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ご利用マニュアル (Ver 1.2)

2019年 6月 西日本電信電話株式会社



No	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



- 1. エンドポイントセキュリティ概要
- 2. ご提供の流れ
- 3. 機能一覧
- 4. 事前準備
- 5. 管理コンソールへのログイン方法
- 6. インストール
- 7.機能を設定する
- 8. アンインストール
- 9. レポート作成

- •••4p
- •••5p
- •••6~7p
- •••8p
- •••9~10p
- •••11~29p
- •••30~41p
- •••42~44p
- •••45~46p

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。



2.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、エンドポイントセキュリティ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。

3.機能一覧(1/2)

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	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				
		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ィ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 たは許可できます。また、ク を特 定できます。	の間に障壁を作り、特 ライアントに対する攻	定の種類のネッ トワーク 撃が疑われるネットワー	7トラフィックを拒否ま クパケットのパターン			
	挙動監視	0						
		OS、レジストリ、ソフトウェ	アに対する不正変更な	を監視・ブロックします。				
	POP3メール検索	0						
		POP3メールメッセージとその ルタイムに保護できます。	の添付ファ イルを介し	、て脅威が広まらないよう	うにコンピュータをリア			
	URLフィルタリング	0						
		業務上必要のないWebサイト の強度、ルール、時間帯等を Webサ イトを設定できます	へのアクセス制御を行 設定する ことで、お客	らいます。全体ま たはグ います。全体ま たはグ	ループ単位でフィルタ ふじて柔軟に規制対象の			

3.機能一覧(2/2)

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 します。	Eプログラムに似た特	性を示すと判定 されたフ	アイルを自動的に隔離	
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、ワイブ	(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://www.trendmicro.com/ja_ip/small-business/worry-free-services.html

※iOSでは、セキュリティおまかせプランのオプションサービスで提供しております「デバイスマネジメントツール」と 併用いただくことができません。

4.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

<Windows 7 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」

<Windows 8/8.1 の場合> 以下のいずれかの方法でアンインストールできます。 ・メトロ画面のアプリー覧から「コントロールパネル」 ⇒「プログラムのアンインストール」

・メトロ画面のアプリー覧から削除したいアプリを右クリックして「アンインストール」をクリックする

Windows 8.1 の場合は、デスクトップ画面にて、以下の手順でも可能です。 「スタートボタンを右クリック」⇒「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。

5.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=fWX6g</u>	— ログイン用URL
アカウントの詳細: アカウント名: TMF●●●●●●●●●●	― アカウント名
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:// ● ● ● ● ● ● ● ●	一 パスワード設定用URL
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。	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。
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)	Powered by Press Licensing Management Platform Powered by Press バスワードのリセット ログインIDを確認し、新しいVにスワードを入力してください。
【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D2: TMF1234512345 新しいパスワード: 数学、大文字、小文学を使用した 6 文字以上25文字以下のパス ワードを設定してください。
*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。	

5.管理コンソールへのログイン方法(2/2)

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=fWX6g

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ジネスセキュ リティサービス)の「コンソールを開く」をクリックします。

TREND Licensing Management Platform Powered by 多いいない とうこそに Kanadeguarder ログアウト								
登録済みの製品/サービス ユーザ登録情報	サポート情報							
登録済みの製品/サービス								
+キーの入力								
 サービスプラン名 	割品/サービス ↓	シート/ユニット 。	ライセンス種別 。	開始日 0	有効期限 🔻	アクション		
•	Cloud Edge 50	3 ジート	製品版	2017/11/15	自動更新	☑ コンソールを開く		
•	9(ルスル゙スタービン゙キスセキュリティサービス(この名称は絶対に変更しないでください) 働い	5シート	製品版	2017/11/15	自動夏斤	□ コンソールを聞く		

※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。

Morry Free	Business Secu	rity Service:		ログオン中のユーザ	アカウントホーム サインアウ
副新ステータス デバイス	8.8	18月 -	~\$7.		
1 ± #10(CF)	イスをVebコンソールに進	ulæ r .			デバイスの進始
セキュリティリスクの検出	出教				通知20日間 -
	() ()	短の景紙	0 #80 8 M	0 #UD-#R	
			影響を受けたデバイス		検出した機関
ウイルスボ正プログラム			a		D
スパイウエアグレーウエア			0		0
Webレビユテーション			a		D
3411-7-70-01-7			D		D

6-1.インストール (ダウンロード用URLの確認)

エンドポイント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

– ダウンロード用UR

6-1.インストール (ダウンロード用URLの確認)

<u>管理コンソールでの確認方法</u>

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」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、 「ビジネスセキュリティクライアントの追加」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。



③インストール方法の選択画面にて、 メールの詳細表示をクリックします。



6-2.インストール (Windows) 1/2

①メールまたは管理コンソールに記載のURLにアクセスし、 ダウンロードボタンをクリックします。

②インストーラのダウンロードが完了いたしましたら、 実行します。

※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。

③インストールのウィザードが起動しますので、「次へ」をクリックします。

④ダウンロードが開始されます。

イルスパスター ビジネスセキュリティサービス - Microsoft Edge	-	
fbs-svc-emea.trendmicro.com/wfbs-svc-tmsupport:77d83be8a4054c59	8247e9bae98254a0/dov	vnload/ja
	ity Services	
ビジネスセキュリティクライアントのインストール		
手順 1. 下の「ダウンロード」をクリックして、ダウンロードプロセスを開始 2. ファイル (WFBS-SVC_Agent_Installer.exe)のダウンロードが完了し ネスセキュリティクライアントのインストールを開始します。	します。 たら、ファイルをダブル・	クリックし
800-F		





6-2.インストール (Windows) 2/2

インストールに成功しました」のメッセージが表示されるので、
 「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		4770		×
		1		END c r o
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 トールされました。	スセキュリティクラー	イアントは	正常にイ	ンス
[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	++	ンセル]

[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]

ビジネスセキュリティクライア =	開通時初期設定 すべてのステータス・ 検索 Q ビジネスセキュリティクライアント:1						
 	+ ビジネスセキュリティ	クライアントの追加	@ 検索 -	🗐 ポリシーの設定		Ŕ	¢
サーバ (初期設定) 0	□ エンドポイント↑	前回の接続日時	IPv4アドレス	MACアドレス	ステータス	アーキテクチャ	ユーザ
デバイス (初期設定) 0		1日前					
開通時初期設定 1							

6-3.インストール (Mac OS) 1/4

①メールまたは管理コンソールに記載のURLにアクセスし、 ダウンロードボタンをクリックします。

②インストーラのダウンロードが完了いたしましたら、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。

ソネスセキュリティクライア	ントのインストール	
所有者情報		
管理者から要求された情報を	入力します。	
デバイス所有者: 名		
于殿		
1. 下の[ダウンロード] をク	リックして、ダウンロードプロセスを開始しま	§ -
 メッセージが表示された ファイル (WFRS-SVC A) 	>、デバイスのわかりやすい場所にファイルを使われていた。 tent Installer nkg zin)のダウンロードが完了し、	《存します。 たら、つァイルをダブルクリックしてビジネスセキュリティクライアントのイン
3. ファイル (WFBS-SVC_A	ent_Installer.pkg.zip) のダウンロードが完了し	たら、ファイルをダブルクリックしてビジネスセキュリティクライアントのイ



<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」を使い実行してください。



6-3.インストール (Mac OS) 2/4

③「続ける」をクリックし、インストールを進めます。

このバッケージは、ソフトウェアをインストールできるかどうかを判断するプログラムを実行します。 このコンピュータのセキュリティを保護するには、必ず信頼でき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ス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頼性を確信できない場合は、*キャンセル*をクリックして、プロ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さい。 キャンセル 続ける

④インストーラが起動しますので、「続ける」を クリックします。

⑤「続ける」をクリックします。

000	⇒ Trend Micro Security のインストール	₽
	ようこそ Trend Micro Security インストーラへ	
 e はじめに e インストール先の選択 e インストールの確範 e インストールの確範 e 板変 	このインストールプログラムガイドは、Trend Wicro Securityのインストールに必要な 学順を進って説明しています。 以下の場合、インストールを続行できません。 他に資件中のインストールフログラムがある場合 他に資件中のインストールフログラムがある場合 他のセキュリティソフトウェアをアンインストールするか 実行中のフログラムを停止させた後インストールしてください。 [続ける]をクリックして次に進みます。	
TREND	夏る 続ける	



6-3.インストール (Mac OS) 3/4

⑥サーバへの接続をテストします。 「続ける」をクリックします。

⑦標準インストール画面が表示されます。 「続ける」をクリックします。





🥪 Trend Micro Security のインストール

000



6-3.インストール (Mac OS) 4/4

⑨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。

①「インストールに成功しました」というメッセージ が表示されたら路登録は完了です。 「閉じる」をクリックして終了します。

※Macのアプリケーション内に右のようなアイ コンが作成されます。





<アプリのアイコン>



6-4.インストール (Android) 1/3

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、[ダウンロード]を タップし、インストーラーのダウンロードを開始します。

 ②「インストールに成功しました」というメッセージが 表示されたら路登録は完了です。
 「閉じる」をクリックして終了します。

③インストールが完了したら、「開く」をタップします。





6-4.インストール (Android) 2/3

④認証コードを入力します。

※メールまたは管理コンソール画面にて確認いただいた ダウンロード用URL下部に記載されたコードです。



ポリシーの設定で、「一般」>「データセキュリティ 対策の有効/無効の切り替えをユーザに許可する」が有 効の場合、右の選択画面が表示されるので、任意の機 能を選択し、「続行」をタップします。

※無効の場合は表示されません。

⑤使用許諾契約書に同意します。



使用許諾契約書	
すべての機能を利用するには、 <u>使用許諾契約書</u> に同意 する必要があります。	
同意しない	同意する

6-4.インストール (Android) 3/3

⑥デバイス管理機能を有効にするか選択する画面で「有効にする」をタップします。

⑦デバイスの登録が開始され、登録完了後、右の画面が表示さ れたら登録は完了です。

※Androidデバイス内のメニュー画面に右のようなアイコンが 作成されます。





デバイス管理機能を有効にします…

VBBSS

保護されています このデバイスは保護されており、最新の ポリシーに準拠しています。

6-5.インストール (iOS) 事前準備 1/4

 パソコンのブラウザ(Google ChromeまたはSafari) にて、管理コンソールにログインし、「管理」タブにて、 「モバイルデバイス登録設定」を選択後
 「APNs証明書のアップロード」をクリックします。

②手順1でTrend Micro CSR(Certificate Signing Request)をダウンロードします。

③手順2で 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>) ヘアクセスし、 サインインします。

④手順2でダウンロードした証明書を手順3の欄に、
 ③でサインインしたApple IDを入力し、アップロードを
 行う。



手順1. Trend Micro Certificate Signing Request (CSR)をダウンロードします

Trend Micro CSRのダウンロード

Sign In.

Apple ID

Forgot your Apple ID?

Password

Forgot your password?



6-5.インストール (iOS) 事前準備 2/4

⑤Get Started画面が表示されます。 「Create a Certificate」ボタンをクリックします。



⑥「Terms of Use」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。



6-5.インストール (iOS) 事前準備 3/4

⑦「Create a New Push Certificate」画面が表示されます。
 「参照」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。

⑧「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。





6-5.インストール (iOS) 事前準備 4/4

⑨手順2でダウンロードした証明書を手順3
 の欄に、③でサインインしたApple IDを入力し、アップロードを行う。

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) をアップロードします。

Apple ID:			
証明書:	ファイルの選択…		
APNs	明書のアップロード		

10アップロードした証明書が表示されます。

APNs計明書。	
iOSデバイスの管理 注意: 証明書の有	割コよ、有効なAPNs (Apple Push Notificationサービス) 証明書が必要です。有効な証明書を 効期限が近づくと、自動的に管理者に通知が送信されます。
証明書の詳細	
シリアル番号 ()	
UID	
有効期限	2015年06月30日
Apple ID 🕦	ai 🦉
APNs IIBE	第46 語語目集合の通信後
使用許諾契約書	- 文面の設定 💿 💿 (スペの・クノストール特には使用)注意的語いが表示されます。(エンドユーザがこの使用)注意 全合よ デンプレードとしてお使いいたらにとき想定した文面をご用意していますが、お客様の
使用許諾契約者 Android/iOSデバイ この画面の利期職 使用許諾契約書 本使用許諾契約書 当社は、モバイル に提供したバイル 「サービス」とは 管理、識別、認知	- 文面の設定 - 文面の設定 こののクノストール特には「使用ド港契約書」が表示されます(エンドユーザがこの使用)計制 を含ま、テンプレードとしてお使いいだとことを想定した文面をご用意していますが、お客様の において、「当社」とは、ユーザに、以下に定義するサービスを提供する組織を意味す デバイスから当社の企業データへのアクセスを、セキュリティの確保された状態で行う だし、このサービスを受けるには、一定の契約条件を理解し同意することが条件ですの 5 5 5 5 5 5 5 5 5 5 5 5 5
使用許諾契約書 AndroidfiOSデバイニの画面の利期職 使用許諾契約書 本使用許諾契約書 当社は、モバイル、 1、サービスの内容 「サービス」とは 管理、識別、認証 本サービスで該当す こもよいものと 2、サービスの使用	- 文面の設定 - 文面の設定 こへの-(ノストール特には「使用ド語契約書」が表示されます(エンドユーザがこの使用注語) 定ては、デンプレードとしてあ使いいだことを想定した文面をご用意していますが、お客様の において、「当社」とは、ユーザに、以下に定義するサービスを提供する組織を意味す デバイスから当社の企業データへのアクセスを、セキュリティの確保された状態で行う だし、このサービスを受けるには、一定の契約条件を理解し同意することが条件ですの 製品。コンピュータブログラム、サービス、および当社ウェブサイトで構成されるも 1、設定、安全確保することに、これらを利用できるものとします(総称して「本サービブ 電子メール、苗宇、名前、全地球期位システム (GPS)上のデバイスの位置、デバイスの 電話会社の情報、デバイス上にインストールされたアブリケーショ します。

6-5.インストール (iOS) 1/3

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。 ※ブラウザはSafariをご利用ください。

②認証コードを入力します。 ※メールまたは管理コンソール画面にて確認いただいた ダウンロード用URL下部に記載されたコードです。

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。

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。





6-5.インストール (iOS) 2/3

- ⑤「プロファイル」の画面が表示されます。 「インストール」ボタンをタップします。 警告画面が 表示されますが、内容を確認の上、右上の「インストール」 をタップします。
 - ※「インストール」タップ後に、「リモート管理」の画面が 立ち上がる場合は、「信頼」をタップします。

T (a)	rend Micro Wo	orry-Free
	検証済み	(ンストール
説明		
軍空入り	wfbs-svc.trendmic	ro.com
有口八了		
受信日	2014/06/30	



6-5.インストール (iOS) 3/3

⑥「パスコードを入力」画面が表示されます。 お使いのデバイスのパスコードを入力してください。

⑦「インストール完了」画面が表示されます。 右上の「完了」をタップしてください。

⑧ブラウザ上で「正常にインストールされました」と 表示されますので、画面を閉じてください。 これでインストールは完了です。



-	インストール完	了 完了
	rend Micro W ●検証済み	orry-Free
説明		
署名入り	wfbs-svc.trendmi	icro.com
受信日	2014/06/30	
内容	2 証明書	



7-1.機能を設定する(Windows)

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	31
ファイアウォール	無効	有効/無効から選択	32
挙動監視	有効	有効/無効から選択	33
ランサムウェア対策機能	有効	有効/無効から選択	34
機械学習型検索	無効	有効/無効から選択	35
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	36
承認済み/ブロックURL登録	無し	追加登録可	37
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)	38
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)	39
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)	40
アラート設定	有効	アラート受信者の変更・追加	41

※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。

(http://esupport.trendmicro.com/ja-jp/enterprise/vbbss/top.aspx)

7-2.機能を設定する(Webレピュテーション)

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「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。

Line output Line Lin	ios	Webレビュテーションは不正Web	サイトの脅威からの保護を強	化します。		
Child Section CE 2 JUF / L / L / L Martin Backin Chik Bot TAB TaB TaB Mobul / 2	度からの保護機能 検索設定					
市政協会 市政法会 市政公式部 市政公式部 市政部 市 日本 市 日本 市 日本	挙動監視	セキュリティレベル				
Webビセュテーション アイパ 'リオールほど 構成高えい対策 デバイスコントロール 構成高ない対策 かせえコントロール URLフィルタ アプリケーションコントロール MUスト 構成添か 系磁気み/ブロックするURL ライアントの設定 () 高 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・			危険	極めて不審	不審	未評価
2747/04 - ル設定	Webレビュテーション	 高 	~	~	~	~
は渡えい好差 Fパイスコントロール 離聴見い好強 Pプロスントロール RUスコントロール RUスコントロール Pプログーションコントロール AW25 FW25	ノアイアワオール設定	中 (初期設定)	~	~		
	服漏えい対策 デバイスコントロール。	○ 低	~			
セスコントロール IRLフィルタ プラウザ脆弱性対策 プラウザ	青報漏えい対策	✓ WebサイトのアクセスをJ	ブロックします 🗊			
IRLフィルタ IRLフィルタ アプリケーションコントロール ・リスト ・ シスト 参数除分・ 全数語み/プロックするURL 9イアントの設定	7セスコントロール	ブラウザ脆弱性対策				
アプリケーションコントロール 4リスト 食業総称・ 発起着み/プロックするURL 9イアントの設定	JRLフィルタ	一下 不正スクリプトを含む	Wehサイトをブロックする			
AUスト 検索論か/ 手部満み/プロックするURL ライアントの設定	アプリケーションコントロール					
原始後か 季認満み/ブロックするURL ライアントの設定	トリスト					
#80月のノロッジックURL ライアントの設定	東来は21					
パイントの設定	AND/ANYJUYYYOURL					
復眠およびその他の段度	ァイアントの設定 権限およびその他の設定					



7-2.機能を設定する(ファイアウォール)





ポリシーの設定:開通時初期設定

|--|

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。

1112 2 - State Mages 1014	
 ☆ 対象とサービスの設定 ● 貸款からの保護機能 ● 検索設定 ● 挙動監視 ● 機械学習型検索 ● Webl メビュテーション、 	 ファイアウォール設定 ファイアウォールは、エンドボイントとネットワークの間にバリアを作成することによって、特定の種類のネットワークトラフィックをブロックまたは許可できます オン 注意:ファイアウォールを有効または無効にすると、一時的にエンドボイントがネットワークから切断されます。接続の中断による影響を最小限に抑えるため、影響少ない時間に設定の変更を行ってください。 第単モード トレンドマイクロの初期設定を使用 詳細モード セキュリティレベル、侵入検知システム、および除外を設定
 ファイアウォール設定 (情報調えい対策 デバイスコントロール 「情報調えい対策 アクセスコントロール URLフィルダ アプリケーションコントロール 膝外リスト 検索協外 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 	



7-3.機能を設定する(挙動監視)





ポリシーの設定:開通時初期設定

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。

♀ 对舔	29-1	こ人の設	(正
-	ú	-	iOS
脅威から	の保護機	lite	
 検索影 	淀		
● 挙動2	這視		
● 機械的	藿智型検	索	
• Webl	ピュテ	ーション	<u>/</u>
ファイ	(アウォ	ール設定	2
情報漏え	い対策		
● デバー	バスコン	トロール	/
● 情報源	見えい対	策	
アクセス	コントロ	1-14	
• URL	7-1ルタ		
● アプリ	リケーシ	ヨンコン	ノトロール
除外リス	Þ		
検索隊	彩		
承認演	<i>₩ブロ</i>	ックする	SURL
クライア	ントの話	定	
権限ま	らよびそ	の他の影	淀

学動監視 挙動監視は、オペレーティングシステム、レジストリエントリ、その他のソフトウェア、ファイルやフォルダへの不正な変更からエンドポイントを保護しま す。

() オン

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。

不正プログラム挙動プロック
オン
◎ 既知および潜在的な脅威のブロック
○ 既知の脅威のブロック
ランサムウェア対策
✓ 不正なファイル暗号化や変更から文書を保護 (1)
☑ 不審なプログラムによって変更されたファイルを自動的にバックアップして復元 ④
🗹 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 🗊
🗹 プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック 🕢

脆弱性対策

脆弱性攻撃に関連する異常な挙動を示すプログラムを終了

() オフ

Intuit™ QuickBook™保護

QuickBooks™ファイルおよびフォルダへの不正な変更を防止

75 🔘

イベント監視

システムイベントを監視して潜在的に不正な処理を検出します 🗊

7 17

R存 キャンセル

X

7-4.機能を設定する(ランサムウェア対策)

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「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。

● 対象とサービスの設定 举動監視 **挙動監視は、オペレーティングシステム、レジストリエントリ、その他のソフトウェア、ファイルやフォルダへの不正な変更からエンドポイントを** ú iOS す。 脅威からの保護機能 () オン 検索設定 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。 ● 機械学習型検索 不正プログラム挙動プロック • Webレビュテーション (1) オン ファイアウォール設定 ・ 既知および潜在的な脅威のブロック 情報漏えい対策 ○ 既知の脅威のブロック デバイスコントロール ランサムウェア対策 信報漏えい対策 ✓ 不正なファイル暗号化や変更から文書を保護 ④ アクセスコントロール ✓ 不審なプログラムによって変更されたファイルを自動的にバックアップして復元 ① • URIフィルタ ☑ 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 ③ アプリケーションコントロール ✓ プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック (i) 除外リスト 榆索除外 脆弱性対策 承認済み/ブロックするURL 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 クライアントの設定 77 17 権限およびその他の設定 Intuit™ QuickBook™保護 QuickBooks™ファイルおよびフォルダへの不正な変更を防止 77 17 イベント監視

システムイベントを監視して潜在的に不正な処理を検出します (i)

77

7-5.機能を設定する(機械学習型検索)

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「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
- ⑤プロセスに対する処理を選択します ⇒終了 or ログのみ
- ⑥「保存」をクリックします。

✿ 対象とサービスの設定	機械学習型検索
📫 单 ios	トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジを使用して、リムーバブルストレージ、Web、メールを経由する不審なプロセスやファ まれる蔓延前の未知のセキュリティリスクを検出します。
脅威からの保護機能 ● 検索設定 ● 特殊部に ● 機械学習型検索	また オン 注意: 機械学習型検索には以下が必要です。 ・ ・ 挙動監視の有効化 ・ Smart Protection Networkに接続するためのインターネット接続
● Webレビュテーション	検出設定
 ファイアウォール設定 情報漏えい対策 デバイスコントロール 	 理項 処理 ✓ ファイル 隔離 ▼
 情報漏えい対策 	 ブロセス 終了 ①
アクセスコントロール • URLフィルタ	



7-6.機能を設定する(URLフィルタリング)

- 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URLカテゴリを指定します。
 ※初期値は「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。



🛚 🤹 🌲 ios	コメルク独臣		
なからの保護性能 検索設定 特勤監視 ARK学習型検索 Vebレビュテーション 7アイアウォール設定	 、東ジロ東には蒙華的な地で は常幼園に常く響きる可能 ・ ・ ・	ニリティ上の骨鉱、不適切なコンテンツま 2性のあるコンテンツ、および未評価のペー 2骨質および不適切なコンテンツをブロック 2骨質をブロックします 7リを指定する	たは有害である可能性のあるコンテンツ、生産性家だ ジモブロックします します
暗えい対策 バイスコントロール	フィルタルール		and the second second second
報源えい対策	URLカテゴリ	• 業務時間	二)業務時間外
alexent to a	王 アダルト		
RLJTUS	田 ビジネス		
/ブリケーションコントロ -ル	□ Ξミュニケーションメディア		D.
リフト	⊞ -殿		
國際外	団 インターネットのセキュリティ		
認済み/ブロックするURL	L ヨイフスタイル	0	
90000722779 2000			



7-7.機能を設定する(承認済・ブロックURL登録)

- 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」 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。



▶ 対象と	サービスの	没定	承認済み/ブロックするURLのリスト	0
-	£ 🐥	IOS	季認済みフロックするURLはWebレビユテーションおよひURLフィルタに適用されます。	
風からの	(保護)(注意)		使用除外:	
検索設定	5		○ グローバル承認済みおよびブロックするURLのリスト ①	
辛動監視	ŧ		 除外の指定 	
機械学習	型検索		承認済みURL (15) ブロックするURL (0)	
WebLL	(ユテーショ	2		
ファイア	クウォール設	定	+ 追加 -	合計: 15
開掘えい	\对策			
デバイス	(コントロー	16	律师用的URL	
情報漏え	い対策		http://*.trendmicro.com/*	A
クセスコ	コントロール		https://*.trendmicro.com/*	
URLフィ	ルタ		http://www.trendmicro.com/*	
アプリケーションコントロ ール http://wustat.windows.com/*				
外リスト	4		http://windowsupdate.microsoft.com/*	
検索除外	F		http://uk.trendmicro-europe.com/*	•
承認済み	#ブロックす	SURL		
/ライアン 種限およ	・トの設定 、びその他の	設定	webアビュナデンヨンで語って方規されている可能性の必らURLを通知するか、URLの安全性の評判を確認す スしてください。 http://sitesafety.trendmicro.com/	BILLY WOWEDDA NEWDE

URL: (j)	



7-8.機能を設定する(アプリケーションコントロール)

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「アプリケーションコントロール」を選択

- ③「アプリケーションコントロールのオンオフ」を 選択します。
- ④アプリケーションの管理を選択し、対象のアプリケーションを指定します。
- ⑤「保存」をクリックします。



7 – 9.機能を設定する(デバイスコントロール)



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 選択します。

④対象のデバイスの権限をそれぞれ選択します。

⑤USB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。

⑥「保存」をクリックします。

ビジネスセキュ ント	リティクライア 耳	開通時初期語	设定	すべての	ステータス • 検索
IT I		ビジネスセキュリティクライ	アント:1		
- 🖵 📮 すべてのと	ジネスセキュリティ (1)				Bi Burn and
👃 🔺 🚞 手動グルー	プ	+ ビジネスセキュリティク	フイアントの追加	() (AR - 1	■ ホリシーの設定
サーバ(初	期設定) 0	□ エンドポイント ↑	前回の接続目時	IPv4アドレス	MACPFUZ
ビーデバイスの	初期設定) (0)				
目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目目	アーンノアイルを使用 (1)				
□ ビジネスセ	パキュリティサービス 0				
は毎とサービフの記字	ニッパノフコント				
MIRCO CAUGUE	デバイスコントロールは、周	・ ローノレ 周辺デバイスへのアクセスを制御しる	ます。		
📫 💰 🌲 ios					
威からの保護機能	() オン				
検索設定	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愛	2更防止サービスを有効	にする必要かありま	<u>g</u> .
挙動監視	ストレージデバイス				
機械学習型検索					
Webレビュテーション	CD/DVD: (i)	フルアクセス	-		
ファイアウォール設定	ネットワークドライブ:	フルアクセス	*		
部編えい対策	USBストレージデバイス	: フルアクセス	*		
デバイスコントロール		□ 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	
情報漏えい対策					
クセスコントロール	モバイルデバイス				
URLフィルタ		5 L 7			
アプリケーションコントロール	XFU-5:	2±2 ₹			
外リスト 検索除外	ストレージ以外のデバイス				
承認済み/ブロックするURL	Bluetoothアダプタ:	💿 許可 🔘 ブロック			
ライアントの設定	COMおよびLPTポート:	💿 許可 🔘 ブロック			
権限およびその他の設定	IEEE 1394インターフェ	ース: 💿 許可 🔘 ブロック			
	イメージングデバイス	💿 許可 🔘 ブロック			
	赤外線デバイス:	💿 許可 🔘 ブロック			
	モデム:	◎ 許可 ○ ブロック			
	プリントスクリーンキー	: • 許可 〇 ブロック			
	ワイヤレスNIC:	🧿 許可 🔘 フロック			

7-10.機能を設定する(アンインストール防止)

6

ς'n

 ①管理コンソールにて、
 「ポリシー」⇒「グローバルビジネスセキュリ ティクライアント設定」

②「クライアントコントロール」を選択

③「アンインストール」にて、「ビジネスセキュ リティクライアントのアンインストール時にパス ワード入力を要求する」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 Fi	ree [∞] Business Security Services
 でです。 では、 でのです。 でです。 ででです。 ででです。 ででです。 ででです。 でです。 ででです。 ででです。 ででです。 ででです。 ででです。 ででです。 ででです。 ででです。 ででです。 でででででででででで	グローバルビジネスセキュリティクライアント設定 グローバル度定はサポートされるすべてのビジネスセキュリティクライアントに適用されます。 セキュリティ設定 クライアントコントロール 警告 ② 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タスクバーには ビジネスセキュリティクライアントのログ ③ 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 監視サービス ② ビジネスセキュリティクライアントの監視サービスを有効にする: ビジネスセキュリティクライアントのステータスを 1・ グ目電で電話 ビジネスセキュリティクライアントを再起動できない場合、 5 * 管理者への問い合わせの通知
	 管理者への間い合わせの通知 ビジネスセキュリティクライアントに管理者への問い合わせ情報を表示する アンインストール ビジネスセキュリティクライアントのアンインストール時にパスワード入力を要求する

7-11.機能を設定する(アラート設定)

①管理コンソールにて、「管理」⇒通知を選択

②「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

③ページ下部の「保存」をクリックします。

管理	通知		
一般設定	要確認および営告イ ストについては、通	ヘントのメールメッセーンを送信するようにワイルスハスター ビンイスセキュリュ 知のカスタマイズを参照してください。	
モハイルテハイス登録設定	設定要研	確認 警告	
通知	送信者	WFBS-SVC@TrendMicro.com	
Active Directoryの設定 Smart Protection Network	受信者:		
回復キーのパスワード			
ツール		複数入力する場合は、セミコロンで区切ってください。	
ライセンス情報		例: user1@example.com; user2@example.com	
	件名の先頭の文字列	I: SumRansomware	
Webコンソール設定			



TREND Worry Free" Pusiness Security Corvises

※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。

8-1.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。



④「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、該当デバイスが消えます。

⇒管理コンソール上での作業は以上で終了です。 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。 8-2.アンインストール

クライアント側での実施方法(Windows7の場合)

①コントロールパネルのプログラムにて、「プログラムのアンインストール」をクリックします

②表示された一覧の中から、「ビジネスセキュリティクライア ント」をダブルクリックします。

③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。

⇒アンインストール処理が進んでいきます。

④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、再起動します。

操作は以上で終了です。

※アンインストール完了後、 管理コンソール上で対象デバイスが表示されている 場合は、前ページの手順にて削除をお願いします。



<参考>利用ライセンス数の確認方法

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。

キュリティリスクの検出数		
	~ ~	
	● ● 100% 田和の會成	
イベントの種類		影響を受けたエンドボイント
ウイルス/不正プログラム		<u>io</u>
スパイウエア/グレーウエア		0
webレビュテーンヨン		0
ンサムウェアの概要	過去30日間 👻	ビジネスセキュリティクライ
() ランサムウェアに関連した処理	ia.	() ビジネスセキュリティクライア
Web Web	D	
クラウド周期	D	0 デスクトップパサーバ
×-л.	0	
(学) 自動実行ファイル	D	0 モバイルデバイス
ローカルまたはネットワークドライブ	D	
ランサムウェア対策機能の詳細	ランザムウェア対策を有効にする	+ ビジネスセキュリティクライアント
	有効期限: 2018年09月30日)
		Î.

9.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」

	TREND Worry Free* Business Security Services			
ດ	レポート			
50	積出された管威の敬妻と詳細を確認できるPDFレホー	トを作成します。レポートには、最も腕髄なエンドボイントを特定するためのランキンクも記載されます。		
ය	十道加 首 制除			
-	□ レポート	検索		
		1回限り		
0		1回限り		
B		1回限り		
		1回限り		
<u>ن</u>		1回限り		
	□ 月一回	月1回		

※【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)

9.レポート作成 2/2

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。

レポート設定

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。

Fャンセル

X