セキュリティおまかせプラン エンドポイントセキュリティ・EDRセキュリティ ご利用マニュアル (Ver 2.1)

2025年 6月 西日本電信電話株式会社

改定履歴

Νο	Date	主な変更内容	Ver
1	2017/12/01	初版	1.0
2	2018/08/30	VBBSSのVer6.5へのバージョンアップによるUI変更箇所の画面イメージの修正	1.1
3	2019/06/14	インストール(ダウンロード用URLの確認)について変更	1.2
4	2022/11/14	10.(参考)チャット連携会社名取得方法を追加	1.3
5	2023/05/11	現行表記と画面イメージの修正	1.4
6	2023/07/27	インストール(Android)手順を変更	1.5
7	2023/09/29	Android VBBSS 旧エージェントから新エージェントへの移行手順を追加	1.6
8	2023/10/20	レポート通知メールの仕様変更、管理コンソールログイン時のPWリセット手順の追加	1.7
9	2024/04/23	iOSの新エージェントリリースのためインストール(iOS)手順を変更	1.8
10	2024/06/03	Mac対応のため手順追加・EDRセキュリティページについて追加	2.0
11	2025/06/05	サポート支援について追記、システム要件URLの変更、VBBSSインストール用リンクの一部廃止 機能について追記、機械学習型検索初期値の修正、Windows11事前準備について追記、 Macアンインストール手順の追記	2.1



1. <u>エンドポイントセキュリティ概要</u>	•••5P
2. <u>エンドポイントセキュリティ 機能一覧</u>	•••6~7P
3. <u>EDRセキュリティ概要</u>	•••8P
4. <u>EDRセキュリティ 機能一覧</u>	•••9P
5. <u>ご提供の流れ</u>	•••10P
6. <u>事前準備</u>	•••11P
7.エージェントのエンドポイントセキュリティ管理コンソール移行について	•••12P
8.管理コンソールへのログイン方法	•••13~14P
9. <u>インストール(ダウンロード用URLの確認)</u>	•••15~17P
10. <u>インストール(Windows)</u>	•••18~19P
11. <u>インストール(Mac OS)</u>	•••20~33P
12.Mac OS端末におけるEDRセキュリティのインストール手順について	•••34P
13. <u>EDRセキュリティ契約時の追加手順(Mac OS)</u>	•••35~45P
14. <u>インストール(Android)</u>	•••46~62P
15. <u>新エージェントへ移行(Android)</u>	•••63~69P

目次

16. <u>新エージェントへ移行(iOS)</u>	•••70~75P
17. <u>証明書の更新について</u>	•••76~79P
18. <u>インストール(iOS)事前準備</u>	•••80~84P
19. <u>インストール(iOS)</u>	•••85~94P
20. <u>機能を設定する(Windows)</u>	•••95~110P
21.EDRセキュリティご利用に伴う、既存設定に関する注意点	•••111~115P
22. <u>Windows/Android/iOS アンインストール</u>	•••116P
23. <u>Windowsアンインストール</u>	•••117P
24. <u>Macアンインストール</u>	•••118~121P
25 <u>レポート作成</u>	•••122~123P
26. <u>月次レポート確認方法</u>	•••124~125P
27 管理コンソールログイン時のID・パスワードについて	•••126~128P

エンドポイントセキュリティ	・・・エンドポイントセキュリティ対象説明
EDRセキュリティ	・・・EDRセキュリティ対象説明
エンドポイント/EDRセキュリティ	・・・エンドポイントセキュリティ・EDRセキュリティ共通説明

1.エンドポイントセキュリティ概要

- ウイルス対策機能だけでなく、企業用に特化したさまざまな管理機能を加えた総合的なエンドポイントセキュリティソフトです
 AIの機械学習型検索を利用した高度なウイルス検知機能により、亜種のウイルスにも対応します
-)管理サーバを通じてセキュリティサポートセンタと接続されており、設定変更や異常検知にも遠隔で対応可能です。



※利用可能な機能はOSによって異なります。

2.エンドポイントセキュリティ 機能一覧 1/2

6

エンドポイントセキュリティで主に提供される機能として、「セキュリティ対策機能」「簡易MDM機能」がご利用可能です。

提供機能はご利用端末のOSによって異なります。

Server対応OSについてはエンドポイントセキュリティ(VBBSS)は動作対象となりますが、セキュリティおまかせプランにおけるサポート支援はエンドポイントセキュリ ティ(VBBSS)のWEB管理コンソール上で実施できる内容に限られますのでご注意願います。(Serverの設定、インストール、アンインストール、リカバリ、データ 移行等のServer自体に触れるようなサポート支援は実施不可、Chromebookはサポート対象外となります)

		Windows	Mac	Android	iOS				
セキュリティ対策	ウイルス対策	0	0	0					
		ウイルスの侵入を検知し、ブロック、隔離、削除を行います。 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。							
	Webレピュテーション	0	0	0	0				
		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	0							
		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。							
	挙動監視	0							
		OS、レジストリ、ソフトウ:	c アに対する不正変更	を監視・ブロックします	0				
	POP3メール検索	0							
		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。							
	URLフィルタリング	Ο							
		業務上必要のないWebサイト 強度、ルール、時間帯等を設 Webサイトを設定できます	へのアクセス制御を行 定することで、お客さ	らいます。全体またはグル きまのビジネス環境に応し	レープ単位でフィルタの びて柔軟に規制対象の				

エンドポイントセキュリティで主に提供される機能として、「セキュリティ対策機能」「簡易MDM機能」がご利用可能です。 提供機能はご利用端末のOSによって異なります。

		Windows	Mac	Android	iOS			
セキュリティ対策	ランサムウェア対応	0						
		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	0						
		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。						
簡易MDM	USBデバイスコント ロール	0						
		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。			
	リモートロック リモートワイプ			0	0			
		端末の紛失時等に、遠隔で端	末のロックや、ワイフ	(初期化)が可能です。				

※対応OS等システム要件は以下URLにてご確認いただきますよう、お願いいたします。 https://success.trendmicro.com/ja-JP/solution/KA-0019415

3. EDRセキュリティ概要

○ EDR(Endpoint Detection and Response)は、エンドポイント(クライアント端末、サーバなど)の操作や動作の 監視を常時記録し、攻撃者による不正な挙動の兆候を検知します ○攻撃の全体像の可視化や、リモートによるエンドポイントの隔離機能などを提供することで、インシデントの根本原因の効率 的な調査と迅速な対応を支援します



EDRセキュリティ提供機能はご利用端末のOSによって異なります。

	機能名	Windows	Mac OS	Android	iOS
	Webレピュテーション	0	0		
	機械学習型検索	0	0		
	挙動監視	0			
	仮想アナライザ	0	0		
	注意が必要なイベント通知	0	0		
セキュリティ	Endpoint Sensor	0	0		
V1W	仮想パッチ	0			
	ファイアウォール	0			
	デバイスコントロール	0	0		
	情報漏えい対策	0			
	URLフィルタ	0	0		
	アプリケーションコントロール	0			
スの曲機能	レポート機能	0	0		
ての他機能	モバイルデバイス制御機能				

EDRセキュリティについて

利用端末に専用ソフトウェアをインストールする必要があります。

利用端末のOSやソフト等との相性によっては、正常に動作しない場合があります。

遠隔サポート対象には、OS等の提供条件があります。

セキュリティ機能は、OSごとに提供機能が異なります。

定義ファイルやプログラムは、「フレッツ光」等接続環境下でダウンロード・更新を行い、常に最新の状態にしていただく必要があります。

※2024年6月3日よりMac OSのEDRセキュリティ機能が提供されております。

5.ご提供の流れ

お申込みいただいたご契約者様には、メールにて、管理コンソールへのログイン情報と、エンドポイントセキュリティ/EDRセキュリ ティのダウンロード用URLをご連絡させていただきます。ご利用端末へのインストールが完了いたしますと、ご契約開始日より サービスをご利用いただけます。



※メールによるご連絡は、ご提供開始の2~3日前までを目安にお送りさせていただきます。 サービスがご利用いただけるのは、ご契約開始日からとなりますので、ご注意いただきますようお願いいたします。 ※メール送付後、お電話にて到着確認をさせていただきます。

6. 事前準備

・ウイルス対策ソフトやMDMソフトが入っている場合、本サービスで提供するエンドポイントセキュリティソフト・EDRセキュリティの 両方で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いたします。

<Windows 10/11の場合> 「スタート」⇒「コントロールパネル」⇒「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、対象のプログラムをクリックしてアンインストールを実施。

7.エージェントのエンドポイントセキュリティ管理コンソール移行について

・エージェントをエンドポイントセキュリティ管理コンソール間で移行する場合、新環境へ移行の前に必ず、既存環境エージェントのアンインストールをお願いいたします。
例:別拠点で使用していたエージェントを新拠点にて利用する

※今回新たに新規でインストールするご契約者様は不要の手順になります。

ご契約者様のエージェントをエンドポイントセキュリティ管理コンソール間で移行する際、下記移行 手順を実施ください。

※事前に移行予定の管理コンソール側で既存と同じ設定のポリシーを利用する場合は、 必要に応じてポリシーの設定を実施ください。 ※移行方法に限らず各種検出等のログは移行されません。

1.既存環境に紐づいたエージェントのアンインストールを実施する。 ※アンインストール方法につきましては、ご利用OSのアンインストール手順を実施ください。

2.移行予定の環境で、インストールを実施する。

※インストール方法につきましては、ご利用OSのインストール手順を実施ください。

8.管理コンソールへのログイン方法 1/2

ご登録いただいております「管理者様アドレス」宛に、メールにて、ログインに必要なURL・アカウントID情報をお送りいたします。 まず、パスワード設定用のURLをクリックいただき、パスワードの設定をお願いいたします。

<メール例>

 □件名【セキュリティおまかせプラン】新規アカウント発行のお知らせ □送信元アドレス no-reply.security-omakase@west.ntt.co.jp □本文 この度はNTT西日本 セキュリティおまかせプランへのお申込みありがとうございます。 	
お客様管理ポータルへのログイン用ユーザアカウントを発行致しました。次のURLからログインできます。 <u>https://clp.trendmicro.com/Dashboard?T=xxxxx</u> アカウントの詳細: アカウント名: TMF ● ● ● ● ● ● ● ● ● ●	— ログイン用URL
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:// ● ● ● ● ● ● ●	— アカワント名 — パフロード設定田URI
変更後のパスワードは大切に保管いただきますようお願いします。 パスワードを忘れるとお客様管理 ポータルにログインできなくなります。 ご不明な点がございましたら、次の連絡先にお問い合わせください。	<u>バスクート設定用してし</u> 初めにこちらのURLより、 パスワードの設定をお願いします。
【本メールに関するお問い合わせ】 セキュリティおまかせプラン開通事務局 TEL : 0120-xxx-xxxx(9:00-17:00 平日 ※年末年始を除く)	ITEND Licensing Management Platform Powered by Powere
【サポートに関するお問い合わせ】 セキュリティおまかせサポートセンタ TEL : 0800-xxx-xxxx(9:00-21:00 平日・土日祝 ※年末年始を除く)	ログインID: TMF1234512345 新しいソスワード: 第7、大文字、小文字を使用した 5 文字以上25文字以下のパス ワードを指定してください。
*このメールアドレスは配信専用です。このメッセージに返信しないようお願いいたします。	20

8.管理コンソールへのログイン方法 2/2

Powered by DIREND

登録情報を入力してくださ

アカウントをまだ取得していない場合 合 すぐ登録

ログインロ:

ログインURLをクリックし、アカウント名と設定したパスワードを入力し、ログインボタンを押します。ログインできますと、「セキュリティ おまかせプラン」にてご契約のサービスが表示されますので、エンドポイントセキュリティ(VBBSS)の「コンソールを開く」を選 択します。

①ログイン画面へアクセス https://clp.trendmicro.com/Dashboard?T=xxxxx

②ID/パスワードを入力し、「ログイン」をクリック

③割り当てられたサービスプランが表示されるので、 エンドポイントセキュリティ(ウイルスバ スタービ シ ネス セキュリティサービス)の「コンソールを開く」をクリック します。

※表記が多少異なる場合がございます。

※初回ログイン時は、トレンドマイクロ株式会社のプライバシー ポリシーが表示されますので、ご確認の上「OK」をクリック いただきますよう、お願いいたします。

④エンドポイントセキュリティの管理コンソールが 立ち上がります。ログインは以上で完了です。



DIREND Licensing Management Platform



エンドポイントセキュリティ/EDRセキュリティのダウンロード用URLは、サービス提供開始前に送付しておりますメールもしくは、 管理コンソールにてご確認いただけます。

メールでの確認方法

 □件名 エンドポイントセキュリティ/EDRセキュリティのダウンロードURLのご案内 □送信元アドレス sec-oma@west.ntt.co.jp □本文 この度はNTT西日本 セキュリティおまかせプランへのお申込みありがとうございます。 本メールはエンドポイントセキュリティ もしくは EDRセキュリティ を 	
インストールいただくソフトのダウンロードURLをご案内させていただきます。 なお、エンドポイントセキュリティ と EDRセキュリティ でインストールするソフトは同一です。 ※複数端末にインストールされる場合は、以下のURLをインストール端末に展開ください。	
http://XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	ウンロード用URL
尚、サービスが有効になるのは、ご利用開始予定日の●年●月●日からとなっております。	
ご不明な点がございましたら、次の連絡先にお問い合わせください。	
【本メールに関するお問い合わせ】 セキュリティおまかせプラン開通事務局 TEL:0120-xxx-xxxx(9:00-17:00 平日 ※年末年始を除く)	
【インストール方法に関するお問い合わせ】 セキュリティおまかせサポートセンタ TEL:0800-xxx-xxxx (9:00-21:00 平日・土日祝 ※年末年始を除く)	
【セキュリティおまかせプラン サポートサイト】 サービスの使い方や、設定方法、よくあるご質問などを掲載しております。ご活用ください。 https://office-support.ntt-west.co.jp/security_omakase/	
*このメールアドレスは配信専用です。このメッセージに返信しないようお願いいたします。	

9. インストール(ダウンロード用URLの確認) 2/3

エンドポイント/EDRセキュリティ

管理コンソールでの確認方法

①管理コンソールにて
 「セキュリティエージェント」タブを選択



- ②グループのデバイス「開通時初期設定」を選択し、 「セキュリティエージェントの追加」を クリックします。
- ※「開通時初期設定」とは、お申込み時に申請いただいた 内容の設定情報を反映させたポリシーグループになります。 新たなポリシーを作成する際は、「グループの追加」より、 作成いただくことが可能です。
- ※「開通時初期設定」がない場合は「デバイス(初期設定)」を選択 してください。
- ※サーバヘインストールする際は、サーバ用のポリシーグループを 選択ください。



17

③インストール方法の選択画面にて、1つ目の項目にある メールの詳細表示をクリックします。



10. インストール (Windows) 1/2

【メールを使用してインストールをする方法】 ①1つ目の項目にある「インストーラリンクの送信」を クリックします。

 ②インストール用のリンクを確認します。
 Windows コンピュータヘインストールする場合、この インストール用のリンクをクリックしてインストールを 開始します。

③「インストーラーリンクの送信」から、自動で作成された メールを送付し、エンドポイント側でリンクをクリックして インストールを実施します。 また、「メールコンテンツの表示」から「コンテンツのコピー」で 内容をコピーしてメモ帳などに保存したものを配布して インストールにご利用いただくこともできます。

④メールからリンクをクリック、またはブラウザを開きリンクを 入力して以下の画面から[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ていきます。

※注意 ハードディスク空き容量が約800MB必要となります。容量不足のエラーメッセージ が表示される場合は、空き容量を確保し、再度インストールを実行します。

⑤次をクリックします。

⑥インストールが開始されます。

⑦インストールが完了するまで待ちます。



10. インストール (Windows) 2/2

8「インストールに成功しました」のメッセージが 表示されますので、「終了」をクリックします。

インストール作業は以上となります。

🦻 ウイルスパスター ビジネスセキュリティサービス	-		×
	t	TR	END cro
✓ インストールに成功しました。			
ウイルスバスター ビジネスセキュリティサービス用ビジネスセキュリティクライ トールされました。	アントは	正常にイ	גע
[終了] をクリックして、 インストールプログラムを閉じます。			
終了	++)	ノセル	

[参考] インストールが完了したデバイスは、ご利用PCのタスクトレイ上のアイコンと、 管理コンソールの「デバイス」画面にてご確認いただけます。

[タスクトレイ上のアイコン]



[管理コンソールのデバイス画面]
-----------------	---

≡	TREND Worry Free Business Security Services								
ର	セキュリティエージェント	ŀ	計開通時初期設定 セキュリティエージェント: 3						すべてのステー
50	🖵 すべてのセキュリティエージェ	3							
R	🔺 🚞 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	国 タスク ▼		
	サーバ (初期設定)	0	□ エンドポイント ↑	種類	前回の接続日時	IPv4アドレス	MACアドレス	IPv6アドレス	オペレーティングシステム
	デバイス (初期設定)	0		Android	31分前	-			Android 9
Θ	-	0		Windows	3日前				Win 10 Enterprise (10.0.19045)
		0		Android	90日以上前			-	Android 13
÷	開通時初期設定	3							
	Ξ 最新のパターンファイルを使用	1							
	Ξ ビジネスセキュリティサービス	0							

11. インストール (Mac OS) 1/14

 インストーラーリンクの送信」からメールで送られた インストール用のリンクをクリックするか、 「インストーラのダウンロード」「このエンドポイントに インストール」にて右の画面を開き、「ダウンロード」を クリックします。 その後、インストーラ(WFBS-SVC_Agent_Installer.zip) のダウンロードが開始されます。

②ダウンロード完了後、「WFBS-SVC_Agent_Installer.zip」 内の「WFBS-SVC_Agent_installer.pkg」をクリックし、 インストールを実行します。

※注意

ハードディスク空き容量が64MB以上必要となります。容量不足のエ ラーメッセージが表示される場合は、空き容量を確保し、再度インストー ルを実行します。

〈以下のようなメッセージが出た場合〉

インストールパッケージを ["]control" キーを押したまま クリックし、「開く」を使い実行します。

この方法はファイルを実行する時だけGateKeeper機能を無効にすることができます。





	000	فر بې 📴 💷 🔤 📰 🔁	×□−ド × 1 0	Q. 検索		
よく使う項目	名約		サイズ	種類	追加日	~
AirDrop	¥ 📄	WFBS-SVC_Agent_Installer		フォルダ	今日 14:58	
		Identifier plist	380 /G/ h	プロパティリスト	今日 14:58	
 最近使った項目 ペ アプリケーション 	L	😺 WFBS-SVCstaller.pkg	95.5 MB	インス…ッケージ	今日 14:58	
🛄 デスクトップ						
四日 御御						
● ダウンロード						
18.76						



11.インストール (Mac OS) 2/14

③「続ける」をクリックし、インストールを進めます。

④「ようこそTrend Micro Securityインストーラへ」画面で 「続ける」をクリックし、インストールを進めます。

⑤「サーバーへの接続をテスト」画面で「続ける」をクリックします。

	このパッケージは、ソフトウェアをインストールでき ちかどうかを判断するプログラムを実行します。 のコンピュータのセキュリティを保護するには、必ず信頼で る提供元のプログラムやソフトウェアのみを実行したりイン トールしたりしてください。このソフトウェアの提供元の信 性を確信できない場合は、"キャンセル"をクリックして、プ グラムの実行とソフトウェアのインストールを中止してくだ い。
•	キャンセル 続ける
 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 	ようこそTrend Micro Security Agentインストーラへ このインストールプログラムでは、Trend Microセキュリティエージェ ントのインストールに必要な手順についてご案内します。 [続ける] をクリックして次に進んでください。
TOTAD	



11. インストール (Mac OS) 3/14

⑥「インストール」をクリックします。

⑦「インストール」が実行されます。

	"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 低更 大切な情報 	この操作には、コンピュータ上に114 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。	
TREND	夏る、インストール	-

0 😑 0	😜 Trend Micro Security Agentのインストール 🔒
 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 インストールの種類 インストール 概要 大切な情報 	Trend Micro Security Agentのインストール パッケージスクリプトを実行中
	戻る 続ける

11.インストール (Mac OS) 4/14

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

⑨macOS 10.14.x Mojave以降で新規インストールを実施した場合、右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、追加で必要な権限のセットアップをご実施ください。なお、ご利用のOSによって必要な作業が異なりますので、下記手順のうちご利用のOSに合わせた手順の実施をお願いいたします。





11. インストール (Mac OS) 5/14 macOS10.14.x~15.x

macOS 10.14.x Mojave以降 ~ macOS 10.15.x Catalina以前のOSをご利用の場合

10「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。

10-1.「セキュリティとプライバシー」画面を開きます。

10-2. 「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。



10-3. [続行]をクリックします。

💡 許可ボタンについて

「セキュリティとプライバシー」にはインストール 後30分間「許可」ボタンが表示されます。 その間に許可をしなかった場合は、macOSを再起動 することで再度「許可」ボタンが表示されます。

11.インストール (Mac OS) 6/14 macOS10.14.x~15.x

①「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。

11-1. 「セキュリティとプライバシー」画面を開きます。「セキュリティとプライバシー」画面を開きます。

10-2. [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。

11-3. 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。

①-4.「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。

①-5. 「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。

11-6. 「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。



11. インストール (Mac OS) 7/14 macOS10.14.x~15.x

12 [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。

13インストールが完了するとMacのアプリケーション内に以下のように表示されます。

Macエージェントを以前にインストールしたことがある場合、上記手順を実施することで、iCoreServiceが複数登録された状態になる場合がありますが、 そのままご利用いただいて問題ありません。





11. インストール (Mac OS) 8/14 macOS 12.x 以前

macOS 11 Big Sur 以降 ~ macOS Monterey 12.x 以前のOSをご利用の場合

10「システム拡張機能を許可」の画面で画面の指示に したがって設定を行います。

10-1. 「セキュリティとプライバシー」画面を開きます。

⑩-2.「一部のシステムソフトウェアでは、使用する前に確認が求められます。」と記載がある横の「詳細」ボタンをクリックします。

10-3. リストから「iCoreService」の項目をすべて選択し、[OK] をクリックします。

	Trend Microセキュリティエージェント	
の要な権限	システム拡張機能を許可	
システム拡張機能	Trend Microセキュリティエージェントで不正プログラムやセキュリティ ークアクティビティを保護するには、システム拡張機能が必要です。	脅威からファイルおよびネットワ
フルディスクアクセス	1. [セキュリティとプライパシー]を開く	
	 変更を行うには、左下にあるカギのアイコンをクリックし、 macOS管理者のパスワードを入力します。 	0
	3. [セキュリティとプライバシー] で [詳細] をクリックします。	
	 リストから「ICore Service」の項目をすべて選択し、[OK]を クリックします。 	:
	 ネットワークアクティビティのフィルタを許可するには、(許 可)をクリックします。 	0
	h	
	(FR) (る 載行

以下の開発元のシステム シフトウ システムを再起動する必要があり	ェアかアッフ ます。	テートされまし	た。使用する則に
iCore Service			
iCore Service			
		العامية مدعام	OK

11. インストール (Mac OS) 9/14 macOS 12.x 以前

10-4. ^{*m*}iCoreService^{*m*}がネットワークコンテンツの フィルタリングを求めています」と表示されるので、 [許可] をクリックします。

10-5.「システム拡張機能を許可」の画面に戻り、[続行]をクリックします。

①「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。

11-1. 「セキュリティとプライバシー」画面を開きます。

11-2.[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。

11-3. 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。

11-4. 「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。





11. インストール (Mac OS) 10/14 macOS 12.x 以前

①-5.「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。なお、下記画面が表示された場合は[あとで行う]をクリックしてください。

①-6. [フルディスクアクセス]の一覧に
 「iCoreService」「Trend Microセキュリティエージェント」「TrendMicro Extension」が表示されており、チェックがついていることを確認します。
 チェックがついていない場合は、チェックを付けてください。

11-7. 「セキュリティとプライバシー」画面を閉じ、 「フルディスクアクセスを許可」の画面で [続行] をク リックします。

② [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。

1³インストールが完了するとMacのアプリケーション内に以下のように表示されます。



11. インストール (Mac OS) 11/14 macOS 13.x 以降

macOS Ventura 13.x 以降をご利用の場合

10「システム拡張機能を許可」の画面で画面の指示に したがって設定を行います。

10-1. 「セキュリティとプライバシー」画面を開きます。

⑩-2.「一部のシステムソフトウェアでは、使用する前に確認が求められます。」と記載がある横の「詳細」ボタンをクリックします。

10-3. リストから「iCoreService」の項目をすべて選択し、[OK] をクリックします。

	Trend Microセキュリティエージェント	
必要な権限	システム拡張機能を許可	
システム拡張機能	Trend Microセキュリティエージェントで不正プログラムやセキュリティ ークアクティビティを保護するには、システム拡張機能が必要です。	脅威からファイルおよびネットワ
フルディスクアクセス	1. [セキュリティとプライパシー] を開く	
	 変更を行うには、左下にあるカギのアイコンをクリックし、 macOS管理者のパスワードを入力します。 	0
	3. [セキュリティとプライバシー] で [詳細] をクリックします。	
	 リストから「iCore Service」の項目をすべて選択し、[OK] を クリックします。 	·
	 ネットワークアクティビティのフィルタを許可するには、(許可)をクリックします。 	0
	*	
	ta .	じる 執行

iCore Service	.9.		
iCore Service			

11. インストール (Mac OS) 12/14 macOS 13.x 以降

エンドポイント/EDRセキュリティ

 ⑩-4「["]iCoreService["]がネットワークコンテンツの フィルタリングを求めています」と表示されるので、
 [許可]をクリックします。

10-5. 「システム拡張機能を許可」の画面に戻り、 [続行] をクリックします。

①「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。

10-1. [フルディスクアクセスを開く] をクリックし、フルディスクアクセスの画面を開きます。

①-2.「フルディスクアクセスを許可」の画面に戻り、
 2番の[ファイルの場所を開く]をクリックして表示された「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。

①-3.「フルディスクアクセスを許可」の画面に戻り、
 3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。



11. インストール (Mac OS) 13/14 macOS 13.x 以降

①-4. 「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。

11-5. 「フルディスクアクセスの画面においてそれぞれの切り替えスイッチが有効になっていることを確認後、「フルディスクアクセスを許可」画面の[続行]をクリックします。

12 [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。

1³インストールが完了するとMacのアプリケーション内に以下のように表示されます。

Macエージェントを以前にインストールしたことがある場合、上記手順を実施することで、iCoreServiceが複数登録された状態になる場合がありますが、そのままご利用いただいて問題ありません。





登録の確認

①管理コンソールに再度、ログインします。



 ②「セキュリティエージェント」メニューをクリックし、 「すべてのセキュリティエージェント」、 「手動グループ」または配下の任意のグループ内の 表示された画面内にインストールを実施したMacが 登録されていることを確認します。

	登録情報を入力してください
	パスワード:
医结本防御	パスワードをお忘れの場合
E30 C101+	

事前準備

EDRセキュリティのアプリケーション(アプリケーション名: Trend Micro XDR Endpoint Sensor)は、 EDRセキュリティをご契約のお客様かつエンドポイントセキュリティがインストールされているMac端末に 自動インストールされます。

インストール後、EDRセキュリティの機能をご利用いただくには、EDRセキュリティ契約時の追加手順 (Mac OS) (3~45P)に沿った設定が必要となりますので、恐れ入りますがご確認のうえ、対応ください。 なお、エンドポイントセキュリティのインストール後、EDRセキュリティの自動インストールまで1営業日かかりますので、 ご了承ください。

また、一度インストールしたEDRセキュリティ アプリケーションをアンインストールされる場合、 サポートセンターでの処理も必要となりますので、大変お手数をおかけしますが、サポートセンターまでご連絡を お願いいたします。

13. EDRセキュリティ契約時の追加手順(Mac OS) 1/11

EDRセキュリティ

①EDRセキュリティのアプリケーション (アプリケーション名:Trend Micro XDR Endpoint Sensor)が 自動インストールされると、 Mac端末上に権限のセットアップ画面が表示されます。

②「Continue」をクリックして権限のセットアップ作業を実施します。 ※Closeボタンを押した場合は、端末上に表示されている 「Trend Micro XDR Endpoint Sensor」アプリをクリックしていただ きますと、再度設定画面を開くことが可能です。



13. EDRセキュリティ契約時の追加手順(Mac OS) 2/11

EDRセキュリティ

③「機能拡張がブロックされました」が表示されるので、
 「OK」をクリックします。

④「Continue」をクリックして権限のセットアップ作業を実施 します。




13. EDRセキュリティ契約時の追加手順(Mac OS) 3/11

⑤「Allow System Extension」が表示されるので、 「1.Open Security & Privacy」をクリックします。

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

EDRセキュリティ

⑥「セキュリティとプライバシー画面」が表示されるので、
 ロックされている場合はカギマークをクリックしてロック解除をします。



13. EDRセキュリティ契約時の追加手順(Mac OS) 4/11

EDRセキュリティ

⑦「ロックの解除について」許可を求められる画面が表示 されますので、「パスワードを使用」をクリックします。



⑧パスワードを入力して、「ロックを解除」をクリックします。



13. EDRセキュリティ契約時の追加手順(Mac OS) 5/11

⑨「使用する前にシステムの再起動する必要があります」の画面が表示されましたら、「iCoreService」の項目をすべて選択し、[OK]をクリックします。



①「System Extension」の設定が完了しましたので、
 「Continue」をクリックします。
 「Full Disk Access」に進みます。

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

13. EDRセキュリティ契約時の追加手順(Mac OS) 6/11

①「1.Open Security & Privacy」をクリックします。

12「セキュリティとプライバシー」の画面が表示されますので、「フルディスクアクセス」が選択されていることを確認します。
 ※ロックされている場合は、カギマークをクリックしパスワード入力してロックを解除ください。
 Allow Full Disk Access画面に戻ります。





13. EDRセキュリティ契約時の追加手順(Mac OS) 7/11

EDRセキュリティ

「4.Open File Location」をクリックすると、
 「com.trendmicro.icore.es.systemextension」が
 表示されます。

 ①「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。





13. EDRセキュリティ契約時の追加手順(Mac OS) 8/11

EDRセキュリティ



●●● < > !!!! セキュ	リティとプライバシー		< > Resources	88 📰 🖽
		よく使う項目	名前	> 変更日
一般 FileV	ault ファイアウォール プライバミ	AirDrop	X Applcon.icns	2023年11月21日 1
		 ・ ・	Assets.car	2023年11月21日 1
J 710	下のアプリケーションに、このMa	▲ アプリケ…	> 🛅 Base.lproj	2023年11月21日 16
	ル、メッセージ、Safari、ホーム、		en Iproi	2023年11月21日 16
山山音声認識	ップなどのデータや特定の管理設定	□ デスクト…	iCore Security.app	今日 17:59
did my man		▶ 書類	InfoPlist.strings	2023年11月21日 16
アクセンビリティ		O Keye	> 📩 ja.lproj	2023年11月21日 1
	Trend Micro XEn		XDR_for_Mac_Licenses.rtf	2023年11月21日 16
入力監視	EndpointBasecam	墙所	and the second se	
フルディスクアクセス	V 🕖 iCore Service	Miacintos	[
ファイルとフォルダ	Trend Micro Extern	41		
画面収録	ł	● レッド		
	+ -	● オレンジ		
メディアとApple Music		- 1ID-		

⑥「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。
 Allow Full Disk Access画面に戻ります。

13. EDRセキュリティ契約時の追加手順(Mac OS)9/11

EDRセキュリティ



18「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。

①「6.Open File Location」をクリックします。

●●● く 〉 !!!! セキュリテ	ティとプライバシー	•••	< > アプリケーション	88 📰 Œ
一般 FileVault	t ファイアウォール プライバシー	よく使う項目	名前	変更日
		AirDrop	X Trend Micro XDR Endpoint Sensor.app	今日 17:59
1 211	下のアプリケーションに このMacd	④ 最近の項目	Irond Microセキュリティエーシェント.app	今日 17:18
Y X Y	ル、メッセージ、Safari、ホーム、T	▲ アプリケ…	Safari.app	今日 2:02
山山音声認識	ップなどのデータや特定の管理設定へ		💿 🌠oogle Chrome.app	一昨日 7:35
ald. Hy prime		□ デスクト…	App Store.app	2020年1月1日 17:00
アクセンビリティ	Trend Micro Extense	● 書類	Automator.app	2020年1月1日 17:00
			FaceTime.app	2020年1月1日 17:00
入力監想	Trand Miara Evtanat		🕍 Font Book.app	2020年1月1日 17:00
		14.15	🔢 Launchpad.app	2020年1月1日 17:00
		O Masiatas	🗊 Mission Control.app	2020年1月1日 17:00
	V V ICore Security	Macintos	🚱 Photo Booth.app	2020年1月1日 17:00
- ファイルとフォルダ	0	@ ネットワ…	🔞 Podcast.app	2020年1月1日 17:00
	✓ 🥑 Trend Microセーティ		QuickTime Player.app	2020年1月1日 17:00
(二) 画面収録		タグ	Siri.app	2020年1月1日 17:00
	·	● レッド	Time Machine.app	2020年1月1日 17:00
		● オレンジ	TV.app	2020年1月1日 17:00
			😭 イメージキャプチャ.app	2020年1月1日 17:00

13. EDRセキュリティ契約時の追加手順(Mac OS) 10/11

EDRセキュリティ

19「Trend Micro XDR Endpoint Sensor.appには、 終了するまでフルディスクアクセスがありません」の 画面が表示されましたら、「あとで行う」をクリック します。

②「OK」をクリックしましたらセットアップは以上になります。

※OSバージョン10.15では、端末再起動が必要です。 ※19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。





EDRセキュリティ

 ④インストールが完了すると、タスクバーに 「Trend Micro XDR Endpoint Sensor」 が追加されます。
 別途インストールしたエンドポイントセキュリティ アプリ(VBBSS)

をクリックして開きます。

20ツールバーエージェントコンソール上「Endpoint Sensor」のステータスがグリーン(有効)になります。

※未インストールや、「Endpoint Sensor」が無効の 場合はグレー表示します。





14. インストール(Android)1/17

エンドポイントセキュリティ

①Android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。

右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。 ※インストールが始まり、「インストール中…」が 表示されます。

②インストールが完了したら、「開く」をタップします。

※「開く」をタップ後、Mobile Securityが起動し、 「どの機能を使用しますか? ウィルス対策 or すべての機能」と表示された場合は

「すべての機能」を選択し、「続行」をタップします。





14. インストール(Android)2/17

エンドポイントセキュリティ

③Mobile Security for Businessが起動し、 「サインインしています… しばらくお待ちください。」と 表示されるため、待ちます。

Mobile Security for Business サインインしていま す... しばらくお待ちくだ さい。

パージョン: 2.0.0.1180

④右のような画面が表示されるため、画面下部の 「続行」をタップします。

← 設定が必要です
デバイスを保護するには、会社がこれ らの権限にアクセスする必要がありま す。
▲ デバイス管理者
リモート検索、ロック、消去、およ びパスワードポリシーを有効にす るには、デバイス管理者でMobile Securityを有効にします。 注意: Mobile Securityをアンインス トールする場合は、この設定を無効 にするか、Mobile Securityのアンイ ンストールメニューを使用してくだ さい。
團 位置情報
Mobile Securityは位置情報データを 収集し、アプリが開いていないとき にリモート管理でデバイスを追跡し ます。
↓ 電話番号を読み取る
電話番号を読み取るには権限が必要 です
■ バックグラウンドで実行
続行

⑤デバイス管理者画面にて「許可」をタップします。



14. インストール(Android)5/17

⑥「デバイス管理アプリの有効化」画面が表示されるため、 下へスクロールします。

⑦「デバイス管理アプリの有効化」画面下部に表示されている、「このデバイス管理アプリを有効にする」をタップします。

デバイス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 行してデバイス内のデータを消 去します。

画面ロックの変更 画面ロックを変更します。

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 すべてのデバイスカメラを使用 できないようにします。

このデバイス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

14. インストール(Android)6/17

エンドポイントセキュリティ

⑧位置情報画面にて「許可」をタップします。

⑨位置情報へのアクセス許可を求められるため、「アプリの使用時のみ」をタップします。



アプリの使用時のみ

今回のみ

許可しない

14. インストール(Android)7/17

エンドポイントセキュリティ

⑩「電話番号を読み取る」画面にて、「許可」を タップします。

①電話の発信と管理の許可を求められるため、 「許可」をタップします。



14. インストール (Android) 8/17

エンドポイントセキュリティ

12「バックグラウンドで実行」画面にて、「許可」を タップします。

13アプリにバックグラウンドでの実行について許可を 求められるため、「許可」をタップします。



14. インストール(Android)9/17

(1)「通知へのアクセス」画面にて「許可」をタップします。

 (15)「通知へのアクセス」画面にて「Mobile Security」を タップします。
 ※一覧に「Mobile Security」のアプリが、

表示されていない場合は画面を下へスクロールし、 確認してください。

÷	設定が必要です	
	Ļ	
	通知へのアクセス	
	5/7	
Mob セス	ile Securityのシステム通知に するには権限が必要です	こアク
	許可	
	許可	
<pre></pre>	許可 通知へのアクセス	Q
÷	許可 通知へのアクセス	Q
 	許可 通知へのアクセス Mobile Security	Q

14. インストール (Android) 10/17

①「通知へのアクセス」画面にて、「通知へのアクセスを
 許可」のトグルボタンをタップし、ONにします。
 ※右図はOFF状態です。

①トグルボタンをONにすると、右のような画面が表示されます。「許可」をタップし、通知へのアクセスを許可します。

いたいです。 Mobile Security 通知へのアクセスを許可

通知へのアクセス

4



Q

14. インストール(Android)11/17

エンドポイントセキュリティ

18「他のアプリの上に重ねて表示」画面にて、「許可」を タップします。

19「他のアプリの上に重ねて表示」設定画面にて、
 「Mobile Security」をタップします。
 ※一覧に「Mobile Security」のアプリが、
 表示されていない場合は画面を下へスクロールし、
 確認してください。

← 設定が必要です
他のアプリの上に重ねて表示
6/7
セキュリティリスクの検出時にアラー トを表示するには権限が必要です
許可



14. インストール(Android)12/17

エンドポイントセキュリティ

⑩「他のアプリの上に重ねて表示」画面で、トグルボタンを タップし、ONにします。 ※右図はOFF状態です。

 アグルボタンをONにすると、「ユーザ補助」画面が表示 されるため、「許可」をタップします。





14. インストール(Android)13/17

エンドポイントセキュリティ

迎ユーザ補助画面にて「Mobile Security」をタップ します。



③「Mobile Securityを使用」のトグルボタンをタップし、
 ONにします。
 ※右図はOFF状態です。

← Mobile Security	
Mobile Security を使用	
オプション	
Mobile Securityの ショートカット _{OFF}	

14. インストール (Android) 14/17

エンドポイントセキュリティ

迎右のような画面が表示されるため、「許可」をタップし、 デバイスのフルコントロールを許可します。



14. インストール (Android) 15/17

エンドポイントセキュリティ

²⁵仕事用メールアドレスを入力後、「続行」をタップします。

※入力したメールアドレスが管理コンソールの エンドポイント項目に表示されるアカウント名と なります。



14. インストール (Android) 16/17

エンドポイントセキュリティ

⑩インストール完了です。
 ※端末のホーム画面にて「Mobile Security」の
 アイコンが表示されます。





■登録の確認

①管理コンソールにアクセスし、ログインします。 ユーザ登録時に設定した「ログインID」と「パスワード」 を入力して、「ログイン」ボタンをクリックします。

②「セキュリティエージェント」タブをクリックし、表示 された画面内にインストールを実施したAndroidデバイス が登録されていることを確認します。

	登録情報を入力してください
	ロダインID:
	パスワード:
	パスワードをお忘れの場合
登録を簡単	ロヴインIDを記憶する

15. 新エージェントへ移行(Android)1/7

エンドポイントセキュリティ

Android端末にてエンドポイントセキュリティの旧エージェントを使用している方は 新エージェントへの移行作業を必ず実施してください。 ※ エンドポイントセキュリティは「ウイルスバスタービジネスセキュリティサービス」を指します。

■新エージェント概要

- Google Playにエージェントを掲載
- ・エージェントコンソールの全体デザインの変更

■移行対象者

Android端末にてエンドポイントセキュリティ バージョン 9.X をご利用中の方。 (2023/7/31 より前に公開されたバージョンをご利用中の方)

■移行対象期間

2023/8/29 ~ 2024/8/31 ※2024年9月1日からエンドポイントセキュリティ バージョン(9.X)はサポート対象外となります。

■移行時の注意事項

移行完了後、ログ情報を含む旧エージェント情報はWeb管理コンソール上から削除されます。

【参考】バージョン確認方法 Android端末で下図を参考にご確認ください。







■移行手順

①PCにて管理コンソールヘログインします。その後、「セキュリティエージェント」タブを選択し、 手動グループのデバイスにて「開通時初期設定」※を選択します。 その後、「セキュリティエージェントの追加」を選択します。

<	🥭 TRENDI 🛛 ウイルスバスター	ビジネスセキュリティサービス	※「開通時初期設定」とは、お申込み時に 申請いただいた内容の設定情報を
の ダッシュボード	セキュリティエージェント 📑	開通時初期設定	反映させたポリシーグループになります。
「」 セキュリティエー…	🖵 すべてのセキュリティエージェ 🕦	セキュリティエージェント: 1	作成したポリシーグループをご指定くださ
Ω ¬-+f	🔺 🚞 手動グループ	+ セキュリティエージェントの追加 🛞 検索 -	υ) <u>。</u>
	サーバ (初期設定) 0	□ エンドポイント↑ 前	
影 ポリシー	デバイス (初期設定) 0		
Q 1#-1	開通時初期設定 1]	

「セキュリティエージェントのインストール方法」画面が表示されるため、 「メールコンテンツの表示」を選択します。



②メールコンテンツ画面が表示されるため、「QRコードのダウンロード」を選択しQRコードを ダウンロードします。

メールコンテンツ	コンテンツをコピー	QRコードのダウンロード
次のリンクをクリックし、手順に従っ い。	てセキュリティエージェント	~をインストールしてくださ
ttp://www.instructure.com/	/lits/suc/download/ja/view	
Sectivation requireksid=EMpkornMexFS	MERSK3IECOCYCC2%/N1A	ehrwite Hitelân 3612/PwyW
.22*1=AUKM0Li,Vkq.22H,Wk9RUKV	Disi <mark>ngPE</mark> C7WHjort8WwqaZe	Mich 899900 98510 5571124 A8161
52cowDV_400mTgjKg%37%sD8gid-	maar filmaata90	
リンクの有効期限:	-	
認証コード (iOS/Chromebook登録用):		
認証コードの有効期限:		

その後、ダウンロードしたQRコードをAndroid端末にて読み込みます。 インストール画面が表示されるため、本マニュアルの 「14.インストール(Android)1/17 ~15/17」を参照し、インストール作業を行います。

※「14.インストール(Android) 15/17」実施後は次ページの③へ進んでください。

15. 新エージェントへ移行(Android)4 / 7

エンドポイントセキュリティ

③「14.インストール(Android)15/17」を実施後、 旧エージェントのアンインストールを促す通知が表示され るため、「続行」を選択します。



15. 新エージェントへ移行(Android)5 / 7

④「このアプリをアンインストールしますか?」と 表示されるため、「OK」を選択します。

VBBSS このアプリをアンインス トールしますか? キャンセル OK

⑤アプリのホーム画面下に「VBBSSをアンインストール しました」と表示されたことを確認します。 ※通知は数秒で消えます。

Android端末のホーム画面にて旧バージョンのアプリアイコンが 削除され、新バージョンのアプリアイコンが追加されます。

旧バージョン







⑥初回スキャン後、移行完了となります。⇒次ページの「移行後の確認事項」をご確認ください。





15. 新エージェントへ移行(Android)6 / 7

■移行後の確認事項

旧エージェントにて下図の赤枠部分を有効にしていた場合、設定は移行されないため、再度設定を行う必要があります。

①管理コンソール上にて「リアルタイム不正プログラム検索、Webセキュリティ設定」を チェック後、設定を保存してください。

【管理コンソール > セキュリティエージェント > 任意のグループ > ポリシーの設定 > Androidのアイコン > 権限およびその他の設定 】

ポリシーの設定: デバイス (初期設定)		
☆ 対象とサービスの設定	権限およびその他の設定 指定した設定をセキュリティエージェント上で有効化/無効化または実行することをユーザに許可します。	
 検索設定 Webレビュテーション パスワード 承認済み/ブロックするURI 	 □ リアルタイム不正プログラム検索、Webセキュリティ設定 ③ □ パスワード/リモート管理設定 ④ 	
権限およびその他の設定		
	保存キャンセル	

⇒次ページに進んでください

15. 新エージェントへ移行(Android)7 / 7

②Android端末にて「Mobile Security」アプリを起動後、画面下部の「設定」を選択します

③表示された一覧から「ポリシー設定」を選択します。

④「①」の手順にて設定権限を与えた、「リアルタイム不正プログラム検索、Webセキュリティ設定」について、任意の設定を行ってください。
 ※右図は「不正プログラムのリアルタイム検索」設定の例です。









16. 新エージェントへ移行(iOS)1/6

iOS端末にてエンドポイントセキュリティの旧エージェントを使用している方は、必ずアンインストールを実施してください。その後、新エージェントへの移行作業を実施してください。 ※ エンドポイントセキュリティは「ウイルスバスタービジネスセキュリティサービス」を指します。 ※ ご新規ユーザーの方は「18.インストール(iOS)事前準備」へお進みください。

■エンドポイントセキュリティ 旧エージェント(Ver2.0未満)をご利用中の場合は、 下記手順の実施をお願いします。

- •17. 証明書の更新について
- ・16. 新エージェントへ移行(iOS)
- •18. インストール (iOS) 事前準備
- •19. インストール (iOS)

■新エージェント概要

①各機能の追加

- •Webレピュテーション
- Wi-Fi保護
- ・設定マネージャ
- ・モバイル検索
- ・承認済み/ブロックするURLリスト

②アプリタイプのエージェントとして登場

■移行対象者

iOS端末にてエンドポイントセキュリティ バージョン(2.0未満)をご利用の方

■移行対象期間

2024年4月22日~2025年4月30日 ※2025年5月1日からエンドポイントセキュリティ バージョン(2.0未満)はサポート対象外と なります。

16.新エージェントへ移行(iOS) 2/6

※旧エージェントのアンインストールを行います。 下記いずれかの手順にてアンインストールを実施してください

- ・Web管理コンソールからアンインストールする場合
 該当ページ「16.新エージェントへ移行(iOS) 2/6~4/6」
- iOSデバイスからアンインストールする場合
 該当ページ「16.新エージェントへ移行(iOS) 5/6~6/6」

■移行手順 Web管理コンソールからアンインストールする場合

管理者がWeb管理コンソールから操作します。

①パソコンのブラウザ(Google ChromeまたはSafari)にて、 管理コンソールにアクセスします。

②ログインIDとパスワードを入力し、 「ログイン」ボタンをクリックします。

登録情報を入力してください
ログインID:
パスワード:
パスワードのリセット (パスワードをお忘れの場合)
▼ ログインIDを記憶する
ロダイン

エンドポイントセキュリティ

■移行手順 Web管理コンソールからアンインストールする場合

③登録済みの製品/サービスから「ウイルスバスター ビジネスセキュリティサービス」欄を確認し、 「コンソールを開く」をクリックします。

C TREND Licensing N	lanagement Platform	Powered by 💋 IREND.					4	•
登録済みの製品/サービス ヘルブ ▼								
製品/サービス								
+キーの入力								
サービスブラン名	⇒ 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 🔻	アケション	_
•	ウイルスバスタービジネス	セキュリティサービス 🍈	15 シート	製品版	2024/01/15	自動更新	🕑 コンソールを開く	
					•	有効期限内	🔒 間七द<期限切れ 🛛 😒 有効期	表切れ

④メニューから [セキュリティエージェント] をクリックし、表示された一覧からアンインストールを 行いたいエンドポイント(iOS)のチェックボックスにチェックを入れ、[タスク] → [セキュリティエー ジェントのアンインストール] をクリックします。

C 10.37 UTC+09.00 C 1.37 UTC+09.00 C 1											
セキュリティエージェント	=	すべてのセキュリテ	ジェント			すべてのステータス • 検索 Q 〒					
🖵 すべてのセキュリティエージェ	. 4	セキュリティエージェント:4									
4 🚞 手動グループ		+ セキュリティエージェントの追加	●検	索 - 目 グロー	バル設定	目 タスク -				0 0	
サーバ (初期設定)	0	 エンドポイント↑ 	種類	前回の接続日時	IPv4アドレ	エクスポート		オペレーティングシステム	ステータス	アーキテクチャ	
デバイス (初期設定)	(1)		-			今すぐアップデート		Android 9	正常		
	0	1.0.000	-		-	m = n	d694:13:1e12:1cfb	Win 10 Enterprise (10.0.19045)	オフライン	x64	
	0	and the second second	-	1011.08		相与1L 復号		Android 13	正常		
	0	A Descention of the	-			≤動グⅡ_ブニ診動		iOS 16.7.7	正常		
關通時初期設定	3										
Ξ 最新のパターンファイルを使用	. 1					セキュリティエージェントのアンインストール					
Ξ ビジネスセキュリティサービス	. 0						-				
		4									
■移行手順 Web管理コンソールからアンインストールする場合

⑤ポップアップが表示されますので [アンインストール] をクリックします。



⑥「コマンドが送信されました」のメッセージがコンソール上に表示されます。 クライアントツリーからも該当のクライアントが消えます。

Web管理コンソール上での作業は以上で終了です。iOS側での操作は必要ありません。

■移行手順 iOSデバイスからアンインストールする場合

iOSデバイス上で操作します。

①[設定] > [一般] > [プロファイルとデバイス管理] を開き、「Trend Micro Worry-Free Business Security Service」をタップします。

②「削除」をタップし、パスコードを入力します。





16.新エージェントへ移行(iOS) 6/6

■移行手順 iOSデバイスからアンインストールする場合

③ [プロファイル] から削除されます。iOSデバイス上での操作は以上です。

※iOSデバイス上のアンインストールをネットワークに未接続の状態で行った場合、 Web管理コンソールのクライアントツリーにデバイス情報が残ったままとなります。 別途削除してください。

17.証明書の更新について 1/4

iOSデバイスを管理するために、エージェントのインストールと有効なAPNs証明書が必要になります。 APNs証明書の有効期限は1年間有効となりますので、必ず期限が切れる前に更新いただきますよう お願いいたします。

有効期限につきまして、Web管理コンソールの 以下設定により、証明書イベントを通知することもできます。(デフォルトは有効) [管理] > [通知] > [要確認]タブ > 「Apple Push Notification Service証明書イベント

■ ØTRENDI ウイルスバスタービジネスセキュリティサービス			
0	管理	ウイルス対策 - 解決されていない脅威	
		ウイルス対策 - リアルタイム検索無効	
50	一般設定	スパイウェア対策 - 解決されていない脅威	
ය	モハイルテハイス登録設定		
_	通知	システムイベント	
2	レポート設定	種類	メール通知
Θ	Active Directoryの設定	アップデート - アップデートが必要なエージェント	
	Smart Protection Network	Smart Protectionサービス - 接続されていないエージェント	
	回復キーのバスワート	ライセンスイベント	
	9-70	種類	メール通知
	ライセンス情報	ライセンス - 有効期限切れ	
	Webコンソール設定	ライセンス - ライセンスの有効期限が残り60日未満	
		ライセンス - シートの使用率が110%を超えています	
		ライセンス - シートの使用率が100%を超えています	
	l l		
		Apple Push Notification Service証明書イベント	
		種類	メール通知
		Apple Push Notification service証明書 - 有効期限切れ	
		Apple Push Notification service証明書 - 取り消されました	
		Apple Push Notification service証明書 - 削除されました	
		Apple Push Notification service証明書 - まもなく有効期限が切れます	

・ 証明書の有効期限の確認画面

	🦻 TRENDボ ウイルスパスター ビジネスセキュリティサービス			
)	管理	モバイルデバイス登録設定		
j _	一般設定	Apple Push Notification Service证明書		
ļ	モバイルデバイス登録設定	10Sデバイスの管理には、特効なAPNs (Apple Push Netification Service) 証明者が必要です。特効な証明書をビジネスセキュリティサービスにアップロードしてください。 注意: ウイルスバスター ビジネスセキュリティサービスで証明書の有効時間が切れる際にメール通知を送信するように設定するには、管理 > 運動に進みます。		
]	レポート設定	証明書の詳細		
)	Active Directoryの設定 Smart Protection Network	รมวามสิต () มอ		
	同復キーのパスワード	有効期限	10000	
	ツール	Apple ID ()		
	ライセンス情報 Webコンソール設定	API6証明書の更新 証明書の削除 Androidあよび905デバイス向けの使用許規契約書 トレンドマイクロでは、使用許規約書をテンプレートとして提供しており、お客様の: キュリティエージェントをインストールするための使用許規約時に開整する必要があい 遅値 カスタマイズ	会社に合わせてデンプレートをカスタマイズすることをお勧めします。使用皆構築的書は、せキ さます。	

 パソコンのブラウザ(Google ChromeまたはSafari) にて、管理コンソールにアクセスし、ログインします。 ユーザ登録時に設定した「ログインID」と 「パスワード」を入力して、「ログイン」ボタンを クリックします。

 コンソールを開く」をクリックしてウイルスバスター ビジネスセキュリティサービスのコンソールを開きます。

③「管理」タブをクリックし、「モバイルデバイス登録 設定」メニューをクリックします。

④登録されている証明書が表示されるため、 「証明書の削除」をクリックします。

Eバイルデバイス登録設定		
pple Push Notification Service羅明書		
iOSデバイスの管理には、有効なAPNs (Apple Push Notification Service) 証明書が必要です。有効な証明書	をビジネスセキュリティサービスにアップロードしてください。	
注意: ウイルスパスター ビジネスセキュリティサービスで証明書の有効期限が切れる際にメール通知を送信	するように設定するには、 管理 > 通知 に進みます。	
証明書の詳細		
シリアル番号()	0.001040	
UD		
有効期限	1010	
Apple ID (3)	to a global a g	
APNs証明書の更新 証明書の削除		

エンドポイントセキュリティ

⑤Apple Push Nodification Service証明書を 削除の確認が表示されますので、 「削除」をクリックします。

```
⑥管理コンソール上で証明書が削除されたことを
確認します。
```



Apple Push Certificate Portal サイト (<u>https://identity.apple.com/pushcert</u>)へ アクセスし、Apple IDを使ってサインインします。 (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。)





エンドポイントセキュリティ

 ⑧ Certificates for Third-Party Servers画面が 表示されますので、該当証明書列の「Revoke」を クリックします。

- ⑨削除するかどうか確認の画面が表示されますので、 「Revoke」をクリックします。
- 1016. 新エージェントへ移行(iOS) 1/6 を参照のうえ アンインストールの手順を実施ください。
- ①<u>19.インストール</u>を参照のうえ インストールの手順を実施ください。

証明書の更新(削除)については、以上になります。 後続の手順にて新規証明書のインストールを行ってください。





18. インストール (iOS) 事前準備 1/5

エンドポイントセキュリティ

Step 1 > APNs 証明書の作成および登録

- パソコンのブラウザ(Google ChromeまたはSafari) にて、管理コンソールにアクセスし、ログインします。 ユーザ登録時に設定した「ログインID」と 「パスワード」を入力して、「ログイン」ボタンを クリックします。
- (2)「コンソールを開く」をクリックしてウイルスバスター ビジネスセキュリティサービスのコンソールを開きます。
- ③「管理」タブをクリックし、「モバイルデバイス登録 設定」メニューをクリックします。
- ④ 「デバイス登録設定」画面が表示されます。「APNs 証明書のアップロード」ボタンをクリックします。
- ⑤「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。

⑥ Appleのサイトで証明書を作成します。
 Apple Push Certificate Portal サイト

 (<u>https://identity.apple.com/pushcert</u>)へ
 アクセスし、Apple IDを使ってサインインします。
 (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。)





	TREND! ウイルスパスタービジネスセキュリティサービス		
	管理	く モバイルデバイス登録設定	
	一般設定	Apple Push Notification Service証明書の更新	
Ľ	モバイルデバイス登録設定	手順1. Trend Micro Certificate Signing Request (CSR)をダウンロードします	
	通知	Trand Micro CSR05ゲンロード	
	UM- NBOE	手順2. Apple Push Notification Service (APNs) 延明書を更新します	
	Active Directoryの設定	1. Apple Push Certificate Portal (https://identity.apple.com/pushcert) にアクセスし、証明書の作成に使用したApple IDでサインインします。	
	Smart Protection Network	2. 更新する証明書を確認します。 a. (Action 別の) [Centificate Into) アイコンをクリックします。 と. Into Action 別の (Centificate Into) アイコンをクリックします。	
	回復キーのパスワード ツール	 UUUアイルルバスター こンネルビイユンティットこんのimeロングールにお水とれていら他と一致していることを確認します。一致している 登録論のOSデバイスをすべて得趣まる設計があります。 c. [Cancel] をクリックして証明書の情報を相じます。 	
		3. [Renew] をクリックします。	
	ライゼンス情報	4. 署名済みのCSR (CSR_signed_by_TrendMicro.b64) をアップロードして、証明書を更新します。	
	Webコンソール設定	5. Apple Push Certificates Portalから証明書をダウンロードします。	
		手順3. APNs证明書をアップロードします	
		証明書 (MDM_Trend Micro Incorporated (Ent)_Certificate.pem) をアップロードします。	
		証明書: ファイルの選択	
		APNs証明書のアップロード	

Apple IDを使ってサインイン	
Apple ID Apple ID	
パスワード	\bigcirc
Apple IDをブラウザに保存	

18. インストール (iOS) 事前準備 2/5

⑦ Get Started画面が表示されます。 「Create a Certificate」ボタンをクリックします。

8 「Terms of Use」画面が表示されます。内容を確認の 上、 [] 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。

「Create a New Push Certificate」画面が表示され (9)ます。「参照」をクリックし、手順1.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。







Apple Push Certificates Portal

ファイルを選択



「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。



 ①管理コンソールへ戻り、⑥で使用したApple IDを入力します。その後、「ファイルの選択」をクリックし、
 ①で作成したAPNs証明書をアップロードします。 アップロードした証明書が表示されます。

	TREND Worry Free" Business Security Services	
	管理	< モバイルデバイス意料設定
🗊 εταυσκατι.	ー級設定 モバイルデバイス脊線設定	新しいApple Push Notification Service証明者 手順1. Trend Micro Certificate Signing Request (CSR)をダウンロードします
& ⊐−# ⊠ #U≥-	通知 レポート設定	Trend Micro CSRのジウンロード 手順2. Apple Push Notification Service (APNs) 注明書を作成します
© иѫ⊣н ⊒ ¤″	Active Directoryの設定 1. Apple Public Certificate Oracle (in the / 近か通道にFireCode y Active Directoryの設定 2. [Create a Certificate (たちリックします。 3. 電気ないため、2. [Create a Certificate (たちリックします。 3. 電気ないため、3. [Create a Certificate (たちリックします。 3. [Create	
() ##	回復キーのパスワード ツール	4. Apple Push Certificates Pental/Poili時間をダウンロードします。 手服3. APNs編明書をアップロードします
	ライセンス休暇 Webコンソール認定	活動さかた成するために任用したApple IDを始まして、活動さ (MOM_Trend Micro Incorporated (Ent)_Conflicate.pem) をアップロードします。 Apple ID にお助き、ファイルの説明、MOM_Trend Micro Incorporated (Ent)_Centificate.pem (1 KB) × Apple (191時のアップロード
		02

①「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します。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保存します。

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面 をご用意していますが、お客様のご利用環境にあわせて 文面を修正してお使いになることをお勧めします。

iOSデバイスを管理するために、エージェントの インストールと有効なAPNs証明書が必要になります。 APNs証明書の有効期限は1年間有効となりますので、 必ず期限が切れる前に更新いただきますよう お願いいたします。

≡	TRENDI ウイルスバスター ビジネスセキュリティサービス	
ର	管理	モバイルデバイス登録設定
۲ <u>ח</u>	一般認定	Apple Push Notification Service証明書
۔ گ اگ	モバイルデバイス登録設定 通知 レポート設定	iOSデバイスの管理には、有効なAPNs (Apple Push Notification service) 証 リティサービスWebコンソールにアップロードしてください。 APNs証明書のアップロード
() ()	Active Directoryの設定 Smart Protection Network	AndroidおよびiOSデバイス向けの使用許諾契約書 トレンドマイクロでは、使用許諾契約書をテンプレートとして提供しており ジェントのインストール中に表示されます。エンドユーザは、セキュリティ
<u>ن</u>	回復キーのパスワード	送信 カスタマイズ

(ター ビジネスセキュリティサービス	() 09 53 UTC=09 80	1 18 Mape, 199 Synt -
ELERATE ADDRESS		
使用許諾契約書テンプレート		
RAI ANNS		
U1 140-0A1 1706		
▲リービスでは、モデメール、際米、名用、お知道水気システムがPRIとのデバイスの営業・デバイスの水セル・ディ とアプリケーションといっと理解したらを把用して「回販データ」とする)を、専門しくためいものとします。	วที่รวรรมกษณะแ-ระว่า และ จากรรมชุด) รักรวกและชุกท	€. FIGLESGLADAH-Adr
2 サービスの発明		
ムリービスにアラセスかつまたは使用するためには、コージはよりービスへの豊好に見かつまたはその後を使用の中で、母菜かった強な サービスへのアクセスと利用のためのアカワント、ユージネ、パスワード、かつまたは用すメールアドレス(1アカワント発展)1分優別	採転を向向することが求められ、ユーザはかかる信都の圧強さを経時することに責任を されるわのとします。ユーザに、目曲のアカウント情報に対しうな差別の身分があり、	は持ちものとします。コーザには、J よってユーザ自身のアカウント体料
を効果に応防したならの物理が行った発展を含め、ユーザのアカウントにおいて起こるすべたの原因に対し、会長任を負きものとします。 e、ここちにも利に満知することに解除します、ユーザが正確な保険を使用しなかったこと、またはアカウント構成のセキュリティを掛け	ユージは、目白のアカウント構成やアカウントが許利なく使用された協会、または他 利しなかったことにななして発生したいかなる場気またな活用に対してた。当社は発行	の何うかの株田伊田に盛灰した場 を負わないものとします。
1 H - P 2044		
ユーガル、場合のをまさまい目的によって、ユーガのモバイルジアイズムのアクセスまたは年かービスの色形が若意または考えたのであ、 されままたは指定たって、当時データが発展されたり分響できないなどを含めこれであまされない参加に対し、当然には一切の美でや4	こと、かいまたは数定料間または多いに内障のことが低くことがあることを早だするも MRがないことに始発します。	02024,2001-94.00
(ZE		
ユーザル、ホサービスのいかな見なかが全要、制品、得たになろうとも、ユーザに対してようないかな活躍三角に対しても知道が出作者 多、かつ次や改善など高量やの時的で、まとしてソフトウェアが実施が考慮的でダウンロードおよびインストールしてもしいであらい次	社会教が違い市のとすることに、問題します。本サービスのあらりる安里に開建し、当 す、オケコーバル、コーゼに入る血サービスの単語の一種としてこれへの回転を当社に	後は、ホワービスの改善、簡化、希 注意すること(そしてユーババニム
		アンプレートがりたい
(4) (株)(株)(株)(株)(株)(株)(株)(株)(株)(株)(株)(株)(株)(

Step 2 > インストール情報の取得

 1「セキュリティエージェント」タブをクリックし、
 表示された画面内の「+セキュリティエージェントの 追加」ボタンをクリックします。

②デバイスの追加画面が表示されます。

該当のデバイスをクリックし、1つ目の項目にある 「メールコンテンツの表示」をクリックします。

③次の2つの情報を取得します。

- ・インストール用のリンク
- ・認証コード

iOSデバイスヘインストールの際、この2つの情報が 必要となります。

「テキストのコピー」で内容をコピーしてメモ帳などに 保存するか、もしくは「メールの送信」をクリックして インストールを行う デバイスへ内容を送信します。

≡	⑦ TREND 『 ウイルスパスタービジネスセキュリティサービス	
<u>୍</u> କ	セキュリティエージェント 📮	すべてのセキュリティエージェント
50	🖵 すべてのセキュリティエージェ 🕚	
ß	🕨 🚞 手動グループ	+ セキュリティエージェントの追加 🛞 検索 🗸 🖹 グローバル設定 🗐 タスク 🔻
	Ξ ビジネスセキュリティサービス 0	
G		

G	セキュリティエージェント 📑	すべてのセキュリティエージュ	:>>	
Q	🖵 すべてのセキュリティエージェ 1	セキュリティエージェント:1		
R	▷ 📷 手動グループ	+ セキュリティエージェントの追加 🛞 検索 🔹	「白 グローバル設定」	
	Ξ 最新のパターンファイルを使用 0	□ エンドポイント↑	前回の接続日時	IPv4アドレス
	∃ ビジネスセキュリティサービス 0	I amazan an		
Θ				



19. インストール (iOS) 1/10

エンドポイントセキュリティ

Step 3 > iOSデバイスへのインストール ①iOS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認証コードを入力します。

[Step2-③] で確認した認証コードを入力し、 [続行] をタップします。

③使用許諾契約書が表示されます。 確認の上、「同意する」をタップします。



🗚 🔒 wfbs-svc-nabu.trendmicro.com 💍
ウイルスパスター ビジネスセキュリティサービス
登録依頼メールに記載された認証コードを入力し、 [続 行] をタップしてください。
LE IRIT



19. インストール (iOS) 2/10

エンドポイントセキュリティ

④プロファイルのダウンロードを実施します。 確認の上、「続行」をタップします。

⑤構成プロファイルのダウンロード許可を求める画面が 表示されますので、「許可」をタップします。



ウイルスバスター ビジネスセキュリティサービス
- MAS
設定プロファイルのインストールの準備 1. デバイスの「恐定」を問きます
この Web サイトは構成プロファイルをダ ウンロードしようとしています。許可し ますか?
無視 許可

19. インストール (iOS) 3/10

⑥ダウンロード完了画面が表示されますので、
 「閉じる」をタップし、ホーム画面から [設定] → [一般]
 を開きます。

⑦[VPNとデバイス管理]を開き、
 該当の「ダウンロード済みプロファイル」から
 「Trend Micro Worry-Free Business Security Services」をタップします。



<	設定 一般	
	iPhoneストレージ	>
	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	>
	辞書	>
	VPNとデバイス管理	>



19. インストール (iOS) 4/10

エンドポイントセキュリティ

⑧プロファイルのインストール画面が表示されましたら、 「インストール」をタップします。

⑨パスコードを入力します。





19. インストール (iOS) 5/10

エンドポイントセキュリティ

10警告画面が表示されましたら内容を確認の上、 「インストール」をタップします。

①リモート管理画面が表示されましたら、「信頼」をタップします。

キャンセル	警告	インストール
モバイルデバイス管理	里	
このプロファイル と、"https://	レをインスト	ールする
Maging Landson Laker-Officiality gh (Pager County	CORE of the	Creation and Company
ACCRETE AND ADDRESS	ACTORNAL AND A	and the second second
の管理者がお他 管理できるように	更いの iPhone こなります。	eをリモートで
管理者に、お使い 収集、アカウント App のインスト- データのリモート	へのiPhone」 - と機能制限 ール/管理/一 - 消去を許可	∟の個人情報の の追加/削除、 ∙覧表示、および します。

キャンセル	警告	インストール
モバイルデバイス管:	理	
このプロファイ <i>]</i> と、"https://	レをインスト	ールする
このプロファ iPhoneをリ	リモート管理 イルの提供元を低 モート管理に登録	。 言頼してこの 录しますか? で
管理 キャンセ 管理 _名 に、の医い 収集、アカウン Appのインスト- データのリモー	ル トと機能制限 ール/管理/一 ト消去を許可	信頼 <u> の 過 へ 雨 </u>

エンドポイントセキュリティ

12インストール完了画面が表示されましたら、「完了」をタップします。

(1) Appのインストールの画面が表示されましたら、「インストール」をタップします。

	インストール完了 完了
\bigotimes	Trend Micro Worry-Free Business Security Services
署名者	wfbs-svc.trendmicro.com 検証済み ✓
内容	モバイルデバイス管理 証明書(2)
詳細	>



19. インストール (iOS) 7/10



Step 4 > iOSデバイスへのインストール

①App storeの画面が表示されましたら、 「インストール」をタップします。

②Appleのサインイン・認証を完了後、 インストールが開始します。

App Sto	ore	×
D	Mobile Security for Business TREND MICRO CANADA TECHNOLOGIES, INC. アプリ	(4+)
アカウント		
	インストール	

③iOSのホーム画面にアプリが表示されていることを確認し、開きます。



19. インストール (iOS) 8/10

エンドポイントセキュリティ

④通知方法の画面が表示されますので、「許可」を選択します。

⑤位置情報の使用を許可の画面が表示されますので、 「Appの使用中は許可」を選択します。





19. インストール (iOS) 9/10

エンドポイントセキュリティ

⑥アプリ画面内の下部にある Web Reputationをタップします。

⑦Web Reputationで、VPNをオンにします。 VPN構成の追加の画面が表示された場合、「許可」をタップします。



Webレピュテーション

Ð

VPNを有効にすると、このアプリはアクセスしているド メイン名を取得し、トレンドマイクロの Web レピュテー ションサービスを使用して分析します。 不正プログラム、スパイウェア、フィッシング詐欺な ど、Web ベースの脅威を含む不正なドメインや Web サ イトへのアクセスを検出してブロックします。また、事 前に定義した望ましくない Web サイトをブロックするこ ともできます。

VPN

ローカル VPN を設定して、デバイスを Web レピ ュテーションで保護します



■登録の確認

①管理コンソールにアクセスし、ログインします。 ユーザ登録時に設定した「ログインID」と「パスワード」 を入力して、「ログイン」ボタンをクリックします。

②「セキュリティエージェント」タブをクリックし、表示 された画面内にインストールを実施したiOSデバイスが 登録されていることを確認します。

	登録情報を入力してください
	ロダインロ:
	パスワード:
	パスワードをお忘れの場合
全緑を簡単	☑ ログインIDを記憶する

iOSのインストール手順につきましては、 以上になります。 初期設定値として、以下の機能が設定されております。ご利用環境やセキュリティポリシーに応じて、設定の変更をお願いいたします。

機能	初期設定値	お客様にて設定可能な項目	ページ 番号
ウイルス対策	スマートスキャン	スマートスキャン	
Webレピュテーション	有効(中)	低/中/高より選択	96
ファイアウォール	無効	有効/無効から選択	97
挙動監視	有効	有効/無効から選択	98
ランサムウェア対策機能	有効	有効/無効から選択	99
機械学習型検索	有効	有効/無効から選択	100
URLフィルタリング	有効(低)	低/中/高/カスタムより選択 業務時間設定が可能	101
承認済み/ブロックURL登録	無し	追加登録可	102
アプリケーションコントロール	無効	有効/無効から選択 (対象アプリケーションを指定可)	103
デバイスコントロール	無効	有効/無効から選択 (権限選択可)	105
エージェントアンインストール防止	無効	有効(パスワード設定)	109
アラート設定	有効	アラート受信者の変更・追加	110

※Mac、Android、iOSの設定方法については、トレンドマイクロ社のWEBページを参照下さい。
(<u>https://docs.trendmicro.com/ja-jp/documentation/article/worry-free-business-security-services-67-server-help-policy-management_001</u>)

20.機能を設定する(Webレピュテーション) 2/16

①管理コンソールにて、
 「ビジネスセキュリティクライアント」
 ⇒グループを選択⇒「ポリシーの設定」

≡	E TREND Worry Free" Business Security Services										
୍କ	セキュリティエージェント 📮 開通時初期設定										
5	ワ すべてのセキュリティエージェ 3 セキュリティエージェント:3										
0	🔺 🖿 手動グループ		+	セキュリティエージェントの	追加 ①	検索 🗐 ポ	リシーの設定	直 タスク ▼			
	サーバ (初期設定)	0		エンドポイント ↑	種類	前回の接続日時	IPv4アドレス	MACアドレス	IPv6アドレス		
	デバイス (初期設定)	0			Android	22分前	-				
Q	test	0			Windows	3日前					
	test(WinServer)	0			Android						
	test2	0			/ and ord	JOH WILLI					
<u>ن</u> ې	開通時初期設定	3									
	😑 最新のパターンファイルを使用	1									
	Ξ ビジネスセキュリティサービス	0									

- ②「Webレピュテーション」を選択
- ③セキュリティレベルを選択します。 (低・中・高) ※初期値は「中」となっております。
- ④ブラウザ脆弱性対策機能を有効にする
 場合は、「不正スクリプトを含むページを
 ブロックする」にチェックを入れます。
- ⑤「保存」をクリックします。

ポリシーの設定:開通時初期	設定			×					
 									
 辛動監視 	セキュリティレベル								
● 機械学習型検索		危険	極めて不審	不審					
- /EtBulan -T	○ 高	\otimes	$^{\circ}$	\otimes					
● Webレビュテーション	 中(初期設定) 	\otimes	\otimes						
 ファイアワオール設定 	() 低	\otimes							
情報派えい対策 ● デバイスコントロール	○ Webサイトのアクセスをブロッ	クします ①							
◎ 情報漏えい対策	未評価のURL								
アクセスコントロール ● URLフィルタ	トレンドマイクロによる評価が	「完了していないWebサイトをブロッ	リクする ①						
● アプリケーションコントロール	ブラウザ脆弱性対策								
除外リスト 検索除外	一 不正なスクリプトを含むWe	bサイトをブロックする							
る切決ル/ゴロックオスIDI ▼				保存 キャンセル					



②「ファイアウォール」を選択

③有効にする場合、チェックを入れます。

④簡易モード/詳細モードを選択します。

⑤「保存」をクリックします。





②「挙動監視」を選択

③不正プログラム挙動ブロックの内 有効にする項目にチェックを入れます。

④「保存」をクリックします。





②「挙動監視」を選択

- ③「ランサムウェア対策」にて、
 設定変更を行います。
 ※初期値はすべて「有効」となっています。
- ④「保存」をクリックします。



	=	TREND Worry Free Business Security Services											
6)	セキュリティエージェント	₹		開通時初期設定								
G	Ē	豆 すべてのセキュリティエージェ	3	セ	キュリティエージェント: 3								
۶ ا	٤	4 🛅 手動グループ		+	 セキュリティエージェントのi 	\$ 50 (1)	検索 🗐 ポ	リシーの設定	タスク •				
	ך א	サーバ (初期設定)	0		エンドポイント ↑	種類	前回の接続日時	IPv4アドレス	MACアドレス	IPv6アドレス			
Ē		デバイス (初期設定)	0			Android	22分前						
C	€	test	0		.	Windows	3日前	_					
	ħ	test(WinServer)	0			Android	90日以上前	-		•			
	5	test2	0										
در د	3	開進时初期設定	3	[
		 最新のハターシンアイルを使用 ビジネスセキュリティサービス 	0										

- ②「機械学習型検索」を選択
- ③機械学習型検索を有効化する場合は、 チェックを入れます。
- ④ファイルに対する処理を選択します
 ⇒隔離 or ログのみ
 ※初期値は「隔離」となっております。
- ⑤プロセスに対する処理を選択します ⇒終了 or ログのみ ※初期値は「終了」となっております。
- ⑥「保存」をクリックします。

ポリシーの設定: 開通時初期	設定					×
◆ 対象とサービスの設定 章 (広からの保護機能 ・ 検索設定 ● 茶動監視 ● 機能学習型検索 ● 仮想パジチ ● Webレビュテーション	 機械学習型 トレンドマイクログ 出します。 オン メロン メロン メロン メロン メロン オンターネット す。 株は設定 	21快索 の機械学習型検索は、高度な機械等 の機械学習型検索は、高度な機械等 なり機構を利用するには、学動監視を有効 ト接続を利用できない場合は、機械	「智テクノロジを使用 にする必要がありま 「学習型検索ローカル・	して、あまり曽及してい す。 Eデル (ファイル検出) ∛	いない不審プロセスやファイ ない不審プロセスやファイ 全使用してポータブル実行可	② 'ルに含まれる未知のセキュリティリスクを検 1部ファイルの脅威に対する保護が継続されま
● ファイアウォール設定	種類	処理				
情報漏えい対策 ● デバイスコントロール	🗹 ファイル	隔離 、				
◎ 情報漏えい対策	✓ プロセス	終了				
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						
**************************************						保存 キャンセル

20.機能を設定する(URLフィルタリング) 7/16

①管理コンソールにて、 「ビジネスセキュリティクライアント」 ⇒グループを選択⇒「ポリシーの設定」

②「URLフィルタ」を選択

- ③フィルタ強度を選択 (低・中・高・カスタム) ※初期値は「低」となっております。
- ④フィルタルールにて、
 ブロック対象のURIカテゴリを指定します。

「インターネットのセキュリティ」が 有効となっております。

- ⑤フィルタリングを適用する時間を指定する場合、 業務時間の設定を行います。 ※初期値は、「終日(24x7)」となっております。
- ⑥「保存」をクリックします。



Ø 白 対象とサービスの設定 URLフィルタ 。 にすると、管理者は、1日のさまざまな時間帯でブロックする特定の経験のWebサイトを設定することができます 📫 🏟 🖨 ios 🎯 🔵 त्र> 検索設定 フィルタ強度 • 杨桃字碧华枝落 0高 既知志たは操在的なセキュリティ上の脅威、不適切なコンテンツまたは有害である可能性のあるコンテンツ、生産性志たは帯域編に影響する可能 性のあるコンテンツ、および未評価のページをブロックします 02切パッチ 0 # 度知のセキュリティトの登成れよび不適切なコンテンツをブロックします 〇 低(初期設定) 既知のセキュリティ上の脅威をブロックします = ファイアウォール:03 ○ カスタム ブロックするURLカテゴリを指定する フィルタルール • デバイスコントローノ ● 情報編えい対体 URLカテゴリ 菜務時間 至我時間? アダルト • URLDAIN 団 ビジネス 除外リスト 団 コミュニケーション/メディア 検索除外 ∃ −般 承認済みプロックするUR インターネットのセキュリティ ロージェントの設定 権限およびその他の設定 団 ライフスタイル 目 ネットワーク URLのカテゴリや安全 某种检查 ○ 終日 (24/7 ○ 業務時間を指定する 08:00 09:00 10:00 11:00 12:00 14:00 15:00 17:00 19:00 業務時間 0 業務時間の

保存 キャンセル

エンドポイント/EDRセキュリティ

20.機能を設定する(承認済・ブロックURL登録) 8/16

エンドポイント/EDRセキュリティ

①管理コンソールにて、
 「ビジネスセキュリティクライアント」
 ⇒グループを選択⇒「ポリシーの設定」

- ②除外登録を行う場合は、 「承認済みURL」タブを選択。 ブロック登録を行う場合は、 「ブロックするURL」タブを選択。 除外登録は③へ ブロック登録は④へ
- ③除外登録を行う場合、「+追加」を クリックし、承認済みURL にURLを 入力し、「追加」をクリック。
 ※登録したURLはWebレピュテーション およびURLフィルタ機能の除外対象に なります。
- ④ブロック登録を行う場合、「+追加」を
 クリックし、ブロックするURL に
 URLを入力し、「追加」をクリック。
- ⑤「保存」をクリックします。

≡	Contraction of the security Services							
ଲ ୮	セキュリティエージェ	ント 📮	開通時初期語 セキュリティエージェント: 3	设定				
▲ 図 ① ■ ②	 ▲ 手動グルーブ サーバ(初期設定) デバイス(初期設定 test test(WinSever) test2 開通時初期設定 Ξ 最新のパターンファ Ξ ビジネスセキュリラ 	0 0 0 0 3 マイルを使用 1 ミィサービス 0	+ tt=uy7rI-9IX	トの追加 ③ 徐 そ知 Android 2 Android 2 Android 2	 (目 ボリジ 前回の接続日時 日 22分前 - 3日前 日 90日以上前 - 	シーの設定 Pv4アドレス	■ タスク ▼ MACアドレス	IPv6アドレス
ポリ	シーの設定: 開通時初期	設定						×
 交対: 脅威から ●検索 ● 後索 	象とサービスの設定 ●	 承認済みブロックす 承認済みブロックす 使用する除外: グローバルは 除外の指定 	ブロックするURLd るURLdWebレビュテーション 転踏みおよびブロックするURL	DUスト およびURLフィルタI のリスト ①	こ適用されます。			Ø
 機械 仮想 Web ファ 情報編 デバ 情報 アクセン URL 	学習型検索 パッチ レビュテーション イアウォール設定 えい対策 イスコントロール 温えい対策 スコントロール フィルタ	承認済み + 追加 承認済みし http://*.tre https://*.tr http://www	URL (15) ブロックするURL 18 マ IRL Indmicro.com/* endmicro.com/* x.trendmicro.com/*	(1)				습計: 15
 アプ 除外リ: 給玄 	リケーションコントロール スト 始外	http://wus 承認済み	tat.windows.com/*				×	v
承認 エージ: 権限	済みプロックするURL エントの設定 およびその他の設定	URL: ①	ebsite.com; http://*.webs	ite.com, http://	www.website*.c	om/		pwebサイトにアクセスしてください。
					追加	+72	セル	102

20.機能を設定する(アプリケーションコントロール)(1/2)9/16

エンドポイント/EDRセキュリティ

①管理コンソールにて、
 「ビジネスセキュリティクライアント」
 ⇒グループを選択⇒「ポリシーの設定」



- ③「アプリケーションコントロールの オンオフ」を「オン」にします。
- ④ ルールの「+ルールの割り当て」を クリックしします。

ポリシーの設定: 開通時初期	設定			×
 ☆ 対象とサービスの設定 4 4 4 4 4 4 5 6 6 6 7 8 7 8 7 8 7 8 8 9 8 9 9 8 9 9 9 10 <li< td=""><td>アプリケーションコン エンドボイントでのアブリケーションの家 オン ・</td><td>トロール 続行やインストールを制限するルールを作成し、 ョンのエンドポイントでの実行をプロック</td><td>έτ.</td><td>٥</td></li<>	アプリケーションコン エンドボイントでのアブリケーションの家 オン ・	トロール 続行やインストールを制限するルールを作成し、 ョンのエンドポイントでの実行をプロック	έ τ .	٥
 機械学習型検索 仮想パッチ Webレビュテーション ファイアウォール設定 	 ● ロックダウン:前回のインベントリ ルール + ルールの割り当て 	リ検索で確認されなかったアプリケーションを	すべてブロック ①	合計: 0
情報編えい対策 ・ デバイスコントロール ・ 情報編えい対策 アクセスコントロール ・ IIPI フィルタ	種類↑ [/	ルール ルールが割り当て レールの割り当て] をクリックしてアプリケーシ	概要 られていません。 -コンコントロールレールを指定してください。	
 アプリケーションコントロール 第外リスト 検索除外 承認済みプロックするURL エーラエントの設定 権限およびその他の設定 	許可ルールはブロックルールよりも低	題先されます。		
				保存キャンセル

20.機能を設定する(アプリケーションコントロール) (2/2) 10/16

エンドポイント/EDRセキュリティ

⑤ 「アプリケーションコントロール」にて、 「+ルールの追加」を選択。

- ⑥許可を行う場合は、「許可」をクリック。 ブロックを行う場合は、「ブロック」を クリック。 許可は⑦へ ブロックは⑧へ
- ⑦許可を行う場合、
 「アプリケーションの管理」をクリック。
 許可するアプリケーションを☑とし、
 「OK」をクリックします。
- ⑧ブロック登録を行う場合、 「アプリケーションの管理」をクリック。 ブロックするアプリケーションを図とし、 「OK」をクリックします。
- ⑨「保存」をクリックします。

	-)L	×
レールを選択:		
Q ルール名	すべてのルール 👻	+ ルールの追加 -
● 種類 ↑	بار—بار	概要許可
ブロック	ブロックリスト	ブロック フィイルまたはフィニニン)
ブロック	ブロック	ファイルまたはフォルダのパス (1)
キ可ルールの設定		×
3前:*		
給方法: アプリケーションレピュテーシ	17UZF	•
アプリケーションの管理		
カテコリ	アノリケー	-932
マプリケーションレピュテーション	ンリスト	×
		たさい。
アプリケーションまたはベンダー名の検索 システムツール(0/860) (Q ロ すべてのアプリケーションを許可: シ	たさい。 バステムツール
アプリケーションまたはペンダー名の検索 システムツール(0/860) / ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75)	Q すべてのアプリケーションを許可: シ アプリケーション	たさい。 バステムツール ベンダー
アプリケーションまたはペンダー名の検索 システムツール(0/860) / ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342)	Q ・ ・ ・	たさい。 パステムツール ベンダー Trend Micro
アプリケーションまたはペンダー名の検索 システムツール(0/860) ' ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301)	Q ・ ・ ・	たさい。 バステムツール ベンダー Trend Micro
アプリケーションまたはペンダー名の検索 システムツール(0/860) ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301) 開発者ツール(0/186)	Q ・ すべてのアプリケーションを許可: シ ・ アプリケーション ・ Deep Security Agent ・ VueScan ・ GOG com Downloader	たさい。 バステムツール ベンダー Trend Micro Hamrick GOG.com
アプリケーションまたはペンダー名の検索 システムツール(0/860) ' ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301) 開発者ツール(0/186) ハードウェアのファームウェアとドライバ((ピアツーピア(0/69)	Q ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	たさい。 バステムツール ベンダー Trend Micro Hamrick GOG.com
アプリケーションまたはペンダー名の検索 システムツール(0/860) プラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301) 開発者ツール(0/186) ハードウェアのファームウェアとドライノ((ピアツーピア(0/69) 暗号化(0/41)	Q ・ すべてのアプリケーションを許可: シ ・ アプリケーション ・ Deep Security Agent ・ VueScan ・ GOG.com Downloader ・ Kaspersky Password Manager	ルステムソール ベンダー Trend Micro Hamrick GOG.com Kaspersky
アプリケーションまたはペンダー名の検索 システムツール(0/860) ' ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301) 開発者ツール(0/186) ハードウェアのファームウェアとドライバ(ピアツーピア(0/69) 暗号化(0/41) ゲーム(0/86)	Q ・ サベてのアプリケーションを許可: シ ・ アプリケーション ・ Deep Security Agent ・ VueScan ・ GOG.com Downloader ・ Kaspersky Password Manager ・ VirtualBox	ルステムソール ペンダー Trend Micro Hamrick GOG.com Kaspersky Oracle
アプリケーションまたはペンダー名の検索 システムツール(0/860) , ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301) 開発者ツール(0/186) ハードウェアのファームウェアとドライバ((ピアツーピア(0/69) 暗号化(0/41) ゲーム(0/86) モバイル同期(0/39)	Q ・ すべてのアプリケーションを許可: シ ・ アプリケーション ・ アプリケーション ・ ロeep Security Agent ・ VueScan ・ GOG.com Downloader ・ Kaspersky Password Manager ・ VirtualBox ・ Avira Fusebundle Generator	ルステムソール ペンダー Trend Micro Hamrick GOG.com Kaspersky Oracle Avira
アプリケーションまたはペンダー名の検索 ジステムツール(0/860) プラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301) 開発者ツール(0/186) ハードウェアのファームウェアとドライバ(ピアツーピア(0/69) 暗号化(0/41) ゲーム(0/86) モバイル同期(0/39) インスタントメッセンジャー(0/108)	Q ・ アプリケーションを許可: シーン ・ アプリケーション ・ アプリケーション ・ Deep Security Agent ・ VueScan ・ GOG.com Downloader ・ Kaspersky Password Manager ・ VirtualBox ・ Avira Fusebundle Generator ・ DownloadStudio	ルステムソール ペンダー Trend Micro Hamrick GOG.com Kaspersky Oracle Avira Conceiva
アプリケーションまたはペンダー名の検索 ジステムツール(0/860) ブラウザとブラウザツール(0/79) 高リスクのアプリケーション(0/75) メディアツール(0/342) 生産性(0/301) 開発者ツール(0/186) ハードウェアのファームウェアとドライバ(ピアツーピア(0/69) 暗号化(0/41) ゲーム(0/86) モバイル同期(0/39) インスタントメッセンジャー(0/108) 分散コンピューティング(0/35) ナンニく、ストレーンジ(0/04)	Q ・ すべてのアプリケーションを許可: シ ・ アプリケーション ・ アプリケーション ・ Deep Security Agent ・ VueScan ・ GOG.com Downloader ・ Kaspersky Password Manager ・ VirtualBox ・ Avira Fusebundle Generator ・ DownloadStudio ・ AVG PC TuneUp	ルステムソール ペンダー Trend Micro Hamrick GOG.com Kaspersky Oracle Avira Conceiva AVG

20.機能を設定する(デバイスコントロール)(1/4)11/16

エンドポイント/EDRセキュリティ

①管理コンソールにて、
 「ビジネスセキュリティクライアント」
 ⇒グループを選択⇒「ポリシーの設定」

- ②「デバイスコントロール」を選択
- ③「デバイスコントロールオンオフ」を 「オン」にします。
- ④エンドポイントの設定を行う場合は、
 「エンドポイントの設定」タブを選択。
 除外を行う場合は、
 「除外」タブを選択。
 エンドポイントの設定は⑤へ
 除外は⑥へ
- ⑤対象のストレージデバイスの権限を それぞれ選択します。

USBストレージデバイスでの 自動実行機能をブロックする場合、 チェックを入れます。



ポリシーの設定: 開通時初期	設定		×
 ◇ 対象とサービスの設定 ● ● 105 ② 今照からの保護機能 ● 検索設定 ● 挙動監視 	デバイスコントローデバイスコントローデバイスコントロールは、周辺デバ シーズ オン 注意: この時間を使用するには、対 エンドポイントの設定 勝利	- ル イスへのアクセスを制御します。 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。 ⁸	0
 ・ (Way 3 = エリバ・) ・ (Way 1 = エリバ・) ・ (Way 2 = エリバ・) ・ ファイアウォール設定 ・ デバイスコントロール ・ 「特徴漏えい(対策) 	ストレージデパイス CD/DVD: ① ネットワークドライブ: USBストレージデパイス:	フルアクセス ・ フルアクセス ・ フルアクセス ・ フルアクセス ・ リンアクセス ・ USBストレージデバイスでの目勤実行機能をプロックする	すべて設定 -
 アクセスコントロール リRL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 承認済みプロックするURL エージェントの設定 権限およびその他の設定 	モバイルデバイス ストレージ: ストレージ2000のデバイス Bluetoothアダブタ: COMおよびLPTボート: IEEE 1394インターフェース: イムージングデバイス 赤が撮デノイイス: モデム: プリントスクリーンキー: ワイヤレスNIC:	 USBストレージブバイスでの目動美行機能をフロックする 許可 ○ ブロック 	
			保存 キャンセル

20.機能を設定する(デバイスコントロール)(2/4) 12/16

Г

エンドポイント/EDRセキュリティ

⑥除外を行う場合、「+許可ルールの追加」 をクリック。

ポリシーの設定:開通時初期	設定		×	
 ☆ 対象とサービスの設定 4 € ♣ IOS Ø 	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。	0	
 南威からの保護機能 検索設定 	大ン 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。	
 挙動監視 機械学習型検索 	エンドポイントの設定 除外			
● 仮想パッチ	ユーザ			
● Webレビュテーション	指定したユーザに制限されたデバイスへのアクセスを許可します。許可ルールはエンドポイントの設定よりも優先されます。			
 ファイアウォール設定 	+ 許可ルールの追加		合計. 0	
● デバイスコントロール	ال−ال ا	ユーザアカウント	許可されたデバイス	
 「特報漏えい対策 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 		ルールが定義されていませ (許可ルールの追加) をクリックしてユーザルー	tん。 ルを作成してください。	
時外リスト 検索除外	USBデバイス			
承認済みプロックするURL エーラエントの高定 権限およびその他の設定	許可されたUSBデバイスのリスト (グローバ) または(読み取り)を選択した場合に適用され フルアクセス - 許可されたUSBデバイスのリストを設定する プログラム	「殺定」の種類を指定します。この種類は、[エン ます。 には、「ポリシー設定」—(グローノいし除外リスト) (ドポイントの設定 タブでUSBストレーシデバイスに対して (プロック) に移動します (許可されたUSBデバイスのリスト内のデバイス数: 0)	
	許可されたプログラムリスト (0) プログラムの さめたはデンシルを名プロバ・ ます。 ①	イダを指定して、プログラムによる、制限された	ストレージデバイスにあるファイルの読み取り書き込みの実行を許可し	
			保存 キャンセル	

20.機能を設定する(デバイスコントロール)(3/4)13/16

エンドポイント/EDRセキュリティ

許可ルールにて、「ルール名」を入力。

除外するストレージデバイスを それぞれ選択します。

許可ルール	×
ルール名:*	
ユーザアカウント:	
	ڻ ۲
ストレージデバイス	
□ ネットワークドライブ	
□ USBストレージデバイス	
□ USBストレージデバイスでの自動実行機能を許可する	
モバイルデバイス	
ストレージ	
ストレージ以外のデバイス	
□ Bluetoothアダプタ	
□ COMおよびLPTボート	
□ IEEE 1394インターフェース	
イメージングデバイス	
□ 赤外線デバイス	
	OK キャンセル

20.機能を設定する(デバイスコントロール)(4/4) 14/16

エンドポイント/EDRセキュリティ

許可されたプログラムリストのリンク先から 許可されたプログラムリストにて、 「+追加」をクリック。

許可されたプログラムリスト	\times
+ 追加 ファイルパス / デジタル署名プロバイダ	
プログラムは追加されていません。 (追加)をクリックして、実行可能なプログラムを指定し、ファイルを制限されたストレージデバイスから 読み取り/書き込みます。	5
OK キャンセノ	L

許可されたプログラムにて、 ファイルパス/デジタル署名プロバイダに EXEを入力し、「OK」をクリック。

許可されたプログラム	\times
ファイルパス/デジタル署名プロバイダ: 🔅	
	_
例: ?¥Installer¥Setuplexe、F:¥*lexe、Trend Micro, Inc.	
OK キャンセ	ı

⑦「保存」をクリックします。
20.機能を設定する(エージェントアンインストール防止) 15/16

エンドポイント/EDRセキュリティ

- ①管理コンソールにて、 「ポリシー」⇒
 「グローバルセキュリティエージェント設定」
 ②「エージェントコントロール」タブを選択
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ⑦
 ⑦
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 <li0
 0
 - 「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」に チェックを入れます。
- ④パスワードを指定します。
- ⑤「保存」をクリックします。

Worry F	ree [∞] Business Security Services	I5:24 UTC+09:00	0	*
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。			0
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 	書告 マ 7 - 日経過してもウイル い(ターンファイルがアップデートされていない場合、W)	Vindowsタスクバーに警告アイ	コンを表	示する
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			
	☑ WebレビュテーションおよびUF、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育成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 ナービスを有効にする:			
	セキュリティエージェントのステ・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」できない場合、 5 - 回まで再試行			
	管理者への問い合わせの遇知			
	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			
	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	王要求する		
	R#			

20.機能を設定する(アラート設定) 16/16

エンドポイント/EDRセキュリティ

- ①管理コンソールにて、
 「管理」⇒「通知」を選択
- ②「設定」タブを選択
- ③「受信者」に変更または追加となる 受信者メールアドレスを入力
- ④ページ下部の「保存」をクリックします。

≡	🕖 TREND. Worry F	ree [™] Business	Security Services	11:25 UTC+09:00	0	2 k
ଜ	管理	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	⑦ はされたトークンのリ
50 八	ー般設定 モバイルデバイス登録設定	ストについては、通知の 設定 東確認	カスタマイズを参照してください。			
) 凤	通知	送信者:	WFBS-SVC(w, no. Nicro.com			
© P	Active Directoryの設定 Smart Protection Network	受信者:				
	回復キーのパスワード					
¢	ライセンス情報	件タッゴレフ ハックフィ	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			
	(TRU /) - JUSSIE	R A	メール通知に件名のプレフィックスを追加するには、プレフィックスを指定 に%SUBJECT_PREFACE トークンを挿入します。 件 [SumRansomware][要確認] ウイルス対策・解決されていない脅威 5	さして、通知デンプレートの	[件名] フィ	ィールド

※注意※

受信者を変更される場合は、サポートセンタにお電話ください。

重要アラートを通知するためのシステムに対し、メールアドレスの変更登録を実施する必要がございます。

■EDRセキュリティご利用に伴う、既存設定に関する注意点

1.EDRセキュリティをご利用いただくにあたり、ご確認いただきたいこと

エンドポイントセキュリティをご利用いただいているお客様で、 下記「2.各種設定項目について」のいずれかの設定を「オフ」にしている場合は、 その設定に関連するEDR機能をご利用いただくことができません。 ※デフォルト設定は全て「オン」となっておりますので、「オフ」に変更されている場合にご対応が必要となります。 ※設定を「オン」にしていただくことで、関連するEDR機能の提供が可能となります。

2.各種設定項目について ※いずれかがオフの場合は設定変更(3.設定変更について)の対応が必要です。

 ①Chrome、FirefoxおよびMicrosoft EdgeでWebレビュテーションと URLフィルタリングのHTTPS確認を有効にする:オフ 影響:WebレビュテーションとURLフィルタリングのHTTPS通信検知ログを元とした注意が必要なイベントが 発生しなくなります。

②Webレピ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]:オフ 影響:VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

③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] :オフ 影響:VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

④Webレピュテーション:オフ

影響:Webレピュテーション検知を元とした、注意が必要なイベントが発生しなくなります。

3.設定確認・変更について

現在の設定の確認及び、各項目を「オン」に変更する手順は、次ページ以降をご参考ください。

21. EDRセキュリティご利用に伴う、既存設定に関する注意点 2/5

対象者:①[Chrome、FirefoxおよびMicrosoft EdgeでWebレピュテーションとURLフィルタリングのHTTPS確認を有効にする]がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。 ⇒WebレピュテーションとURLフィルタリングのHTTPS通信検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールヘログイン後、

「ポリシー」-「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」タブにて下記を設定

「HTTPS Web評価」の項目から

[Chrome、FirefoxおよびMicrosoft EdgeでWebレビュテーションとURLフィルタリングのHTTPS確認を有効にする] をオン (チェックを入れたば能)

(チェックを入れた状態)

②保存をクリック

の ポリシー設定	✓ 圧縮ファイルの検索制限
追加の設定	圧縮ファイルのサイズが 2 MBを超える場合はファイルを検索しない (1-1000)
 グローノ0ルセキュリティエー ジェント設定 グローノ0ル除外リスト グローノ0ル除外リスト ボリシーリソース アブリケーションコントロー ルルール ☆ ☆ 	 圧縮ファイル内では、最初のファイルから 100 番目までのファイルを検索する(1-100000)
	→ 20mot

対象者:②[Webレピ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]がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。 ⇒ VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールヘログイン後、

「ポリシー」-「グローバルセキュリティエージェント設定」-「エージェントコントロール」タブにて下記を設定 [Webレピ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]:オン(チェックを入れた状態)

②保存をクリック

∩ ダッシュボード	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。
「」 セキュリティエー	追加の設定 グローバルヤキュリティエー	セキュリティ設定 エージェントコントロール
گ – پ	ジェント設定	활告
🛃 ポリシー		✓ 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タスクパーに警告アイコンを表示する
() и#-н	ボリシー リリース 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
		✓ 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
{ 〕} 管理		✓ 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 Exatt ビフ
		▲ボジ レネコ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
		保存

21. EDRセキュリティご利用に伴う、既存設定に関する注意点 4/5

対象者:③[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] がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。 ⇒ VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールヘログイン後、

「ポリシー」-「グローバルセキュリティエージェント設定」-「エージェントコントロール」タブにて下記を設定 [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] :オン(チェックを入れた状態)

②保存をクリック

∩ ダッシュボ−ド	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。
「」 セキュリティエー	追加の設定	
ਲ 1-4	クロー/ いレゼキュリティエー ジェント設定	
ポリシー	グローバル除外リスト	■ 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タスクパーに警告アイコンを表示する
0 L#-r	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
		✓ 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
{ 〕} 管理		✓ 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 マ 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
		保存

対象者:④[webレピュテーション] がオフのユーザ

■下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。 ⇒Webレピュテーション検知を元とした、注意が必要なイベントが発生しなくなります。

①管理コンソールヘログイン後、 「セキュリティエージェント」-「開通時初期設定」※-「ポリシーの設定」 -対象のOSを選択し、 「webレピュテーション」タブにて下記を設定 [webレピュテーション]をオン

②保存をクリック

※「開通時初期設定」とは、お申込み時 に申請いただいた内容の設定情報を 反映させたポリシーグループになります。 新たなポリシーを作成している際は、 作成したポリシーグループをご指定くだ さい。

		使用しているOSを ご指定ください	ポリシーの設定:開通時初期	服定					×
ର	セキュリティエージェント		 	Webレピュ Webレピュテーショ	テーション コンは不正Webサイトの脅威	からの保護を強化します。			0
50	🖵 すべてのセキュリティエージェ (通常検索の開始 アグレッシブ検索の開始 	 今成からの保護機能 検索設定 						
Q	🔺 🛅 手動グループ	検索停止	 学勤監視 機械学習型検索 	2+197100	<i>JV</i>	危険	極めて不審	不審	
\Box	サーバ (初期設定)		● 仮想パッチ	○高		\otimes	0	0	
5	デバイス (初期設定)	0	 ファイアウォール設定 情報漏えい対策 	 中(初期設)低 	8定)	0	Ø		
\bigcirc	開通時初期設定	ボリシーの設定	 デバイスコントロール 情報源えい対策 	⊘ Webサイト	のアクセスをブロックしま	f (i)			
	Ⅲ 最新のパターンファイルを使用…	設定の複製0	アクセスコントロール ・ URLフィルタ		イクロによる評価が完了して	ていないWebサイトをブロッ	クする 🕕		
l	≡ ビジネスセキュリティサービス	0 名前変更	 アプリケーションコントロール 	ブラウザ脆弱性対	策 5.1.プレカ会かりいた4.7.1.	*******			
্ৰি		削除	検索除外 承認済み/ブロックするURL	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	〈ソリノトを言むWebサイト	をノロックする			
			···· ·					保存	キャンセル

22. Windows/Android/iOS アンインストール

パソコンの買い替え時など、アンインストールを行う場合は下記手順にて実施します。 アンインストールが完了しますと、ライセンスは再利用可能となり、新デバイスへのインストールが可能になります。 アンインストール作業は管理コンソール側とクライアント側の両方から実施可能です。 ※Macのエンドポイントアンインストール方法につきましては、118Pを参照ください。 ※MacのEDRセキュリティアンインストール方法につきましては、120Pを参照ください。

<u>管理コンソール側での実施方法</u>

①管理コンソールにログインします。

- ②[セキュリティエージェント]
 タブをクリックし、デバイスの登録情報
 を探しチェックボックスに
 チェックを入れます。
- ③[タスク]から、 [セキュリティエージェントの アンインストール]を選択します。
- ④管理コンソール上から、 該当のデバイスの登録が削除されます。

以上で、アンインストール作業の完了です。 クライアントコンピュータ側では、コンソールからの 削除通知を受信後、アンインストールが進められます。





23.Windowsアンインストール

クライアント側での実施方法(Windows10/11の場合) ※「ユーザーアカウント制御」により、許可、または管理者の パスワードを求められる場合があります。操作を続行するため には、[続行]、または[はい]をクリックします。

① [スタート] ボタンから[コントロール パネル]を開きます。

- [プログラム]の項目にある[プログラムのアンインストール]を クリックします。
- ③表示された一覧の中から[セキュリティエージェント]を ダブルクリックします。
- ④アンインストール用パスワードを設定している場合は、下記の 画面が表示されます。この場合はWeb管理コンソールで設定した パスワードを入力し、アンインストールを実行します。 本設定はWeb管理コンソールの[ポリシー]>[グローバルセキュ リティエージェント設定]>[エージェントコントロール]タブ内の 「アンインストール」での設定となります。アンインストールす るためのウィザードが起動しますので、[次へ]をクリックします。
- ⑤途中で「ユーザ アカウント制御」の画面が表示される場合は、 [はい]をクリックします。

⑥アンインストール処理が進んでいきます。

⑦しばらく待つと、アンインストール完了のメッセージが表示されます。[完了]をクリックし、Windows を再起動します。



操作は以上で終了です。

キャンセル

< 戻る(B) 完了(F)

24. Macアンインストール(1/3)

クライアント側での実施方法 (Macの場合)

Mac OS版のエンドポイントセキュリティ (VBBSS) エージェントはWeb管理コンソールより専用の アンインストーラを入手し、それを用いてMac端末側でアンインストールを実施後、 Web管理コンソール上から該当Mac端末の登録情報を削除します。

①エンドポイントセキュリティのWeb管理コンソール にログインします。

②左メニューの「管理]をクリックし、「ツール]をクリック。

- ③ツールの一覧が表示されますので、 その中の「アンインストーラ(Mac)」内の 「ツールのダウンロード] リンクをクリックし、 パッケージをダウンロードします。 * WFBS-SVC Agent Uninstaller.app.zip というファイルがダウンロードされます。
- ④アンインストールを実施したいMac OS へ ダウンロードしたパッケージをコピーし、 ファイルをダブルクリックして実行します。

⑤実施の許可を促す画面が開くので、 Mac端末側で設定されている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

- ⑥「このアプリをアンインストールしますか?」という メッセージが表示されるので「OK」をクリック。
- ⑦ Mac OS版のエンドポイントセキュリティエージェントのアンインストールが 実行されます。

アンインストールが完了したら「閉じる」をクリックして、終了します。



•••	く 〉 ダウンロード	:≡ ≎	· · · · · · · · · · · · · · · · · · ·	0 • ·
よく使う項目	名前	サイズ	租成	追加日
RirDrop	WFBS-SVC_Agent_Uninstaller	2.3 MB	アプリケーション	今日 12:40
● 最近の項目	> WFBS-SVC_Agent_Installer		フォルダ	今日 10:22
A アプリケーション	> 🛅 Mac端末用_ODS検証環境インストーラ		フォルダ	今日 8:53
デスクトップ	> Mac端末用_支店向けトライアルインストーラ		フォルダ	2025年4月1日 18:10
🕒 書類				
④ ダウンロード				



24. Macアンインストール(2/3)

エンドポイントセキュリティ

クライアント側での実施方法(Macの場合)

⑧エンドポイントセキュリティのWeb管理 コンソールにログインします。

⑨左メニューの[セキュリティエージェント]をクリックし、

エージェント端末の一覧画面を表示させます。

⑩先ほど端末側でアンインストールを実施 した

Mac端末のチェックボックスにチェック を入れます。

⑪上部の[タスク▼]をクリックし、「セキュリティエージェントのアンイン

ストール」を選択します。

12一覧から該当のMac端末の情報が削除されたのを確認します。

以上で、Mac OS版のエンドポイントセキュリティエージェン トのアンインストール作業は終了となります。

セキュリティエージェント	4	9	すべてのセキュリティ:	エージェ	すべてのステータス	• 技術	Q T (2)
↓ すべてのセキュリティエージェ	3	セ	キュリティエージェント:3				
🖌 🚞 手動グループ		+	- セキュリティエージェントの追加	⊕ 検索 ▼	70-110 z	i 9スク ▼	0 \$
サーバ (初期設定)	0		エンドポイント 🕆	通常検索の開始	アグレッシブ検索(エクマポート	-2771
デバイス (初期設定)	(1)		LAPTOP-No1			今すぐアップデート	
test	0		DDS-NewZero2			2010 A	
test(WinServer)	0		DDS-NewZero4noMacBook-Air			復号	
test2	0					KALMU TUR	
開通時初期設定	2					手動クルークに参加	
Ξ 最新のパターンファイルを使用	2				Ц	セキュリティエージェントの	アンインストール
Ξ ビジネスセキュリティサービス	0						



24. Macアンインストール(3/3)

EDRセキュリティ

クライアント側での実施方法(Macの場合)

MacアプリのEDRセキュリティ アプリケーションのアンインストールにつきましては、 サポートセンター側での処理も必要となりますので、大変お手数をおかけしますが、 サポートセンターまでご連絡をお願い致します。

※Mac端末でセキュリティおまかせプランをご利用中のお客さまは ご解約される前にEDRセキュリティの削除(アンインストール)申請が必要になりますので、 ご注意ください。 セキュリティおまかせプランご解約後にはアンインストール方法が複雑になり、お客様にお手間を

かけることになるため、必ずご解約前にアンインストールの申請をお願いいたします。

121

ご利用中のライセンス数、未利用ライセンス数の確認は、管理コンソールの「ダッシュボード」でご確認可能です。

	Extension Securit	ty Services		11:43 UTC+09:00	0	*
ດ G	● 必要な処理はありません。お使いのエンドポイントは保護さ	れています。				0
 ☑ □	セキュリティリスクの検出数	Į.	0 未知の脅威	О ポリシー違	反	過去30日間 -
<u>ئ</u>	イベントの種類	影響を受け	モエンドボイント			検出数
	ウイルス/不正プログラム		0			0
	スパイウェア/グレーウェア Web/レビュテーション		0			0
	ネットワークウイルス		0			0
	感染経路別の検出数 0 検出数 すべての ① Web	過去30日間 - 育威 - 上	セキュリティエージェン 3 セキュリティエージェン	トのステータス バターンファイル	,のアップ ;	デートが& 1
	クラウド同期	0		オフライン		1
	X-JL	0	2 EXTNEXTA	パターンファイル	のアップ;	デートが必 1
	(1) リムーバブルストレージ	0		警告		0
	 ローカルまたはネットワークドライブ う>サムウェア対策機能の詳細 	0	+ セキュリティエージェントの油	創加 ◎ コンポーネントステ・	- タスの確	認
	ライセンスのステータス シートの使用率 3	IJ用数 □⊐		→ ご	〕 契	約ライ

25.レポート作成 1/2

セキュリティおまかせプランのご契約者さまには、毎月1度検出されたウイルスや不正コード等に関するレポートを登録されたメー ルアドレス宛に配信します。セキュリティの状況把握だけでなく、設定やポリシーの最適化検討を図る材料としても活用いただ けます。月次レポートだけでなく、お客様任意の期間・対象を選択し、出力いただくことも可能です。

<u> レポートの作成方法</u>

①管理コンソールにて、「レポート」⇒「追加」

≡	Worry Free [™] Business Security Services O 11:47 UTC+09:00					±		
ର 	レポート 検出された脅威の概要と詳細を確認できるPDFレポートを作成します。レポートには、最も脆弱なエンドポイントを特定するためのランキングも記載されます。							
	十 追加 前 削除							
四回		検索	生成↓	表示	有効			
		月1回	2023年05月1日 00:12:13	10				
÷								

※【セキュリティおまかせプラン】月次レポート_エンドポイントセキュリティは、開通時に登録している月次レポート となりますので、変更・削除しないようお願いいたします。(送付先メールアドレスは変更可)

25.レポート作成 2/2

エンドポイント/EDRセキュリティ

②任意のレポート名を入力します。

③レポートの予約を「検索」で指定します。

③対象のデバイスを選択します。

④レポートの内容を選択します。

⑤レポートの受信者のアドレスを 指定します。

⑥「保存」をクリックします。

レポート設定	\times
一般設定	
レポート名.*	
検索	
 1回限り □ 週1回 ○ 週1回 終了: Ⅲ 2023-04-21 	
対象	
 すべてのエンドポイント グループ 	
レポートの内容	
🕀 🗹 ウイルスパモプログラム	
🕀 🗹 スパイウェア/グレーウェア	
Webレビュテーション Webレビュテーション	
IRLフィルタ	
王 🗹 挙動監視	
🗄 🗹 デバイスコントロール	
田 🗹 ネットワークウイルス	
受偿者	
メールアドレス:	
例: user1@example.com; user2@example.com 体育・レポートは将たったた感信表演でにOPE形式の透けファイルとして详信されます	
action、レバー「FieldFill」とイロンス(Minergy Clumber 75 Upper (All Control Con	
	保存 キャンセル

26. 月次レポート確認方法 1/2

レポート通知メールの仕様変更に伴い2023年11月1日より、エンドポイントセキュリティの月次レポートの確認方法が変わります。

■変更概要

- レポートメールに添付しているファイルを削除し、管理コンソールへログイン後にレポートを確認
 いただくことでメール誤送信時の個人情報漏洩リスクを低減します。
- ・メール本文にて素早く検出概要を把握することが可能となります。

■変更内容

• 変更前

レポート通知メールにPDFファイルを添付。 添付ファイルの内容にてエンドポイント名・ 検出ファイルパス等を確認。

キュリティサービスレポート		
1 di mana n		
,pdf ∽		
ウイルス/不正プログラムが検出されたエンド	ポイント (サーバを除く)の上位5件
エンド ポイント	検出した脅威	%
該当なし	該当なし	該当なし
[
ウイルス/不正プログラムが検出る	されたサーバの上位5件	
エンド ポイント	検出した脅威	%
該当なし	該当なし	該当なし
	キュリティサービスレポート	キュリティサービスレポート

変更後

レポート通知メールの本文にて、 レポート概要・レポート名等を記載。 PDFのレポートファイルについては 管理コンソールヘログイン後、確認。

メールイメージ

件名:ウイルスバスター ビジネスセキュリティサービスレポート
本文:
新しいレポート月次通知レポート1 がYYYY/MM/DDに生成されました。
(レポート概要)
ウイルス/不正プログラム検出:あり
スパイウェア/グレーウェア検出:なし
ネットワークウイルス検出:なし
Webレピュテーション違反:あり
挙動監視違反:なし
デバイスコントロール違反:なし
URLフィルタ違反:なし

■レポート確認方法

- レポート通知メールに記載しているリンク先「Webコンソールにアクセス」から管理コンソールへ ログインします。その後、左側メニューから「レポート」を選択し、
 【セキュリティおまかせプラン月次レポート】(エンドポイント)」※を確認します。
 ※開通時のレポート名です。レポート名を変更している場合は任意のレポートを確認してください。
- ②「表示」欄から数字をクリックします。

	TRENDI ウイルスバスター ビジネスセキュリティサービス					
⋒ ダッシュポード ⋒ セキュリティエー	レポート 検出された脅威の概要と詳細を確認できるPDFレポートを作成します。レポートには、最も脆弱なエンドポイントを特定するためのランキングも記載されます。					
- - #	+ 追加 ① 削除					
一 内 #us		レポート		検索	生成 ↓	表示
<u>い。</u> - - - - -		【セキュリティおまかせプラン月次レポート】(エンドポイント)		月1回	2023年10月1日 00:09:44	10

③「レポート履歴」が表示されるため、対象のPDFをクリックし、レポートファイルを ダウンロード後、レポートの内容を確認してください。

パート履歴【セキュリティおまかせプラン月次レポート】(エンドポイント)						
前 削除						
開始:↓	終了:	生成	表示			
2023年09月01日	2023年10月01日	2023年10月1日 00:09:45	PDF			
2023年08月01日	2023年09月01日	2023年09月1日 00:09:48	PDF			
2023年07月01日	2023年08月01日	2023年08月1日 00:09:49	PDF			
	 ト履歴【セキュリティま 削除 開始:↓ 2023年09月01日 2023年08月01日 2023年07月01日 	−ト履歴【セキュリティおまかせプラン月次レポート 別除 期除:↓ 終了: 2023年09月01日 2023年09月01日 2023年09月01日 2023年09月01日 2023年09月01日 2023年09月01日	 ト履歴【セキュリティおまかせプラン月次レポート】(エンドポイント) 削除 開始:↓ 終了: 2023年09月01日 2023年10月01日 2023年09月01日 			

27. 管理コンソールログイン時のID・パスワードについて1/3

エンドポイント/EDRセキュリティ

PCにて管理コンソールへログインする際のPWをお忘れの場合は、下記手順よりリセットすることが可能です。※IDを忘れた場合も下記の手順にて確認することが可能です。

■ログインIDの確認・パスワードリセット方法

 LMPログイン画面にて「パスワードのリセット (パスワードをお忘れの場合)」を選択します。

パスワードリセット画面にてログインIDまたは、 メールアドレスを入力します。 その後、認証をチェックし、「送信」ボタンを クリックします。

※ログインIDをお忘れの場合は、登録している メールアドレスを入力してください。



Need	Need help signing in?				
© //	[©] スワードのリセット(パスワードをお忘れの場合)				
ਟੀ	自身のアカウントのログインDを入力してください。パスワードをリセットするためのメッセージが送信されます。ご質問がある場合は、 <u>サポートプロパ</u>				
⊴2	ダロお問い合わせください。				
⊡:	グインDまたはメールアドレス:				
□ 私	はロボットではあり				
ま	せん				
送信	E2				

③数分後、パスワードリセットメールが届きます。 メール内のパスワードリセット用のURLへ アクセスします。

※ログインIDをお忘れの場合はメール本文の 上部からID名を確認することが可能です。



④パスワードのリセット画面が開くため、
 新しいパスワードを設定してください。
 設定後、「送信」ボタンをクリックします。

※メールアドレスでリセットした場合 1つのメールアドレスで複数のアカウントを 登録している場合は、アカウント名の プルダウンからパスワードをリセットしたい アカウントを選択してください。

OTREND Licensing	Powered by 💋 IREND	
パスワードのリセット ログインIDを確認し、新しいパスワード	を入力してください。	
アカウント名: 新しいパスワード:		
パスワード の確認入力:	数子、大文子、小文子を使用した 6 文字以上2 ワードを投定してください。	5274 NO/CZ
送信		

27. 管理コンソールログイン時のID・パスワードについて 3/3

エンドポイント/EDRセキュリティ

⑤パスワード変更後、右図のような画面が表示 されます。「OK」ボタンをクリックし、 ログインしてください。

