おまかせアンチウイルス 初期設定簡易マニュアル

Ver5

2025年1月

東日本電信電話株式会社

<u>『おまかせサイバーみまもり セキュリティパッケージ』を</u> ご利用の方へ

本資料は、「おまかせアンチウイルス」をご利用の皆様に向けて作成されたものですが、 「おまかせサイバーみまもり セキュリティパッケージ」をご利用の皆様にも、 共通の資料としてご活用いただけます。

「おまかせサイバーみまもり セキュリティパッケージ」をご利用の方は 『おまかせアンチウイルス』及び『おまかせアンチウイルスEDRプラス』という表記を 『端末セキュリティ』へ読み替えてご確認ください。

	ページ番号	
サービスの概要		4
サービス提供までの流れ		6
機能一覧	7	
ご利用までの流れ		8
事前準備		9
サービスへのログイン		10
	エージェントインストールの流れ	12
	Windows	16
エージェントインフトール	Мас	19
	Android	38
	iPadOS/iOS	45
	Chromebook	58
機能の設定(Windows)		60

サービス概要

◆おまかせアンチウイルス概要

中小規模の企業向けのエンドポイント向けクラウド型セキュリティサービス



※ ③の監視・設定代行は『おまかせアンチウイルス ライト』では提供しておりません。

サービス概要(おまかせアンチウイルス EDRプラス)

◆おまかせアンチウイルス EDRプラス概要 中小企業向けエンドポイント向けクラウド型EDRセキュリティサービス ※おまかせアンチウイルスとEDRプラスオプションを契約した場合の表記となります

「おまかせアンチウイルスEDRプラス」

ウイルスの侵入を検知・防御する従来のウイルス対策ソフトの機能に加え、万が一ウイルスが端末へ侵入した場合も早期に発見し、他端末への感染拡大を未然に防止するEDR機能 を付加したサービスです。NTT束日本のセキュリティサポートデスクが、ウイルス感染時の詳細調査・端末隔離・復旧支援まで一元的にサポートいたします。



サービスポイント



※ EDRプラスオプションは『おまかせアンチウイルス ライト』では提供しておりません。

サービス提供までの流れ



※お客さまの設定によっては、メールが迷惑メールフォルダなどに振り分けられる場合がございます。
※パスワード設定URLのアクセス期限は事前にお申込みいただいたご利用開始日から1週間以内です。
※送付先メールアドレスは別途送付書面「開通のご案内」をご確認ください。
※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WEBサイト」 https://business.ntt-east.co.jp/service/antivirus/
※その他、メールの不着、およびURLのアクセス期限を経過した場合は、セキュリティサポート
デスクまでお問い合わせください。



PC等におまかせアンチウイルスをインストールし、 ご利用開始

				対応プラン				対応OS			
カラ	י ב י	機能名	説明	E D R プ ラ ス	スタンダード	ライト	Windows	Mac OS	Android	ios/iPados	Chromebook
		ウイルス対策/ セキュリティリスク保護	ウイルス/不正プログラム、スパイウェア、メール、フィッシングサイトなど幅広い脅威に対応することができ、脅威をブロック・隔離することができます。	0	0	0	0	0	0	-	-
		機械学習型検索	AI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		0	0	0	0	-	-	-
	挙動監視機能		プログラム単体では判定困難な場合でも、既知のウイルスと似た挙動を検知した際には自動的にプログラムの実行を停止	0	0	0	0	_	-	-	-
		ファイルレス攻撃対応	挙動監視、機械学習型検索、リアルタイム検索にて、メモリ上にのみ存在するウイルスを検知・隔離 します。	0	0	0	0	_	_	_	_
		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。	0	0	0	0	_	_	_	_
		仮想パッチ	セキュリティパッチを早急に適用する事が難しい環境へ、暫定的なセキュリティを担保するためのソ リューションです。	0	0	0	0	_	-	-	-
	- 문	ファイアウォール機能	端末とネットワーク間の通信において、特定の種類のトラフィックを拒否または許可	0	0	0	0	-	-	-	-
セキュ		Webレピュテーション	フィッシング詐欺やウイルスが仕込まれたWebサイトなど、危険なサイトへのアクセスをブロック	0	0	0	0	0	0	0	0
リティ		URLフィルタリング	ング 業務上必要のないWebサイトへのアクセスを制御 C		0	0	0	0	-	-	0
微能		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。		0	0	0	-	-	-	-
		デバイスコントロール	USBメモリなどに対し、「コピー」「移動」「開く」「保存」「削除」「実行」などの操作を制御	0	0	0	0	0	-	-	_
		アプリケーション コントロール	カテゴリ、ペンダー、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。	0	0	0	0	_	-	-	-
		パスワード/パスコード	エンドボイントの画面をロックするためのパスワードを設定するよう、ユーザに通知がされます。また、パ スワードボリシー(文字数等)を指定することができます。	0	0	0	_	_	0	0	-
		クラウドサンドボックス	パターンファイルで検知困難な新種のウイルスをクラウド上の仮想環境で解析し、悪性なウイルスか判定		_	-	0	0	_	-	_
	侵入後	EDR機能	EDR機能(Endpoint Detection and Response)が端末内のファイル操作、プログラム実行 等様々な端末のログを監視し、不審な挙動を検知した場合、侵入経路や実行履歴、影響範囲を 管理画面に表示	0	_	_	0	0	_	_	_
	対処	遠隔端末隔離	感染を広げる可能性が高い感染端末を早期にネットワークから遮断	0	_	-	0	0	-	-	-
	-	インストールサポート	おまかせアンチウイルスエージェントのインストール支援	0	0	0	0	0	0	0	0
		設定代行	アンインストール禁止や、USB禁止など、WEB管理画面のセキュリティ設定を代行	0	0	-	0	0	0	0	0
		感染監視	端末にインストールされているおまかせアンチウイルスの検知状況や防御、隔離等の実行状況を監視	0	0	-	0	0	0	0	0
1	監視/	EDRログ分析	EDR機能を活用して、端末のログを分析し、ウイルスかどうかの判定および感染原因や影響範囲を 特定	0	-	-	0	0	-	-	-
7	ナ ポ ー	初動対応支援	感染の疑いがある場合は、管理者へ通知し、感染拡大防止のために端末のNW隔離や不審なプロ グラムの一時的ブロックを支援	0	-	-	0	0	_	-	_
	1.	対処復旧支援	万が一ウイルスに感染し支援が必要な場合には、管理者へ通知し、ウイルス駆除や対処を支援	0	0	_	0	0	0	0	0
			月に一度、ウイルス対策や挙動監視機能、URLフィルタリングなどの検知状況をまとめたレポートを提供	0	0	-	0	0	0	0	0
			月に一度、EDR機能の検知状況およびセキュリティ推奨設定をまとめたレポートを提供	0	-	-	0	0	_	-	_
基本機能 一元管理機能 ウイルスの検知状況や各端末のポリシー		一元管理機能	ウイルスの検知状況や各端末のポリシー設定をWEB管理画面にて一元管理	0	0	0	0	0	0	0	0

機能一覧

ご利用までの流れ

【STEP1】事前準備

既存でご利用中のウイルス対策ソフト及びMDMソフトをアンインストールする

<u>【STEP2】サービスへのログイン</u>

開通日に届くメールを準備します。

※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

2 パスワードを設定します。

3 管理者用URLをクリックし、ログイン画面を開きます。

4 アカウント名、手順2で設定したパスワードを入力し、ログインします。

【STEP3】エージェントツールのインストール ※利用者へメール通知する方法で記載

1 エージェントインストール用URLを利用者へ通知する。

2 エージェントをインストールする機器でURLをクリックし、インストーラをダウ ンロードする。

3 インストーラを実行し、インストールする。

【STEP4】 各種機能を設定する

既存でご利用中のウイルス対策ソフト及びMDMソフトのアンインストール

・ウイルス対策ソフトやMDMソフト(※1)が入っている場合、本サービスのインストールが行えない 場合があるため、事前にアンインストールをお願い致します。

※市販のウイルス対策ソフトは、本サービスインストール時に自動でアンインストールされますが、 失敗する事例もあるため、必ず手動でアンインストールを実施ください。

・アンインストール後は、必ず端末の再起動を実施下さい。

<u><Windows10の場合></u>

「スタートボタンを右クリック」 ⇒「アプリと機能」 ⇒「プログラムのアンインストール」

<Macの場合>

・App Store からインストールしたアプリを削除するには、まず Launchpad を開きます。

- ⇒ LaunchPad を起動後、どれか一つアプリを長押しします。
- ⇒ アプリの左上に × マークが表示されます。
- ⇒ 削除したいアプリの × マークをクリックします。

・App Store 以外からインストールしたアプリの場合、アンインストールプログラムが 用意されている場合は、そのプログラムをクリックしてアンインストールを実施。

※他社の法人向けウイルス対策サービスをご利用中の場合、 アンインストールを行う際にアンインストールパスワードを要求される場合がございます。 その場合は、アンインストールパスワードを確認の上、アンインストールを実施します。

(※1)MDMとは…

モバイルデバイスマネジメントの略。スマートフォンやタブレット端末を安全に利用するための 各種機能制限などを実施するサービスを指します。

サービスへのログイン

<u>おまかせアンチウイルスご利用いただくために必要なPWを設定し、おまかせ</u> アンチウイルスにログインします。

<u>件名: 【NTT東日本】おまかせアンチウイルス・サイバーみまもり・データレスPC・クラウド</u> アップセキュリティ新規アカウント発行のお知らせ_のメールを使います。



サービスへのログイン

<u>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</u> 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/



エージェントのインストールの流れ

<u>ウイルス対策を行いたい端末に対し、専用のエージェントのインストールが</u> <u>必要です。</u>



<u>次ページより、管理者作業および各OS毎のエージェントのインストー</u> ル方法を記載しております。

エージェントツールのインストール





エージェントツールのインストール

Г

利用者作業

0	サービスブラン名 💠	製品/サービス 💠	シート/ユニッ	ライセンス種 別	開始日 ♀	有効期 限	アクション
9	おまかせアンチウイルス ライト	ウイルスハ [®] スター ヒ [®] ジネスセキュリティサー ヒ [®] ス	5シート	製品版	2017/05/17	自動更 新	ご コンソールを 開く

しコンソールを用くから管理コンソールにいきます

¢	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▼	
0	おまかせアンチウイルス EDRブラス	I W orry-Free Co-Managed XDR for Endpoint (3 : ンボーネント)		1 シート	製品版	2024/02/07	自動更新	
	コンボーネント							
	Worry-Free Managed Detection and Response 👘							
	ウイルスパスター ビンプネスセキュリティ サービス EDR 👘							
	ウイルスハ'スター ビシ'ネスセキュリティサービス 👘	▶ コンソールを開く						

※「おまかせアンチウイルスEDRプラス」の場合は、▼ボタンを押下し、「コンソールを開く」をクリックします。

②セキュリティエージェントタブをクリックします ※一番上の「=」マークをクリックするとタブの名前を確認できます

≡	OU Tree Bu	usiness Security Services	G 11:05 UTC+09:00	0	*
ନ ମ	 サイズのセキュリティエージェンナ ・ ・ ・	すべてのセキュリティエージェント セキュリティエージェント: 5	CO27-92 - (88		Q Y Ø
2 9 9	 ▲ 手物グルーグ サーバ(和用設定) 0 デバイス(初用設定) き test 0 三 最新のパターンファイルを使用して… 0 三 ビジネスセキュリティサービスで管… 0 	+ セキュリティエージェントの通知 ● 州市 - 田 グローバル設定 田 タスク - ・ レドボイント ・ マ ・ マ ・ マ ・ マ ・ マ ・ マ ・ マ	BESR Windows Windows Windows Windows Windows Windows Windows		0
		③セキュリティエージェントの追加 をクリックします			

エージェントツールのインストール



○ セキュリティエージェント 耳	すべてのセキュリティエージェント	すべてのステータス • 検索 Q T ⑦
セキュリティエージェントのインストール方法		×
インストール方法の選択:		セキュリティエージェントの追加先: 初期設定 🔻 🕃
インストール用リンクの送信 「「 「 「 「 「 「 「 「 「 「 「 「 「	インストーラのダウンロード レレン グウンロード パワン パワン レン パワン パワン パワン パワン パワン パロ パロ	Rem >のfm とキュリティエーシェン/をこのエンドポイントにインストールします。 まつ ()管理者の端末にインストールす る場合は、コチラをクリリックします
メールコンテンツ - 次のリンクをクリックし、	<mark>コンテンツをコピ</mark> ー 手順に従ってセキュリティエージェ	QRコードのダウンロード ントをオートールしてくださ
UN₀ https://wfbs-svc-nabu trend id=yAlOzBu0g3PBwM-9gv 8SciMantIN_JV12TF: 412: IQF 1ZEImnv1FqG7PkTM30 Uw%I3D%5D&sto ∋=18.pso	tmicro.com/wfbs-svc/download/ia/vie vUXDBTOdw- sייוּרְקִיי(op _ˆT¨HEDrE´`guQDbXY0Y bnjTxL' /kM∿u5ייg9UJxAmUFQG'TVso cd: ∋vaL`\izc	w/activ ①テキストをコピーし、利用 者にメール送付します qw ⁻¹ 1K5
リンクの有効期限: 認証コード (iOS/Chromeb 認証コードの有効期限:	ook登録用):	- 9 al \' 2023年08月30日 15:13:05

エージェントツールのインストール

管理	者	作	業

【EDRプラスをご利用の場合】 Windowsエージェントは、EDR機能は自動で有効化されるため、有効化作業は不要となります EDRプラスを新規でご利用される場合は、下記手順に従い、アンチウイルスエージェントのインストール 作業を実施してください ※MacのEDR有効化は有効化作業が必要なため、後の「EDRエージェント有効化」を参照ください

1. Windowsコンピュータでブラウザを開き、管理者から周知されたインストール用のリンクを入力します。

2. 下のような画面が表示されたら、[ダウンロード]をクリックします。インストールプロセスが開始されたら[実行] をクリックして、インストールを進めます。

※ラベル情報の記入欄が表示された場合、指定の内容を記入します。

ひイルスバスタービジネスセキュリティサービス
ピジネスをキュリティクライアント の インストー ル
ラベル情報 単数 水 応義 ままれ * 佐藤 あ 2 やり * す デバイスラベル: デバイスラベル:
手順 下の「ダウンローF」をクリックして、インストールプロセスを開始します。 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((借存)をクリックしないでだたれい)。 ダウンロード 法義: 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。

- 3. インストールプロセスが開始されたら[実行]をクリックして、インストールを進めます。
- 4. 下の画面が表示されたら、[次へ]をクリックします。



エージェントツールのインストール

Windows

管理者作業	利用者作業
5. インストールが開始されます。	ウイルスパスタービジネスセキュリティサービス ー X
	セキュリティエーシェントのインストールフロクラムは、エーシェントをインストールしています。 確認しています…
	全体の進行状況: 16%完了
	次へ キャンセル

6. インストールが完了したら、[終了]をクリックして終了します。



7. タスクトレイ上に右記のようなアイコンが作成 されます。インストールは完了です。



エージェントツールのインストール

Windows



番号	機能		詳細
	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。
		\bigcirc	保護が有効
1		\bigotimes	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	<u>設定</u>		エージェントの各設定の表示および設定に使用されます。
4	<u>ユーザツール</u>	<u> </u>	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。
4	ユーザツール	<u> </u>	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。

エージェントツールのインストール



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



MAC

エージェントツールのインストール



エージェントツールのインストール



5. 標準インストール確認画面が表示されます。[インストール]をクリックします。

	🥪 Trend Micro Securityのインストール 🔒
	"Macintosh HD"に標準インストール
 はじめに インストール先 サーバに接続 インストールの種類 インストール 概要 大切な情報 	この操作には、コンピュータ上に95.7 MBの領域が必要です。 ディスク"Macintosh HD"にこのソフトウェアを標準インストールす るには、"インストール"をクリックしてください。
MICRO"	戻る インストール

6.「インストーラが新しいソフトウェアをインストールしようとしています。」と表示された場合は、名前(ご利用の Mac OSのユーザ名)とパスワードを入力し、[ソフトウェアをインストール]をクリックします。

インフトーラが新しいソフトウェアたインフトールしょうとしてい
ます。 許可するにはパスワードを入力してください。
 ユーザ名:
パスワード:
キャンセル ソフトウェアをインストール

エージェントツールのインストール



7. インストールが開始されます。画面が変わるまでお待ちください。

0 0 0	🥪 Trend Micro Securityのインストール
	Trend Micro Securityのインストール
 はじめに インストール先 サーパに接続 インストールの種類 インストール 概要 大切な情報 	パッケージスクリプトを実行中
	戻る「続ける

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



エージェントツールのインストール

管理者作業

Macエージェントのアイコン上に警告が表示される時の対処方法

利用者作業

概要

おまかせアンチウイルス Mac版エージェントのアイコン上に警告が表示されます。また、アイコンにマウスオーバーすると「セキュリティ権限が必要です」と表示されます。



詳細

おまかせアンチウイルス Mac版エージェントは動作にあたりいくつかの権限を必要とします。2020年10月24日の メンテナンスにおいて、必要な権限が足りない場合はUI上から確認できるようになりました。おまかせアンチウイル スに必要な権限が不足している場合、アイコン上に警告が表示されます。警告が表示された場合は以下の作業 を実施し、おまかせアンチウイルスに必要な権限を付与してください。

なお、おまかせアンチウイルスエージェントを新規にインストールした場合や、おまかせアンチウイルスエージェントが アップグレードされた場合には、下記の画面が表示されますので、その場合は [続行] をクリックし、次ページ以降 の「作業手順」 3.から作業を実施ください。

Trend Microセキュリティエージェント 編集	ウィンドウ ヘルプ	
	Trend Microセキュリティエージェント	
	and the second se	
	-	
,	X車な権限のセットアップ	
34	- Seater College Col	
Trend Microセキュリティエー	ジェントでコンピュータを保護するには、システム拡張機能、フルデ	
4277922, 8201-9	「エントノロクラムをロートする権限が必要です。	
[続行] をクリックし、画面に表 のコンピュータで棚けるように	{示される手順に従って、Trend Microセキュリティエージェントをこ 「指定してください」この処理は数分で完了します。	
	開じる	

エージェントツールのインストール



作業手順

- 1. Mac端末上の「アプリケーション」から「Trend Microセキュリティエージェント」を選択して開きます。
- 2. 「セキュリティ権限が必要」と表示されますので [詳細を表示] をクリックします。



エージェントツールのインストール





3. 「トレンドマイクロの証明書を許可」の画面で画面の指示にしたがって設定を行います。



3-1.「セキュリティとプライバシー」画面を開きます。

3-2. 「開発元"Trend Micro.Inc"のシステムソフトウェアの読み込みがブロックされました」と記載がある横の 「許可」ボタンをクリックします。複数の製品で承認が必要な場合、は許可ボタンをクリック後、署名元が表示され ます。「Trend Micro,Inc.」にチェックボックスを入れて許可を完了してください。なお、すでに許可済みの場合、 「Trend Micro,Inc.」は表示されませんので、その場合は本手順はスキップしてください。

3-3. [続行] をクリックします。

エージェントツールのインストール



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



- 4-1. [セキュリティとプライバシー]画面を開きます。 ※イメージ図は次ページ参照
- 4-2. [プライバシー]タブを開き、画面左下のカギマークをクリックしてロックを解除します。
- 4-3. 続いて、[フルディスクアクセス]を開いて[+]をクリックします。

4-4.「フルディスクアクセスを許可」の画面に戻り、4番の「ファイルの場所を開く」をクリックして表示された 「iCoreService」を[フルディスクアクセス]の一覧にドラッグアンドドロップします。

4-5. 「フルディスクアクセスを許可」の画面に戻り、5番の「ファイルの場所を開く」をクリックして表示された 「Trend Microセキュリティエージェント」を [フルディスクアクセス] の一覧にドラッグアンドドロップします。

※「iCoreService」につきましては、すでに追加されている場合でも、改めて4-4の手順をご実施ください。

※「Trend Microセキュリティエージェント」がすでに追加されている場合には、チェックが入っている事をご確認く ださい。もしチェックが入っていない場合には、チェックを入れてください。

※ macOS 11 Big Sur をご利用の場合は、「TrendMicro Antivirus Extension」についても追加とチェックが必要となります。

エージェントツールのインストール





4-6.「セキュリティとプライバシー」画面を閉じ、[続行]をクリックします。

一般 FileVau	alt ファイアウォール プライバシー)
 マイク 	下のアプリケーションに、このMacの ル、メッセージ、Safari、ホーム、Tir ップなどのデータや特定の管理設定へ	すべてのユーザのメー me Machineバックア のアクセスを許可。
 アクセシピリティ 入力監視 	CoreService	Extension
フルディスクアクセス ファイルとフォルダ	Trend Microセキュリテ	ィエージェント
	+ -	
HomeKit		
Bluetooth		

5. [OK] をクリックすると自動的にセキュリティエージェントが再起動されます。 再起動が完了したら必要な権限の付与設定は完了です。



管理者作業



【EDRプラスをご利用の場合】

Macについては、既におまかせアンチウイルスをインストール済みのお客様もEDRエージェントの有効化 作業が必要となりますので、以下手順を参考に実施をお願いいたします。

1. 以下セットアップ画面において、「Continue」をクリックします

※「Close」を押下して表示されていない状況であれば、XDRアプリ「ン」のアイコンをクリックすることで再度権限セットアップ画面の再表示が可能です。

••	Trend Micro Permissions
Set	
Set	op Required Permissions
Endpoint sensor requires that you allo Access in order to monitor your comp	w the Trend Micro Certificate, System Extension, and Full Disk uter.
Click "Continue" and follow the on-sci It only takes a few minutes.	reen instructions to allow endpoint sensor to monitor this computer.
	Close

2. 以下画面が表示された場合は、「システム設定を開く」をクリックします。







3. 「Allow System Extension」画面において、「Open Security & Privacy」をクリックします

• • 0	Trend Micro Permissions	
Required Permissions System Extension Full Disk Access	Allow System Extension In order to enable endpoint sensor monitoring on your computer, Security & Privacy.	sion you must allow the System Extension in
	 Open Security & Privacy Click the lock icon in the bottom left corner and provide your macOS administrator password to make changes. Click "Details" in Security & Privacy. 	©
	 Select all "iCore Security" options in the list and click "OK". 	
	5. Click "Allow".	
		Close

4. 「セキュリティとプライバシー」画面において、「詳細...」をクリックします。







5. 以下画面において、ユーザ名、パスワードを入力し、「設定を変更」をクリックします。

プライバシーとセキュリティ
プライバシーとセキュリティがシステム設定を 変更しようとしています。
許可するにはパスワードを入力してください。
Omakase Mac
パスワード
キャンセル 設定を変更

6. 以下画面において、iCoreサービスを全て選択し、OKをクリックします

以下の開発元のシステムソフトウェアがアップデートされました。使用する 前にシステムを再起動する必要があります。

iCore Security		
iCore Security		
	キャンセル	OK

7. 以下画面において、許可をクリックします





利用者作業

8. 「Allow System Extension」の設定が完了したので、「Continue」をクリックします。



9. 「Allow Full Disk Access」画面にて、「Open Security & Privacy」をクリックします。



管理者作業

利用者作業

10. 「フルディスクアクセス」を確認します。

•••	く 〉 フルディスクアクセス
Q 検索	下のアプリケーションに、このMacのすべてのユーザのメール、メッセージ、
Q #1212	Safari、ホーム、Time Machineハックアックなどのテータや特定の管理設定へのアクセスを許可。
	Appicon
Wi-Fi	EndpointBasecamp
8 Bluetooth	
💮 ネットワーク	🧕 iCore Service
通知	smbd 💽
動 サウンド	C Trend Micro Extension
() 集中モード	
スクリーンタイム	Trend Micro Extension (XDR)
<u>⊙</u> -₩	X Trend Micro XDR Endpoint Sensor
◎ 外観	Trend Microセキュリティエージェント
⑦ アクセシビリティ	+ -
🔡 コントロールセンター	

11. 「Allow Full Disk Access」画面にて、「4.Open File Location」をクリックします。



管理者作業



12. 「フルディスクアクセス」を選択し、「com.trendmicro.icore.es.systemextension」をフルディスクアク セスの一覧にドラッグアンドドロップします。ドロップする該当アイコンがONに変わります。

_	Safari、ホーム、Time Machine バック		< >	04169D7E-9EAD-4C47-95D	88	:= п		
Apple IDでサインイン	のアクセスを計り。	よく使う項目	名前		変更日		サイズ	0
😞 Wi-Fi	Appicon	MirDrop	🔹 🔍 com.tr	endmicro.icore.es.sa.systemextension	20234	E11月21日 1	6:14	
8 Bluetooth	EndpointBasecamp	 ② 最近の項目 ▲ アプリグ… 						
	🧕 iCore Service	📮 デスクト…						
3 通知	📰 smbd	 ・・・ ・・・ ・・・						
 ・ ・ ・	Trend Micro Extension	場所 → Macintos						
ス スクリーンタイム	Trend Micro Extension (XDR)	@ ネットワ…						
• 一般	Trend Micro XDR Endpoint Ser	タグ ● レッド						
● 外観	🕗 Trend Micro セキュリティエージ	● オレンジ						
⑦ アクセシビリティ		-DIT -				2		

13. 「Allow Full Disk Access」画面にて、「5.Open File Location」をクリックします。



管理者作業



14. 「フルディスクアクセス」を選択し、「iCore Security」をフルディスクアクセスの一覧にドラッグアンドドロップ します。ドロップする該当アイコンがONに変わります。

	く 〉 フルディスクアクセス	•••	< > Resources	88 (Ⅲ) Ⅲ
Q 検索	下のアプリケーションに、このMac	よく使う項目	名前	へ 変更日
	Safari、ホーム、Time Machineパ	(AirDrop	X Applcon.icns	2023年11月21日 16
● サインイン	のアクセスを許可。	● 最近の項目	Assets.car	2023年11月21日 16
Apple ID でサインイン		▲ アプリケ…	> 🚞 Base.lproj	2023年11月21日 16
	Applcon		> Contra	2023年11月21日 16
🛜 Wi-Fi		ニ デスクト…	, 🚽 🙋 iCore Security.app	今日 17:59
	EndpointBasecamp	▶書類	InfoPlist.strings	2023年11月21日 16
Bluetooth	-	▲ 村内2000000000000000000000000000000000000	> 🚞 ja.lproj	2023年11月21日 16
🐵 ネットワーク	🧕 iCore Service	場所	XDR_for_Mac_Licenses.rtf	2023年11月21日 16
🚨 通知	📕 smbd	🖂 Macintos		
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Trend Micro Extension			
スクリーンタイム	Trend Micro Extension (XDI	● レッド		
 	Trend Micro XDR Endpoint	● オレンジ ● イエロー		
◎ 外観	Irend Microセキュリティエー	ジェント		
 ⑦ アクセシビリティ ③ コントロールセンター 	(+			

15. 「Allow Full Disk Access」画面にて、「6.Open File Location」をクリックします。

	Trend Micro Permissions
Required Permissions	Allow Full Disk Access
System Extension	In order to enable endpoint sensor monitoring on your computer, you must allow Full Disk Access in
Full Disk Access	Security & Privacy.
	1. Open Security & Privacy
	2. Select "Full Disk Access" from the list of services.
	3. Click the lock icon in the bottom left corner and provide your macOS administrator password to make changes.
	4. Open File Location
	Locate the "com.trendmicro.icore.es.systemextension" file and drag and drop the file into the Full Disk Access table.
	5. Open File Location
	Locate "iCore Security" and drag and drop the app into the Full Disk Access table.
	6. Open File Location Locate "Trend Micro XDR Endpoint Sensor" and drag and drop the app into the Full Disk Access table.
	7. Make sure the following apps are selected: • Trend Micro Extension (XDR) • iCore Security • Trend Micro XDR Endpoint Sensor Close

管理者作業



16. 「フルディスクアクセス」を選択し、「Trend Micro XDR Endpoint Sensor」をフルディスクアクセスの一覧にドラッグアンドドロップします。ドロップする該当アイコンがONに変わります。

•••	く 〉 フルディスクアクセス		< > アプリケーション	88 ≔ 00
Q. 検索	下のアプリケーションに、このMacのすべてのユーザ	よく使う項目	名前	変更日
● サインイン	Safari、ホーム、Time Machine バックアップなどのテ のアクセスを許可。	AirDrop	X Trend Micro XDR Endpoint Sensor.app	今日 17:59
Apple ID でサインイン	Andrean	 最近の項目 	Trend Microセキュリティエージェント.app	今日 17:18
Mi-Ei	Appicon	▲ アプリケ…	Ø Safari.app	今日 2:02
Wi-Fi	EndpointBasecamp	-	Google Chrome.app	一昨日 7:35
Bluetooth		□ デスクト…	🛃 App Store.app	2020年1月1日 17:00
💮 ネットワーク	🧕 iCore Service	▶ 書類	🚰 Automator.app	2020年1月1日 17:00
	🖬 smbd 🔺	O Mary In	FaceTime.app	2020年1月1日 17:00
🦲 通知		() ダウンロ…	Font Book.app	2020年1月1日 17:00
● サウンド	Trend Micro Extension	48.15	🔛 Launchpad.app	2020年1月1日 17:00
(集由王 15		C Mariatas	Mission Control.app	2020年1月1日 17:00
	Trend Miner Extension (VDD)	A Macintos	🚱 Photo Booth.app	2020年1月1日 17:00
X スクリーンタイム	Irend Micro Extension (XDR)	@ ネットワ…	Podcast.app	2020年1月1日 17:00
D n	Yrend Micro XDR Endpoint Sensor		QuickTime Player.app	2020年1月1日 17:00
		97	🛃 Siri.app	2020年1月1日 17:00
◎ 外観	Irrend Micro セキュリティエージェント	● レッド	Time Machine.app	2020年1月1日 17:00
⑦ アクセシビリティ		● オレンジ	TV.app	2020年1月1日 17:00
コントロールセンター	+ -		😭 イメージキャプチャ.app	2020年1月1日 17:00

17. 以下画面が表示された場合、「あとで行う」をクリックします。



18. 以下画面にて、「OK」をクリックします。

※OSバージョン10.15では、端末再起動が必要です

※17で[終了して再度開く]をクリックした場合は、こちらの画面は表示されませんが、設定作業は正常に完了しています







以上で、MacEDRの有効化作業は完了となります。

インストール完了しますと、以下赤枠のアイコン(おまかせアンチウイルス)をクリックすると「Endpoint Sensor」のステータスが、緑(有効化)になっております


(Macのみ) EDRのアンインストール





Mac版のEDRエージェントアンインストール作業については、専用のアンイン ストールツールが必要となりますので、NTT東日本セキュリティサポートデスク までご連絡ください。

※管理コンソールの「ツール」よりダウンロード可能なアンインストーラ(WFBS-SVC_Agent_Uninstaller.app.zip)は使用しないでください。実行した場合、おま かせアンチウイルスエージェントのみアンインストールされEDRエージェントが残ってしまいま す。

エージェントのインストール





1.Androidデバイスからインストール用のリンクにアクセスします。

2.下記のような画面が表示されたら、[インストール]をタップし、インストールを開始します。



3.インストールが開始されたら「インストール中...」が表示されます。



4.インストールが完了したら開くをタップします。



エージェントのインストール



利用者作業

5.メールアドレスを入力してサインインします



6.デバイス管理機能を有効にするか選択する画面で「続行」をタップします。



エージェントのインストール

管理者作業

利用者作業

7.端末管理アプリの有効化を行います。



10:56 🔳 🖪 🕑 💼 🔸
端末管理アプリの有効化
Mobile Security
この管理アプリを有効にすると、アプリ(Mobile Security)に次の操作を許可することになります:
すべてのデータを消去 警告せずにデータの初期化を実行してタブレット内のデータ を消去します。
画面ロックの変更 両面ロックを変更します。
パスワードルールの設定 両面ロックのパスワードとPINの長さと使用できる文字を制御 します。
画面ロック解除試行の監視 画面のロック解除に正しくないパスワードを入力した回数を 監視し、回数が多すぎる粘合はタブレットをロックするかタ ブレットのデータをすべて消去します。
画面のロック 両面をロックする方法とタイミングを制御します。
画面ロックのパスワード有効期限の設定 画面ロックのバスワード、PIN、パターンの変更が必要になる 頻度を変更します。
ストレージ暗号化の設定 保存したアプリデータが暗号化されるようにします。
カメラを無効にする すべての端末カメラを使用できないようにします。
この端末管理アプリを有効にする
キャンセル
アプリをアンインストール

8.位置情報へのアクセスを許可します。





エージェントのインストール





9.電話の発信と管理を許可します。





10.バックグラウンドでの実行を許可します。





エージェントのインストール





11.「通知へのアクセス」画面でスイッチを切り替え、設定を有効化します。

10:56 🖪 🖪 🖸 🖿 🔸	10:56	. • • • • • • • • • • • • • • • • • • •		10:57	■ ¤ (> ■ ·	
← 設定が必要です	通知	へのアクセス		通知	へのアクセス	
.	*	Google Play開発者サービス Chromebook	۲	*	Google Play開発者サービス Chromebook	۰
通知へのアクセス	D	Mobile Security			Mobile Security	
5/7						
Mobile Securityのシステム道知にアウセスするには権限が必要です					Mobile Securityでの通知への7 しますか? Mobile Security はすべての選知を できます。通知には、連続そないには、連続そなな 愛信したメッセージの本文を含ま、 通知を非素不にしたり、通りのの 行したりすることもできます。 これにより、アフリがマナーモー えたり、開連する波定を変更した 能になります。	ククセスを許可 読み取ることが どの個人情報や れます。また、 ポタン操作を実 ド設定を切り替 りすることも可 可しない 許可
許可						

12.「他のアプリのうえに重ねて表示」画面でスイッチを切り替え、設定を有効化します。



エージェントのインストール



10:57 🖪 🖪 🕞 💼 🔸

利用者作業

13.ユーザー補助を許可します。



<u>д-</u> -	ザー補助	
	音量 キーのショートカット サービスが選択されていません	
	ダウンロード済みサービス	
Þ	Mobile Security OFF / ユーザー補助で権限を設定してください	
	スクリーン リーダー テキスト読み上げの出力	
	表示 フォントサイズ デフォルト	
	表示サイズ デフォルト	
0	拡大 OFF	
	大きなマウスポインタ	
	アニメーションの削除	
	操作のコントロール	
	停止時間	



14.Mobile Securityの利用を開始します。

Solid Security Mobile Security ウービスの使用 ● ● の参考を使用するにはコーザー補助での相助設により、ブ タウザタメロージアンリンコーザー補助での相助設により、ブ タウザタメロージアンリからの加減額の取得、URLとさ オウザタメロージアンリからの加減額の取得、URLとさ オウザタメロージアンリからの加減額の取得のないますのない ができます。 ● ● ● Mobile Securityを Mobile Securityを利用しますか? ●	Mobile Security ケービスの使用 ・ のの爆を受加するにはコーゲー構築定定でMobile Securityに 相応と立ってつきが、コーゲー構築定でMobile Securityに かの進たション・ユーゲー構築での機構設定により、プ ラブサキンタセージアブリからの回転電気では、 いたいとユーゲー かってスクを見まるの、のないの、 かってスクを見まるの、のないの、 かってスクを見まるの、のないの、 のの描述をついては、 いたいの、 かってスクを見まるの、のないの、 のの描述をついては、 、 からしてスク・ション・ユーゲー 本のないの、 、 ののたいの、 たってスク・ のの描述 ののの思えの ののでは、 いたいの のの描述 ののの思えの ののでは、 いたいの ののでは、 いたいの ののでは、 いたいの ののでは、 いたいの ののでは、 いたいの ののでは、 いたいの ののでは、 いたいの のので、 ののでは、 いたいの のので、 ののでは、 いたいの のので、 ののでの のので、 ののでの のので、 ののでの ののでの のので、 ののでの ののでの ののでの のので、 ののでの のので、 ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの のので ののので のので のので のので のので のので のので ののので のので のので のので ののので のので ののので のので ののので ののので のので のので のので のので のので ののので のので のので のので のので のので のので のので ののので ののので のので のので ののので のので	Mobile Security ケービスの使用 ・ の、物理の医学する必要がありましたはニーザー検知度定により、プ ウブサグスタモージアブリからのURL開始の発行、URLにどっ ウナウシタンクモージアブリからのURL開始の発行、URLにどっ ウナウシタンクモージアブリからのURL開始の発行、URLにどっ ウナウシタンクモージアブリからのURL開始の発行、URLにどっ ウナウシタンクモージアブリからのURL開始の発行、URLにどっ ウナウキンクをモージアブリからのURL開始の発行、URLにどっ ウナウキンクをモージアブリからのURL開始の発行、URLにどっ ウナウキンクをモージアブリたらのURL開始の発行、 かービングアクキュンスーザー検知度のURL的の クラウキングを使いていたいたい かービングアクキュンスーザー検知度のURL的の ローザーがアグロスしているとさいたい シービングワクキュンスにいるとさいたい ウォントクロンクテンツの取得 コーザーがアグロスしているとさいたい マキャンセル	Mobile Security かービスの使用 の の の の の の の の からしたコターション・ユーゲー構成での構成などにより、 かっサンタンをモージアブリル市のロルに構成な時、URLレビュ かっサンタンをモージアブリル市のロルに構成な時、URLレビュ かっサンタンをモージアブリル市のロルに構成な時、URLレビュ かっサンタンをモージアブリル市のロルに構成な時、URLレビュ かっサンタンをモージアブリル市のロルに構成な時、URLレビュ かっサンシンターディング かったコックをなせるののの の の の の たっションの の たっションの の たっションの の たっションの の たっ の たっ の たっ の たっ たっ の たっ たっ たっ たっ たっ たっ たっ たっ たっ たっ	
	 サービスの使用 ふの強化を使用するにはユーサー補助告定でMobile Securityに 権限を設定する必要があります。 Webレビュテーンコンコーザー構成での構成法になり、 プランタンクチェック、プログロの加圧局での構成に応じた アーションのチェック、安全でないURLのプロックを行うこと ができます。 Mobile Securityでは以下が必要です。 Mobile Securityでは以下が必要です。 Mobile Securityでは以下が必要です。 Mobile Securityでは以下が必要です。 Mobile Securityでなってはいるとさに 気が取っているす。 ウインドウコンテンシの原理 コーデーがアンをとしてものなったのの原理 マーデーがアンをといるのようにものなったのの原理 マーデーがアンをといるインドのコン フを経過します。 	 ウービスの使用 への感感を受用するにはユーザー構築設定であるきまなります。 () への感感を受用するにはユーザー構築の構成を定します。 () への感感を受用するにはユーザー構築の構成を定します。 () への感感を受用するにはユーザー構築の構成を定つます。 () への感感を受用するによーザー構築の構成を定つます。 () への感感を受用するによーザー構築の構成を定つます。 () への感感を受用するによーザー構築の構成を定つます。 () への感感を受用することが、の意味を受用することが、の意味を受用することが、の意味を受用することが、の意味を受用することが、 () への感感を受用することが、の意味を受用することが、 () への感感を受用することが、 () への感じたいのすることが、 () へのしたいのすることが、 () へのしたいのするこか。 	 ウービスの使用 への強振を受用するにはユーサーは認識定であめ始らescurityに 能と認定するおきがあります。 いたビュテーションコーザー通知での相互応により、ブ やテレタンのチェック、日本のでも「地域」のプロックを行うこと かできます。 のの構成を受用するにはユーサーは認知ではない かっしょうから、マクマンパンらつは見知のプロックを行うこと かできます。 のの構成を受用するにはユーサーは認知でない たいの見知ののでした。 小さいの見れい、「ローサー」にはなったいの のたいのようがあります。 いたビュテーションコーザーは知道ではない かっしまったのです。 のの構成を受用するにはユーサーは認知でない のたいのようがあります。 いたビュテーシンコンコーザーは認知でない のたいのようがあります。 いたビュテーシンコンコーザーは認知でない のためます。 いたビュテーシンコーデーン のではないためます。 いたビュテーシンコーデーン のでないためまうます。 いたビュテーシン のためます。 いたビュテーション のためます。 いたビュテーシン のためます。 いたビュテーション のためます。 いたビュテーション のためます。 いたビュテーシン のたます。 いたビュテーション のためます。 いたビュテーシン のためます。 いたビュテーシン のためます。 いたビュテーション のためます。 いたビュテーシン のためます。 いたビュテーシン のためます。 いたビュテーシン のためます。 いたビュテーシン のためます。 いたビュテーシン のためます。 いたビュテーシン のためます。 いたビュテーシン のためます。 <	bile Security
 文の優先を使用するにはユーザー補助設定でMobile Securityに 相応を設定する必要があります。 Webビビュテーションユーザー補助での相関設定により、ブ ラウザマネットビップブリからのUNL構成の原用。UNLビュ テーションのチェック、要定でないUNLのブロックを行うこと かできます。 Mobile Securityでは以下が必要です。 操作の監視 コーザーがプクセスしているとさに 思知のます。 ウインドウコンテクションの取得 コーザーがプクセスしているとさに 思知のます。 	 ⑦ 次の構成を空用するにはユーサー補助設定でMobile Securityに 権限を設定する必要があります。 ⑦ 次の構成を空用するにはユーサー補助設定でMobile ランサキメッセージアブリカシロロ価格の政策、URLUビュ ティションのチェック、安全でないURLのブロックを行うこと ができます。 ⑦ 次の構成を空用するにはユーサー補助定でMath 別グロサインセージアブリカンロロ価格の政策、 のなしてエーシュンユーサー補助での構成 フリサインセージアブリカンロロ価格の政策、 デーションのチェック、安全でないURLのブロックを行うこと ⑦ 次の構成を空用するにはユーサー補助定でMath 別グロサインセージアブリカンロロ価格の政策、 のかしたエテーションユーサー補助定でMath 別グロサインセージアブリカンロロ価格の政策、 のかしたエテーションコーサー構成での構成 アーションのチェック、安全でないURLのブロックを行うこと ⑦ 次の構成を空用するにはコーサー補助定でMath 別グロサインセージアブリカンロロ価格の政策、 のかしたエクションコーサー構成での構成 フロサンクをついて構成での構成 の構成での構成での構成ではない、 のかしたエクランジョンコーサー構成での構成での構成ではない、 のかしたエクションコーサー構成での構成での構成での構成での構成 のないため、 のかしたエクションコーサー構成での構成での構成での構成での構成 のかしたコーサー構成での構成での構成での構成での構成での構成での構成での構成での構成での構成での	 ⑦ 次の機能を空閉するにはユーザー構築設定でModels Securityに 構想を認定する必要があります。 ⑦ 次の機能を空閉するにはユーザー構築設定でModels Securityに 指導を認定する必要があります。 ⑦ 次の構成で空間するにはユーザー構築設定でModels Security かできます。 ⑦ 次の構成で空間するにはユーザー構築設定でModels Security かできます。 ⑦ 次の構成で空間するにはユーザー構築設定でModels Security かられるのない場合の知識にあります。 ⑦ 次の構成で空間するにはユーザー構築設定でModels Security かられるのない場合の知識にあります。 ⑦ 次の構成で見ずするがあります。 ※ からないのまかのための見たのの構成の空間 かられるのない場合の知識にあります。 ※ のためのための見たの知識にあります。 ※ Models Securityを利用しますか? Models Securityを利用しますか? Models Securityでお以下から要です。 ※ 当たのでガロントのもついたのよう。 ※ ついたのための見 ついたのでないたいもうくンドのついたのです。 ※ ないためのないは、 ※ ないないは、 ※ ないは、 ※ ないは、 ※ ないないは、 ※ ないないは、 ※ ないないは、 ※ ないないないないないないないないないないないないないないないないないないない	 ① かの無度を切用するにはユーザー補助設定でModele Securityに 相比を設定するが差からすよ。 ① かの無度を切用するにはユーザー補助定でModele Securityに かつザウメウォークエブリからの加入場合の時間応じた。 ① かの無定を切用するにはユーザー補助定でModele Securityにより、 プロウォックのチェク、安全でない回応クロックを行うこと かできます。 ② かの用意を切用しますか? Modele Securityを利用しますか? Modele Securityを利用しますか? Modele Securityを利用しますか? Modele Securityでを利用しますか? Modele Securityでありましているときに構成のます。 ○ サインドウアンパンワクの見得 コーサーがアクセスしているときに構成のまた。 ○ サインドウアセスしているときに構成でいる のす。 ○ サインドウアングのの取得 ○ サインドウアングの取得 ○ サインドウアングングの取得 ○ サインドウアングングの取得 ○ サインドウアングングのない ○ サインドウアングングの取得 ○ サインドウアングングの取得 ○ サインドウアングングングの取り ○ サインドウアングンしているショング・ 	サービスの使用 🕘
Nable ビュア・ションコーゲー構成での構成を定える。ブ ラブゲッシャン・シラブリからの加速層の意味、UNLビュ テーションのチェック、安全でないUNLのブロックを行うこと ができます。 Mobile Securityを利用しますか? Mobile Securityを利用しますか? Mobile Securityでは以下が必要です。 ・ 場合の監視 コーレージブリックの文字のの表示。 のインドクロンテンツの取得 コーレージブリックでないしているウィンドののコ ッを抽点します。	Webレビュテーションコーリー語でで周期短度により、プ うテレシンジテェック、安全でないURLのクロックを行うこと ができます。	Webレビュアーション:ユーザー構成での情報認定になり、プ ウサヴメッセージアブリからOURL簡単の構築、URLレビュ かできます。	Webレビュアーションユーザー構成での視測定数により、ブ ウウサウネッセージアブリがらのUTL構成の意味、UTLレビュ かできます。 Mebレビュアーションユーザー構成での視測定数 かできます。 Mebレビュアーションユーザー構成での視測定数 かつサウネック、空空でないMARのクロックを行うこと かできます。 Mebレビュアーションユーザー構成での視測定数 クロックスタークアブリでクローズの のために見ていた。 のためです。 のために見ていた。 のために見ていた。 のためです。 のためです。 のために見ていた。 のためです。 のためです。 のためです。 のために見ていた。 のためです。 のためです。 のためです。 のために見ていた。 のためです。 のためです。 のためです。 のためです。 のためです。 のためでは、 のためです。 のためです。 のためでは、 のためです。 のためです。 のためでは、 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためでは、 のためです。 のたのです。 のためです。 のためです。 のたのです。 のためです。 のためです。 のためです。 のためです。 のためです。 のためです。 のたのです。 のためです。 のためです。 のためです。 のたのです。 のためです。 のためです。 のたのです。 のためです。 のためです。 のためです。 のためです。 のたのです。 のためです。 のためです。 のためです。 のたのです。 のためです。 のたのです。 のためです。 のたのです。 のためです。 のたのです。 のたのです。 のためです。 のたのです。 のたのです。 のためです。 のためです。 のたのです。 のためです。 のたのです。 のためです。 のためです。 のためです。 のたのです。 のたのです。 のたのです。 のたのです。 のためです。 のたのです。 のたのです。 のたのです。 のたのでのです。 のたのです。 のためです。 のたのです。 のたのです。 のたのです。 のたるです。 のたのです。 のたのです。 のたるです。 のたのでのです。 のたのです。 のたのです。 のたのです。 のたのです。 のたのでででのです。 のたのでででする のたのです のたのです。 のたのでする のたのでです のたのででのです。	次の機能を使用するにはユーザー補助設定でMobile Securityに 権限を設定する必要があります。
Mobile Securityを利用しますか? Mobile Securityでは以下が必要です。 ·	Mobile Securityを利用しますか? Mobile Securityでは以下が必要です。 通信の監視 コーケーガブリでアクセスしているとさに違うが知ります。 ウィンドウコンテンツの取得 コーケーガアクセスしているウィンドウロコン フを検査します。 キャンセル	 Mobile Securityを利用しますか? Mobile Securityでは以下が必要です。 操作の監視 ユーサ・ガアプリでアクセスしているときに違い知ります。 ウィンドウコンテンツの取得 ユーサ・ガアクセスしているウィンドクのコン シモ検査します。 	 Mobile Securityを利用しますか? Mobile Securityでは以下が必要です。 操作の監視 ユーザーがアプリでアウセスしているときに選 に対応する。 ヴィンドウコンテンツの取得 ユーザーがアクセスしているやインドウロコン マを検査します。 	Webレビュテーション: ユーザー補助での権限設定により、ブ ラウザやメッセージアプリからのURL情報の取得、URLレビュ テーションのチェック、安全でないURLのプロックを行うこと ができます。
Mobile Securityでは以下が必要です。 ・ 操作の監視 コーローガングでアクセスしているときに 安け取ります。 ・ ウィンドウコンテンツの取得 コーサーガングセスしているウィンドウロコ ッモ転金します。	Mobile Securityでは以下が必要です。 ・ 操作の監視 ユーサーがプリでアクセスしているときに当 安元初します。 ・ ウインドウコンテンツの取得 ユーサーがアクセスしているウインドウロコン フを検査します。 キャンセル	Mobile Securityでは以下が必要です。 ・ 操作の監視 ユーサンボアガルでアクセスしているときに当 ポポルマ・ボアウコンテンツの取得 ユーサーボアクセスしているウィンドクのコン 少を検査します。 キャンセル	Mobile Securityでは以下が必要です。 ・ 操作の監視 ユーサーがアプリでアクセスしているときに選 受け取ります。 ・ ウィンドウコンテンツの取得 ユーサーがアクセスしているウィンドウロコン ッを検査します。 キャンセル	
 操作の監視 ユーザーガアプリでアクセスしているときに 受け取ります。 ウィンドウコンテンツの取得 ユーザーがアクセスしているウィンドクのコ ツを検査します。 	 操作の監視 ユーサーがアプリでアクセスしているときに当 実は取ります。 ウインドウコンテンツの取得 ユーサーがアクセスしているウィンドウのコン ツを授立します。 	 操作の監視 ユーサーがアプリでアクセスしているときにま 気が取りま. ウィンドウコンテンツの取得 ユーサーがアクセスしているウィンドウのコン ツを秋直します。 	 操作の監視 ユーサーがアプリでアクセスしているときに選 式切ります。 ウインドウコンテンツの取得 ユーサーがアウマスしているウィンドウロコン ツを検査します。 	
・ ウィンドウコンテンツの取得 ユーザーがアクセスしているウィンドクのコ ツを検査します。	・ ウィンドウコンテンツの取得 ユーザーがアクセスしているウィンドウロコン ツを検査します。 キャンセル	・ ウィンドウコンテンツの取得 コーマードアクセスしているウィンドウのコ ッを検査します。 キャンセル	・ ウィンドウコンテンツの取得 コーサージアなしているウィンドウのコン ツを検査します。 キャンセル	
	+v>t/	**>±n	+*>t/	
キャンセル				

エージェントのインストール





15. デバイスの登録が開始され、登録完了後に下記の画面が表示されたら登録は完了です。



16.Androidデバイス内に下記ようなアイコンが作成されます。



エージェントツールのインストール



はじめにお読みください

- Apple社のサイトへアクセスする際には、必ずSafariまたはGoogle Chromeでアクセスしてください。
- iPadOS/iOSモバイルデバイスを登録する際に、管理者はAPNs証明書を作成する必要があります。
 ※1つの管理コンソール画面につき1つの証明書が必要です。
 ※ご利用端末数分の証明書は必要ありません。
- APNs証明書を作成するには、Apple IDが必要です。更新時には、 作成時に使用したApple IDを紛失すると、各デバイスへ再インス トールとなります。使用したApple IDは必ず保管しておいてください。
- iPadOS/iOSデバイスへは「Trend Micro Worry Free Business Security Service」がプロファイルとしてインストールされ ます。
- iOS,iPadOS端末ヘインストールする場合には、Web管理コンソー ルを利用するためのWindows/Mac端末が別途必要です。

エージェントツールのインストール

iOS

管理者作業		利用	者作業
=バイルデバイス登録	≡	TREND Worry F	Free" Business Security Services
	の 「1 と 圏	管理 - 厳設定 モリバイルデバイスを接設定 通知 Active Directoryの設定	 モバイルデバイス登録設定 Apple Push Notification Service証明書 iOSデバイスの管理には、有効なAPNs (Apple Push Notification service) 証明書が必要で キュリティサービスWebコンノールにアップロートしてください。 APNs証明書のアップロード AndroidあよびHOSデバイス向けの使用許諾交換す書
		Trend Micro Remote Manager Smart Protection Network 回復キーのパスワード ツール	トレンドマイクロでは、使用許諾茲の違をテンプレートとして提供しており、お客様の会社に合 ライアントのインストール中に表示されます。エンドユーザは、ビジネスセキュリティクライアン 送信 カスタマイズ

管理	く モバイルデバイス変精設定
一般設定 モバイルデバイス登録設定	新しいApple Push Notification Service証明書 手順1. Trend Micro Certificate Signing Request (CSR)をダウンロードします
通知	Trend Micro CSR0/ゲンロード
Active Directoryの設定	手順2. Apple Push Notification Service証明書を作成します
Trend Micro Remote Manager	1. Apple Push Certificate Portal (https://identity.apple.com/pushcert)にアクセスし、Apple IDでサインインします。③
Smart Protection Network	2. 証明書を作成します。をクリックします。
	3. 署名深みのCSR (CSR_signed_by_TrendMicro.b64)をアップロードして、APNs証明書を作成します。
回復キーのバスワード	4. Apple Push Certificates Portalから設用書をダウンロードします。
シール	手順3. Apple Push Notification Service証明書をアップロードします
ライセンス情報	証明書を作成するために使用したApple Idを指定して、証明書 (MDM_Trend Micro Incorporated (Ent)_Certificate.pem) をアッ
Webコンソール設定	Apple ID:
	1005 90 10 0 10 0 10 0 10 0 10 0 10 0 10

≡	🕖 TREND Worry F	ree" Business Security Services
ର	管理	< モバイルデバイス登録設定
S	一般設定	新しいApple Push Notification Service証明書 手順1. Trend Micro Certificate Signing Request (CSR)をダウンロードします
8	モハイルテハイス量数加支上	Trend Micro CSRのダウンロード
	Active Directoryの設定	手順2. Apple Push Notification Service識明書を作成します
	Trend Micro Remote Manager Smart Protection Network	 Apple Push Certificate Portal (https://dentity.apple.com/pushceri)にアクセスし、Apple IDでサイン 諸明書を作成します。をクリックします。 第一次の中の「パタロー」を行ったります。
٢	回復キーのバスワード	 A Explosition (con_angine_up_rendminicture) シックロードします。 A Apple Push Certificates Portativら証明書をダウンロードします。

1.「管理」タブを開き、「モバイルデバイス登録 設定」をクリックします。

2. [APNs証明書のアップロード]ボタンをクリックします。

3. [Trend Micro CSRのダウンロード]をクリッ クし、Trend Micro CSR (Certificate Signing Request) をダウンロードします。

4. Apple Push Certificate Portalサイトへ アクセスます。(SafariまたはGoogle Chrome を使用してアクセスしてください。その他のブラウザ の場合、表示が崩れたり正しい証明書が作成で きないことがあります。)

Apple Push Certificate Portal https://identity.apple.com/pushcert/

エージェントツールのインストール

iOS

管理者作業	利用者作業	

5. エージェントをインストールする端末で利用しているAppleIDを入力してサインインします。

•	Mac	iPad	Phone	Watch	Music	Support
Арр	le Push	Certifica	ates Porta	al		
	Sign In.					
8	Forgot your Apple	e 10?				
	Forgot your pass	word?				O)B
			Sig	jn In		12 All

指定したAppleIDで2ファクタ認証を有効として いる場合、右の画面が表示されます。 信頼されたデバイスで取得した確認コードを入力 し、[Continue]ボタンをクリックします。

y your identity. ople ID is protected with two-factor authentication. Enter tion code shown on your other devices.
Verification Code:
Don't have access to trusted devices?

- < 確認コードの取得方法 (iOS 10.3 以降) >
 - 1. 信頼されたデバイスで[設定]を開き、 ユーザ名をタップします。

10.4h	Apple 10
設定	0
A second readers	
6	6.8. 12289. X-6
	パスワードとセキュリティ
💙 W-R	85-V-28-88
Burtoth 87	
	 iCloud
Ne 🐱	R Runnak App Store 877
3>>0-At>7-	
5 89765-F	3 7717-ANNER

3. [確認コードを入手]をタップします。



2. [パスワードとセキュリティ]をタップします。



4. 確認コードが表示されます。



※確認コードの取得方法はOSのバージョンおよび利用状況 によって異なります。詳しくは下記をご確認ください。 https://support.apple.com/ja-jp/HT204974

エージェントツールのインストール

iOS

管理者作業

利用者作業

Apple Push Certificates Portal

Mobile Device Management

Mobile Device Management

Certificates for Third-Party Servers Vendor

(Ent)

6. Certificates for Third-Party Servers 画面が表示されます。[Create a Certificate] ボタンをクリックします。

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

Mobile Device Management Trend Micro Incorporated (Ent) Feb 19, 2019 International Centre for Dispute Resolution in accordance with its International Arbitration Rules. The place of arbitration shall be London. England, the language shall be English, and the number of arbitrators shall be three too hereby wave any right of immunity as to Yourserial and Your property with mesolet to the enforcement and execution of any arbitral award rendered pursuant to this clause. Upon Apple's request, You agree to provide eldence of Your Status as an intergovermental agranization with such privileges and immunities.

Trend Micro Incorporated (Ent) Aug 24, 2018

Trend Micro Incorporated

Expiration Date*

Sep 19, 2018

Expired

Active

Active

s Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of ods, the application of which is expressly excluded.

9.9 Entire Agreement; Governing Language. This Agreement constitutes the entire agreement between the parties with respect to the use of the MDM Certificates provided hereunder. This Agreement may be modified only, of all by a written anerdment signed by both parties, or (10) to the exent expressly permitted by this Agreement (for example, by Apple by written or email notice to You). Any translation of this Agreement is done for local requirements and in the event of a dispute between the English and any non-English version, the English version of this Agreement shall govern.

If You are located in the province of Quebec, Canada, the following clause applies: The parties hereby confirm that they have requested that this Agreement and all related documents be drafted in English. Les parties ont exigé que le présent contrate tous les documents comcenses soient rédigée en anglais. Rev. 3/6/15 EA1235



8. [Create a New Push Certificate 画 面が表示されます。「ファイルを選択」をクリックし、 3 でダウンロードしたCSRファイルを選択し、 [Upload]ボタンをクリックします。

	Store	Mac	iPod	iPhone	iPad	iTunes	Support	٩
ople i	Push Cei	rtificate	s Porta				cloudnw199607	01@icloud.co
Creat	te a New	Push Cei	rtificate					
Upload y vendor to	our Certificate Si o create a new pu	gning Request s ish certificate.	signed by your I	hird-party server				
Notes								
								-
								1
Vendor-9	Signed Certificate	signing Reque	st			. (<u> (</u>)	4
ファイル	レを選択 CSR_sig	neMicro.b64					HY.	A
			Cancel	Upload				D

エージェントツールのインストール

iOS

9. 「Confirmation」画面が表示されます。 [Download]ボタンをクリックして、証明書をダウ ンロードし、任意の場所へ保存します。



10.管理コンソールへもどり、証明書を作成す るために使用したApple IDを入力します。



11. [ファイルを選択]をクリックし、9 で作成したAPNs証明書を選択し、[APNs証明書のアップロード]ボタンをクリックします。



エージェントツールのインストール

iOS

管理者作業

利用者作業

12.「カスタマイズ」ボタンをクリックして使用許 諾契約書を編集できます。

Android/iOSデバイスへのインストール時には 「使用許諾契約書」が表示されます。エンドユー ザはこの使用許諾契約書に同意してインストー ルします。この画面の初期設定では、テンプレート としてお使いいただくことを想定した文章をご用意 していますが、お客さまのご利用環境に合わせて 文面を修正してお使いになることをお勧めします。

≡	TREND Worry Free Business Security Services				
ດ	管理	モバイルデバイス登録設定			
ភា	一般設定	Apple Push Notification Service証明書			
 ب	モバイルデバイス登録設定	iOSデバイスの管理には、有効なAPNs (Apple Push Notification service) 証明書が必要です。[APNsig キュリティサービス Webコンソールにアップロートしてください。			
<u>ج</u> ا	通知	APNsi証明書のアップロード			
G G	Active Directoryの設定	AndroidおよびiOSデバイス向ナの使用許諾契約書			
	Smart Protection Network	トレンドマイクロでは、使用許諾契約者をテンプレートとして提供しており、お客様の会社に合わせてテンプレー ライアントのインストール中に表示されます。エンドユーザは、ビジネスセキュリティクライアントをインストールマ			
٩	回復キーのバスワ <i>ード</i> ツール	送信 カスタマイズ			

13. 編集が完了したら[保存]をクリックします。

	🕖 IREND Worry F	ree" Business Security Services	() 12:13 UTC+09:00	0	& demo_anti_2 +
○ ○	管理 一動設定 モバイルデバイス象動設定	・セトイル・アンドノンEMBE ・ 使用許諾契約書テンプレート ・ ・ ・			Ø
	通知 Active Directoryの設定 Trend Micro Remote Manager Smart Protection Network 回販モーのバスワード ワール	警導のパサービス」((株役で交叉 を複数モルトイルプラットフォーム ・・ティングシステムの構成と)	サービス」(14時で定義)をユーザに接利します 5)「-01-ブラットフォームで常想、顔別し 18日2日		
	ライビン2種種 WebCジンール総定	ав — 102.8.0 6+-26-			₽ン⊐L-+©U⊄>+

14. 変更後は、利用許諾契約書の送付ができます。[送信]ボタンをクリックしメール送付します。 (ご利用中のメールソフトが起動します。)



エージェントツールのインストール

管理者作業

利用者作業

iOS および iPadOSでは、初期設定でSafariの「デスクトップ用Webサイト」が有効になっています。

※インストール前に、一時的にSafariをモバイル用Webサイト表示にする必要があります。

1. ホーム画面より [設定] > 「Safari」をタップします。

	設定	
prover a special bundhed and and	計測	
	Safari	>
	株価	
•	ヘルスケア	
	ショートカット	

2. 「デスクトップ用Webサイトを表示」をタップします。

く設定	Safari	
履歴とWebサイトデージ		
WEBサイトの設定		
ページの拡大/縮小		
デスクトップ用Webサ-	イトを表示	
リーダー		

3. 「すべてのWebサイト」をスライドし、オフにします。



エージェントツールのインストール

iOS



詳細

エージェントツールのインストール iPadOS

iOS



10. iOSの設定アプリを起動します。

利用者作業



11.「一般」を選択します。

	設定	
F	通知	
4 :0	サウンドと触覚	
C	集中モード	
X	スクリーンタイム	
Ø	一般	>
2	コントロールセンター	>

12. 「VPNとデバイス管理」を選択します。

	-#x	
iPhoneストレ		
Appのバック	グラウンド更新	
日付と時刻		
キーボード		
フォント		
言語と地域		
時書		
VPNとデバイ	ス管理	

エージェントツールのインストール

iOS

管理者作業	利用者作業
13. 「Trend Micro Worry-Free Business Security Services」を選択します。	<mark>く</mark> 一般 VPN とデバイス管理
	VPN 未接続 >
	勤務先または学校のアカウントでサインインし てください
	ダウンロード済みプロファイル Trend Micro Worry-Free Business >

14. 「インストール」を選択します。



15. 警告が表示されますが「インストール」を選択します。



エージェントツールのインストール

iOS



17. 「完了」を選択します。



18. Appのインストール確認が表示されますので、「インス トール」を選択します。



エージェントツールのインストール

iOS



利用者作業

19. アプリ(Mobile Security)がインストールされるので 開きます。



20. 通知の送信を許可します。

通知方法は、テキスト、サウンド、アイコ ンバッジが利用できる可能性があります。 通知方法は"設定"で設定できます。

"Mobile Security"は通知を送信 します。よろしいですか?

許可しない

```
許可
```

*Mobile Security に位置情報の 使用を許可しますか?
この相限は、Wi-Fi保護の実行にのみ使用 されます。地理的位置データは収集されま せん。
1度だけ許可
Appの使用中は許可
許可しない

21. 位置情報の使用を許可します。

エージェントツールのインストール

iOS



利用者作業

22. アプリ(Mobile Security)がインストールされるので開きます。



23. Webレビュテーションを使用するためにVPNをONにします。



エージェントツールのインストール



※Chrome同期でブラウザの拡張機能が同期されている場合は、本ページの手順は不要です。 拡張機能が同期されている場合は次の手順のみご参照ください。

>

Website Blocked by Trend Micro Worry-Free Restricted website blocked

<

エージェントツールのインストール





5. 認証コード入力画面が表示されるので、認証コードを入力しアクティベートする (必要に応じてデバイス名を変更してください)

認証コード:通知された認証コード デバイス名:ログイン中のgoogle アカウント名(@より前)が自動表示されます ※管理コンソール上でエンドポイント名として表示

	:		
保護機能を有効にするには、以下の情報を指 定してください。			
認証コード:			
デバイス名:			
layar 30120 (Chromebook)			
保護機能のアクティベート			

6. アクティベートが完了すると、ポリシーのステータスが表示されます



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

2. 全端末に適用されるポリシーを定める方法

《 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。
 - クルーノとは異なりますのでご注息くにさい
- 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。

≡	E BICK STREND	usiness Security Services		
ଜ	セキュリティエージェント	test		すべてのステー
50	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	セキュリティエージェント: 1	3	
ম	🔺 🚞 手動グループ	+ セキュリティエージェントの追加 🐵 検索 …	■ ポリシーの設定 ■ タスク	
ے ا	サーバ (初期職定) (0)	□ エンドポイント ↑	经资源	
	デバイス (初期設定) (4)		Vindows	
G	1051 三 最新のパターンファイルを使用して (4)			
B	Ξ ビジネスセキュリティサービスで管 0			
ු				

!!Configure Policy: test!!		\times
🌣 対象とサービスの設定	検索設定	()
iOS	検索方法	
	◎ スマートスキャン	
 検索設定 	- スマートスキャンは、クラウドに格納された不正プログラム対策およびスパイウェア対策シグネチャが利用されます。	
 挙動監視 	○ 従来型スキャン	
● 機械学習型検索	従来型スキャンは、ビジネスセキュリティクライアントに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。	
● Webレビュテーション	リアルタイム検索	
 ファイアウォール設定 		
情報漏えい対策	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。	
● デバイスコントロール		
	静定	

《 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。

E 🕖 TREND Worry F	ree [∞] Business Security Services	15:25 UTC+09:00	?	1	,
 ポリシー設定 道加の設定 グローバルオキュリティエー 	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。			(3
2 ジェント設定	セキュリティ設定 エージェントコントロール				
グローバル除外リスト	一般検索				
ウロ-00と世キュリティエ・ コーク10と線タリスト ウロ-00と使みりスト プレーリソーズ プレーリソーズ プレーション プレーシーン プレーシーン </td <th>7ンスは向上しますが、セキュレ する① 1ます。 こする① す。 、で、アイコンの上部に通知を書</th> <td>リティリス</td> <th>クをもたらす可能性</th> <td></td>		7ンスは向上しますが、セキュレ する① 1ます。 こする① す。 、で、アイコンの上部に通知を書	リティリス	クをもたらす可能性	

機能を設定する(グループ: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。

≡	ポリシーの設定: test		× ^{ti}	i149 👻
6	🏠 対象とサービスの設定	検索設定 (2)	?	?
5	貫 🗯 🏟 ios 🥥	検索方法		
ප	<u>衆戚からの保護機能</u> ● 検索設定	○ 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。		\$
	 挙動監視 機械学習型検索 	○ 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ボーネントを利用します。		
Θ	● 仮想パツチ	リアルタイム検索		
ß	● Webレビュテーション ● ファイアウォール設定	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。		
૽ૺ	情報漏えい対策 ● デバイスコントロール	設定		
	● 情報漏えい対策	予約検索		
	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	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。 〇〇 オフ	2	
	除外リスト 絵表院外	手動検索	_	
	承認済み/ブロックするURL	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。		
	エージェントの設定 権限およびその他の設定	3		
		<i>保持</i> キャン	セル	

「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(グループ: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。

	ポリシーの設定: test		\times	ıti149 -
6	☆ 対象とサービスの設定	検索設定	?	?
G	👯 🗯 🏟 iOS 🥥	検索方法		
<u>گ</u>	 脅威からの保護機能 検索設定 	○ 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。		
\bigcirc	● 仮想パッチ	リアルタイム検索		
ß	● Webレビュテーション ● ファイアウォール設定	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。		
ંંગ	情報漏えい対策			
	 テ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	予約検索		
	• URLフィルタ	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、エンドボ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。		
	● アプリケーションコントロール			
	除外リスト	手動検索		
	検系际外 承認済み/ブロックするURI	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。		
	エージェントの設定	設定		
	権限およびその他の設定			
		保存 キャン	セル	
				¢ >

機能を設定する(グループ: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XX	
対象 処理	i.e
検索設定 3	
検索するファイル:	
○ 検索可能なすべてのファイル	- 1
● 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 ③	
○ 指定された拡張子を持つファイル	- 1
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 4	
✓ POP3メッセージを検索する	
✓ IntelliTrapを有効にする ④	
✓ 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 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。	
□ 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 ③	- 1
最大階層数: 2 🔺	- 1
	- 1
▼ JOSTINA (JEC/CR) する時間10000/JJJJ ZZCR#する ✓ Wabおよびメールからダウンロードしたファイルに対するCVFセキュリティホールの検索を有効にする	
5 OK キャンセル	
● UKLノイルタ 認足C14に対面次US規度し使用で美10より。」将引使用で成用すると、エノトリパイノトしの定例の少な使用で日割にしい、月間の目生で別年化りることがしてより。	_
 アブリケーションコントロール オフ 	
除外リスト 手動検索	
本認済みパロックするURL Webコンソール上の[ゼキュリティエージェント] 画面またはゼ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。	
エージェントの設定	
権限およびその他の設定	
6 <i>保存</i> キャンセル	< >

「保存」を押して終了です。

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

	ポリシーの設定: test			
	✿ 対象とサービスの設定	検索設定		
	iOS 🖨	検索方法		
1)	 	● 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。		
	● 挙動監視	○ 従来型スキャン		
	◎ 機械学習型検索	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。		
	● Webレビュテーション	リアルタイム検索		
	● ファイアウォール設定			
	偕報漏えい対策	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。		
	● デバイスコントロール			
	● 情報漏えい対策	設定		
	アクセスコントロール	予約秋索		

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
iOS 📫	税索方法
書威からの保護機能	
 検索設定 	● スマートスキャンでは、インターネットクラウドに移動されている不正プログラム対策シグネチャお上びスパイウェア対策シグネチャが利用されます。
● 挙動監視	
● 機械学習型検索	○ れんエス・ハラ 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ブログラムやスパイウェア対策コンボーネントを利用します。
● Webレビュテーション	リアルタイム検索
● ファイアウォール設定	
皆報漏えい対策	ファイルを受信、聞く、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。
● デバイスコントロール	
● 情報漏えい対策	設定 3
アクセスコントロール	予約換索

リアルタイム検索設定	\times
対象 如理	
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 ③	
○ 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 🔅	
✓ 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 ④ 4 4 2.2.2.2.000000000000000000000000000000	
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 ③	
最大階層数: 2 🔺	
✓ ユーザの許可なくプロセスを終了する可能性のあるアプリケーションを検索する	
ー ✔ Webおよびメールからダウンロードしたファイルに対するCVEセキュリティホールの検索を有効にする	
(5) 💽	キャンセル

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5》 ポリシーの設定: test \times 🌣 対象とサービスの設定 機械学習型検索 ? 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を使用して、あまり普及していない不審ブ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。 É iOS -Ä (**10**) **骨感からの保護機能**)オン 検索設定 9 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。 ● 挙動監想 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。 機械学習型検索 検出設定 • Webレビュテーション 種類 処理 ファイアウォール設定 🔽 ファイル 隔離 -情報漏えい対策 デバイスコントロール -🔽 ブロセス 総了 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

項目1~5を全て設定し、「保存」を押して終了です。

腟外リスト

キャンセル

機能を設定する(グループ: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。



「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(グループ: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。



◆おまかせアンチウイルスのランサムウェア対応機能

<u>I:不正なファイル暗号化や変更から文書を保護</u>

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。

<u> 皿: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</u>

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(グループ: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(グループ: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。

ポリシーの設定:デバイス (ネ	刀期設定)	\times
	仮想パッチ ウイルスバスター ビジネスセキュリティサービスでは、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 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 一部です。	⑦ -ス 能の
 ・ ジェネムと ・ 挙動監視 ・ 機械学習型検索 ・ 仮想/パッチ ・ 仮想/パッチ 	オン 2 ウイルス/(スタービジネスセキュリティサービスで対策可能な脆弱性の検索:	
 ファイアウォール設定 情報漏えい対策 デパイスコントロール (情報用2) い対策 	95: CVE-2016-4140, MSCVE-2020-14/2/6C	
 ・		
^{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		
	3 係存 キャンセ	ZJL

「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 (グループ: 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。

!!Configure Policy: test!!						\times
 ☆ 対象とサービスの設定 ● 値のS ● 奈広からの信濃機能 ● 検索設定 ● 挙動監視 	Webレビュテーション Webレビュテーションは不正Webサ で オン をキュリティレベル	✓ イトの脅威からの保護を強化します	t.			0
● 機械学習型検索		危険	極めて不審	不審	未評価	
● Webレビュテーション	() 高	~	~	~	~	
• ファイアウォール設定	 中(初期設定) 	\checkmark	\checkmark			
修報漏えい対策 ● デバイスコントロール	〇 低	~			\sim	
● 情報漏えい対策	✓ Webサイトのアクセスをブロ	コックします 🕕			(3)	
アクセスコントロール	ブラウザ脆弱性対策					
	─── 不正スクリプトを含むWeb	ebサイトをブロックする				
・ ノラック ションユイロール 総外リスト 検索除外 承認済みパブロックするURL クライアントの設定 権限およびその他の設定						
				(4 保存 ++	ッンセル

「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 (グループ: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。



機能を設定する(グループ: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

※ここでは、USDデバイスを読み取り等用にし、情報の持ち山しを崇正する 設定を行います。

!!Configure Policy: test!!		\times
 ☆ 対象とサービスの設定 ● ● iOS ● ● なからの保護機能 ● 検索設定 ● 挙動監視 	デバイスコントロール デバイスコントロールは、周辺デバイスへのアクセスを制御します。 マンプン・フィン・ 東田するには、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。	0
 ・	CD/DVD: ① 読み取り ・ ネットワークドライブ: 読み取り ・ USBストレージデバイス: 読み取り ・	
 ・ デハイスコンドロール ・ 情報振漏えい対策 アクセスコントロール ・ URLフィルタ ・ アブリケーションコントロール È外リスト 検索除外 近郊落みにブロックオるUBL 	□ USBストレージデバイスでの自動実行機能をプロックする 許可されたUSBデバイスの権限を設定する 許可されたプログラムを設定(0) モバイルデバイス ストレージ: フルアクセス ▼	
クライアントの設定 権限およびその他の設定	XLL - ク以外のデバイス ・ドゴ ・ ブロック Bluetoothアダブタ: ・ドゴ ・ ブロック COMおよびLPTボート: ・ドゴ ・ ブロック IEEE 1394インターフェース: ・ドゴ ・ ブロック イメージングデバイス ・ドゴ ・ ブロック 赤外線デバイス: ・ドゴ ・ ブロック モデム: ・ドゴ ・ ブロック ブリントスクリーンキー: ・ドゴ ・ ブロック ワイヤレスNIC: ・ドゴ ・ ブロック	
	5 【#荐 +*	ンセル

《 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 (全端末:デバイスコントロール)

		Worry Free Business Security Services					() 15:05 UTC+09:	00 🕜 🌡	
<u>م</u>	ポリシー設計	Ē	グローバ	ル除外リスト 用するために必要な時	· 外設定を構成 ::	हत.			
Ģ	追加の設定 グローバ	許可されたUSBテ	「バイスのリスト						×
2 P	ント設定 グローバ,	十追加	C インボート 📋	削除 📑 エクス	スポート			Q	
1 Northern	ポリシーリン	ベンダー/製造	沅	機種/製品ID		シリアルID/番号	×	E	
Θ	アプリケー								
デバイス ・外部 。 ・ ・ デバ	・情報を取得する。 デバイスが接続去 Windows: デバイ) Mac: システム面容 イスニントロール道	方法 4 れたエンドポイントで以下 スリストツールを生むシロー などの確認とます。詳細情報 定が発生した場合にデッ デバイス情報を取得す。	を実行します。 ードして実行します。 ぶイスコントロールログの あ方法 3	の詳細を確認します。	デバイスにお追加 C、USBストレー	はれていません。 ジデバイスを指定します。	10件/ページ	▲ 1 / 1 < >	
								閉じる	
			機械学習型構 指定されたS	食索除外リスト (0) HA-1ハッシュ値を機械	学習型検索から	余外します。(Windows)			
4					(†/2方) キオやの		eta/= (p)		
	wfbs	-svc-nabu.trendmicro	o.com 706 listDevid	einto.exe を実行また	は1禾仔しますか?		実行(<u>R</u>)	(¥存(S) ▼ キャ	ッンセル(<u>C</u>) ×

⑤「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

<u>]</u> nihei				- - ×
整理 マ 新しいフォルダー				= - 🔟 📀
🚖 お気に入り	名前 ▲	更新日時	種類	サイズ
◎ ダウンロード ◎ 見にまニ」も掲載	🥏 listDeviceInfo.exe	2019/04/12 14:52	アプリケーション	341 KB
□□ 取过扱いいこあり ■ デスクトップ		⑥ダブルクリック	して、 実	行します
 ライブラリ ドキュメント ピクチャ ピデオ ミュージック エンピューター ローカル ディスク (C:) 1 個の項目 	_			

⑦端末に接続しているUSB情報が表示されます

ルビュータ	ユーザ	ボート	説明	ベンダ	モデル	シリアル番号
PC001	Security Manager	USB	USB Device	SONY	0310	0123456789
F可されたUSB (+ 追加 ダー際	デバイスのリスト 8 1	ロンボート	シリア/JUD/番号	ׯ		
り、イス情報を取得	(道加)をクリッ する方法	だして、USBストレー	許可されたUS ベンダー/製造元:* SONY	Bデバイス		>
			機種/製品ID: 0910 シリアルID/番号: 0122456789			V
			·····································	⑨表示	された値をフ	人力します
					10	保存 キャンセル

機能を設定する(グループ: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。

!!Configure Policy: test!!					\times
 ◆ 対象とサービスの設定 ・ 「「」」」	情報漏えい対策 は、ネットワーク全体の想 「 ・ なか た 、 な ・ か た ・ か り 、 ネットワーク全体の想 2 2 注意: 初めて情報 は漏えい対策を有効化す	県密データの転送を監視またはブロック る場合は、ユーザがエンドポイントを再	わます。 記動し、設定を適用する必要があります	-o	0
 機械学習型検索 Webレビュテーション 		データのまご送去服物またはナポロックには	-+		
 ファイアウォール設定 6報漏えい対策 			.9.		0/40
● デバイスコントロール	1-n 4	テンプレート	チャネル	処理	有効
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 睦外リスト 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		ル・ [j島加] をクリックして	ールが定義されていません。 、情報記見たい対策ルールを作成してくださ	\$U №	
					保存 キャンセル

機能を設定する (グループ:情報漏えい対策)

情報漏	えい対策ルールの設定	×
□ 一般語 ✓ こ ルール 説明:	設定 :のルールを有効にする レ名:* test 5	
 テノン 情報》 すべ 	ルート・ 属えい対策テンブレートを選択し、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 べてのテンブレート → Q	
	テンプレート (1/239)	
	台湾:携蒂電話番号	^
	台湾:日盛銀行の口座番号	
	台湾:銀行口座番号	
	日本:パスボート番号	
	日本:マイナンバー (法人)国の機関 10件以上で検出	
	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	
	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	
	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	
	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	~

□ チャネル	
情報漏えい対策で監視するチャネルの種類を選択してください。	
田 Z ネットワークチャネル	
□ 処理	
選択したネットワークチャ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 … 8	
	9
	追加キャンセル

機能を設定する(グループ: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 ● 前の ● 承述からの保護機能 ● 検索設定 ● 学動監視 ● 機械学習型検索 ● ひゃくのなどを ● ファイアウォール設定 佐藤瀉えい対策 ● 情報漏えい対策 	JRLフィルタを有効にすると、管理者は、1日のさまざまな時間帯でブロ・ オン オン アルク強度 ・ 高 ・ 尻知または送着在的なセキュリティ上の脅威ホージをプロックは コンテンツ、あよび未評価のページをプロックします ・ プロックするURLカテコリを指定する ・ 低 (初期設定) ・ 別スタム ・ フレックするURLカテコリを指定する	ックする特定の種類のWebサイトを設定することができ 適切なコンテンツまたは有害である可能性のあるコン ます コンテンツをブロックします 3	ます。 テンツ、生産性または帯域物副に影響する可能性のある
	URLカテゴリ	■ 業務時間	□ 業務時間外
 アプリケーションコントロール 	アダルト		
除外リスト	 ビジネス 		
検索除外	 ヨミュニケーション/メディア 		
承認済み/ブロックするURL	▪ →般		
権限およびその他の設定	 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		
37	美務時間		
	 ● #2日 (4×7) ● 業務時間を指定する 		
			保存キャンセル

機能を設定する(グループ:URLフィルタ)

!!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 	
ios	ヨイフスタイル	
 ★ 底からの保護機能 検索設定 	≢ ネットワーク	
● 挙動監視	業務時間	
 ● 機械学習型検索 ● Webレビュテーション 	 	
 ファイアウォール設定 デバイスコントロール 情報漏えしは対策 アクセスコントロール URLフィルタ アブリケーションコントロール 酸・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 	日 日 次 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	5 業務で利用する曜日、時間 帯をクリックして選択
	18:00 19:00 ● 業務時間 ○ 業務時間外	6) 保存 ++ンセル

機能を設定する (グループ: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。

≡	ペーク ポリシーの設定: test				×	149
റ പ	 ☆ 対象とサービスの設定 ■ iOS () 	アプリケーション エンドポイントでのアブリケーショ	コントロール コンの実行やインストールを制限するルールを作成	します。	0] (
2	脅威からの保護機能 ● 検索設定					\$
	 挙動監視 機械学習型検索 仮想パッチ 	 〇〇 フロック: 指定したアフリク 〇 日 ロックダウン: 前回のインペ 〇 トレンドマイクロの信: 〇 Microsoftの署名付きの) 	テンヨンのエントボイント Cの美行をノロック Cシトリ検索で確認されなかったアプリケーション 頼済みベンダーのアプリケーションを除外 (推奨) プログラム (Windows Updateを含む) によるプロセ	をすべてブロック ① 3		
ß	● Webレビュテーション ● ファイアウォール設定	ルール				
÷	情報漏えい対策 ● デバイスコントロール	+ ルールの割り当て			合計: 0	
	 情報漏えい対策 アクセスコントロール 1 	種類 ↑	ルール	概要		
	 ● URLフィルタ ● アプリケーションコントロール 		ルールが割り当 [ルールの割り当て] をクリックしてアプリケー	てられていません。 -ションコントロールルールを指定してください。		
	除外リスト 検索除外 承認済み/ブロックするURL	許可ルールはブロックルールよ	りも優先されます。			
	エージェントの設定 権限およびその他の設定					
	_			4	保存	

※EDRプラスオプションをご利用されている場合の機能となります

Endpoint Sensorの機能を有効にします。 →端末の不審な挙動を検知およびクラウドサンドボックス機能を有効化します



端末のロックを解除する際に、パスワードの入力を要求します。 ※ここではAndroidの中レベルの設定をしています。



機能を設定する (グループ: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 (グループ:除外設定)

《 挙動監視から除外する場合 》

ー ポリシーの設定: test		×
☆ 対象とサービスの設定	検索除外リスト 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。	?
 ■ ■ ■ ■ ● ●<td>リアルタイム検索/予約検索/手動検索</td><td></td>	リアルタイム検索/予約検索/手動検索	
 検索設定 挙動監視 	フォルダ(0) ファイル(0) ファイル拡張子(5)	
 機械学習型検索 仮想パッチ 	+ 違加	合計: 0
 Webレビュテーション ファイアウォール設定 	フォルダパス リアルタイム検索 予約検索 手動検索	
 「「報知記しい対策 デバイスコントロール 「常報温えい対策 アクセスコントロール 	フォルダ除外が追加されていません。 [追加] をクリックして、フォルダバスを指定します。	
 URLフィルタ アプリケーションコントロール 除外リスト 	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。 ダ リアルタイム検索 ダ 予約検索 ダ 手動検索 スパイウェアパリーウェア	
検索除外	+ 追加	合計: 0
エージェントの設定 権限およびその他の設定	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 ※動監視により自動的にまべての支援の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)	
	+ 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。除外を指定するには、[ポリシー設定]→[グローバル除外リスト]に進み?	ます。
	5	キャンセル

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。

ポリシーの設定: test		\times
 ☆ 対象とサービスの設定 	承認済み/ブロックするURLのリスト 承認済み/ブロックするURLはWebレビュテーションおよびURLフィルタに適用されます。 使用除外:	0
 検索設定 挙動監視 機械学習型検索 Webレビュテーション 	 グローバル承認済みおよびブロックするURLのリスト ① 除外の指定 承認済みURL (15) プロックするURL (0) 	
 ファイアウォール設定 皆板漏えい対策 デバイスコントロール 	(3) + 追加 ・ 合計: 15 承認済みURL	j
 ● 情報漏えい対策 アクセスコントロール 	http://*.trendmicro.com/* https://*.trendmicro.com/*	^
● URLフィルタ ● アプリケーションコントロール	http://www.trendmicro.com/*	
除外リスト 検索除外	http://wustat.windows.com/* http://windowsupdate.microsoft.com/*	-
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	WeDレビュアーションで読って対象時でにいる可能性の)めるURLを通知するか、URLの女全性の海判価を確認するには、次のWebサイトにアクセスしてください。 http://sitesafety.trendmicro.com/	
	保存 キャンセン	ν

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。

≡		ree [™] Business Secur	rity Services	① 10:40 UTC+09:00
ର	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	
G	追加の設定	シローハル設定よりホートされる97		
ප	ク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 エージェン	<u></u> <u> </u>	
圆				
		2 7 → 日経過してもウー	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
G	・ フリケーションユンドロール ルール	セキュリティエージェントのログ		
		✓ Webレビュテーションおよび の あばくべい 小の詳細を発化す	URLフィルタのログをサーバに送信する	
ن ې				
			こ 2月1十二ビフズ 石がり ニオス・	
		▼ セキュリティエージェントのス		
		セキュリティエージェントを再	記動できない場合、 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	F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	シインストール時にバスワード入力を要求する	
		終了口ック解除		
		🗌 セキュリティエージェントの終	?7時、または詳細設定のロック解除時ごパスワード入力を要求す?	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 ントのリソースを多く使用するた に影響が出る可能性があります。	≧に比べてエンドポイ こめ、パフォーマンス
保存	字」を押して終了	です。	メモリ : 最大21MB程度/通常 HDD : 最大213MB程度/通常	4MB程度 常40MB程度

《 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。

microsoftedgecp.exe

ഹ _	ログ							C
μ Ω	セキュリティリスクの	検出: すべて 👻 📋 過去	30日間 -				28/‡ [5 I07#-> 0
	日時↓	カテゴリ	脅威強反	ファイルのパス/対象	処理/結果	エンドポイント	ユーザ	计相
<u>×</u> :	2019年01月30日 17:3	橡枝学習型検索	Ransom.Win32.TRX	c ¥users¥yokoj¥downib	SILRE	DESKTOP		= * Q
G	2019年01月30日 17:3	ウイルス/不正プログ	Ransom.Win32.TRX	c¥users¥yoko,¥downio	NETR	DESKTOP-		🗉 🔍 Q
B	2019年01月30日 17:3	ウイルス/不正プログ	Ransom.Win32.TRX	c ¥users¥yoko,¥appdat	枢除	DESKTOP		🖂 🐄 😡
	г	AND THE REAL AND A LOCAL					A	· ·
		拡張脅威分析			クリッ	クすると表示		×
		Ransom.Win32.TRX 2019年01月30日 17:38:3	XXPE1					
		(回) エンドポイント DESKTOP-HHK490 ド 部後のユーザ		() 超地超調 () Web microsofted	jecp.exe	RedtU.Adm Strendy	tež sign-a.exe	Q
			е –		-)		e,	

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

trendx_sign-a.exe

https://doc-0c-...nload

機能を設定する(全端末:隔離した端末の通信許可)

※EDRプラスオプションをご利用されている場合の機能となります

《隔離した端末の通信許可方法》

- ・隔離した端末において許可したい通信を設定することはできます。
 - 許可された受信トラフィック: IPアドレス、通信プロトコル、ポート番号
 - 許可された送信トラフィック: IPアドレス、通信プロトコル、ポート番号

≡	🕖 TREND. Worry Fi	ree [™] Business Security Service	?S		
ଜ	ポリシー設定	グローバルセキュリティエーミ 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	ジェント設定 エージェントに適用され	1ます,	
Г С	追加の設定 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 トラフィックコントロール	隔離したエンドポイ	> 3	
ତ୍ତ	901-700時かりスト 2	隔離したエンドボイントはネットワークから切り離され	ます。すべての隔離し1	モエンドポイントに対する送受信	トラフィックについて、許i
	骨感インテリジェンス ユーザ指定の不南オブジェク ① (UDSO) ① (UDSO) ① (UDSO) ③ □ ③	許可された受信トラフィック 送信元IPアドレス:*	プロトコル:	ポート: ①	
	● 仮想アテライザの不備オブシ エクト (VASO)	IPアドレス] ज्ञारत	・ 」 すべてのポート	Ē
ු	ポリシーリソース アプリケーションコントロー ルルール	+ 追加			
		- 死先IPアドレス:* 5	プロトコル:	ボート: (j)	
		IPアドレス 十 追加	すべて	すべてのポート	Ē
		6			
		保存			

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

≡	TREND Worry Free [™] Business Security Services (☉ 15:02 UTC+09:00					
റ പ 2	ポリシー設定 追加の設定 グローバルゼキュリティエー ジェント設定 グローバル除外リスト	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 書告				
₿ () () ()	ポリシーリソース アプリケーションコントロー ルルレール	 ▼ 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/ セキュリティエージェントのログ WebレビュテーションおよびURLフィルタのログをサーバに送信する 	(ーに警告アイコンを表示する			
÷		図 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 監視サービス				
		 マ 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 	インストールに必要 パフロードを入力	ēな		
		 ✓ 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 パスワード: 4~20文字 				
		パスワードの確認: 				
		 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 				

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

≡	🕖 TREND Worry Fi	ree" Business Security Services	(b) 15:04 UTC+09:00	0	
ດ	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 ^{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。}			
Д Д	追加の設定 グローバルゼキュリティエー ジェント設定				
		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		
Φ	ホリシーリソース アプリケーションコントロー ルルール	セキュリティエージェントのログ			
ا چ		✓ WebレビュテーションおよびURLフィルタのログをサーバに送信する ✓ 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			
		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	エージェントの終了に 必要なパスワードを入力		
		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 パスワード: 4~20文字 	力を要求する		
		パスワードの確認:			
		<u>\$</u>#5			

機能を設定する(管理: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。

≡	Worry Fr	ee [™] Business Security Services	15:59 UTC+09:00	?	v
ର	管理 2	一般設定			?
ភា	一般設定	エンドボイントのラヘル付け			
ے لا	モバイルデバイス登録設定 	この機能を使用すると、セキュリティエージェントのインストール中または ます。詳細情報 マ エンドポイントのラベル付けを有効にする	Webコンソール上の [セキュリティエージェント] 画面でエンドポイ	ントをラ	◇レ付けすることができ
A	Active Directoryの設定	エンドボイントのラベル付けのヒントとして、セキュリティエージェン	トのインストール中にラベル形式が表示されます。例: フルネーム、	従業員ID	、メールアドレフ
	Smart Protection Network 回復キーのバスワード アイセンス情報 Webコンソール設定	マンレビャン、 従属員じ セキュリティエージェントのインストール用リンク ウイルスパ(スター ビジネスセキュリティサービスでは、ユーザにより処理が ドリンクと認証コードの有効期限を設定するよう選択できます。 有効期限を 14 日後とする(1~999)① セキュリティエージェントツリーのクリーンナップ ウイルスパ(スター ビジネスセキュリティサービスは、セキュリティエージェントを目動的に削除できます。接続が再度確立されると、サーバ 次の期間アクセスがないエージェントをセキュリティエージェントツリー	[ラベル形式]に記入した エージェントのダウンロード時 示されます。 -から自動削除する: 30 日(1~999)	:ワー の画	ドが 面に表 [」] [」]
		ヤシフルシュ フィンツ ヤキュリティエージェント			
		□ 障害発生時に、デバッグログを有効化して下記の情報を収集することを	トレンドマイクロのテクニカルサポートに許可する		
		Windowsエンドポイントの場合: デバッグログ、Windowsイベントログ、 ィエージェントの設定 (レジストリ) など	パフォーマンスカウンタのデータ、システム情報、カーネルダンフ	プ、 ク ラッ	シュ情報、セキュリテ
		Macエンドポイントの場合: デバッグログ、システム情報、カーネルダン ど	ブ、クラッシュ情報、システムプロファイラのデータ、セキュリテ	ィエージ	ェントの設定 (.plist) な
		Webコンソール			
		□ 診断とトラブルシューティングを目的としたウイルスパスター ビジネス する	セキュリティサービスWebコンソールへのアクセスをトレンドマイ	クロのテ	クニカルサポートに許可
		R # 5			
「仔	禄存」を押して 縦	冬了です。			

機能を設定する(管理:ラベル表示)

【参考】エージェントインストール時の画面



「セキュリティエージェント」タブからラベルを入力・訂正することもできます。

≡	TREND. Worry Free Business Security Services O 13:14 UTC-09:00						9:00	1	*
ര 5	セキュリティエージェント	すべてのセキュリティエー セキュリティエージェント:1	ジェント		すべてのステージ	22 - 秋市		Q 7 0	D
2 2 12		+セキュリティエージェントの追加 エンオポイン ト・	1 ⊕ 88 - 5%4	-7.482	 9スクー 38の抽取日時 	PH7Fb2	ステータス	0 Ø	9
0 1	test 1 Ξ 最新のパターンファイルを使用して… 0 Ξ ビジネスセキュリティサービスで登… 0		0123456789	3	1920 1	_	37540		
٢									

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。



機能を設定する(グループ:リモートロック/消去)

端末の盗難・紛失時に、遠隔で端末をロックします。

MREND Worry Free[™] Business Security Services 6 セキュリティエージェント $(\mathbf{1})$ = セキュリティエージェント:3 G すべてのセキュリティエージェント (4) + セキュリティエージェントの追加 ④ 検索、 උ 手動グループ 2 前回の接続日時 エンドポイント ↑ 0 サーバ (初期設定) 圆 11分前 \checkmark デバイス(初期設定) 0 (\mathbf{r}) 1日前 1 たった今 \Box B 3 ී ビジネスセキュリティサービス… 0



リモートロックとは:紛失した携帯端末を第三者が利用できないようにします リモート消去とは:紛失した携帯端末のデータを消去します(※)

機能を設定する(全端末: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。



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。

	Worry Free Business Security Services O 13.24 UTC-0900								1	٠	
ଜ	セキュリティエージェント	η.	L.	べてのセキュリティエーシ	ジェント	71	くてのステータス	* (km		Q 7	0
50	📮 すべてのセキュリティエージェ	新規グ	ループ	ティエージェント:1							
۹ (1 単手動グループ	P-812	47.3	ビジネスセキュリティクライアントの道知	③ 秋余 ~ 回 グローバル設定	₫ \$7.2 -				0	٥
0	サーバ (73期間2年)	٥		エンドポイント・	514	解剖の無能日	1) II	PW77FL2 2	マテータス	ユーザ	r
X	デバイス(信用規定)	(1)	0	•		24512340		2	10540		
θ	Ξ 最新のパターンファイルを使用して										
	Ξ ビジキスセキュリティサービスで管	۲									

新規グループ ×	
名前:	
test	3
□ ポリシー設定をインポートする	
ソース: サーバ (初期設定) -	
(4) 保存 キャンセル	



「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。

E Worry Free Business Security	Services		③ 13:24 UTC+0	9:00	*
	ィエージェント	すべてのステー	9 2 - (8)		Q 7 0
名 1 ● 手助グループ パタネスセキュリティクライ	アントの通知 ③ 秋余 - 🗏 グローバル鉄定	₩ 97.2 -			0 0
サーバ (江西県北)	510	範囲の無能目時	IPv47Fb2	ステータス	ユーザ
		24句题的		30542	
□ ビジネスセキュリティサービスで音… ⑧					
Ø					
新規フィルター		×			
4					
エンドポイント名					
手動ドメイングループ					
_ IPアドレス		(5)			
エンドポイントの種類	本へ	++>>+			
オペレーティンクシステム ラペル					
新規フィルタンンン		コノルカのタ	かちだら		z //+)
2 2		ノイルクの余	計で相比	(AND5	≷1+)
		_			
test					
	~ フィルタ名を指定				
	0				
Worry Free Busines	s Security Services				
	test				
	きれたビジネスセキュリティクライアント: 0(オペレ	›ーティングシステム: W	indows 7)		
▶ 📄 手動グループ 🛞 禎	索				
▲ ▼ フィルタ機能の実装					
test					
日 最新のパターンファイルを使用して… 3					
Ξ ビジネスセキュリティサービスで管 0					

「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(グループ: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。

ポリシーの設定: test		×
☆ 対象とサービスの設定	検索設定	?
ios 🥑	検索方法	- 1
脅威からの保護機能	○ スマートスキャン (推奨)	
 検索設定 ※動影響 	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ブ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。	- 1
 手動監抗 機械学習型検索 	○ 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ボーネントを利用します。	_ 1
● 仮想パッチ	117711 / / / 44-55	_ 1
● Webレビュテーション	リアルタイム検索	- 1
● ファイアウォール設定	ファイルを受信、聞く、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。	_ 1
情報漏えい対策		_ 1
 テバイスコントロール 信報浸きい対策 	sx//E	_ 1
マクセスコントロール	予約検索	- 1
 URLフィルタ 	2 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。	_ 1
● アプリケーションコントロール		_ 1
除外リスト	頻度:	_ 1
検索除外	閻隔: 月曜日 → 3	
承認済み/フロックするURL	開始時刻: 12 ▼ : 30 ▼ 時:分	
エージェントの設定 権限およびその他の設定		
		_ 1
	手動検索	- 1
	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。	_ 1
	設定	_ 1
		_ 1
		_ 1
予約検索設定	× 5	
対象 処理	予約検索設定 ×	L
检查稳定	71歳 乾曜	-
検索するファイル:	CPU提用 CPUL CPUL	
 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 指定された拡張子を持つファイ 	(使業でパランドイルシイノ) () () () () () () () () () () () () ()	
✔ 圧縮ファイルの検索 🗊	81回の中報時間からくない、そのカウロウリンーA77時回されます。 ウイルス体モプログラム	
最大階層数: 2 🔺	● トレンドマイクロの推測処理 ①	
詳細設定	 ○ カスタマイズ回達 ② 和助剤にファイルシバックアップする 	
✓ IntelliTrapを有効にする ④	スルイウエア/クレーウェア	
☑ ン人ナム領域を検索する	○ 転換 プロセンを除了するが、レジストリ、Cookle、およびショートカットを削除する	
	○ 対策 スパイウエアウジレーウェア9株団結果を紛紛のために記録します	
	(X キャンセル	

「保存」を押して終了です。

機能を設定する(グループ: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

≡	🕖 TREND Worry Free Bu	usiness Security Services	⊙ 09.44 UTC+09.00 😧 👗
ഹ 9		test セキュリティエージョント: 1	すべてのステータス - 他士 Q Y ⑦
2 11 0 11 0	 ・ ・ ・	+ to+2074I-U2UHORS * ## - # #UU-ORS ZUF#4UH + Z 3	回 タスク - こ ゆ エジスボート 5 サオペアップデート 日春化 採号 日春化 採号 日春化 採号 千輪グループに移動 セキュリティエージェントのアン・パンストール
今 W う 対	マケップデート indows、Mac、またはAndroidビジネスセ に通知しますか? 条:	× キュリティクライアントに手動で更新を実行するよ 6 アップデート キャンセル	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。
e	TREND Worry Free Busi	ness Security Services	(b) 16:
セキ	ュリティエージェント 📮	✓ コマンドが送信されました。サポートされているセキュリティエージ は、5~10分かかります。	アエントにコマンドを配信するに ×

+ セキュリティエージェントの追加 ④ 検索 ▼ 🗐 ポリシーの設定 🗐 タスク ▼

「アップデート」を押して終了です。

🔺 🚞 手動グループ

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(グループ:手動アップデート)

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。



● ITEND アップデート ? × すべてのコンボーネントをアップデートしています...
経過時間: 0:00:09
(存止

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。





ファイルのダウンロードが始まります。