遅延検索を有効にする  
注意: この機能を有効にすると、ファイルをコピーする際の検索処理のタイミングが遅延します。パフォーマンスは向上しますが、
- Microsoft Exchange Server 2003フォルダを除外する ①
- Microsoft®メインコントローラフォルダを除外する  
(スライウェア/グレーウェアの手動および予約検索には適用できません)
- シャドウコピーセクションの除外 ①
- 行われなかった予約検索を翌日の同じ時刻に実行

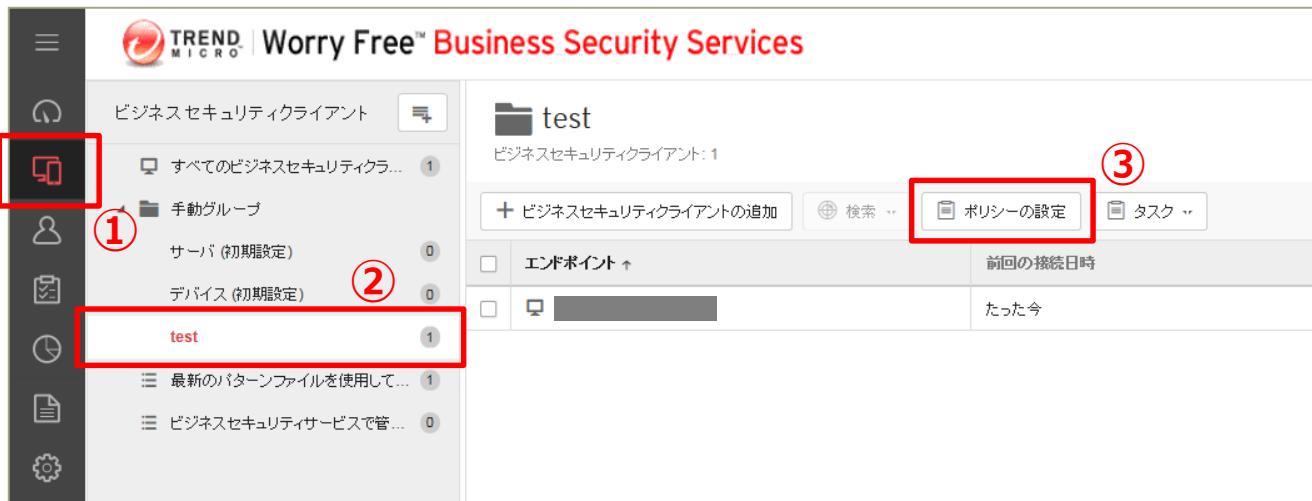
ウイルス検索

- 圧縮ファイルの検索制限

2

# 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。



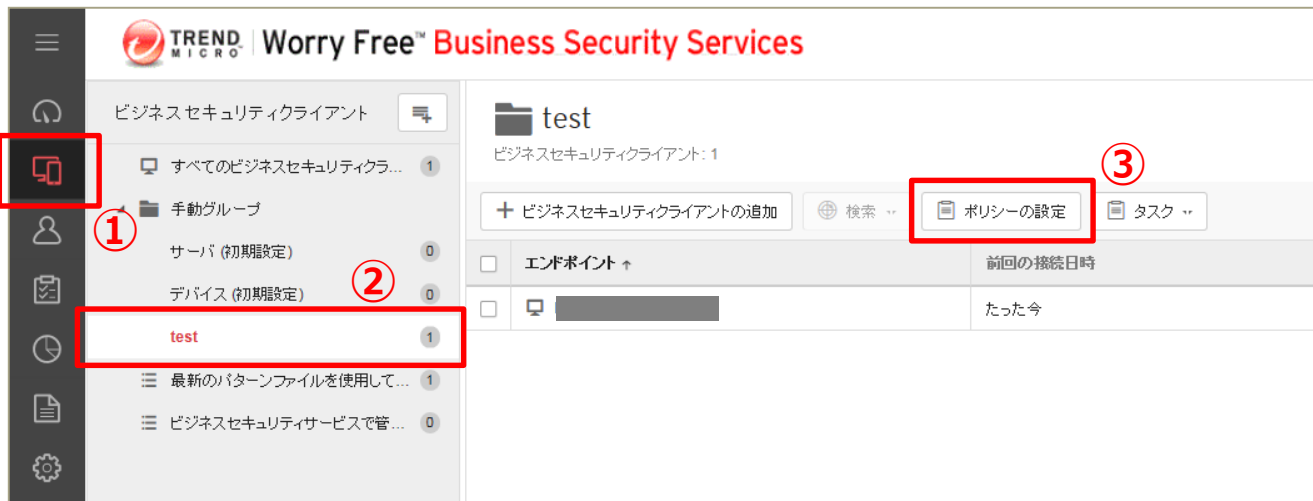
「保存」を押して終了です。

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。

リアルタイム検索設定

⑥

対象 処理

検索設定

検索するファイル:

- 検索可能なすべてのファイル
- トレンドマイクロの推奨設定で検索されるファイルタイプ ⓘ
- 指定された拡張子を持つファイル

ファイルに対するユーザのアクティビティ

- 作成、変更、またはファイルの読み込み
- ファイルの読み込み
- 作成または変更

詳細設定

- POP3メッセージを検索する ⑦
- IntelliTrapを有効にする ⓘ
- 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 ⓘ  
注意: この機能を使用するには、管理者がリアルタイム検索と挙動監視を有効にしている必要があります。
- ネットワークドライブおよび共有フォルダを検索する
- システムのシャットダウン時にフロッピーディスクを検索する
- 圧縮ファイルの検索 ⓘ

最大階層数: 2 ▲

OK キャンセル ⑧

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

検索除外

承認済み/ブロックするURL

クライアントの設定

権限およびその他の設定

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 [ビジネスセキュリティクライアント] 画面またはビジネスセキュリティクライア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 ⑨

「保存」を押して終了です。

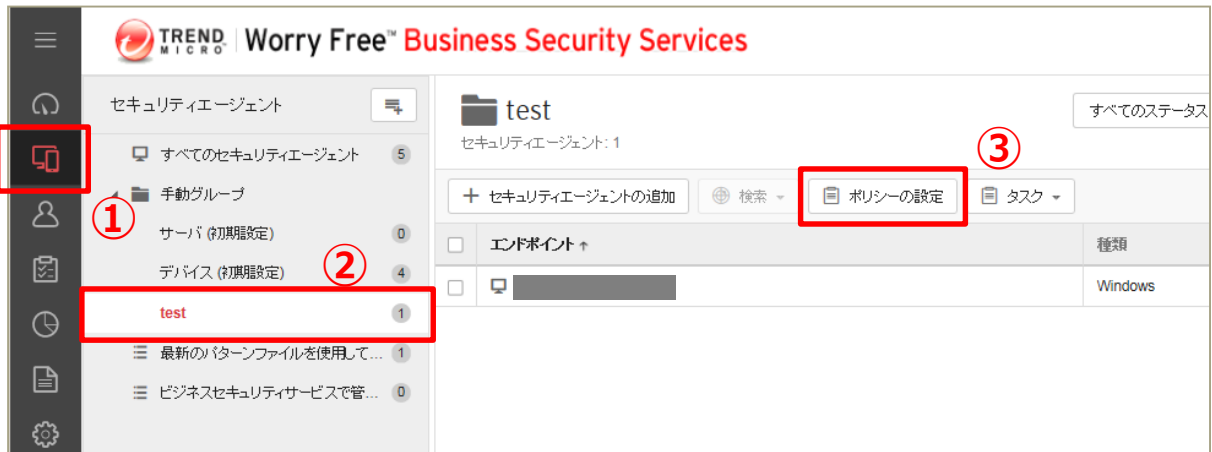
# 機能を設定する（ファイルレス攻撃対応）

ファイルレス攻撃対応機能を有効にします。

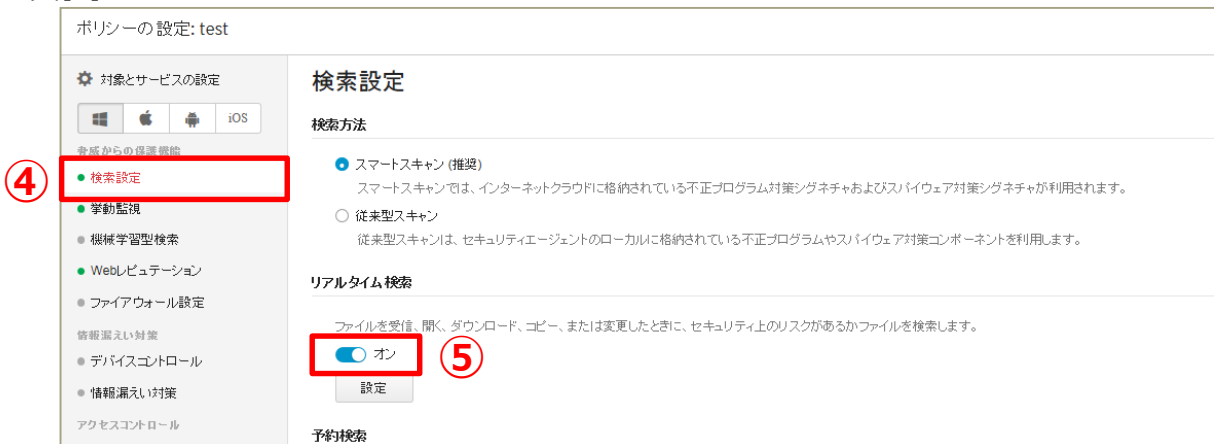
→ハードディスクに保存されない(メモリ上にのみ存在)ウイルスを検出できます。

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 》

ポリシーの設定: test

対象とサービスの設定

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バ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バ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

⑥

予約検索

リアルタイム検索設定

対象 処理

検索設定

検索するファイル:

- 検索可能なすべてのファイル
- トレンドマイクロの推奨設定で検索されるファイルタイプ ①
- 指定された拡張子を持つファイル

ファイルに対するユーザのアクティビティ

- 作成、変更、またはファイルの読み込み
- ファイルの読み込み
- 作成または変更

詳細設定

- POP3メッセージを検索する
- IntelliTrapを有効にする ①
- 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 ① ⑦  
注意: この機能を使用するには、管理者がリアルタイム検索と挙動監視を有効にしている必要があります。
- ネットワークドライブおよび共有フォルダを検索する
- システムのシャットダウン時にフロッピーディスクを検索する
- 圧縮ファイルの検索 ①

最大階層数: 2 ▲

⑧ キャンセル



# 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 》

ポリシーの設定: test

対象とサービスの設定

OS: Windows, Apple, Android, iOS

脅威からの保護機能

- 検索設定 (9)
- **挙動監視 (10)**
- 機械学習型検索
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済み/ブロックする URL

エージェントの設定

- 権限およびその他の設定

### 挙動監視

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。

注意: この機能を使用するには、対象とサービスの設定で不正変更防止サービスを有効にする必要があります。

オン (10)

#### 不正プログラム挙動ブロック

オン

- 既知および潜在的な脅威のブロック
- 既知の脅威のブロック

#### ランサムウェア対策

- 不正なファイル暗号化や変更から文書を保護 (1)
- 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 (1)
- 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 (1)
- 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およびブロック (1)

#### 脆弱性対策

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 (11)

オン

Intuit™ QuickBooks™ 保護

## 《 項目 5 》

ポリシーの設定: test

対象とサービスの設定

OS: Windows, Apple, Android, iOS

脅威からの保護機能

- 検索設定 (13)
- 挙動監視
- **機械学習型検索 (14)**
- Webレピュテーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

### 機械学習型検索

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジーを使用して、あまり普及していない不審プロセスやファイルに含まれる未知のセキュリティリスクを検出します。

注意:

- 機械学習型検索を使用するには、挙動監視を有効にする必要があります。
- インターネット接続を利用できない場合は、機械学習型検索ローカルモデル (ファイル検出) を使用してポータブル実行可能ファイルの脅威に対する保護が継続されます。

#### 検出設定

種類	処理
<input checked="" type="checkbox"/> ファイル	隔離
<input checked="" type="checkbox"/> プロセス	終了 (1)

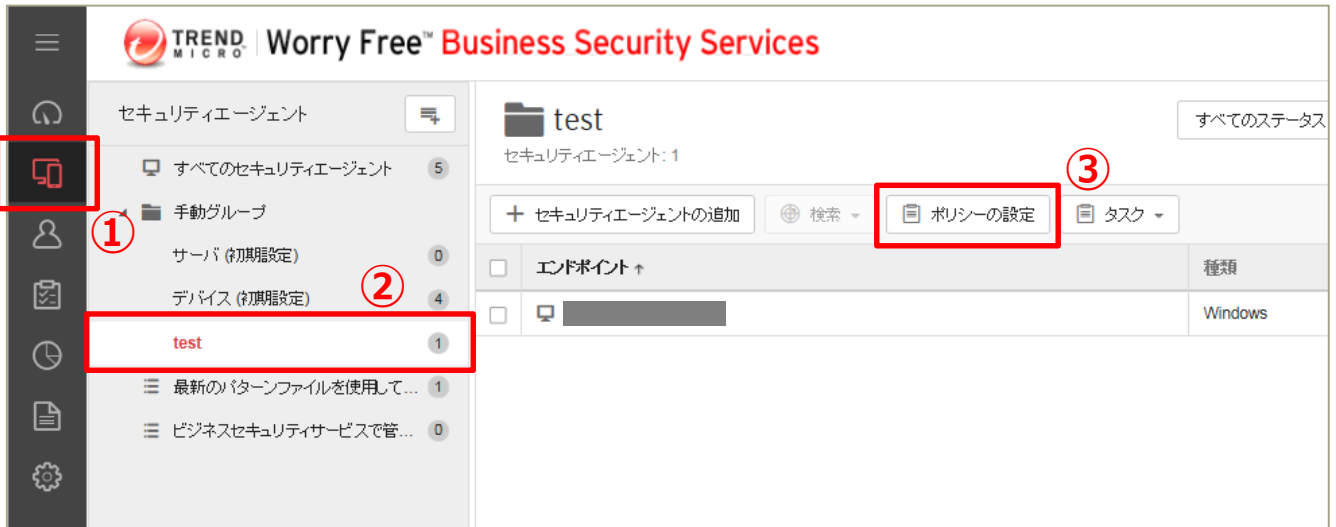
保存 (15)    キャンセル

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、レジストリなどを不正に変更されないように  
エンドポイントを保護します。



「保存」を押して終了です。

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

# 機能を設定する（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

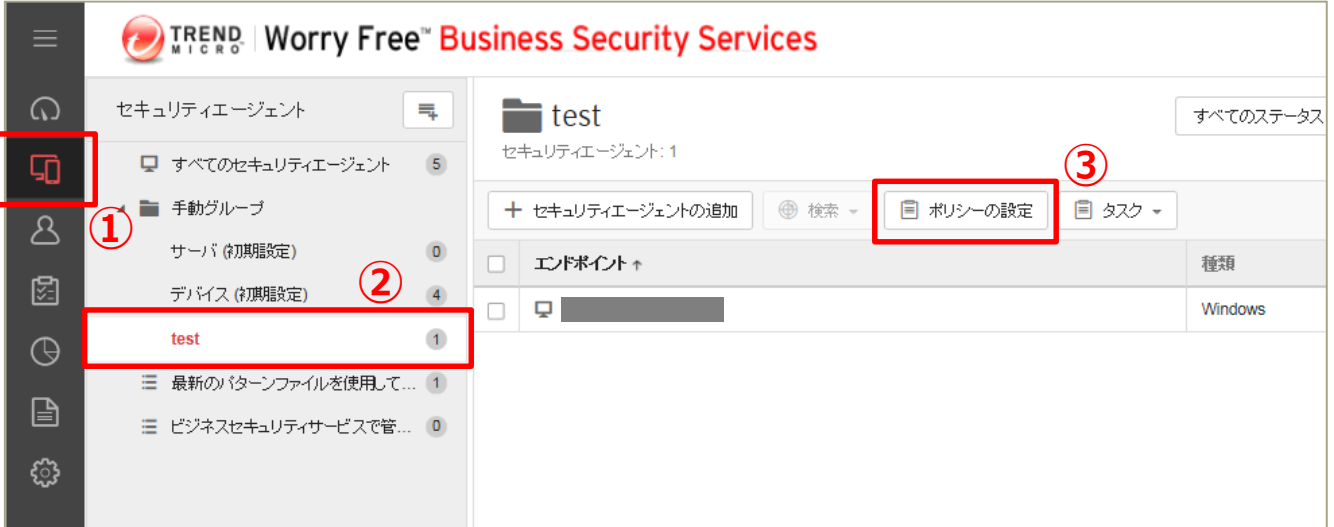
コンピュータのプロセス挙動監視を強化し、ランサムウェア特有の挙動をする実行可能ファイルを検出しブロックします。

# 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。



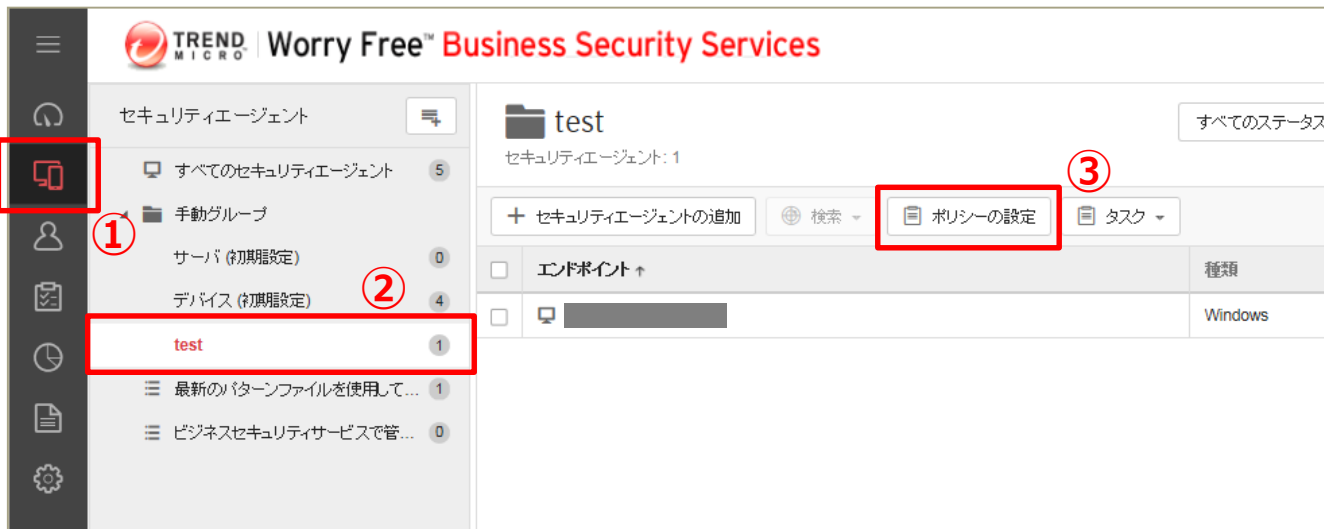
「保存」を押して終了です。

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。

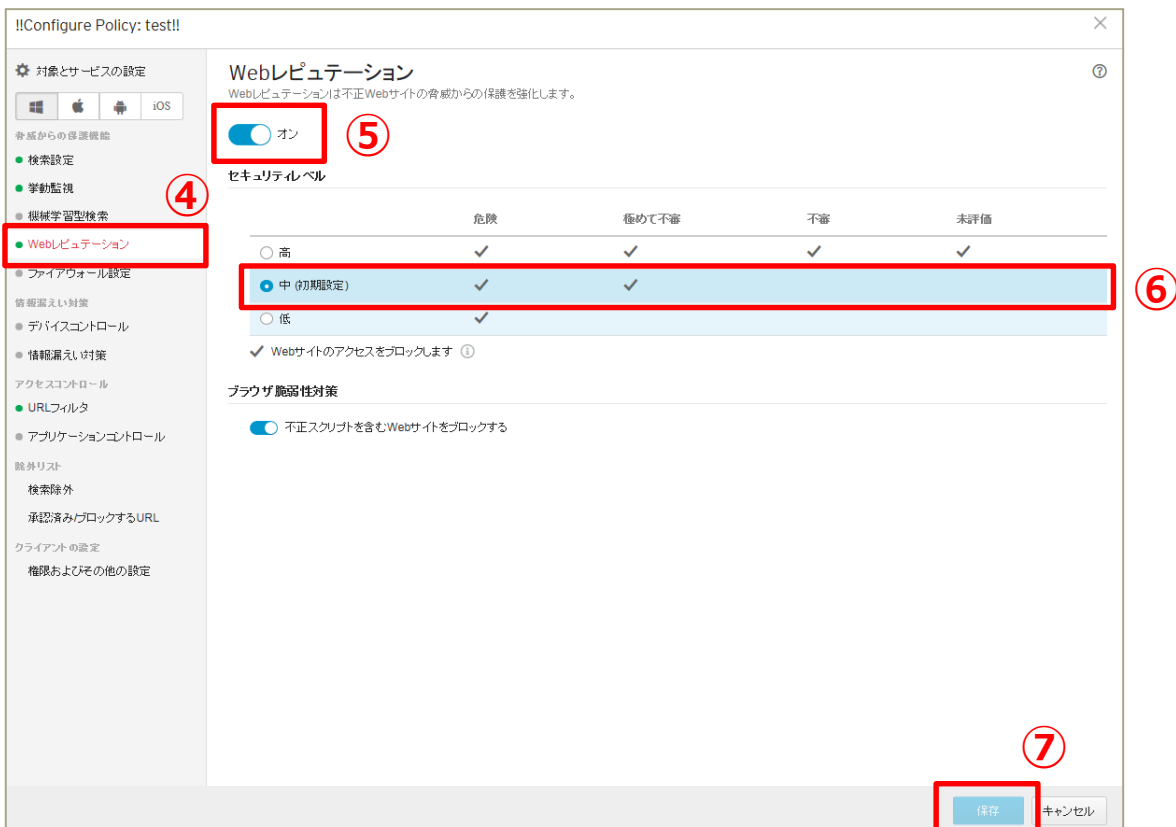
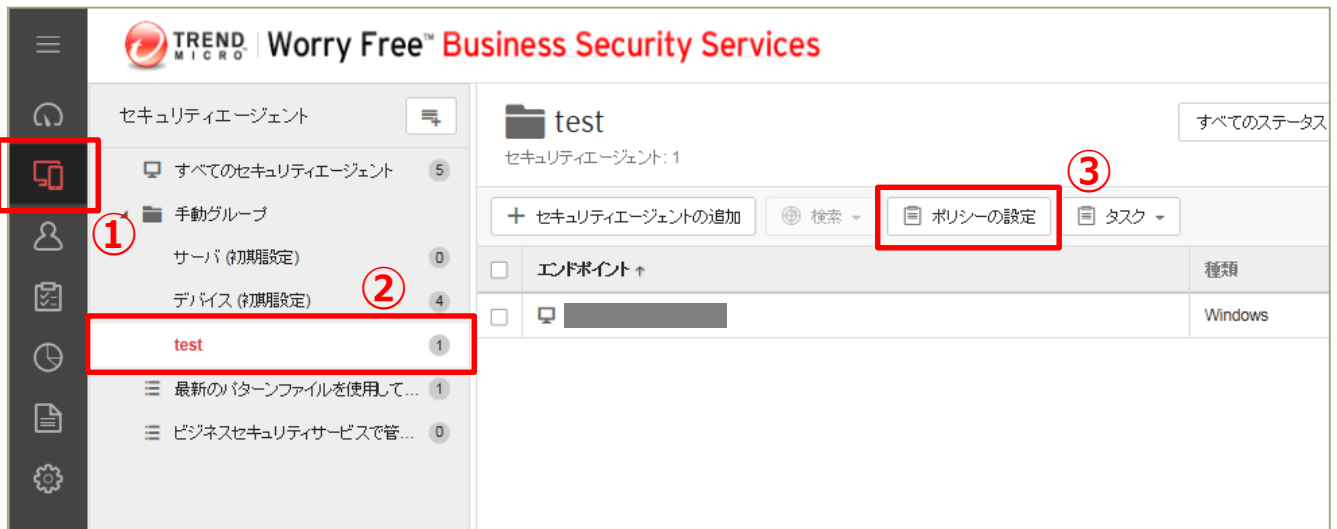
仮想パッチとは：脆弱性そのものを修正する正規パッチとは異なり、脆弱性を突く攻撃をネットワークレイヤで検知およびブロックするものです。脆弱性発覚後、各ベンダーから正規パッチがリリースされるまでの間、仮想パッチにより、本脆弱性を衝く攻撃のリスクを軽減することができます。

# 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。

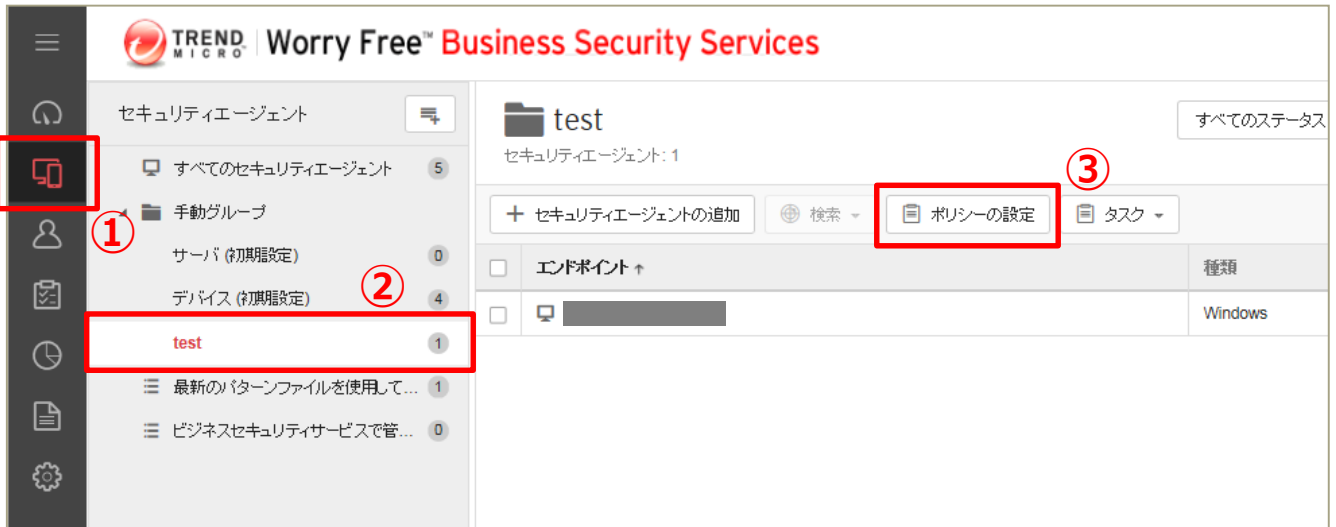
Webレピュテーションとは：不正なWebサイトへのアクセスをブロックするWebセキュリティ機能

# 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。

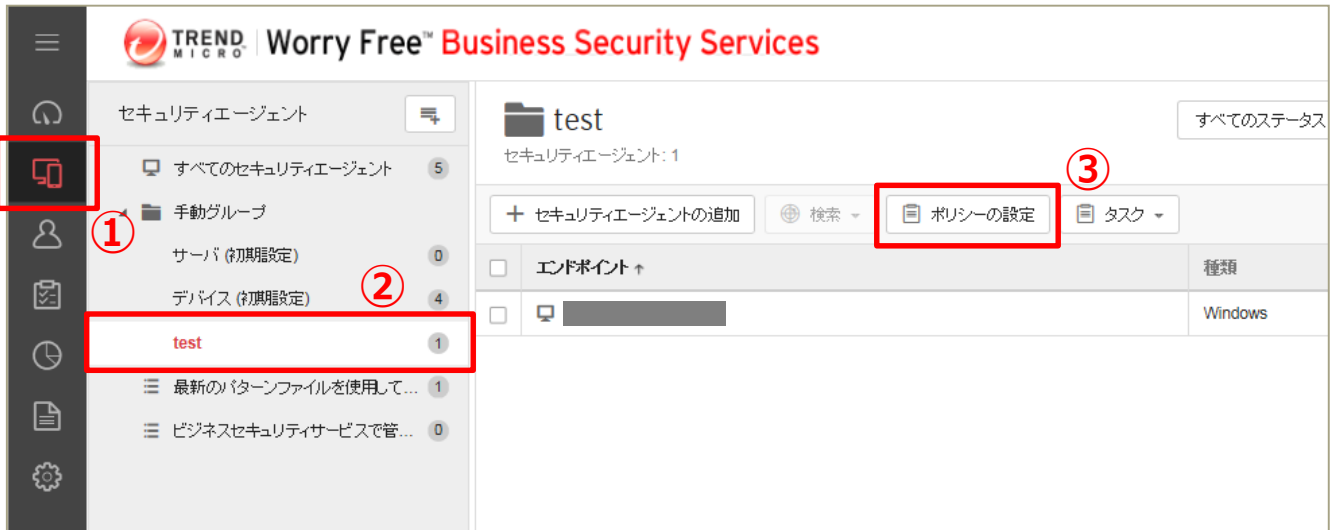


「保存」を押して終了です。

# 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。



「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。

The screenshot displays the Trend Micro Worry Free Business Security Services interface. The left sidebar contains navigation options: 'ポリシー設定' (Policy Settings), '追加の設定' (Additional Settings), 'グローバルセキュリティエージェント設定' (Global Security Agent Settings), 'グローバル除外リスト' (Global Exemption List), 'ポリシーリソース' (Policy Resources), 'アプリケーションコントロールルール' (Application Control Rules), and '設定' (Settings). The 'グローバル除外リスト' option is highlighted with a red box and a circled '4'. The main content area is titled 'グローバル除外リスト' (Global Exemption List) and includes a description: 'ポリシー設定を使用するために必要な除外設定を構成します。' (Configure exemption settings required to use policy settings). Below this, there are sections for 'Webレピュテーション/URLフィルタ' (Web Reputation/URL Filter), '不正プログラム検索除外' (Malware Search Exclusion), and 'デバイスコントロール' (Device Control). The 'デバイスコントロール' section is highlighted with a red box and a circled '5', and it contains a sub-section '許可されたUSBデバイスのリスト (0)' (List of Allowed USB Devices (0)), which is also highlighted with a red box.

# 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。

許可されたUSBデバイスのリスト

ベンダー/製造元	機種/製品ID	シリアルID/番号	メモ
----------	---------	-----------	----

デバイス情報を取得する方法 ⑦

- 外部デバイスが接続されたエンドポイントで以下を実行します。
  - Windows: **デバイスリストツール**をダウンロードして実行します。
  - Mac: システム情報を確認します。 [詳細情報](#)
- デバイスコントロール違反が発生した場合にデバイスコントロールログの詳細を確認します。

デバイス情報は追加されていません。  
デバイスが追加された後、USBストレージデバイスを指定します。

10件ページ 1 / 1

デバイス情報を取得する ⑥

wfbs-svc-nabu.trendmicro.com から listDeviceInfo.exe を実行または保存しますか? 実行(B) **保存(S)** キャンセル(C) x

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

nihei

整理 新しいフォルダー

名前	更新日時	種類	サイズ
<b>listDeviceInfo.exe</b>	2019/04/12 14:52	アプリケーション	341 KB

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

リムーバブルディスクドライブ:

コンピュータ	ユーザ	ポート	説明	ベンダ	モデル	シリアル番号
PC001	Security Manager	USB	USB Device	SONY	0910	0123456789

許可されたUSBデバイスのリスト

⑩

+ 追加    インポート    削除    エクスポート

ベンダ/製造元    機種/製品ID

デバイス情報を取得する方法

許可されたUSBデバイス

ベンダ/製造元\*  
SONY

機種/製品ID:  
0910

シリアルID/番号:  
0123456789

メモ:

⑪ 表示された値を入力します

⑫ 保存    キャンセル

「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。

このスクリーンショットは、Trend Micro Worry Free Business Security Servicesの管理画面を示しています。左側のナビゲーションメニューには、モバイルデバイスのアイコンが赤い箱で囲まれています（1）。メインメニューには「test」というグループが赤い箱で囲まれています（2）。右側の操作ボタンには「ポリシーの設定」が赤い箱で囲まれています（3）。

このスクリーンショットは、ポリシー設定画面の「情報漏えい対策」セクションを示しています。左側のメニューで「情報漏えい対策」が選択されています（4）。設定は「オン」に切り替わっています（5）。また、「ルール」ボタンが赤い箱で囲まれています（6）。下部には「+ 追加」ボタンが赤い箱で囲まれています（7）。右側の表には、現在定義されたルールがないことが示されています。

ルール	テンプレート	チャネル	処理	有効
ルールが定義されていません。 [追加] をクリックして、情報漏えい対策ルールを作成してください。				

# 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。

情報漏えい対策ルールの設定

一般設定

このルールを有効にする

ルール名: test 8

説明:

テンプレート

情報漏えい対策テンプレートを選択し、監視する機密データの種類を定義してください。 [詳細情報](#)

すべてのテンプレート

テンプレート (1/239)
<input type="checkbox"/> 台湾: 携帯電話番号
<input type="checkbox"/> 台湾: 日盛銀行の口座番号 <span>9</span>
<input type="checkbox"/> 台湾: 銀行口座番号
<input checked="" type="checkbox"/> 日本: パスポート番号
<input type="checkbox"/> 日本: マイナンバー (法人) 国の機関 10件以上で検出
<input type="checkbox"/> 日本: マイナンバー (法人) 地方公共団体 (団体コードあり) 10件以上で検出
<input type="checkbox"/> 日本: マイナンバー (法人) 地方公共団体 (団体コードなし) 10件以上で検出
<input type="checkbox"/> 日本: マイナンバー (法人) 設立登記のある法人 10件以上で検出
<input type="checkbox"/> 日本: マイナンバー (法人) 設立登記のない法人・人格なき社団・人格なき財団 10件以上で検出

チャンネル

情報漏えい対策で監視するチャンネルの種類を選択してください。

ネットワークチャンネル 10

システムおよびアプリケーションチャンネル

処理

選択したネットワークチャンネルを通じて転送される機密データを検索した後、ログの記録および指定された処理を実行します。

処理: ブロック 11

追加 キャンセル 12

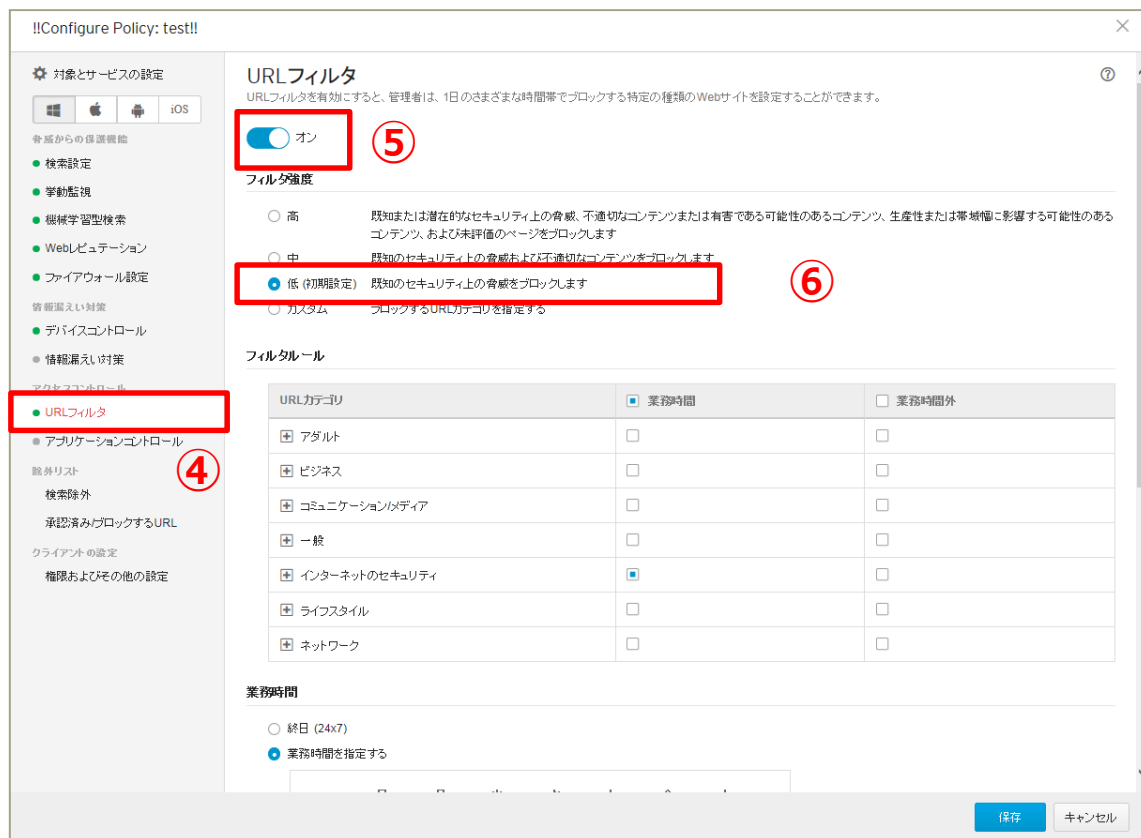
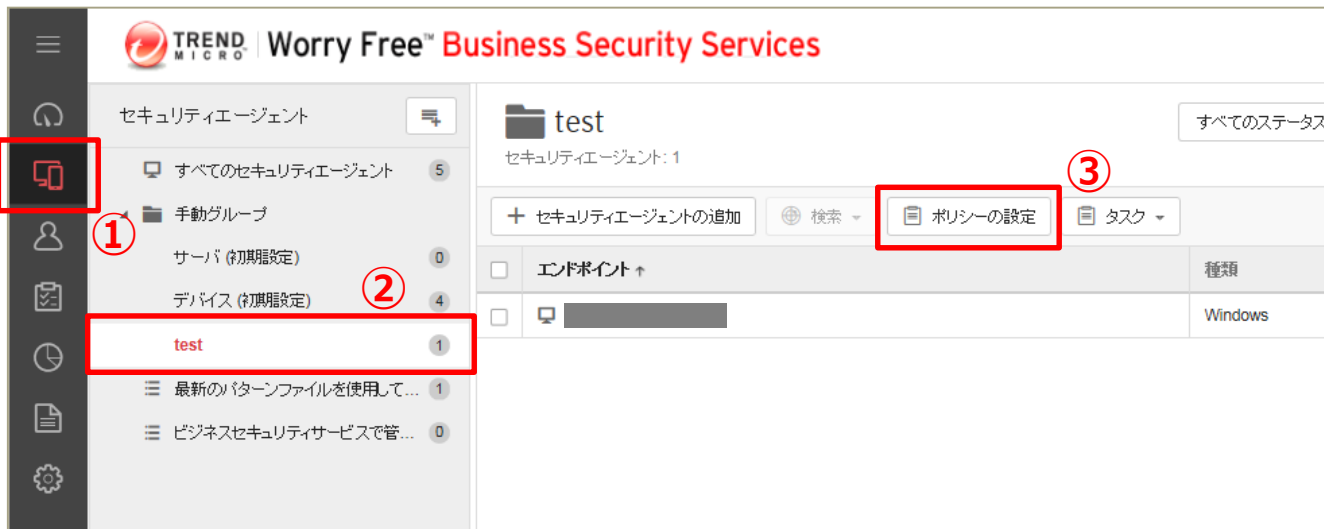
「保存」を押して終了です。

# 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。

!!Configure Policy: test!!

対象とサービスの設定

インターネットのセキュリティ

ライフスタイル

ネットワーク

業務時間

終日 (24x7) 7

業務時間を指定する

日 月 火 水 木 金 土 8

08:00

09:00

10:00

11:00

12:00

13:00

14:00

15:00

16:00

17:00

18:00

19:00

● 業務時間 ○ 業務時間外

業務で利用する曜日、時間帯をクリックして選択

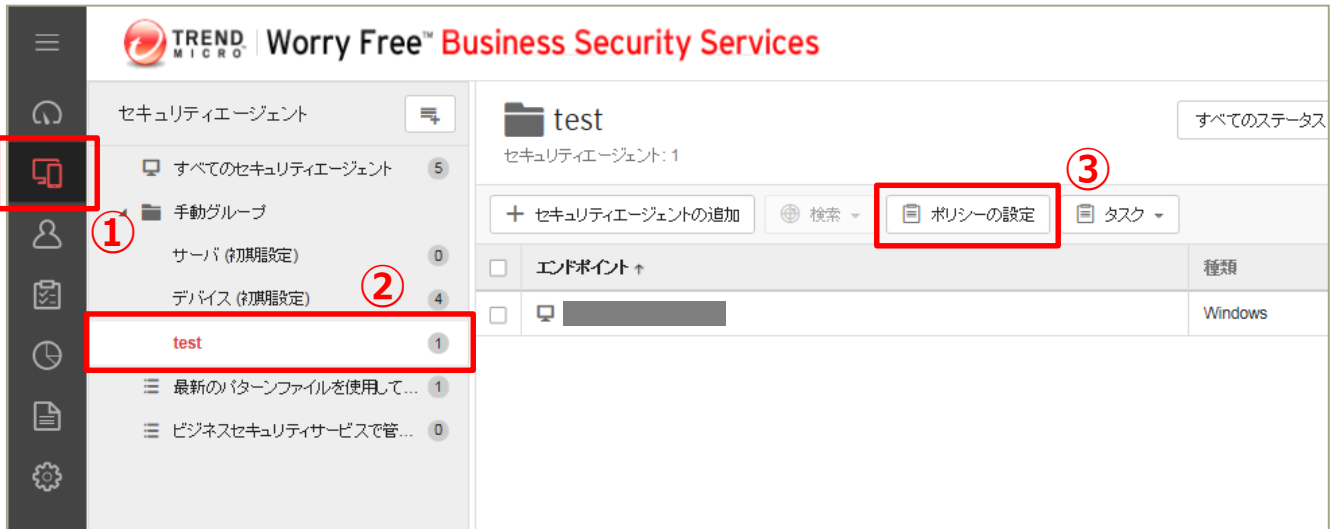
9

保存 キャンセル

「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。

ブロックするアプリケーションを管理

ブロックするアプリケーションを次のソフトウェア安全性評価リストから選択してください。

アプリケーションまたはベンダー名の検索

アプリケーション	ベンダー
<input checked="" type="checkbox"/> アプリケーション	
<input checked="" type="checkbox"/> Password Revealer	Rekenwonder Software
<input checked="" type="checkbox"/> Ardamax Keylogger	Ardamax Software
<input checked="" type="checkbox"/> Proxifier	Initex Software
<input checked="" type="checkbox"/> Hola	Hola
<input checked="" type="checkbox"/> Freenet	Freenet
<input checked="" type="checkbox"/> Actual Keylogger	Actual Spy Software
<input checked="" type="checkbox"/> Spyrix Free Keylogger	Spyrix
<input checked="" type="checkbox"/> Desktop Shark	Desktop Shark
<input checked="" type="checkbox"/> iSafe Free Keylogger	iSafesoft

高リスクのアプリケーション(68/68)

高リスクのアプリケーションカテゴリに追加される新しいアプリケーションをブロックします。

9 OK キャンセル

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済みブロックするURL

クライアントの認定

- 権限およびその他の設定

ブロックするパスリスト

ファイルまたはフォルダのパスを利用し、エンドポイントでアプリケーションの実行をブロックします。  
注意: この機能を使用するには、対象とサービスの設定で不正変更防止サービスを有効にする必要があります。

+ 追加 合計: 0

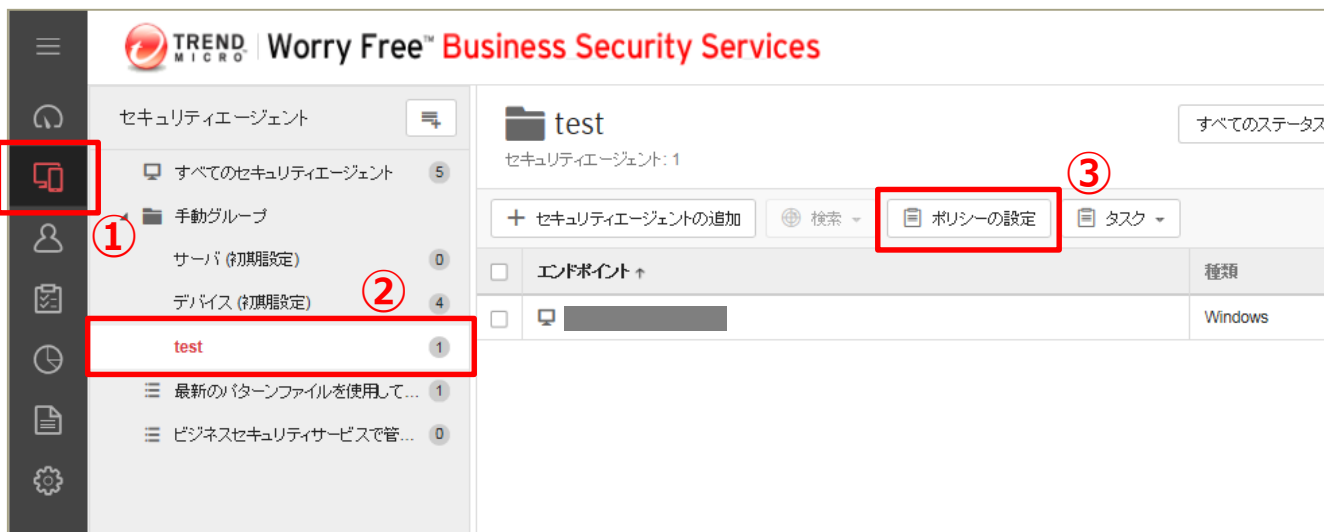
ファイル/フォルダのパス	メモ
パスが追加されていません。 [追加] をクリックしてファイルまたはフォルダのパスを指定します。	

10 保存 キャンセル

「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 》

ポリシーの設定: test

対象とサービスの設定

OS: Windows, Apple, Android, iOS

脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- Webシミュレーション
- ファイアウォール設定

情報漏えい対策

- デバイスコントロール
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済みブロックするURL
- エージェントの設定
- 権限およびその他の設定

トレンドマイクロ製品がインストールされているディレクトリを次の場所から除外します。

リアルタイム検索  予約検索  手動検索

スパイウェアグレーウェア

+ 追加 合計: 0

スパイウェアグレーウェア

スパイウェアまたはグレーウェアの除外は追加されていません。  
[追加](#) をクリックしてスパイウェアまたはグレーウェアの除外を指定します。

**挙動監視**

挙動監視により自動的に、すべての承認済みプログラムの実行が許可され、すべてのブロックするプログラムの実行が阻止されます。

**承認済みプログラムリスト (0)** **ブロックするプログラムリスト (0)** **⑥**

+ 追加 合計: 0

プログラム ファイルパス

承認済みプログラムは追加されていません。  
[追加](#) をクリックして、ファイルパスを指定してください。

機械学習型検索

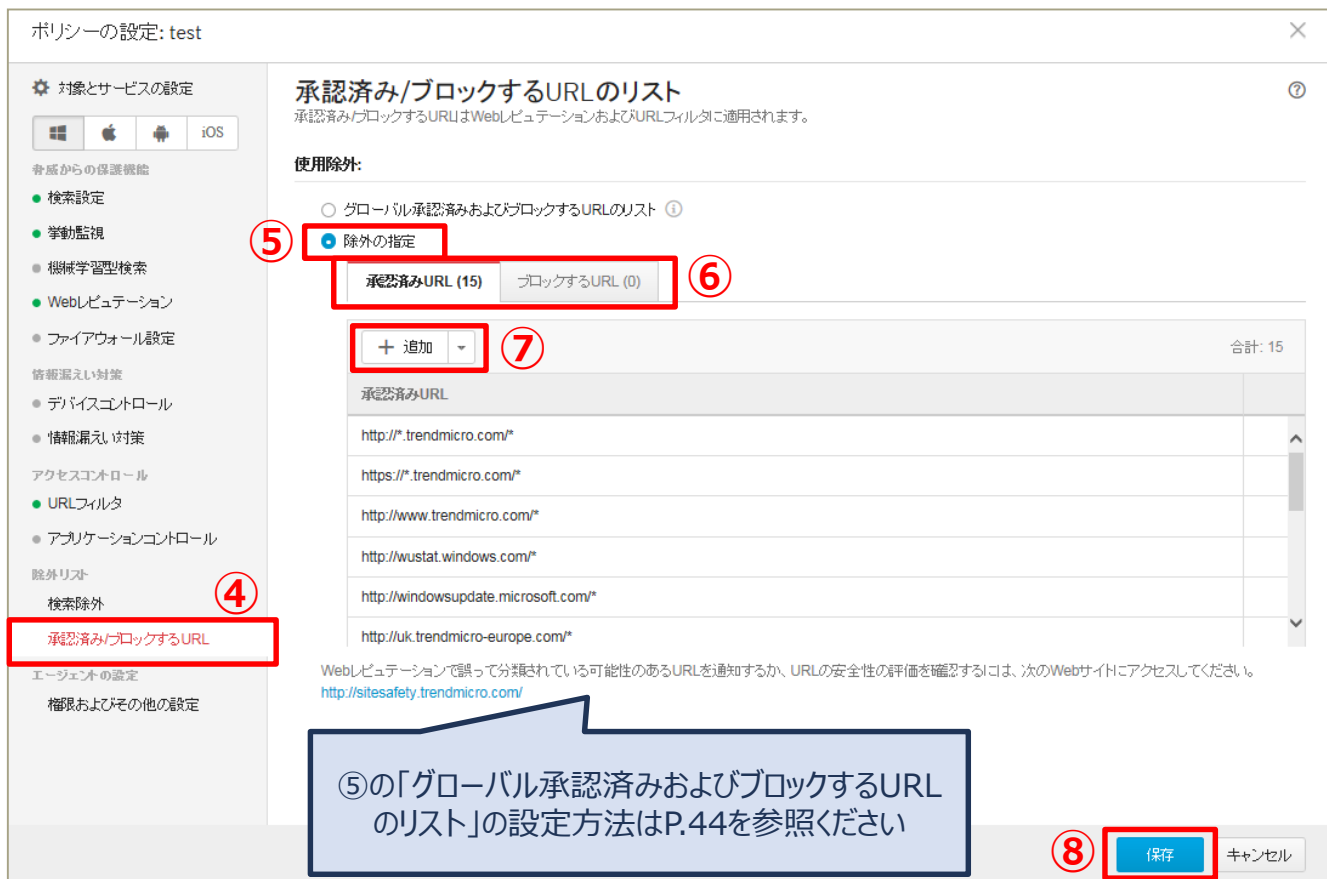
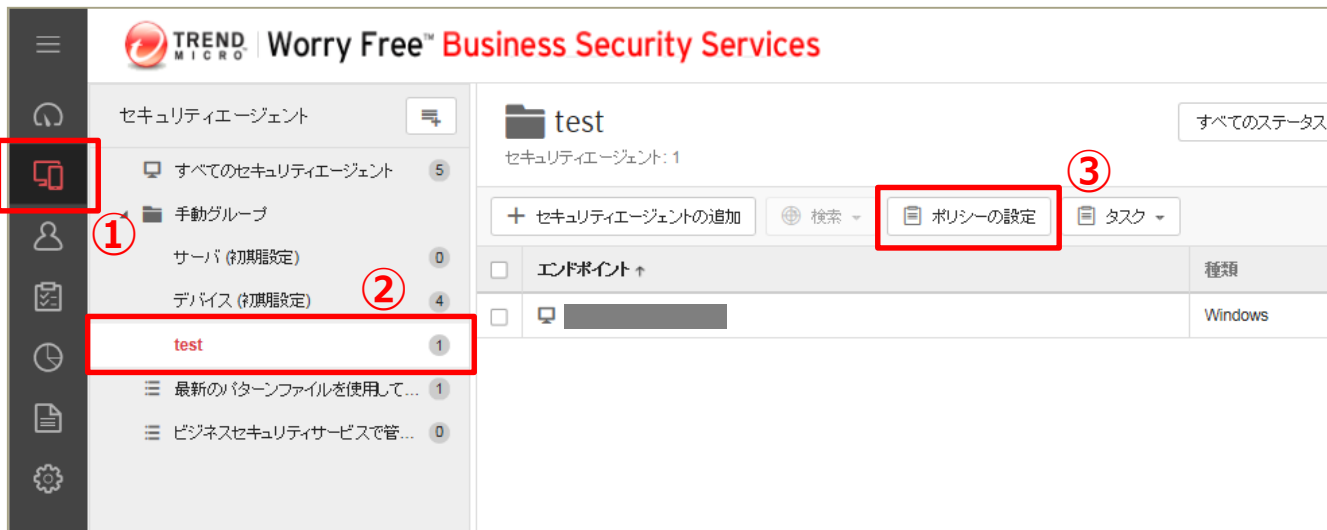
機械学習型検索の除外は、すべてのセキュリティエージェントに適用されます。除外を指定するときは、[ポリシー設定]→[グローバル除外リスト]に進みます。

**⑦** **保存** キャンセル

「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。

グローバルセキュリティエージェント設定  
グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール ③

警告

7 日経過してもウイルスパターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

セキュリティエージェントのログ

WebレピューションおよびURLフィルタのログをサーバーに送信する

脅威イベントの詳細を強化型脅威分析のためにサーバーに送信する ④

監視サービス

セキュリティエージェントの監視サービスを有効にする:  
セキュリティエージェントのステータスを 1 分間隔で確認  
セキュリティエージェントを再起動できない場合、5 回まで再試行

管理者への問い合わせの通知

セキュリティエージェントに管理者への問い合わせ情報を表示する

アンインストール

セキュリティエージェントのアンインストール時にパスワード入力を要求する

終了ロック解除

セキュリティエージェントの終了時、または詳細設定のロック解除時にパスワード入力を要求する

保存 ⑤

## 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。

ログ

セキュリティリスクの検出: すべて | 過去30日間 | 28件 | エクスポート

日時 ↓	カテゴリ	脅威/違反	ファイルのパス/対象	処理/結果	エンドポイント	ユーザ	詳細
2019年01月30日 17:3...	機械学習型検索	Ransom.Win32.TRX...	c:\users\yoko_\downlo...	隔離	DESKTOP-HHK490J	yoko_	
2019年01月30日 17:3...	ウイルス/不正プログ...	Ransom.Win32.TRX...	c:\users\yoko_\downlo...	駆除	DESKTOP-HHK490J	yoko_	
2019年01月30日 17:3...	ウイルス/不正プログ...	Ransom.Win32.TRX...	c:\users\yoko_\appdat...	駆除	DESKTOP-HHK490J	yoko_	

①

拡張脅威分析

**クリックすると表示**

Ransom.Win32.TRX.XXPE1  
2019年01月30日 17:38:38

エンドポイント  
DESKTOP-HHK490J  
IP: 192.168.126.13  
最後のユーザ: yoko\_

感染経路  
Web  
microsoftedgecp.exe

検出した脅威  
trendx\_sign-a.exe

microsofedgecp.exe → https://doc-0c-...nload → trendx\_sign-a.exe

### 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

グローバルビジネスセキュリティクライアント設定

グローバル設定はサポートされるすべてのビジネスセキュリティクライアントに適用されます。

セキュリティ設定 クライアントコントロール

警告

7 日経過してもウイルス/パターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

ビジネスセキュリティクライアントのログ

WebレジュレーションおよびURLフィルタのログをサーバに送信する

監視サービス

ビジネスセキュリティクライアントの監視サービスを有効にする:

ビジネスセキュリティクライアントのステータスを 1 分間隔で確認

ビジネスセキュリティクライアントを再起動できない場合、5 回まで再試行

管理者への問い合わせの通知

ビジネスセキュリティクライアントに管理者への問い合わせ情報を表示する

アンインストール

ビジネスセキュリティクライアントのアンインストール時にパスワード入力を要求する

パスワード:  4~20文字

パスワードの確認:

終了ロック解除

ビジネスセキュリティクライアントの終了時、または詳細設定のロック解除時にパスワード入力を要求する

保存

アンインストールに必要なパスワードを入力

「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

①

②

グローバルビジネスセキュリティクライアント設定

グローバル除外リスト

③

セキュリティ設定 クライアントコントロール

警告

7 日経過してもウイルスパターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

ビジネスセキュリティクライアントのログ

WebビューションおよびURLフィルタのログをサーバに送信する

監視サービス

ビジネスセキュリティクライアントの監視サービスを有効にする:

ビジネスセキュリティクライアントのステータスを 1 分間隔で確認

ビジネスセキュリティクライアントを再起動できない場合、 5 回まで再試行

管理者への問い合わせの通知

ビジネスセキュリティクライアントに管理者への問い合わせ情報を表示する

アンインストール

ビジネスセキュリティクライアントのアンインストール時にパスワード入力を要求する

終了ロック解除

ビジネスセキュリティクライアントの終了時、または詳細設定のロック解除時にパスワード入力を要求する

パスワード:  4~20文字

パスワードの確認:

④

⑤

保存

エージェントの終了に必要なパスワードを入力

「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。

管理 ② 一般設定

①

③

⑤

[ラベル形式]に記入したワードがエージェントのダウンロード時の画面に表示されます。

「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

TREND MICRO ウイルスバスター ビジネスセキュリティサービス

ビジネスセキュリティクライアントのインストール

ラベル情報  
管理者から要求された情報を入力します。

デバイスラベル: 従業員ID

手順

1. 下の [ダウンロード] をクリックして、インストールプロセスを開始します。
2. [実行] をクリックして、インストーラをダウンロードします。([保存] をクリックしないでください)。

ダウンロード

注意: WFBS-SVC\_Agent\_Installer.exeは他のコンピュータにコピーできません。インストールプロセスは、ダウンロードURLから開始する必要があります。

ラベル形式で指定された内容を入力できるようになります。

# 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。

「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。

すべてのセキュリティエージェント

エンドポイント	ラベル	前回の接続日時	IPv4アドレス	ステータス	ユーザ
[Redacted]	0123456789	2時間前	[Redacted]	オフライン	[Redacted]

# 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。

管理

TREND Worry Free™ Business Security Services

13:19 UTC+09:00 demo\_anti\_3

通知

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ウイルスバスター ビジネスセキュリティサービスを設定します。事前定義されたトークンのリストについては、[通知のカスタマイズ](#)を参照してください。

設定 要確認 警告

送信者: WFBS-SVC@TrendMicro.com

受信者: **管理者メールアドレス**

複数入力する場合は、セミコロンで区切ってください。  
例: user1@example.com; user2@example.com

件名の先頭の文字列: **【おまかせアンチウイルスからの通知】**

メールの件名の先頭に文字列が追加されます。  
例【おまかせアンチウイルスからの通知】[要確認] 解決されていない脅威: 5

保存

「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。

**TREND MICRO | Worry Free™ Business Security Services**

ポリシー設定

追加の設定

グローバルセキュリティエージェント設定

**グローバル除外リスト**

ポリシーリソース

1 アプリケーションコントロールルール

2

## グローバル除外リスト

ポリシー設定を使用するために必要な除外設定を構成します。

### Webレピュテーション / URLフィルタ

**承認済みURLリスト (15)**  
指定されたWebサイトへのアクセスを許可します。(Windows/Mac/Android)

**ブロックするURLリスト (0)**  
指定されたWebサイトへのアクセスをブロックします。(Windows/Android)

**承認済みIPアドレスリスト (0)**  
指定された宛先IPアドレスへのアクセスを許可します。(Windows)

**許可されたプロセスのリスト (0)**  
指定されたプロセスがWebサイトにアクセスすることを許可します。(Windows)

### 不正プログラム検索除外

**信頼済みWindowsプログラムリスト (0)**  
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Macプログラムリスト (0)**  
特定のプログラムおよび関連プロセスをリアルタイム検索から除外します。

**機械学習型検索除外リスト (0)**  
指定されたSHA-1ハッシュ値を機械学習型検索から除外します。(Windows)

### デバイスコントロール

**許可されたUSBデバイスのリスト (0)**  
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。(Windows/Mac)

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。



新規グループ

名前:

ポリシー設定をインポートする

ソース:

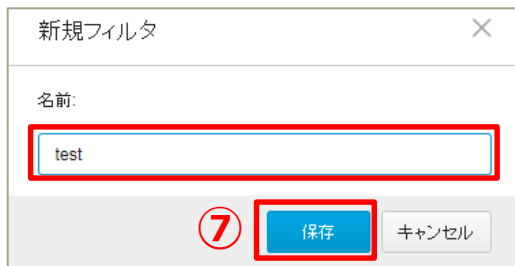
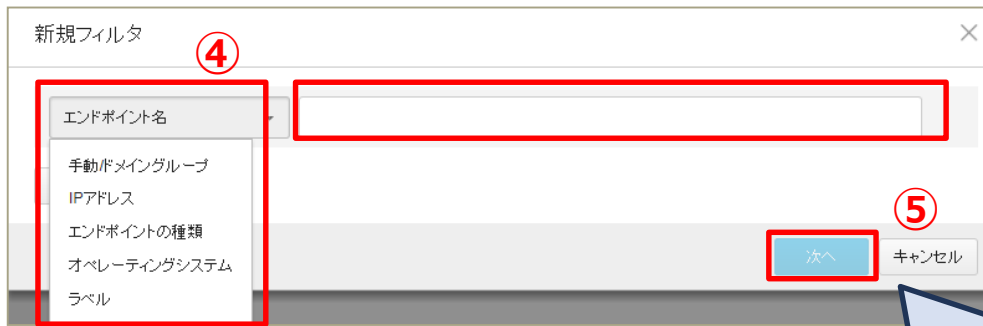


「手動グループ」の配下に新規グループが作成されます。

# 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）

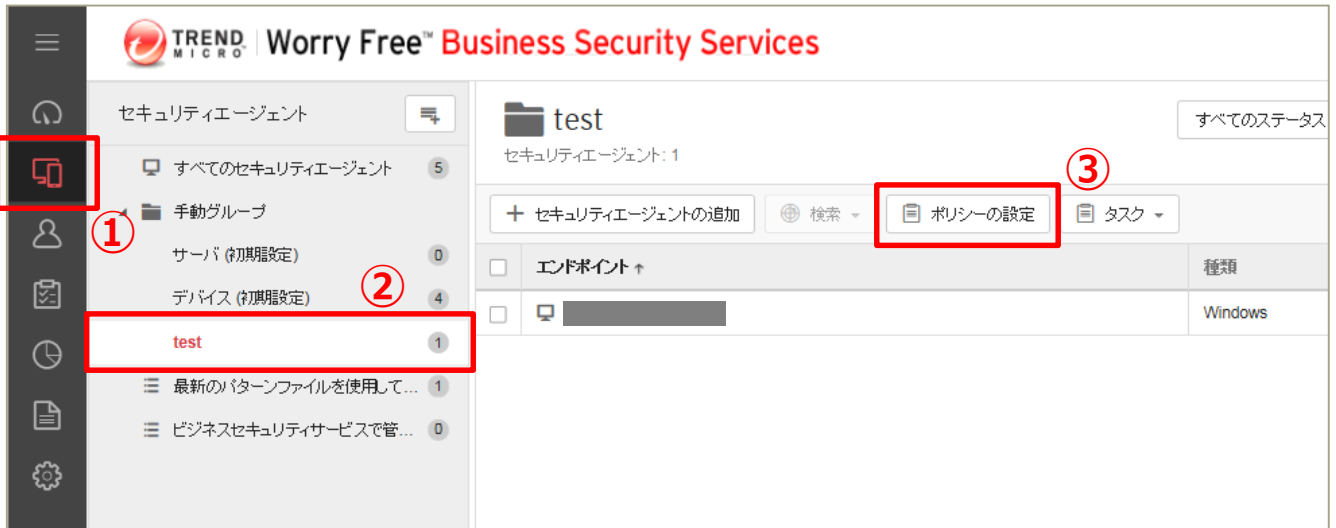
フィルタ名を指定



「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

The screenshot shows the Trend Micro Worry Free Business Security Services interface. On the left sidebar, the 'Security Agents' (セキュリティエージェント) section is expanded, and the 'test' agent is selected (1). In the main area, the 'test' agent's details are shown, including a list of endpoints (2). A checkbox is checked for the selected endpoint (3). The 'Tasks' (タスク) menu is open, and the 'Update Now' (今すぐアップデート) option is selected (4, 5).

The dialog box titled '今すぐアップデート' (Update Now) asks for confirmation to manually update pattern files on Windows, Mac, or Android business security clients. It includes a field for the target (対象) and two buttons: 'アップデート' (Update) and 'キャンセル' (Cancel). The 'アップデート' button is highlighted with a red box (6).

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。

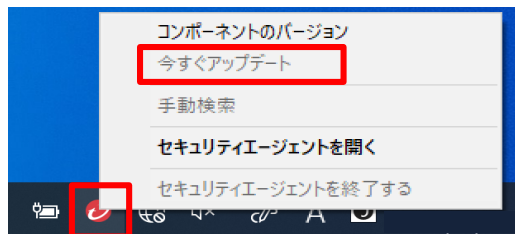


# 機能を設定する（手動アップデート）

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

