RICOH

# ITKeeper シリーズ
# クラウドサービス　for　MVB
# クラウドサービス　for　MVB　EDR

## ユーザーマニュアル　V3.2 マニュアルについて：

※　本マニュアルは以下サービスに関する共通のマニュアルとなります。

『クラウドサービス　for　MVB』

『クラウドサービス　for　MVB　EDR』

※　本マニュアル内掲載画面イメージとお客様環境では表示が異なる場合がございます。

改訂履歴：

| Version | 改訂日 | 更新内容 |
|---|---|---|
| 1.0 | 2012/07/05 | 初版作成 |
| 1.1 | 2012/08/07 | UI の修正 |
| 1.2 | 2013/03/08 | Windows 8 対応 |
| 1.3 | 2013/06/27 | Windows Server 2012 対応 |
| 1.4 | 2013/10/11 | Android OS 対応 |
| 1.5 | 2014/07/07 | Android OS 更新、Windows8.1 対応 |

| | | |
|---|---|---|
| 1.6 | 2014/11/06 | Google Chrome 対応 |
| 1.7 | 2015/04/10 | 動作環境の修正<br>UI の修正<br>Windows と Android の機能比較の修正 |
| 1.8 | 2017/06/21 | Windows Server 2016 対応<br>Windows 10 対応 |
| 1.9 | 2018/09/04 | VBBSS6.5 対応 |
| 2.0 | 2019/01/10 | P44　ルート証明書/中間証明書の URL 更新 |
| 2.1 | 2020/01/27 | Windows Server 2019 対応<br>クライアントソフトの表示変更<br>（VBBSS6.6 から「ビジネスセキュリティクライアント」⇒「セキュリティエージェント」に変更） |
| 2.2 | 2020/03/24 | UTM と同時利用時の留意事項追記 |
| 2.3 | 2020/09/10 | UTM と同時利用時の留意事項修正 |
| 2.4 | 2020/10/21 | 対応 OS 改訂<br>FAQ 追加 |
| 2..5 | 2021/04/28 | FAQ.7 変更 |
| 2.6 | 2022/3/8 | Windows11 対応<br>Windows Server 2022 対応<br>付録 B：サーバと AA 間の通信について修正<br>FAQ.10 変更 |
| 2.7 | 2022/5/13 | インストール完了台数確認方法追加 |
| 2.8 | 2023/6/13 | お問い合わせメールアドレス変更 |
| 2.9 | 2023/10/23 | 対応 OS 改訂 |
| 3.0 | 2024/3/28 | クラウドサービス for MVB EDR サービスについて追加 |
| 3.1 | 2024/6/6 | お問い合わせメールアドレス変更 |
| 3.2 | 2024/6/21 | Android OS インストール手順変更 |

本マニュアルは最終改訂日現在の情報を元に作成しております。

# 目次

【第1章】　Windows OS 編 ..... - 4 -
1. 事前環境確認 ..... - 5 -
2. システム要件 ..... - 6 -
3. インストール手順 ..... - 8 -
4. Web 管理コンソールへのログイン手順 ..... - 20 -
5. Web 管理コンソールの機能について ..... - 23 -
6. クライアント用コンソールの機能について ..... - 27 -
7. アラート通知、レポート通知メールについて ..... - 28 -
8. アンインストール手順 ..... - 32 -

【第2章】　Android OS 編 ..... - 37 -
1. 事前環境確認 ..... - 38 -
2. システム要件 ..... - 38 -
3. インストール手順 ..... - 39 -
4. アンインストール手順 ..... - 45 -

【第3章】　FAQ・付録　編 ..... - 47 -
1. 関連情報 ..... - 48 -
2. FAQ ..... - 49 -
3. 付録 ..... - 57 -

RICOH

ITKeeper シリーズ

クラウドサービス　for　MVB

クラウドサービス　for　MVB　EDR

# 【第1章】　Windows OS 編

## 1. 事前環境確認

### 既存アンチウイルスソフト等の確認と対処

- 他のウイルス対策、スパイウェア対策ソフトが導入されている又は、正常にアンインストールされていない場合、クライアントのインストールが正常に行われず、プロセスやフォルダが存在しない、アイコンがオフラインになる、通信が出来ずパターン更新がされない等の現象が発生する可能性がございます。
  他のウイルス対策、スパイウェア対策ソフトが導入されている場合は、そのアプリケーションのアンインストールをお願いいたします。

※ クラウドサービス for MVB（以下 CSMVB）のインストール時に自動的に削除されるウイルス対策、スパイウェア対策ソフトもありますが、CSMVB インストールの際には、事前に各メーカーホームページを参照の上、他のウイルス対策、スパイウェア対策ソフトのアンインストールを実施してください。

### ファイアウォール、通信に関する問題

- クライアントの通信（パターンファイル取得、サーバへのログ送付等）には、インターネットに向けて SSL で 443 ポートでの通信を行います。また、パッケージのダウンロードには 80 ポートでの通信を行います。詳細は、[付録 B：サーバと AA 間の通信について]をご参照ください。

### 再起動について

- 利用状況によって、インストール・アンインストールを完了するには再起動が必要です。再起動しても問題が無いことを確認して作業してください。
- 再インストールまたはアップグレードを完了するには、コンピュータを再起動する必要があります。また、ファイアウォールやプロキシドライバなどのコンポーネントをアップデートしたときも、再起動が必要です。

### Windows Defender 無効化について

- Windows Server OS へ MVB インストールする時は、手動で Windows Defender 無効化する必要があります。
  Windows Defender とは、Microsoft 社が Windows に標準で搭載している、悪意のあるファイルやソフトウェア（ウイルスやスパイウェアなど）を検出し、削除するソフトウェアです。
  MVB でご提供するビジネスセキュリティサービスには、同様の機能があるため、競合が発生し、コンピュータの動作に影響を与える可能性があります。
  そのため、ビジネスセキュリティサービスをインストールする際は、Windows Defender を無効にしてください。
  詳細・手順については、下記トレンドマイクロ社 Web ページと、Microsoft 社 Web ページをご参照ください。
- トレンドマイクロ社 Web ページ
  『Windows Defender との併用について』
  https://success.trendmicro.com/jp/solution/1105933

- Microsoft 社 Web ページ『Windows セキュリティによる保護を利用します』
  http://windows.microsoft.com/ja-jp/windows/turn-windows-defender-on-off

## 2. システム要件

CSMVB のシステム要件は以下の通りです。

但し、下記の動作環境を満たしていても、その他ソフトウェア利用状況等により、PC／スマートデバイス／サーバの動作が遅くなる場合や、ご利用頂けない場合がございます。

◆ ソフトウェア動作環境

| | | |
|---|---|---|
| パソコン<br>（Windows） | 対応 OS<br>（※1） | Windows 10 Home/Pro 22H2 (※)<br>Windows 10 Pro for Workstations<br>Windows 10 Enterprise/Education November 2021 Update/22H2 (※)<br>Windows 11 Home/Pro/Enterprise/Pro for Workstations/22H2<br>Windows 10 Enterprise 2015 LTSB / 2016 LTSB / LTSC 2019 / LTSC 2021<br>Windows 10 IoT Enterprise LTSC 2019 / LTSC 2021<br><br>※Windows 10 Mobile には対応しておりません。 |
| | メモリ | 1GB 以上、2GB 以上を推奨 |
| サーバ<br>（Windows） | 対応 OS<br>（※1） | Windows Server 2016 Standard/Essentials<br>Windows Server 2019 Standard/Essentials/Datacenter<br>Windows Server 2022 Standard/Datacenter/Datacenter: Azure Edition<br>Windows Storage Server 2016 Workgroup/Standard（※）<br>Windows Server IoT 2019 for Storage Workgroup/Standard（※）<br>Windows Server IoT 2022 for Storage Workgroup/Standard（※）<br><br>※富士通株式会社製の一部対象機器に限ります。SV パックの対象機種に準じます。SV パックの対象機種一覧にてご確認ください。 |
| | メモリ | 2GB 以上、8GB 以上を推奨 |
| Windows 共通 | CPU | x86 アーキテクチャの Intel Pentium4 プロセッサまたは互換プロセッサ<br>x64 アーキテクチャのプロセッサ（AMD 64 テクノロジおよび Intel EM64T テクノロジ対応）<br><br>※各対応 OS が、快適に動作すること<br>※IA64(Itanium プロセッサ)、および ARM プロセッサには対応していません。 |
| | ハードディスク | 1.5GB 以上の空き容量、2GB 以上を推奨 |

| | | |
|---|---|---|
| | Web ブラウザ（ソフトウェアインストール、Web レピュテーション、URL フィルタ） | Internet Explorer 11.0（※2）<br>Mozilla Firefox（※3）<br>Google Chrome（※3）<br>Microsoft Edge（※3） |
| | ディスプレイ | 256 色以上、解像度 800x600 ピクセル以上 |
| その他対応機種 | | RICOH e-Sharing Box タイプ M4（※4） |

※1：各 OS の主要エディションおよび 64 ビットバージョンを含みます。
マイクロソフト社の対応OSサポートの終了に伴い、本サービスもサポート対象外となります。

※2：Internet Explorer 11 は Windows (Modern) UI 上での利用には対応していません。
また、マイクロソフト社 が Internet Explorer 11 をサポートしている OS 上で動作している場合にサポートします。

※3：最新バージョン含め3世代のバージョンをサポートします。

※4：商品詳細につきましては、『RICOH MP C6003/C5503/C4503/C3503/C3003』の発売通知を確認ください。
RICOHe-Sharing Box タイプ M3 は OS が Windows7 であるため、サポート終了しています。

※MacOS および iOS についてはサポート対象外となります。

◆ 管理画面（Web）動作環境

| | | |
|---|---|---|
| Web 管理サイト | Web ブラウザ | Internet Explorer 11.0（※1）<br>Mozilla Firefox（※2）<br>Google Chrome（※2）<br>Microsoft Edge（※2） |
| | PDF リーダー（レポート用） | Adobe Acrobat Reader 6.0 以降（最新バージョン推奨） |
| | ディスプレイ | ハイカラー、解像度 1366×768 ピクセル以上 |

※1：Internet Explorer 11 は Windows (Modern) UI 上での利用には対応していません。

※2：最新バージョン含め3世代のバージョンをサポートします。

本書に記載の内容は、OS のサポート終了、トレンドマイクロ社による製品の改良などの理由により、予告なく変更となる場合があります。

最新の情報については、トレンドマイクロ社の下記サイトをご参照ください。

「ウイルスバスター™ ビジネスセキュリティサービス」

https://www.trendmicro.com/ja_jp/small-business/worry-free-services.html

## 3. インストール手順

【概要】

CSMVB クライアントインストール方法は、以下の 2 通りあります。

※再起動が発生する場合がありますので、再起動しても問題が無いことを確認して作業してください。

❖ Welcome メールを利用したインストール

Welcome メールは CSMVB サービス開始時に送られてきます。

この Welcome メールを利用してのインストールは、以下の手順で行います。

- Welcome メールに記載されているインストール URL をクリックします。
- ダウンロードが始まりますので、インストールを実行します。（詳しくは【詳細】に記載）

❖ Web 管理コンソールからのインストール

Web 管理コンソールにログインしてインストールすることも可能です。

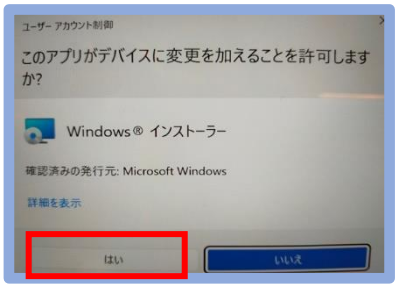
Welcome メールを無くしてしまった場合などに行います。

- Web 管理コンソールにログインします。([4 Web 管理コンソールへのログイン手順]を参照)
- [セキュリティエージェント]-[セキュリティエージェントの追加]をクリックします。
- [インストール]をクリックします。※Web 管理コンソールのパスワードを忘れてしまった場合、FAQ1 を参照してパスワードを初期化してください

【詳細】

※10／11 の場合、

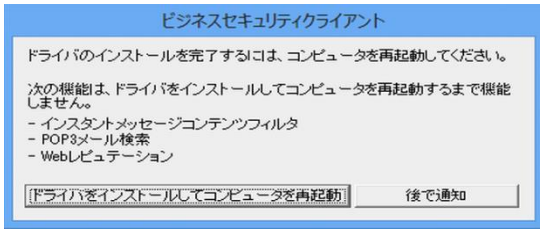
インストール途中に「ユーザーアカウント制御」のメッセージが表示されることがあります。 [はい]をクリックしてください。

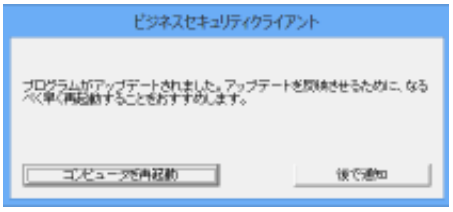



※インストール完了後に、下図のような再起動を促すメッセージが表示される場合があります。

・すぐに再起動しても問題ない場合は、[再起動]をクリックします。

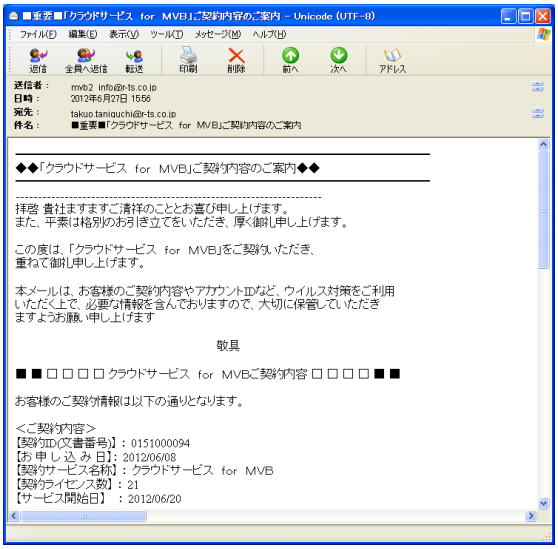
・すぐに再起動しない場合は、[後で通知]をクリックします。



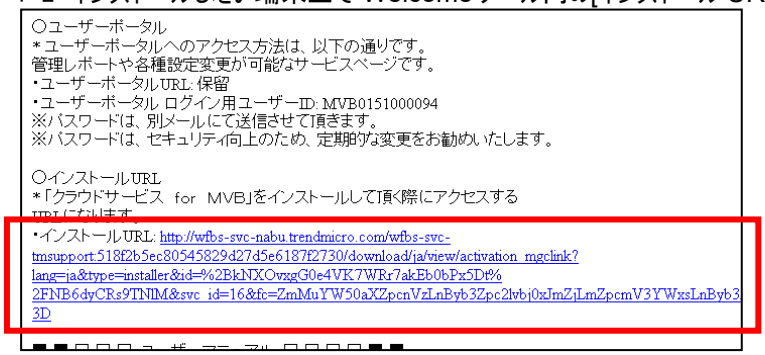



## 3-1 Welcome メールを利用したインストール方法（Windows OS）

3-1-1 CSMVB サービス開始準備が完了しますと、以下のような Welcome メールが送付されます。

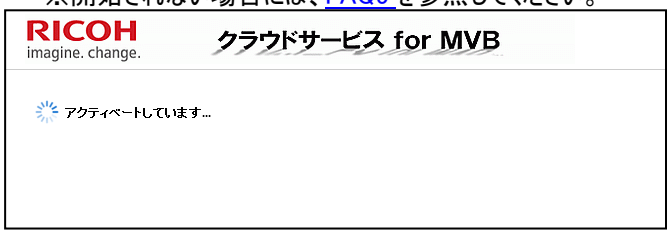



3-1-2 インストールしたい端末上で Welcome メール内の[インストール URL]をクリックします。




※インストール URL は、お客様毎に異なります。

3-1-3 ブラウザが自動的に開き、アクティベートが開始されます。
※開始されない場合には、FAQ5 を参照してください。

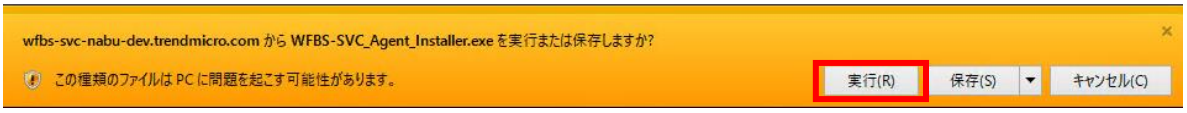



※既に CSMVB が導入されている場合は、以下の画面が表示されます。
この場合は、インストール不要ですのでウィンドウを閉じて終了してください。

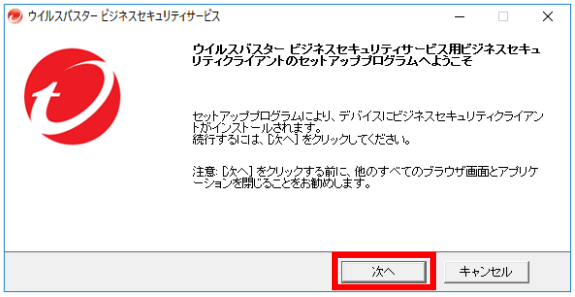
※ビジネスセキュリティクライアント⇒セキュリティエージェント


3-1-4 ［ダウンロード］をクリックします。

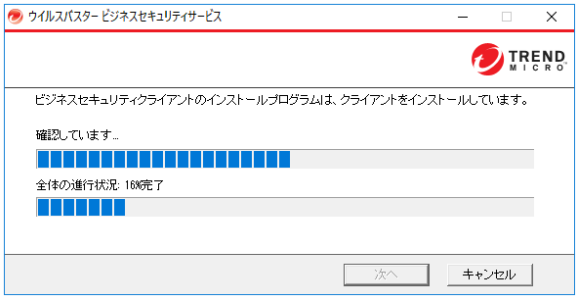

3-1-5 ファイルのダウンロードダイアログが表示されますので、［実行］をクリックします。
※ダウンロードしたファイルは、その端末専用のものです。保存しても他の端末での利用は出来ません。




3-1-6 インストール画面が開きますので、［次へ］をクリックします。

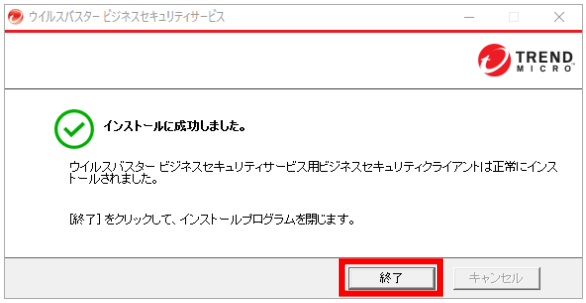



インストール中は下記のような画面になりますので、完了までお待ちください。（数分～十数分かかります）
※ダウンロードしながらのインストールとなりますので、インターネット環境によって実行時間は異なります。




※プロキシサーバご使用の場合：付録 B：プロキシサーバご使用のお客様へ をご確認ください。

3-1-7 インストールが完了しますと、下記のような画面になりますので[終了]をクリックします。




※[終了]をクリックすると自動的に再起動する場合もありますので、作業中のファイルがある場合は、[終了]をクリックする前にファイルの保存をしてください。

3-1-8 タスクトレイにアイコンが表示されましたらインストール完了です。


※アイコン状態の情報は付録 E をご参照ください。

**タスクトレイにアイコンが表示されていない場合**

画面右下のタスクトレイにある三角形のアイコンをクリックします。

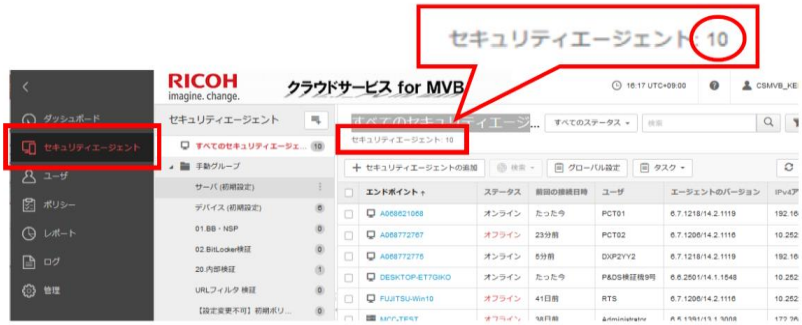
3-1-9 インストールが正しく完了したこと確認します。

[重要]

Web管理コンソール※にて、セキュリティエージェントに表記された台数を確認します。

「インストールしたすべての台数」と「セキュリティエージェントに表記された数字」に差が無いことの確認を行います。

数値に差がある場合は、参考情報をもとに正しくインストールが行われているか確認してください。



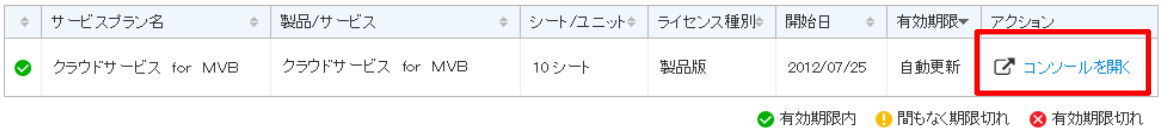

[参考]

- <u>セキュリティエージェント ： インストールが完了した端末数</u>
- エンドポイント ： インストールが完了した端末のホスト名
- ステータス ： 端末のネットワーク通信状態
- 前回の接続日時 ： 端末が最後に通信した日時

※ログイン手順は「4. Web 管理コンソールへのログイン手順(P20)」をご確認ください

## 3-2 Web 管理コンソールからのインストール方法

3-2-1 Web 管理コンソールにログインします。([4 Web 管理コンソールへのログイン手順]を参照)





3-2-2 [セキュリティエージェント]-[セキュリティエージェントの追加]をクリックします。

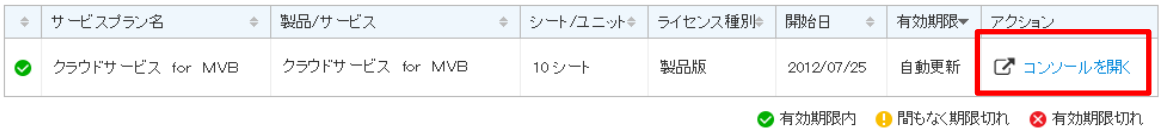
3-2-3 [このエンドポイントにインストール]をクリックします。


3-2-4 [ダウンロード]をクリックします。

※ここから先は Welcome メールからのインストールと同様です。手順 3-1-4 (P10) 以降をご参照ください


## 3-3 インストールパッケージによるインストール方法

3-3-1 Web 管理コンソールにログインします。([4 Web 管理コンソールへのログイン手順]を参照)

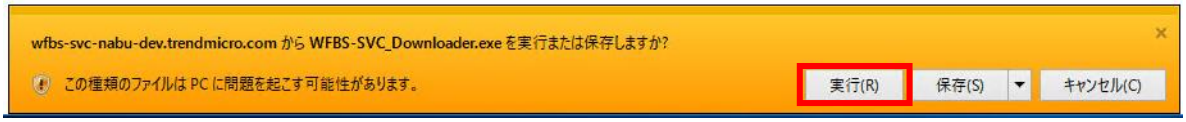


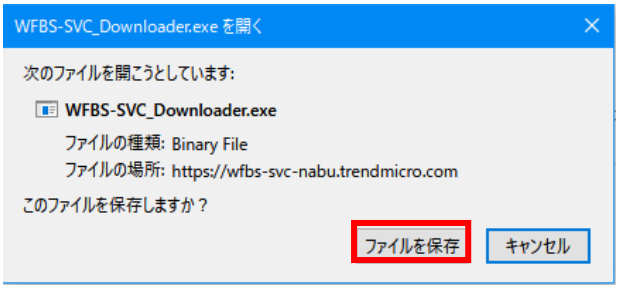

3-3-2 ［セキュリティエージェント]-[セキュリティエージェントの追加］をクリックします。


3-3-3 ［インストーラのダウンロード]をクリックします。

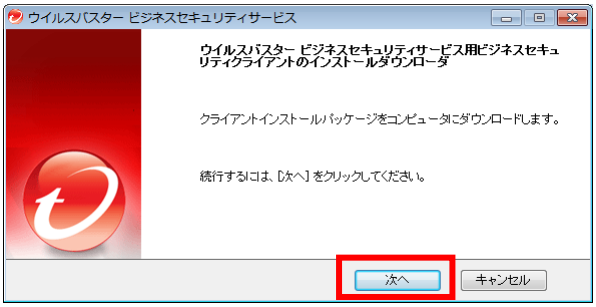

3-3-4 ［ダウンロード]をクリックします。

3-3-5 [実行]をクリックします。OS によって異なるた[実行]がない場合は[ファイルを保存]してからダウンロードしたファイルをクリックします。

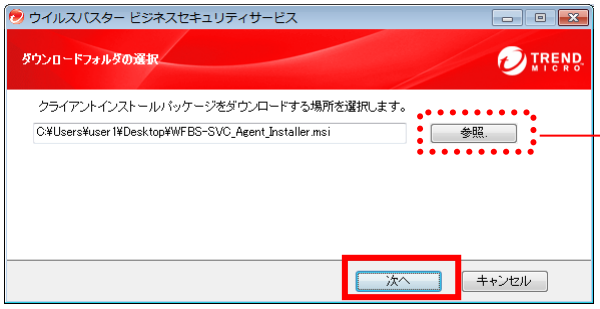


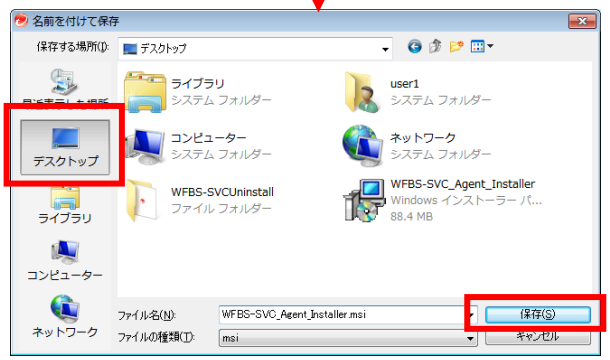

3-3-6 [次へ] をクリックします。



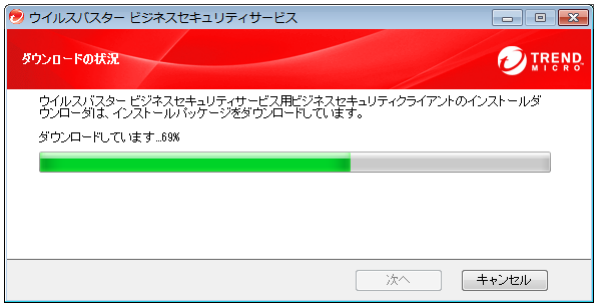

3-3-7 [次へ] をクリックします。



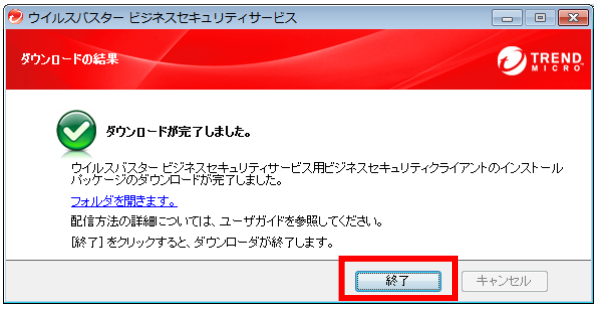

※ ファイルの保存場所を変更するには、
[参照] をクリックします。
「名前つけて保存」ウィンドウにて、
ファイル保存先を選択し、[保存]をクリックします。



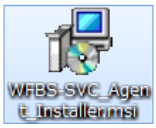

3-3-8 ダウンロードが終わるまで待ちます。



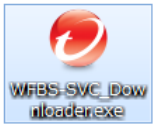
3-3-9　［終了］をクリックします。



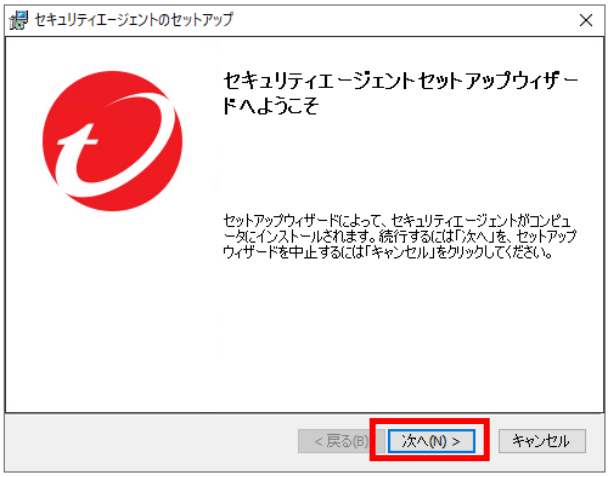

3-3-10　保存した msi ファイルをダブルクリックで開きます。



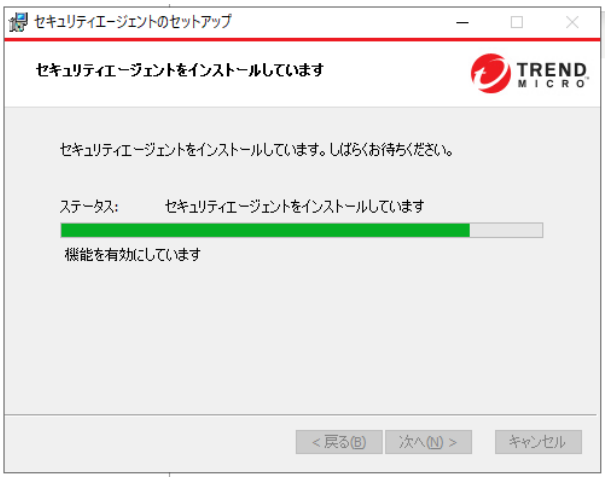

※ ファイルが下図の様な赤いアイコンの場合、ファイルダウンロードに失敗しています。
手順書をよく確認し再度ダウンロードし直してください。




3-3-11　［次へ］をクリックします。




3-3-12　インストールが終わるまで待ちます。



3-3-13　［終了］をクリックします。


3-3-14　タスクトレイにアイコンが表示されたらインストール完了です


※アイコン状態の情報は付録 E をご参照ください。

**タスクトレイにアイコンが表示されていない場合**

画面右下のタスクトレイにある三角形のアイコンをクリックします。

3-3-15 インストールが正しく完了したこと確認します確認します。

[重要]

Web管理コンソール※にて、セキュリティエージェントに表記された台数を確認します。

「インストールしたすべての台数」と「セキュリティエージェントに表記された数字」に差が無いことの確認を行います。

数値に差がある場合は、参考情報をもとに正しくインストールが行われているか確認してください。


[参考]

・ <u>セキュリティエージェント ： インストールが完了した端末数</u>

・ エンドポイント ： インストールが完了した端末のホスト名

・ ステータス ： 端末のネットワーク通信状態

・ 前回の接続日時 ： 端末が最後に通信した日時

※ログイン手順は「4. Web 管理コンソールへのログイン手順(P20)」をご確認ください

## 4. Web 管理コンソールへのログイン手順

【概要】
お客様は、Web 管理コンソールにアクセス・ログインして、自社の設定と管理を行うことができます。

URL　https://4fhyh.login.trendmicro.com/simplesaml/saml2/idp/SSOService.php

✧ ログイン

Welcome メールに記載されているアカウントとパスワードを入力し、[ログイン]をクリックします。

| | |
|---|---|
| アカウント | お客様のアカウント ID |
| パスワード | アカウント ID に紐付くパスワード |

✧ ログオフ

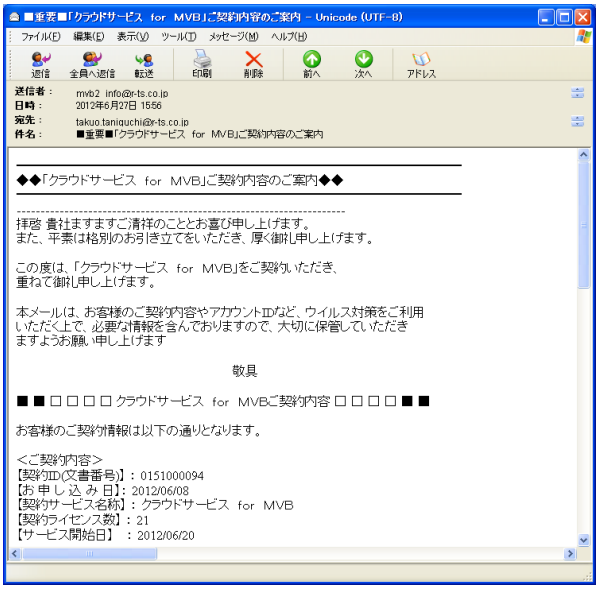
・ ログオフをクリックします。
・ 無操作状態が 30 分以上続くと、自動的にログオフします。

✧ 管理コンソールのシステム要件

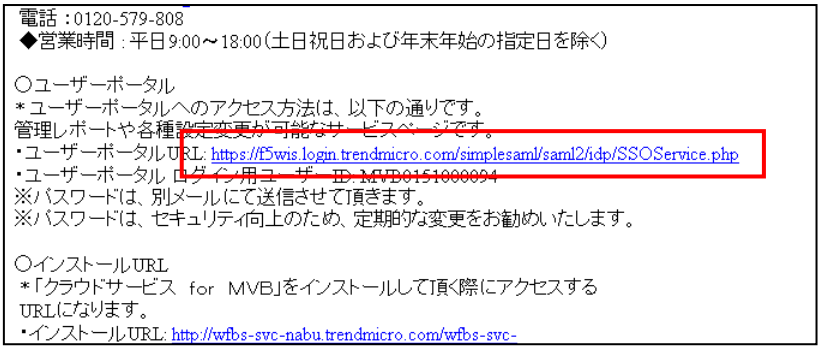
| | |
|---|---|
| Web ブラウザ | ・Internet Explorer 11.0(※1)<br>・Mozilla Firefox 64.0、65.0、66.0、67.0、68.0<br>・Google Chrome(※2)<br>・Microsoft Edge(※2)<br>※1 Internet Explorer 11 は Windows (Modern) UI 上での利用には対応していません。<br>※2 特に断りのない限り、最新バージョン含め 3 世代のバージョンをサポートいたします。新バージョンがリリースされた際には、順次検証を実施し、サポート対象となります。<br>(注) Android 端末上からの利用には対応しておりません。 |
| PDF リーダー<br>(レポート用) | Adobe Acrobat Reader 6.0 以降(最新バージョン推奨) |
| ディスプレイ | ハイカラー、解像度 1366×768 ピクセル以上 |

【詳細】

4-1. CSMVB サービス開始準備が完了しますと、以下のような Welcome メールが送付されます。



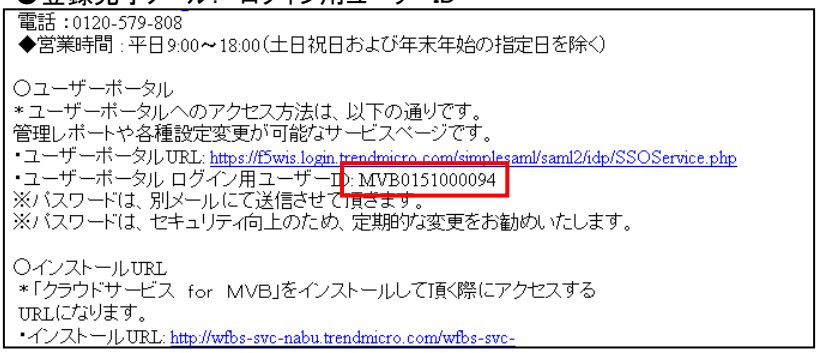

4-2. Welcome メールの Web 管理コンソール URL（ユーザーポータル URL）をクリックします。




4-3. Welcome メールの【アカウント】と【パスワード】を確認します。

※ 【アカウント】と【パスワード】はそれぞれ別メールにて送付されます。

●登録完了メール： ログイン用ユーザーID



●パスワード通知メール： パスワード

◆◆「クラウドサービス for MVB」パスワードのご案内◆◆

---

拝啓 貴社ますますご清祥のこととお喜び申し上げます。
また、平素は格別のお引き立てをいただき、厚く御礼申し上げます。

この度は、「クラウドサービス for MVB」をご契約いただき、
重ねて御礼申し上げます。

本メールは、ユーザーポータルをご利用いただく上で、必要なお客様のパスワードを含んでおりますので、大切に保管していただきますようお願い申し上げます。

敬具

■■□□□□ユーザー ポータルのパスワード□□□□□■■

ユーザー ポータルのパスワードは以下の通りとなります。

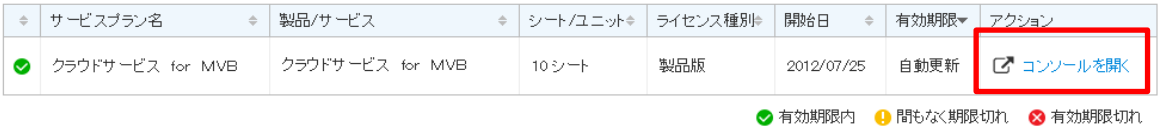
【パスワード】: shtwitns
※契約情報・URLやアカウントIDなどは、別メールにて送信させて頂いております。
※パスワードは、セキュリティ向上のため、定期的な変更をお勧めいたします。

4-4. Web 管理コンソールにアカウントとパスワードを入力します。


※ ログインパスワードのリセットについては FAQ1 をご確認ください。
※ 表示されない場合、正常にログインできない場合には、FAQ5 を参照してください。

4-5. [コンソールを開く]をクリックします。

※開始日が Welcome メールのものと異なる場合がございますが、
Welcome メールのものが正しい開始日となります。

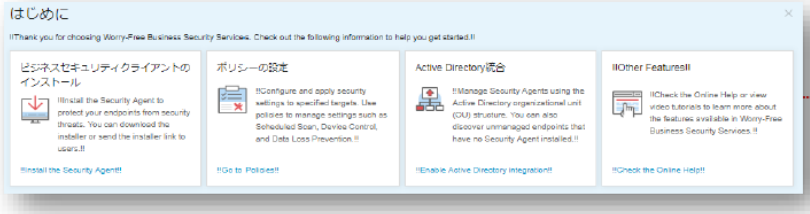


| サービスプラン名 | 製品/サービス | シート/ユニット | ライセンス種別 | 開始日 | 有効期限 | アクション |
|---|---|---|---|---|---|---|
| クラウドサービス for MVB | クラウドサービス for MVB | 10 シート | 製品版 | 2012/07/25 | 自動更新 | コンソールを開く |

有効期限内　間もなく期限切れ　有効期限切れ

※Web 管理コンソールにログインするユーザーに対して、適切な情報が表示されます。

新規ユーザがログインすると「はじめに」メッセージを表示します。




構築・運用手順などを表示

既存ユーザがログインすると「新機能」メッセージを表示します。


新機能の紹介、オンラインヘルプへのリンクなど

4-6. ログイン完了です。


4-7. インストールが完了した端末数を確認する場合は、[セキュリティエージェント]をクリックし確認します。
[セキュリティエージェント: ]のあとの数字がインストール完了した端末数になります。


※参考情報

セキュリティエージェントの画面で確認できる情報は以下になります。

- セキュリティエージェント　：インストールが完了した端末数
- エンドポイント　：インストールが完了した端末のホスト名
- ステータス　：端末のネットワーク接続状況
- 前回の接続日時　：端末が最後に通信した日時

## ・5.Web 管理コンソールの機能について

【概要】

Web 管理コンソールでは、管理するコンピュータのセキュリティ対策とその管理を行うことが可能です。

管理コンソールで利用可能な機能

| | |
|---|---|
| ダッシュボード | ウイルスバスター ビジネスセキュリティサービスは、セキュリティエージェントの管理に役立つ視覚的なクイックリファレンスとして機能するウィジェットを提供します。 |
| セキュリティエージェント | デバイス管理をセキュリティエージェント画面に統合します。 |
| ユーザ | ユーザごとのエンドポイント一覧やイベントを確認できるようになります。 |
| DETECTION & RE…<br>注意が必要なイベント<br>脅威の調査 | ・注意が必要なイベント<br>注意が必要なイベントとして、検出された不正プログラムが表示されます。<br>・脅威の調査過去 30 日間に指定した脅威のインジケータが含まれているエンドポイントを検出します。<br>※『クラウドサービス for MVB EDR』をご契約のお客様のみ表示されます。 |
| ポリシー | 検索の設定や除外設定などのセキュリティ設定やクライアントの設定を行います。 |
| レポート | レポートには、特定の期間にネットワーク上で発生したセキュリティイベントの概要情報とトップ統計が表示されます。 |
| ログ | ログは、ネットワークに影響を及ぼすセキュリティおよびシステムイベントに関する詳細なデータを提供します。 |
| 管理 | 各種設定やメール通知やツールのダウンロードなどを提供します。 |
| オンラインヘルプ | オンラインヘルプを表示します。 |

【詳細】

5-1　Web 管理コンソールにログインします。（[4　Web 管理コンソールへのログイン手順]を参照）

5-2　利用したい機能のアイコンをクリックします。


※各機能の詳細を知りたい場合は、各種タブの右上の　?　をクリックして表示されるヘルプを参照してください。

【クラウドサービス for MVB EDR をご契約のお客様：注意が必要なイベントについて】


脅威の検出に 1 つ以上の疑わしい不審オブジェクトが関連付けられる場合、注意が必要なイベントが作成されます。注意が必要なイベントには、対象エンドポイント、分析チェーン、最初に確認されたオブジェクト、および注意が必要なオブジェクトに関する情報が含まれます。
“分析チェーン”に記載のリンクをクリックすることにより詳細を確認することができます。


| | |
|---|---|
| 概要 | 検出された脅威に関する説明です。 |
| 推奨される処理 | 検出された脅威に関する対処方法です。 |
| エンドポイント | 調査されたエンドポイントの詳細情報が表示されます。 |
| 最初に確認されたオブジェクト | 調査対象オブジェクトの作成に関与したとみられる分析チェーン内の最初のオブジェクトです。多くの場合、これは標的型攻撃の開始地点です。 |
| セキュリティ上の脅威 | 注意が必要なイベントを作成するために CSMVB で使用される、検出された脅威です。 |
| 注意が必要なオブジェクト | 不正オブジェクトの可能性があるチェーン内のオブジェクトを強調表示し、値は、チェーン内にある一意の注意が必要なオブジェクト数を表します。 |

※ 検出された脅威に関する詳細につきましてはご登録された管理者メールアドレスへインシデントレポートを送付いたしますのでご確認ください。

## 6. クライアント用コンソールの機能について

【概要】
クライアント用コンソールは、タスクトレイにある CSMVB クライアント用のアイコンをクリックするか、右クリックして[セキュリティエージェントを開く]をクリックして開きます。クライアント用コンソールでは下記の機能を提供します。

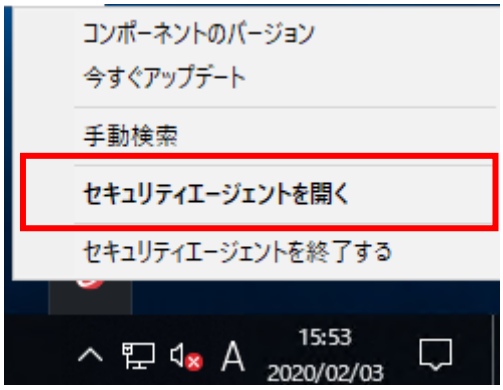
| | |
|---|---|
| 検索 | 手動で CSMVB がインストールされたコンピュータのウイルス/スパイウェア検索ができます。 |
| アップデート | 手動でパターンファイル/エンジンの更新を行うことができます。 |
| ログ | 検出された脅威に関する詳細情報が記載されたログファイルを作成および表示できます。 |
| 設定 | ログデータを保存する期間、アラートを出すイベントの設定を行うことができます。 |
| ツール | 問題が発生した際の調査に必要となる情報を採取可能な「ケース診断ツール」をダウンロードできます。 |
| ステータス | スマートスキャン機能やリアルタイム検索機能の状態を確認できます。 |

【詳細】
6-1　導入済みお客様端末の右下のアイコンを右クリックします。


**タスクトレイにアイコンが表示されていない場合**

画面右下のタスクトレイにある三角形のアイコンをクリックします。


6-2　[セキュリティエージェントを開く]をクリックします。




6-3　クライアント用コンソールが表示されますので、利用したい機能をクリックします。

## 7. アラート通知、レポート通知メールについて

CSMVB ではアラートや週次レポートをメールにて送付することが出来ます。
サービス開始当初の通知設定は以下の通りです。

| | | |
|---|---|---|
| アラート通知 | 送信先 | ご契約時のメールアドレス |
| | アラート対象 | ・ウイルスの処理に失敗した場合<br>・リアルタイム検索機能が無効になった場合 |
| レポート通知 | 送信先 | ご契約時のメールアドレス |
| | 送信間隔 | 週1回　月曜日　00 時 00 分 |
| | レポート内容 | 設定可能な全ての項目 |

### 7-1. アラート通知の設定方法について

【概要】
管理下にある CSMVB クライアントで各種セキュリティイベントが発生した場合のメール通知に関する設定変更方法です。

【詳細】

7-1-1　Web 管理コンソールにログインします。([4　Web 管理コンソールへのログイン手順]を参照)

7-1-2　トップ画面の[管理]-[通知]をクリックします。
※イベントの内容はデフォルトのままで設定する必要はありません。

7-1-3 表示されたページで、セキュリティイベントのメール送信有無がお客様固有の設定に変更できます。
詳細を知りたい場合は、各種タブの右上の ? をクリックして表示されるヘルプを参照してください。


7-1-4 メールの受信者変更を行いたい場合には、[設定]タブをクリックします。

7-1-5　受信者の欄にアドレスを入力してください。入力しましたら保存をクリックします。
（複数の項目を指定する場合は、セミコロン（;）で区切って入力してください）
例） user1@example.com; user2@example.com


7-1-6　[設定が保存されました]と表示されれば作業は完了です。

## 7-2. レポート通知設定方法について

【概要】

CSMVB では、一定期間のセキュリティイベントを集計し、レポートとして PDF で出力、メールでの自動送付が可能になっております。

以下の手順は、デフォルトで設定されているレポートの通知設定の変更方法です。

【詳細】

7-2-1 ［レポート］タブの該当レポートをクリックします。


7-2-2 レポートが開きますのでレポートの内容を確認し、下にスクロールしてください。
［受信者］にアドレスを入力し［保存］をクリックします。
（複数の項目を指定する場合は、セミコロン（；）で区切って入力してください。


7-2-3 ［成功］と表示されれば作業は完了です。

# 8. アンインストール手順

【概要】

クライアントアンインストール方法は、以下の 2 通りの方法が可能です。
※再起動が発生する場合がありますので、再起動しても問題が無いことを確認して作業してください。

✧ Web 管理コンソールからのアンインストール

Web 管理コンソールから CSMVB クライアントをアンインストールする場合は、以下の手順で行います。

・Web 管理コンソールにログイン
・[コンピュータ]のクライアント管理ツリーから、対象のクライアントを選択
・[削除]タブをクリックしてアンインストールを実行
※クライアント上でのアンインストールは、管理コンソールでの削除作業後、
最初にクライアントが接続された時に実施されます。

✧ お客様コンピュータでのアンインストール

コンピュータのローカルで CSMVB クライアントをアンインストールする場合は、
[プログラムと機能]からアンインストールをします。※Windows11 では[アプリと機能]の表記。

・Windows の[プログラムと機能]を起動
・「セキュリティエージェント」を選択して、アンインストールを実行

【詳細】

## 8-1. Web 管理コンソールからのアンインストール方法

8-1-1 Web 管理コンソールにログインします。（[4 Web 管理コンソールへのログイン手順]を参照）

8-1-2 [セキュリティエージェント]をクリックし、該当のコンピュータを選択し、[タスク]より[セキュリティエージェントのアンインストール]をクリックしてください。


8-1-3 アンインストール確認のポップアップが出ますので、[アンインストール]をクリックします。

8-1-4　該当のコンピュータが画面から削除され、[コマンドが送信されました。]と表示されれば完了です。


※アンインストールの実施のタイミングについて

アンインストールは、Web 管理コンソールから実行後すぐには行われず、該当のクライアントが CSMVB サーバに接続したタイミングで行われます。

（サイレントアンインストールが実行されますので、ポップアップなどがクライアントに表示されることはありません

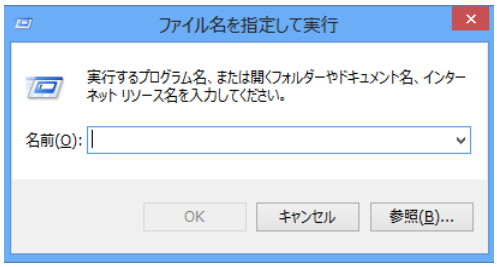
## 8-2. お客様のコンピュータでのアンインストール方法

8-2-1　[プログラムと機能]を開きます。（OS に依って[アプリと機能]の場合があります）

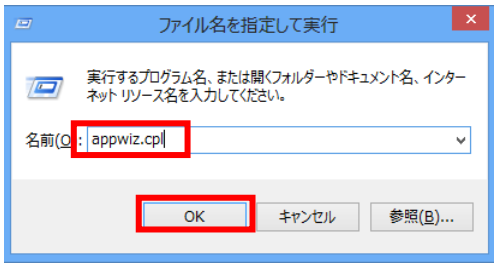
[プログラムと機能]の開き方は OS に依って様々ですが、いくつか起動例をあげます

### 各 OS 共通

Ⅰ. [Windows]キー　＋　[R]キーを押下し、
[ファイル名を指定して実行]を表示させます。

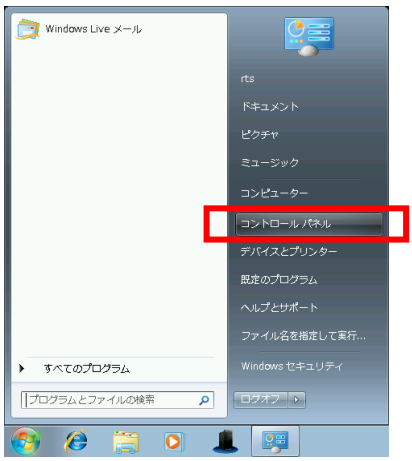



Ⅱ. [appwiz.cpl]と入力し、[OK]をクリックします。

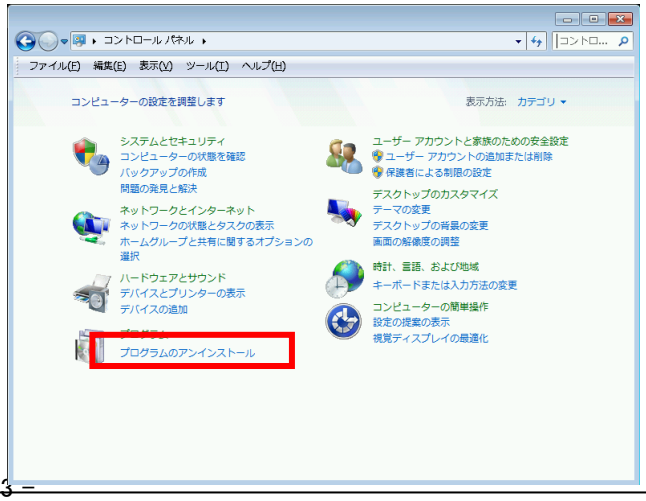



### Windows Server 2016 の場合

Ⅰ. [スタート]→[コントロールパネル]を選択します

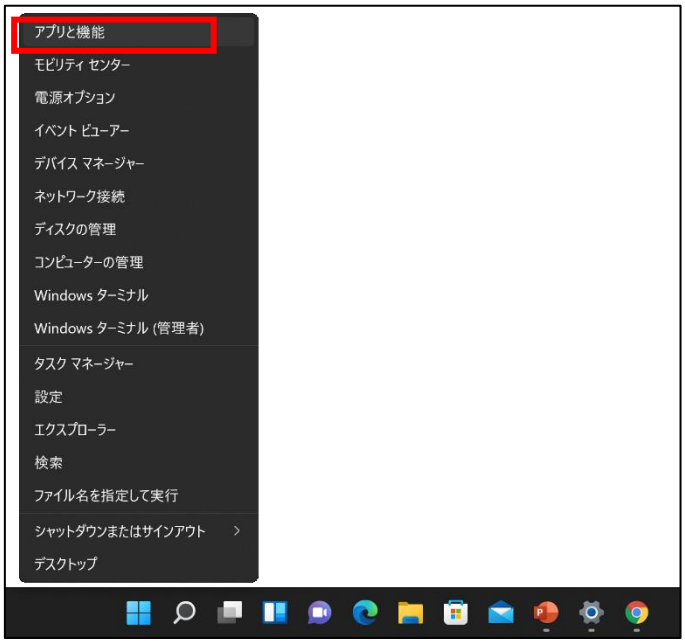



Ⅱ.　[プログラムのアンインストール]をクリックします
（Windows Server 2016 の場合は[プログラムと機能]）

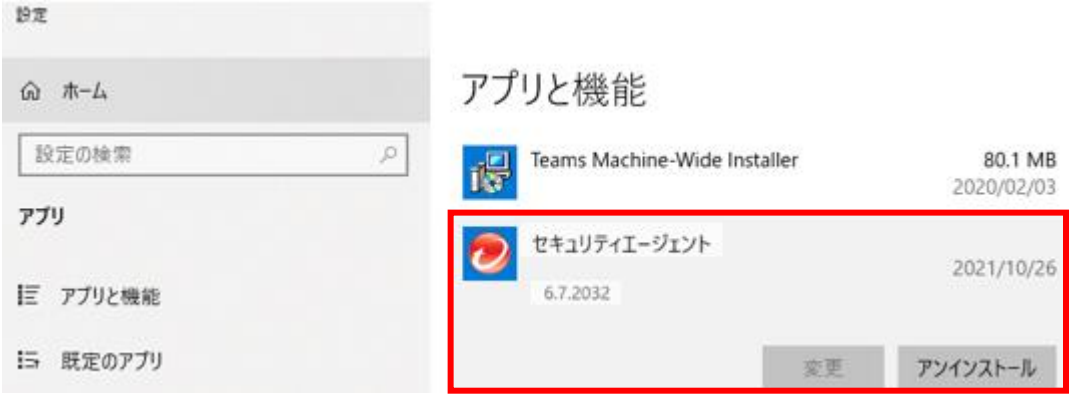


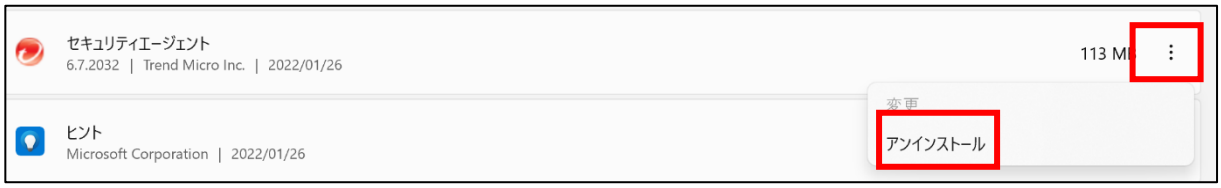
Windows10、Windows11 の場合

Ⅰ．[スタート]を右クリック→[アプリと機能]をクリック

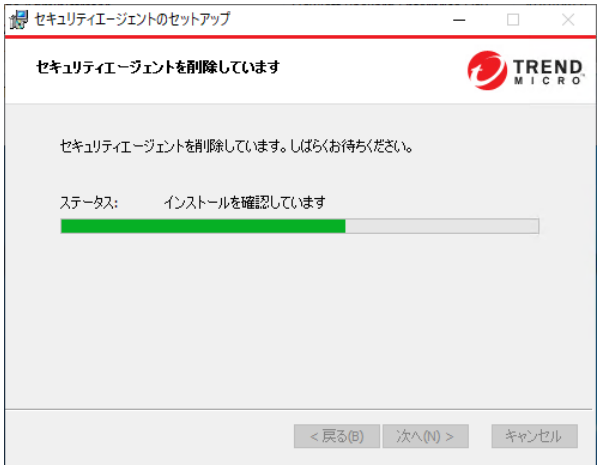


8-2-2　一覧から「セキュリティエージェント」をクリックしアンインストールを選択します。
（下記は Windows10 や Windows11 の画面です）

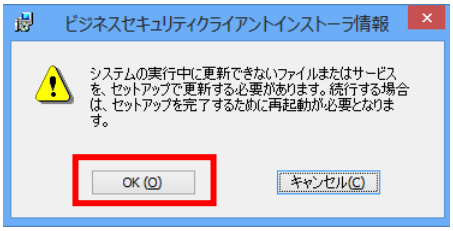


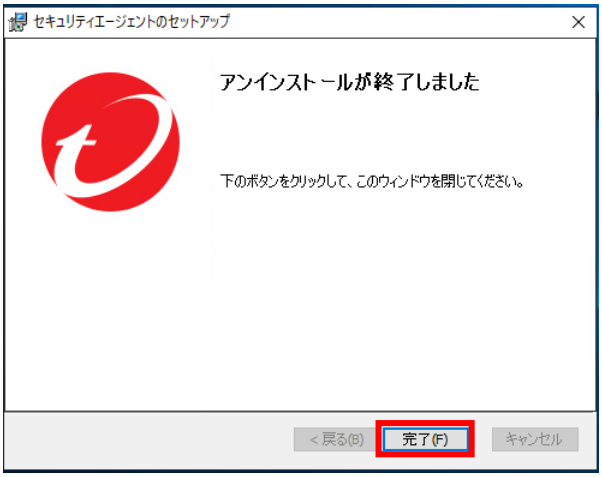

8-2-3「セキュリティエージェントのセットアップ」が開きアンインストールが開始されます。
アンインストールが実施されますので、数分お待ちください。



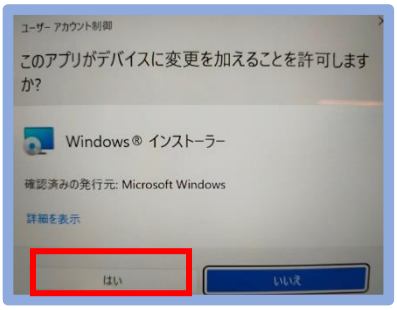

※利用状況によっては、再起動が必要なメッセージが表示されます。
[OK]を押しても自動的に再起動されるわけではありませんので、[OK]をクリックします。



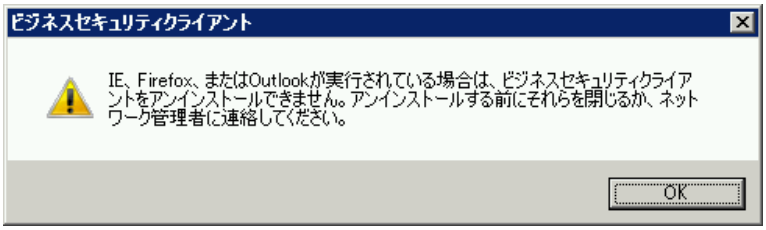
8-2-4 暫く待って、下画面が表示されたら、アンインストールは完了です。
※上記の再起動が必要なメッセージが表示された場合には、完全なアンインストール完了のために手動で再起動をしてください。




※OS によって、ユーザーアカウント制御のポップアップが出ることがあります。
表示された場合には、[はい]をクリックしてください。


※InternetExplorer、Firefox や Outlook が起動していると下図のような画面が出ることがあります。
その場合には、終了させてからもう一度操作をしてください。



RICOH

ITKeeper シリーズ

クラウドサービス　for　MVB

クラウドサービス　for　MVB　EDR

# 【第2章】　Android OS 編

## 1. 事前環境確認

### 既存アンチウイルスソフト等の確認と対処

- 他のウイルス対策、スパイウェア対策ソフトが導入されている又は、正常にアンインストールされていない場合、クライアントのインストールが正常に行われず、プロセスやファイルが存在しない、アイコンがオフラインになる、通信が出来ずパターン更新がされない等の現象が発生する可能性がございます。
  他のウイルス対策、スパイウェア対策ソフトが導入されている場合は、そのアプリケーションのアンインストールをお願いいたします。

### ファイアウォール、通信に関する問題

- クライアントの通信（パターンファイル取得、サーバへのログ送付等）には、インターネットに向けて SSL で 443 ポートでの通信を行います。
- パッケージのダウンロードには 80 ポートでの通信を行います。
- CSMVB サーバから設定の同期などのコマンドを発行する場合は、FCM(Firebase Cloud Messaging)を利用してデバイスへ通知を送信します。GCM はポート、443 ポート、5228 ポート、5229 ポート、5230 ポートでの通信を行います。
- 詳細は、[付録 C：サーバと AA 間の通信について]をご参照ください。

### Android 端末の条件

CSMVB インストールにあたり、下記確認をお願いします。

- 提供元不明のアプリ(サードパーティアプリケーション)のインストールを許可している
- バックグラウンド同期が有効である
- JavaScript が有効である
- Cookie が有効である

## 2. システム要件

CSMVB のシステム要件は以下の通りです。

◆PC／スマートデバイス動作環境（Android OS）

| | | |
|---|---|---|
| スマートデバイス（Android） | 対応 OS（※） | Android 10.0<br>Android 11<br>Android 12<br>Android 13 |
| | Web ブラウザ（ソフトウェアインストール、Web レピュテーション） | Android デバイスのデフォルトのブラウザ<br>Google Chrome |

※ 最新バージョン含め5世代のバージョンをサポートします。
※ iOS についてはサポート対象外となります。

※ （「クラウドサービス for MVB EDR」のご契約中のお客様）クラウドサービス for MVB EDR」ではEDR機能をご提供しますが、スマートデバイスではEDR機能は動作しません。

最新の情報については、トレンドマイクロ社の下記サイトをご参照ください。

「ウイルスバスター™ ビジネスセキュリティサービス」

https://www.trendmicro.com/ja_jp/small-business/worry-free-services.html

## 3. インストール手順

【概要】

Android 端末へのインストールは下記方法で行えます。

❖ メールを利用したインストール

管理コンソールにログインし、Android 端末へメールを送付します。

このメールを利用してのインストールは、以下の手順で行います。

・メールに記載されているインストール URL をクリックします。（またはQRコードからインストールリンクへアクセス）

・Google プレイで、インストールを実行します。（詳しくは【詳細】に記載）

※Web 管理コンソールのパスワードを忘れてしまった場合、FAQ1 を参照してパスワードを初期化してください

【詳細】

操作方法は機種・AndroidOS バージョンによって違います。詳しくは各機種の取扱説明書をご確認ください。

3-1 Windows 端末から Web 管理コンソールにログインします。

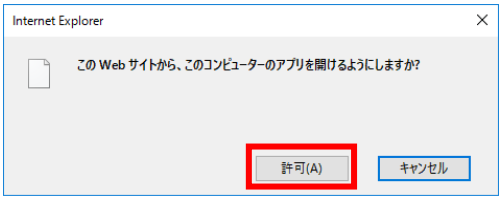
Android OS 標準ブラウザでは Web 管理コンソールを正常に表示できません。

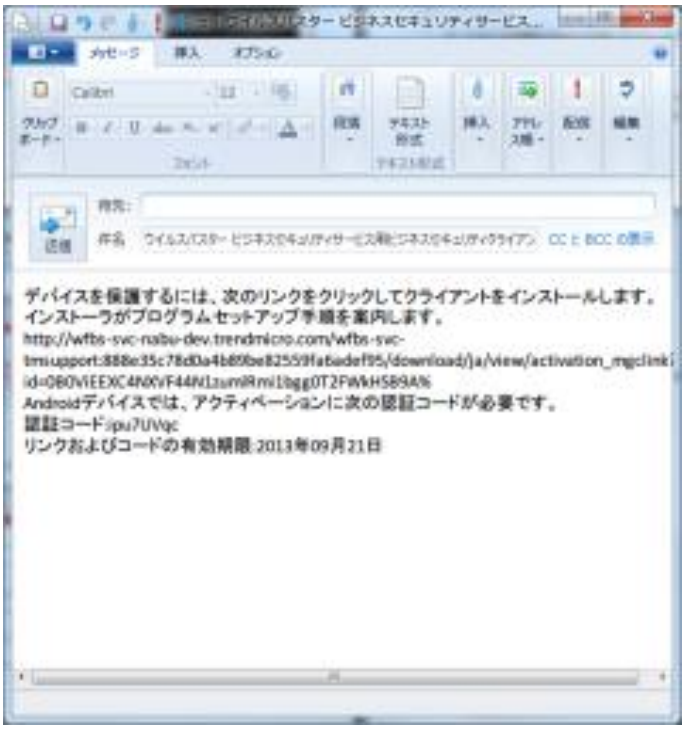
（【第 1 章】WindowsOS 編 [4 Web 管理コンソールへのログイン手順]を参照）

3-2 [セキュリティエージェント]-[セキュリティエージェントの追加]をクリックします。

3-3 [インストーラリンクの送信]をクリックします。

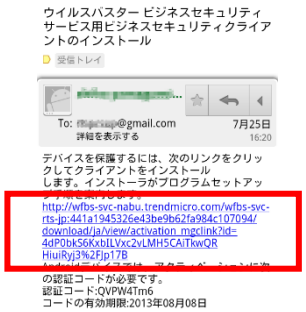

3-4 メールソフトが起動しますので、Android 端末へメールを送ります。




3-5 ここからの作業はインストールする Android 端末で行います。

3-6 「手順 3-4」で送信したメールを開き、「インストール URL」をタップします。

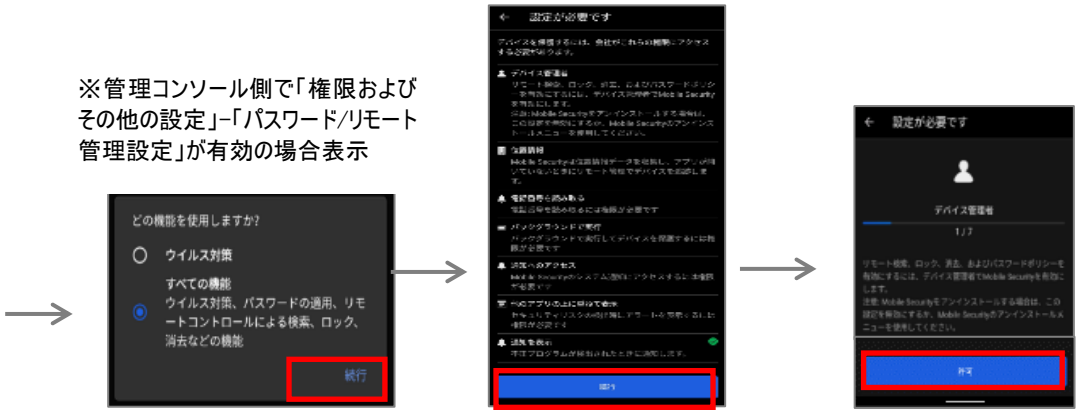



※インストール URL は、お客様毎に異なります。

3-7 Google Play からインストール。


権限の設定

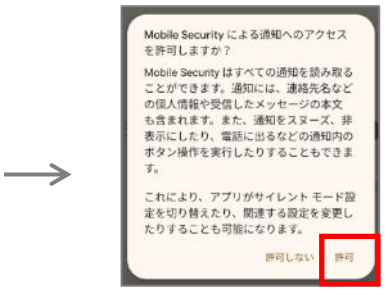
※管理コンソール側で「権限およびその他の設定」-「パスワード/リモート管理設定」が有効の場合表示



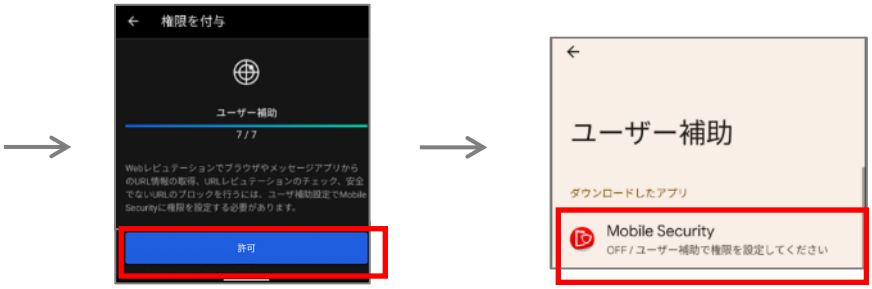



設定が必要です
バックグラウンドで実行
1 / 7
許可
アプリにバックグラウンドでの常時実行を許可しますか？
Mobile Security にバックグラウンドでの常時実行を許可すると、電池消費量が増加する場合があります。
この設定は、[設定] > [アプリと通知] から後で変更できます。
許可しない
許可


設定が必要です
通知へのアクセス
5 / 7
許可
デバイスとアプリの通知
許可されたアプリ
Android System Intelligence
Pixel Launcher
Android Auto
許可されていないアプリ
Google Play 開発者サービス
Google
Mobile Security
デバイスとアプリの通知
Mobile Security
Mobile Security
通知へのアクセスを許可

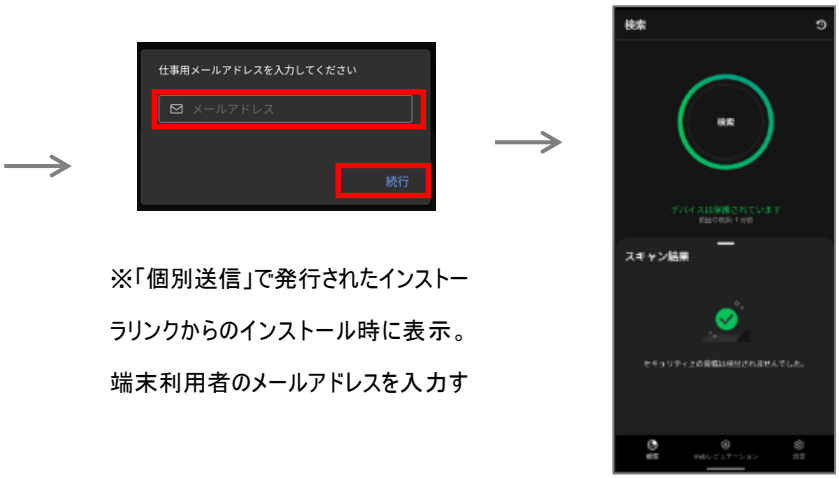

Mobile Security による通知へのアクセスを許可しますか？
Mobile Security はすべての通知を読み取ることができます。通知には、連絡先名などの個人情報や受信したメッセージの本文も含まれます。また、通知をスヌーズ、非表示にしたり、電話に出るなどの通知内のボタン操作を実行したりすることもできます。
これにより、アプリがサイレント モード設定を切り替えたり、関連する設定を変更したりすることも可能になります。
許可しない
許可


権限を付与
他のアプリの上に重ねて表示
6 / 7
許可
他のアプリの上に重ねて表示
フォト
許可しない
Mobile Security
許可しない
他のアプリの上に重ねて表示
Mobile Security
2.0.0.111
他のアプリの上に重ねて表示できるようにする





**インストール完了！**




※「個別送信」で発行されたインストーラリンクからのインストール時に表示。端末利用者のメールアドレスを入力す

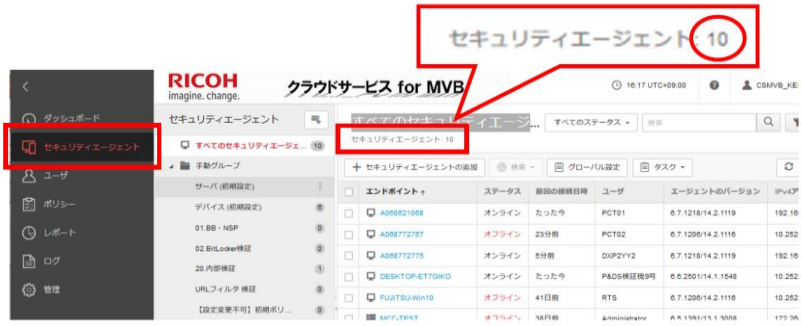
3-8 インストールが正しく完了したこと確認します。

[重要]

Web管理コンソール※にて、セキュリティエージェントに表記された台数を確認します。

「インストールしたすべての台数」と「セキュリティエージェントに表記された数字」に差が無いことの確認を行います。

数値に差がある場合は、参考情報をもとに正しくインストールが行われているか確認してください。




[参考]

- <u>セキュリティエージェント ： インストールが完了した端末数</u>
- エンドポイント ： インストールが完了した端末のホスト名
- ステータス ： 端末のネットワーク通信状態
- 前回の接続日時 ： 端末が最後に通信した日時

※ログイン手順は「4. Web 管理コンソールへのログイン手順(P20)」をご確認ください

## 4. アンインストール手順

【概要】

Android 端末からのアンインストールは下記方法で行えます。

❖ Android 端末上でのアンインストール

Android 端末上の[設定]>[アプリケーションの管理]からアンインストールを実行します。
また、Web 管理コンソールのデバイスツリー上の該当端末を削除します。

※ Android 端末でアンインストールを行う場合は、ローカルでのアンインストールを実施してください。
Web 管理コンソール上で対象の Android デバイスを削除しても、Android 端末上から CSMVB は
アンインストールされません。

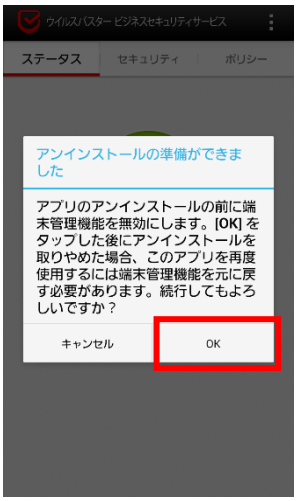
【詳細】

操作方法は機種・AndroidOS バージョンによって違います。詳しくは各機種の取扱説明書をご確認ください。

4-1 Android 端末上の[アプリケーション]アイコンを開き、[VBBSS]をタップします。


4-2 右上のメニューボタンをタップし、[アンインストール]をタップします。

4-3 ［OK］をタップします。




4-4 ［OK］をタップします。


4-5 アプリケーション一覧からアイコンが消えます。


4-6 Web 管理コンソールのデバイスツリー上の該当端末を削除します。

（【第 1 章】WindowsOS 編「8-1 Web 管理コンソールからのアンインストール方法」参照）

RICOH

ITKeeper シリーズ

クラウドサービス　for　MVB

クラウドサービス　for　MVB　EDR

# 【第3章】　FAQ・付録　編

# 1. 関連情報

## サービス関連 URL:

### クラウドサービス for MVB Web 管理コンソール

クラウドサービス for MVBの Web 管理コンソール ログイン URL です。

https://4fhyh.login.trendmicro.com/simplesaml/saml2/idp/SSOService.php

### メンテナンス・障害情報

メンテナンスや障害情報を掲載いたします。

http://itkeeper.ricoh.co.jp/isp/index.html

### ユーザーマニュアル

最新のユーザーマニュアルを掲載いたします。

https://itkeeper.ricoh.co.jp/isp2/cs_mvb/usermanual.html

## お問い合わせ窓口:

メール: mvb_support@gmb.ricoh.com

電話 : 0120-579-808

営業時間 : 平日 9:00 ～ 18:00 （土日祝日および年末年始の指定日を除く）

## 2. FAQ

### FAQ.1 （Windows OS）

Q, Web 管理コンソールの「パスワード」を忘れてしまいました。

A, パスワードの再発行を行ってください。

パスワードを忘れた場合は、下記の手順で再発行を行います。

・Web 管理コンソールのログイン画面右上の[パスワードを忘れた場合]にて、ログイン ID またはメールアドレスを入力します。

・登録のメールアドレスに、パスワード再設定のメールが送信されます。

・送信されたメールの内容に従って、パスワードの再設定を行ってください。

※メールに記載されているリンクは 24 時間で無効となります。

※入力するメールアドレスは登録されている管理者メールアドレスとなります。

### FAQ.2 （Windows OS）

Q, Web 管理コンソールの「アカウント」を忘れてしまいました。

A, CSMVB お問い合せ窓口（[1 関連情報]を参照）へご連絡ください。

### FAQ.3 （Windows OS）

Q, Welcome メールを無くしてしまいました。再インストールはどうすれば良いのでしょうか。

A, Welcome メールが無くても、Web 管理コンソールからのインストールが可能です。

詳しい実施手順は、[3 インストール手順] の Web 管理コンソールからのインストール方法を参照してください。また、パスワードも忘れてしまった場合には、FAQ1 を参照し、パスワードを再発行してください。

### FAQ.4 （Windows OS）

Q, Welcome メールと Web 管理コンソール内の開始日や終了日が違いますが、どちらが正しいのですか。


A, Welcome メール上の期間が正しい契約期間となります。

Web 管理コンソール内は、事前に設定代行をさせて頂くため、実際のご契約期間より少し前が開始日となっております。お客様のご契約は、あくまで Welcome メールに記載されている日付が正しいものとなります。

## FAQ.5 （Windows OS）

Q, Internet Explorer を起動しても Web 管理コンソールにログインできない、
または Web 管理コンソールが正常に表示できない(空白で表示される)。

A, 信頼済みサイトへの登録が必要です。

お客様がお使いになられている Internet Explorer のセキュリティレベルにより
ページが表示できない、または、ログインできない場合がございます。
※特にサーバ OS では、標準のセキュリティレベルが高く設定されておりますので、下記設定が必須です

下記の手順で信頼済みサイトへの登録を実施してください。

・Internet Explorer の[ツール ]-[インターネットオプション]をクリックします。
・[セキュリティ]タブの、[信頼済みサイト]を選択し、[サイト]をクリックします。
・"この Web サイトをゾーンに追加する"の[追加]をクリックします。サイトが信頼済みに追加されます。
・[閉じる]-[OK]をクリックして閉じます。

A, ルート証明書の追加が必要です。

Internet Explorer の環境によっては、ルート証明書の追加が必要となる場合がございます。
下記の手順でルート証明書の追加を実施してください。

・ https://www.affirmtrust.com/resources/ を開きます
・「AffirmTrust Commercial」の[Download]をクリックします
・[開く]をクリックします
・[証明書のインストール]をクリックします
・[次へ]をクリックします
・[証明書をすべて次のストアに配置する]を選択し、[参照]をクリックします
・「信頼されたルート証明機関」を選択し、[OK]をクリックます
・[次へ]をクリックします
・[完了]をクリックします
・「正しくインストールされました」が表示されたら完了です

A, 中間証明書の追加が必要です。

Internet Explorer の環境によっては、中間証明書の追加が必要となる場合がございます。
下記の手順で中間証明書の追加を実施してください。

・ https://www.affirmtrust.com/resources/ を開きます
・「AffirmTrust Certificate Authority – OV1」の[Download]をクリックします
・[開く]をクリックします
・[証明書のインストール]をクリックします
・[次へ]をクリックします
・[証明書をすべて次のストアに配置する]を選択し、[参照]をクリックします
・「中間証明機関」を選択し、[OK]をクリックします
・[次へ]をクリックします
・[完了]をクリックします
・「正しくインストールされました」が表示されたら完了です

## FAQ.6 （Windows OS）

Q,Web 管理コンソール内で住所などの情報を変更出来ますが、変更すると契約情報も変更になりますか。

A, 契約情報の変更は、担当営業までご連絡ください。
Web 管理コンソール内で契約情報の変更を実施頂いても、実際の契約情報は変更されません。
契約情報に変更がある場合には、お手数ではございますが、担当営業までご連絡をお願いいたします。

※ 営業にご連絡頂いた場合には、Web 管理コンソール内の契約情報も変更になります。
※ アラート通知やレポート通知のメール送信先は、契約情報ではございませんので、変更されません。「7 アラート通知、週次レポートメール」をご参照頂き、必要に応じた変更をお願いいたします。

## FAQ.7 （Windows OS）

Q, ［8 アンインストール手順］でアンインストールを実施しましたが、アンインストールに失敗してしまいます。

A, 指定のメールアドレスに、ご連絡ください。
宛先：mvb_support@gmb.ricoh.com
件名：クラウドサービス for MVBのアンインストールツールの提供依頼

---------- 本文 ----------
・クラウドサービス for MVBの契約 ID：
・ご担当者名：
・ご連絡先電話番号：

## FAQ.8 （Windows OS）

Q, プログラムの除外設定方法はどのようにおこなうのですか。

A, 【フォルダ除外設定方法】につきましては、下記の手順で除外設定を実施してください。

・管理画面ログイン後、[コンソールを開く]をクリックします。
・Web 管理コンソールのメニューアイコンより[セキュリティエージェント]を選択します。
・[手動グループ]フォルダを展開し、除外設定したい PC が所属しているグループを選択し、[ポリシーの設定]をクリックします。
（グループに所属しているデバイスすべてに除外設定が反映されます）
・[検索除外]の[リアルタイム検索/予約検索/手動検索]にある[フォルダ]タブに除外設定したいソフトのフォルダパスを入力します。
フォルダパスの最後に「¥」を付けてください。
・[検索除外]の[挙動監視]にある[承認済みプログラムリスト]タブにフォルダパスを入力します。
フォルダパスの最後に「¥*」を付けてください。
・[保存]をクリックします。
・設定が反映されるまで時間がかかるため、15 分ほどお待ちいただいてから動作確認をお願いします。

A, 【プログラムファイル除外設定方法】につきましては、下記の手順で除外設定を実施してください。

・ログイン後[コンソールを開く]より[ダッシュボード]画面を表示します。
・画面左側にあるメニューアイコンの[ポリシー]を選択します。
（MVB をインストールしているデバイスすべてに除外設定が反映されます）
・[ポリシー]画面で[グローバル除外リスト]の[信頼済み Windows プログラムリスト]へ実行ファイルのパスをフルパスで登録します。
・[保存]をクリックします。
・設定が反映されるまで時間がかかるため、15 分ほどお待ちいただいてから動作確認をお願いします。

Q, ファイルを右クリック検索できるようにしたい。

A, 下記の手順で設定を実施してください。

・ログイン後[コンソールを開く]より[ダッシュボード]画面を表示します。
・画面左側にあるメニューアイコンの[ポリシー]を選択します。
（MVB をインストールしているデバイスすべてに設定が反映されます）
・[ポリシー]画面で[グローバルセキュリティエージェント設定]の[エンドポイントの Windows ショートカットメニューに手動検索を追加]へチェックを入れます。
・[保存]をクリックします。
・設定が反映されるまで時間がかかるため、15 分ほどお待ちいただいてから動作確認をお願いします。

## FAQ.9 （Windows OS：『クラウドサービス for MVB EDR をご契約のお客様）

Q. 注意が必要なイベントとして影響を受けたエンドポイント（コンピュータ）が隔離されました。エンドポイント（コンピュータ）の隔離解除はどのようにおこなうのですか。

A. エンドポイント（コンピュータ）の隔離解除につきましては**脅威が解消されたことを十分にご確認のうえ**隔離除外を実施してください。

・管理画面ログイン後、隔離を解除したい[エンドポイント名]をクリックします。


・[タスク] － [接続を復元]を選択します。


※隔離の状態である場合、こちらのアイコンが表示されています。

・[復元]をクリックします。


・復元が実行された画面が表示されます。




※　隔離の状態アイコンが消えます

・以上により、通常の状態となり隔離が解除されます。

## FAQ.10 （Android OS）

Q,　CSMVB をダウンロード後、インストールがブロックされてしまいます。回避方法を教えてください。

A,　「提供元不明のアプリ」（サードパーティ アプリケーション）をインストールできるように設定を変更してください。

**※ 機種によって操作方法が違いますので、詳しくは各機種の取扱説明書をご確認ください。**

## FAQ.11 （共通）

Q, クラウドサービス for MVB お客様情報の変更方法またはパスワードリセット方法を教えてください。

A, パスワードリセットは、管理コンソールのログオン画面、[パスワードのリセット（パスワードをお忘れの場合)]にアクセスし、[アカウント名]に管理者アカウントを入力し、送信してください。
※登録アドレスへパスワードリセットメールが配信されます。

登録情報変更は、管理コンソールのログオン後、画面上部の[ユーザー登録情報]をクリック後のページにて、[担当者(指名)][メールアドレス]を変更後、[送信]ボタンをクリックしてください。

弊社にてクラウドサービス for MVBの管理者メールアドレスやご担当者名を変更の上、パスワードリセットメールを送信させて頂くための手順となります。
※クラウドサービス for MVBにて、現在登録されているお客様管理者が既に退社されているなど、ログインパスワードが分からず、且つパスワードリセットメールも受信出来ないような状況でご利用ください

■登録メールアドレスを利用できない場合の変更依頼方法について
何らかの理由で現在の登録メールアドレスが使用できずパスワードのリセットもできない場合、下記 URL の情報を参照の上、指定のメールアドレスに、変更したいメールアドレスから、変更依頼内容を記載した Excel ファイルを送付してください。15時までに依頼を受け付けた場合は受付日の当日中に、15時以降に依頼を受け付けた場合は翌営業日に登録メールアドレスの変更処理を行います。

変更完了後、新しい登録メールアドレス宛にパスワードリセット用 URL が記載されたメールが送信されますので、新しいパスワードを設定してください。パスワードリセット用 URL は発行から24 時間の有効期限がある為、有効期限が切れている場合は改めてパスワードリセットを実施してください。

■クラウドサービス for MVB お客様情報の変更依頼について
https://itkeeper.service.ricoh.co.jp/isp2/mvb/post_128.html

※登録情報変更依頼で変更した登録メールアドレスはレポート、及び通知の送信先メールアドレスと連動しておりません。必ず別途各設定を見直すようにお願いします。

**要・Excel のテンプレート**

## 3. 付録

### 付録 A：プロキシサーバご使用のお客様へ（Windows OS）

インストール開始時と完了時にプロシキサーバのユーザー名、パスワード入力が必要です。

・インストール開始時にプロキシ認証ポップアップが出現します。
・プロキシサーバのユーザー名、パスワードを入力します。
・［次へ］をクリックすると、インストールが続行します。

尚、インストール完了後も必要に応じてユーザー名、パスワード入力を求めるポップアップが出現しますので、同様にユーザー名、パスワードを入力してください。

## 付録 B：サーバと AA 間の通信について

CSMVB サーバと CSMVB クライアント（エージェント）間で発生する通信は次の通りです。

❖ クライアント側からサーバ側への通信

CSMVB クライアントから、CSMVB サーバに対する通信は次の通りです。（Windows OS）

| ポート | URL | 説明 |
|---|---|---|
| 443 | https://wfbs-svc-nabu-aal.trendmicro.com/* | エージェントからの定期的なアクセス<br>･エージェントのステータス更新<br>･設定情報の取得<br>･エージェントの情報、ログ送信 |
| 443 | https://wfbs-svc-nabu.trendmicro.com | Web 管理コンソールへのアクセス |
| 80/443 | wfbs-svc-nabu-aal.trendmicro.com/*<br>wfbs-svc-nabu.trendmicro.com/*<br>wfbs-svc-dl-tokyo.trendmicro.com/*<br>wfbs-svc-dl-nabu.trendmicro.com/*<br>hotfix-nabu.wfbs-svc.trendmicro.com/* | インストールパッケージおよび Hotfix のダウンロード |

CSMVB クライアントから、CSMVB サーバに対する通信は次の通りです。（Android）

| ポート | URL | 説明 |
|---|---|---|
| 443 | https://wfbs-svc-nabu-mobile-aal.trendmicro.com<br>https://wfbs-svc-nabu.trendmicro.com | 定期的なアクセス<br>･端末情報の更新<br>･設定情報の取得<br>インストールアプリのダウンロード<br>アップデートモジュールの取得 |
| 443 | *.mobile.trendmicro.com<br>*.xdr.trendmicro.com | アカウント認証<br>プッシュ通知<br>インストーラリンク接<br>※Agent 2.0.0 以降で使用 |

❖ CSMVB サーバからクライアントへの通信

サーバからクライアントへの通信は基本的にはありませんが、Android 版クライアントをご使用の場合、CSMVB サーバから設定の同期などのコマンドを発行する際に、GCM FCM(Firebase Cloud Messaging)を利用してデバイスへ通知を送信します。

| ポート | 使用ポート | 説明 |
|---|---|---|
| 443<br>5228<br>5229<br>5230 | *.googleapis.com<br>*.firebase.com<br>*.google.com | CSMVBサーバからのコマンドの通知 |

## 付録 C：クライアントのアイコン一覧（Windows OS）

クライアントに表示されるアイコン表示は以下の通りです。

❖ タスクトレイに表示されるクライアントのアイコン

| アイコン | 意味 |
|---|---|
| | ステータスは正常です |
| | （アニメーションで表示） 手動検索または予約検索を実行中です |
| | アップデートを実行中です |
| | 処理が必要です。<br>・リアルタイム検索が無効です<br>・不正プログラムを完全に駆除するために再起動が必要です<br>・エンジンがアップデートされたため再起動が必要です<br>・アップデートが必要です<br>（注意） CSMVB のメインコンソールを開いて、必要な処理を確認してください |

❖ コンソールのフライオーバアイコン

| 機能 | アイコン | 意味 |
|---|---|---|
| 接続 | | ビジネスセキュリティサーバに接続されています |
| | | ビジネスセキュリティサーバには接続されていませんが、リアルタイム検索は引き続き実行されています。パターンファイルが最新でない可能性があります。Windows タスクバーで CSMVB アイコンを右クリックし、[今すぐアップデート]をクリックします。 |
| リアルタイム検索 | | オン |
| | | オフ |
| スマートスキャン | | ビジネスセキュリティサーバのスキャンサーバに接続されています |
| | | グローバルスマートスキャンサーバに接続されています |
| | | スキャンサーバまたはグローバルスマートスキャンサーバに接続できません |
| | | スマートスキャンが無効です。従来型スキャンを使用しています。 |
| ・POP3 メール検索<br>・ファイアウォール<br>・Web レピュテーション<br>・URL フィルタ<br>・挙動監視<br>・デバイス制御 | | オン |
| | | オフ |

## 付録 D：Windows と Android の機能比較 （Windows OS、 Android OS）

| 提供サービス/機能 | | Windows OS | Android OS |
|---|---|---|---|
| セキュリティ対策 | ウイルス対策 | ○ | ○ |
| | スパイウェア対策 | ○ | — |
| | Web レピュテーション | ○ | ○ |
| | URL フィルタ | ○ | — |
| | ファイアウォール | ○（※1） | — |
| | 挙動監視 | ○ | — |
| | 機械学習型検索 | ○ | — |
| | アプリケーションコントロール | ○（※1） | — |
| | USB デバイスコントロール | ○ | — |
| | 情報漏えい対策機能 | ○（※1） | — |
| | 不正アプリ対策 | — | ○ |
| | 仮想パッチ | ○（※1） | — |
| モバイルデバイス管理 | パスワードポリシー設定 | — | ○（※2） |
| | リモート検索 | — | ○（※2） |
| | リモートロック／消去 | — | ○（※2） |
| | パスワード/PIN の制御（複雑性等） | — | ○（※2） |
| | パスコードをクリア | — | ○（※2） |
| セキュリティポリシー管理 | | ○ | ○ |
| 通知サービス | | ○ | ○ |
| レポートサービス | | ○ | ○ |
| ヘルプデスク | | ○ | ○ |

（※1）：初期設定は無効です。管理コンソール（Web）にて設定することができます。
（※2）：端末インストール時に、機能利用有無の選択ができます。

## 付録 E：UTM 製品との同時利用時の留意事項 （Windows OS）

●UTM と CS for MVB を同一 LAN 環境に導入されている場合、CS for MVB のスマートスキャン機能が継続的に使用不可となる可能性があります。

＜原因＞

CS for MVB で使用している TrendMicro ウイルスバスター ビジネスセキュリティサービスでは独自の証明書を使用しているため、Windows に UTM 機器の証明書をインポートした場合でも UTM 機器の証明書を用いた HTTPS の通信ができません。

●事象を発生させない為に以下の対応を実施ください。

1.UTM とクライアントの参照する DNS サーバを同一となるよう設定してください。
2.FQDN を SSL インスペクションの除外となるよう設定してください。
wfbssvc65-jp.icrc.trendmicro.com
wfbssvc63-attk.icrc.trendmicro.com
wfbss660-ja.fbs25.trendmicro.com

※UTM 機器の設定方法については、購入元の販売会社もしくはメーカーにお問い合わせください。
※リコージャパンから導入され GSP に関しては、FortiOS6.2.4 以降のベース Config に除外設定が入っており、導入時に設定いたしますが、それ以前の FortiOS バージョンは、必要に応じて除外設定を追加して頂く必要があります。
※リコージャパンから導入された PaloAltoNetworks 運用パックに関しては導入時にベースコンフィグに除外設定が実施されております。