RICOH

ITKeeper シリーズ
ネットワークセキュリティパック
オプションメニュー　PC ウイルス対策
クラウドサービス　for　MVB

ユーザーマニュアル　V1.0

改訂履歴:

Version	発行日・改訂日	更新内容
1.0	2016/7/15	初版作成

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

RICOH

ITKeeper シリーズ
ネットワークセキュリティパック
オプションメニュー　PC ウイルス対策
クラウドサービス　for　MVB

【第1章】

1. 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。

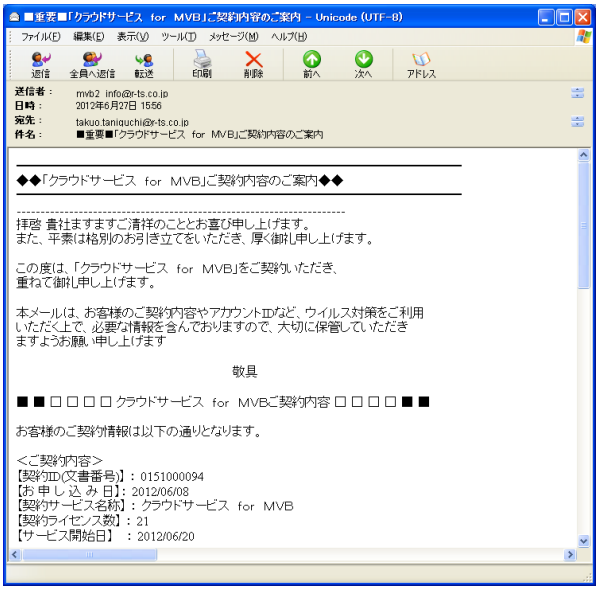
✧ 管理コンソールのシステム要件

Web ブラウザ	・ Internet Explorer 8.0、9.0、10.0*1、11.0*1 (32 ビットおよび 64 ビット) ・ Firefox 24(ESR)、26、27、28 ・ Chrome*2 *1 InternetExplorer10.0、11.0 は Windows(Modern)UI での利用には非対応 *2 Chrome は自動的にバージョンが更新されていき、且つ自動更新を止めるにはレジストリの変更が必要となる仕様であるため、CSMVB では常に最新のバージョンまでサポートします。
PDF リーダ(レポート用)	Adobe Reader 10.0 以降
ディスプレイ	解像度 1024×768 ピクセル以上

【詳細】

※　Windows8／8.1 では、ModernUI(タイルが表示されるスタート画面)からインストールや Web 管理コンソール操作は行えません。デスクトップ画面から操作してください。

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。


■重要■「クラウドサービス for MVB」ご契約内容のご案内 - Unicode (UTF-8)

ファイル(F) 編集(E) 表示(V) ツール(T) メッセージ(M) ヘルプ(H)

返信 全員へ返信 転送 印刷 削除 前へ 次へ アドレス

送信者： mvb2 info@r-ts.co.jp
日時： 2012年6月27日 15:56
宛先： takuo.taniguchi@r-ts.co.jp
件名： ■重要■「クラウドサービス for MVB」ご契約内容のご案内

◆◆「クラウドサービス for MVB」ご契約内容のご案内◆◆

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、お客様のご契約内容やアカウントIDなど、ウイルス対策をご利用
いただく上で、必要な情報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

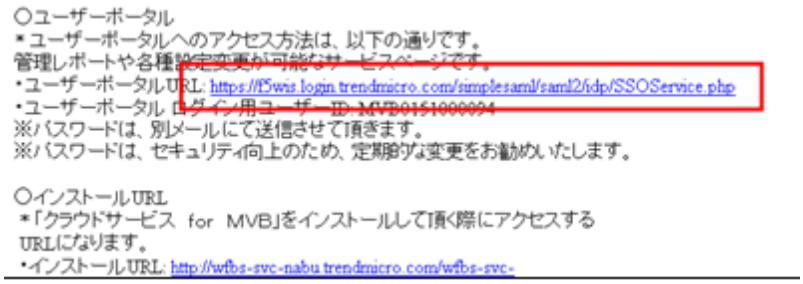
敬具

■ ■ □ □ □ □ クラウドサービス for MVBご契約内容 □ □ □ □ ■ ■

お客様のご契約情報は以下の通りとなります。

<ご契約内容>
【契約ID(文書番号)】：0151000094
【お 申 し 込 み 日】：2012/06/08
【契約サービス名称】：クラウドサービス for MVB
【契約ライセンス数】：21
【サービス開始日】 ：2012/06/20

1-2.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。

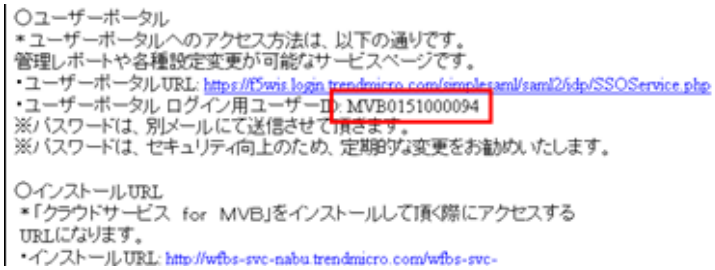

○ユーザーポータル
＊ユーザーポータルへのアクセス方法は、以下の通りです。
管理レポートや各種設定変更が可能なサービスページです。
・ユーザーポータルURL: https://f5wis.login.trendmicro.com/simplesaml/saml2/idp/SSOService.php
・ユーザーポータル ログイン用ユーザーID: MVB0151000094
※パスワードは、別メールにて送信させて頂きます。
※パスワードは、セキュリティ向上のため、定期的な変更をお勧めいたします。

○インストールURL
＊「クラウドサービス for MVB」をインストールして頂く際にアクセスする
URLになります。
・インストールURL: http://wfbs-svc-nabu.trendmicro.com/wfbs-svc-

1-3.Welcome メールの【アカウント】と【パスワード】を確認します。

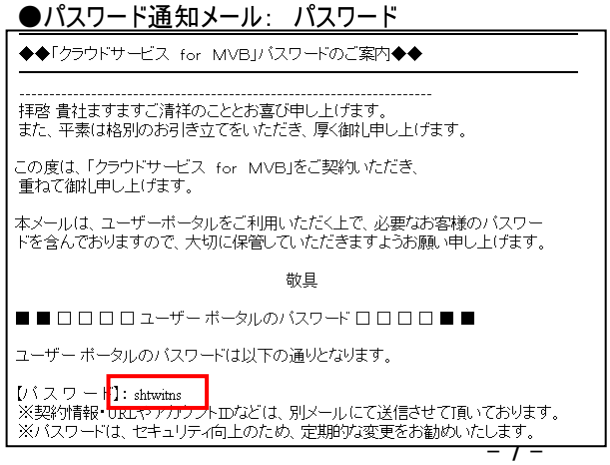
※ 【アカウント】と【パスワード】はそれぞれ別メールにて送付されます。

●登録完了メール： ログイン用ユーザ ID


○ユーザーポータル
＊ユーザーポータルへのアクセス方法は、以下の通りです。
管理レポートや各種設定変更が可能なサービスページです。
・ユーザーポータルURL: https://f5wis.login.trendmicro.com/simplesaml/saml2/idp/SSOService.php
・ユーザーポータル ログイン用ユーザーID: MVB0151000094
※パスワードは、別メールにて送信させて頂きます。
※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。

○インストールURL
＊「クラウドサービス for MVB」をインストールして頂く際にアクセスする
URLになります。
・インストールURL: http://wfbs-svc-nabu.trendmicro.com/wfbs-svc-

●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。

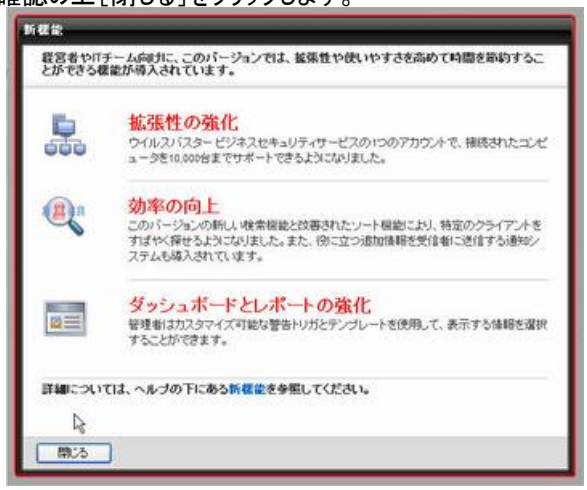
1-4.Web 管理コンソールにアカウントとパスワードを入力します。

※ 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。

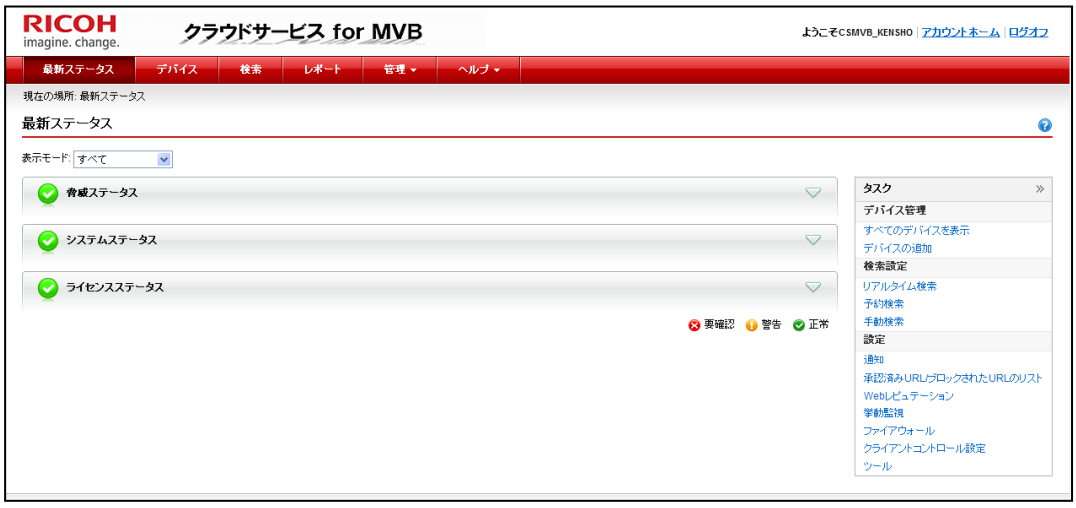
1-5.[コンソールを開く]をクリックします。

※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。

※アップデートなどで機能が拡張された場合には新機能の説明ポップアップが出現します。
確認の上[閉じる]をクリックします。



1-6.ログイン完了です。



2. 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。

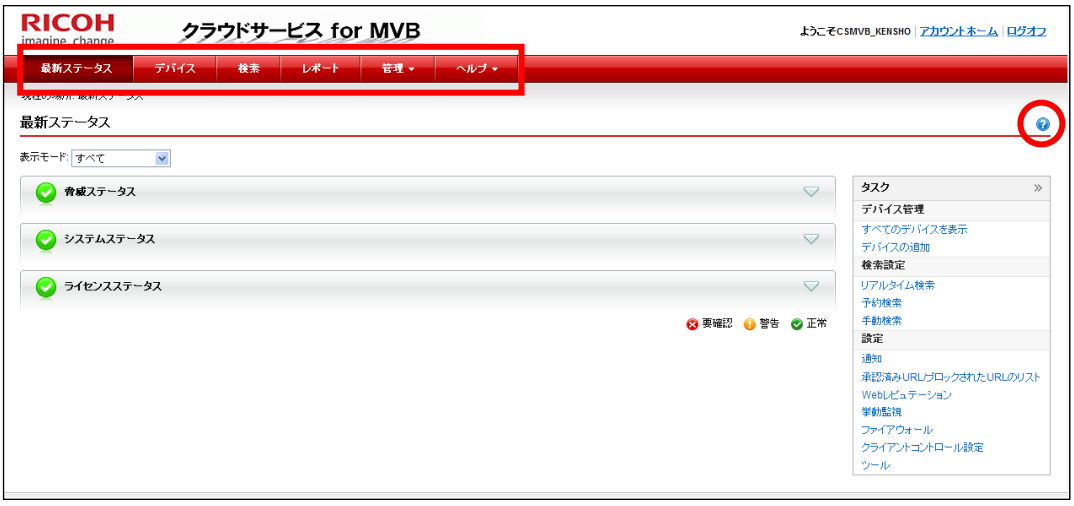
管理コンソールで利用可能な機能

最新ステータス	セキュリティに対する脅威を把握できます。
デバイス	クライアントをインストールしたコンピュータを管理、追加、削除が可能です。
検索	全てのコンピュータの手動検索と予約検索を設定します。
レポート	検出された脅威に関する詳細情報が記載されたレポートを作成および表示できます。
管理−通知	各種イベントを設定します。
−グローバル設定	グローバル設定を行います。
−ツール	各ツールをダウンロードできます。
−ライセンス	ライセンス情報を表示します。
−SmartProtectionNetwork	トレンドマイクロスマートフィードバック機能を利用できます。
−WorryFreeRemoteManager	サービスを委任する認証キーを入力できます。 ※弊社にて事前に設定を実施しております。お客様側での設定は不要です。
ヘルプ	ヘルプを表示します。

【詳細】

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

2−2　利用したい機能のタブをクリックします。



※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。

3. 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[ビジネスセキュリティクライアントを開く]をクリックして開きます。クライ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】
3-1　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。

3-2　[ビジネスセキュリティクライアントを開く]をクリックします。

3-3　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。

4. 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 ・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

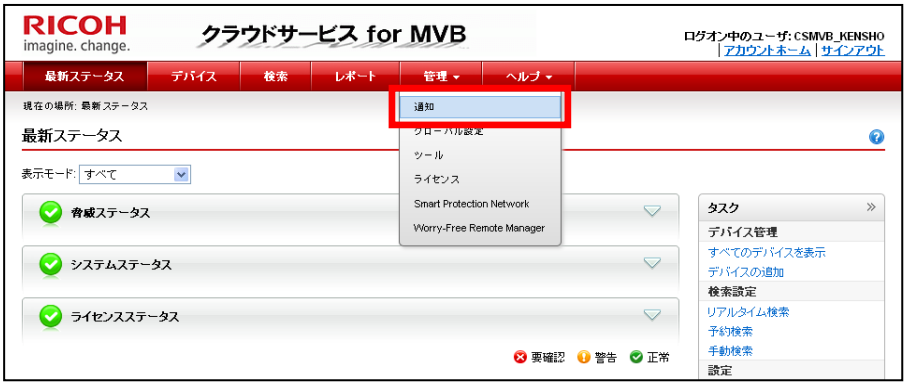
4-1.アラート通知の設定方法について

【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】

4-1-1　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)

4-1-2　トップ画面の[管理]タブの[通知]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。

4-1-3　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。

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

4-1-5　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

4-1-6　[成功しました]と表示されれば作業は完了です。

4-1.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。

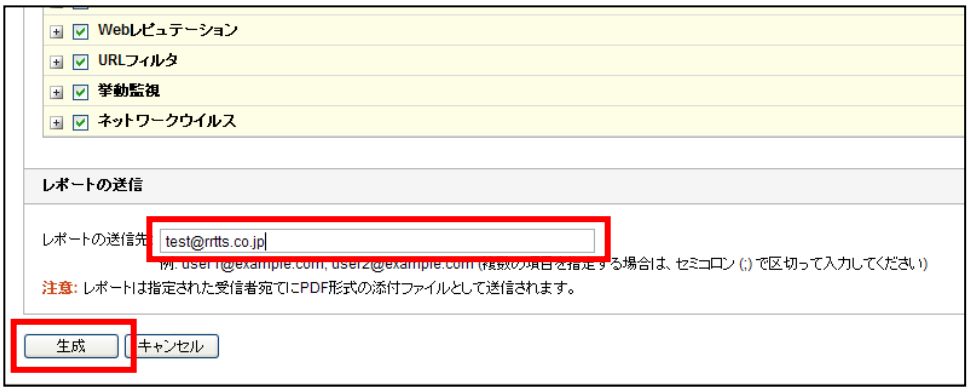
【詳細】

4-2-1 ［レポート］タブの該当レポートをクリックします。

4-2-2 レポートが開きますのでレポート名を確認し、下にスクロールしてください。

［レポートの送信先］にアドレスを入力し［生成］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。



4-2-3 ［成功しました］と表示されれば作業は完了です。

RICOH

ITKeeper シリーズ
ネットワークセキュリティパック
オプションメニュー　PC ウイルス対策
クラウドサービス　for　MVB

【第2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。

http://itkeeper.ricoh.co.jp/isp/nsp/usermanual.html

お問い合わせ窓口:

電話 : 0120-653-920

営業時間 : 平日 8:30 ～ 18:00 （土日祝日およびリコーの指定日を除く）

2. FAQ

FAQ.1

Q, Web 管理コンソールの「パスワード」を忘れてしましました。

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、アカウント ID と最初に登録したメールアドレスを入力します。

・入力したメールアドレスに、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 1 時間で無効となります。

FAQ.2

Q, Web 管理コンソールの「アカウント」を忘れてしましました。

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

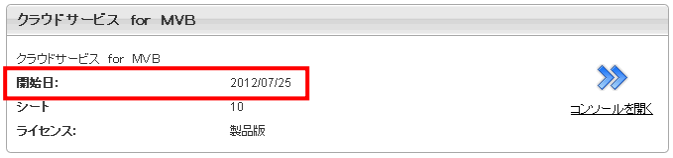
Q, Welcome メールを無くしてしまいました。再インストールはどうすれば良いのでしょうか。

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

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

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 のセキュリティーレベルにより
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。

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://ssl.trendmicro.com/resources/root-certs/ を開きます
・「AffirmTrust Networking」の[ダウンロード]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://ssl.trendmicro.com/resources/root-certs/ を開きます
・「Trend Micro CA」の[ダウンロード]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

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。

3. 付録

付録 A:サーバ、クライアントの通信について

CSMVB では、ネットワーク内で、代表 CSMVB クライアントが「パターンファイルのダウンロード」や「各種設定」の取得を行う「アクティブエージェント」という技術を使用しています。

■アクティブエージェントの機能

代表となった CSMVB クライアントは、アクティブエージェント(以下、AA)と呼ばれます。AA は、同一 LAN 内上のクライアントの代表として、パターンやエンジンのアップデートの実施、CSMVB サーバから最新の設定の取得を行います。AA 以外の CSMVB クライアントは、インアクティブエージェント(以下 IA)と呼ばれ、AA からパターンの更新、最新の設定の取得を行います。

CSMVB クライアントは、必ず AA か IA のどちらかとして動作します。

❖ 一台の AA が管理できる IA の数

1 つの AA で管理できる IA は 10 台となっています。例えば、同一 LAN 内に 22 台のコンピュータがあった場合、2 台のコンピュータが AA に選出され 20 台のコンピュータが IA となり、AA からパターンファイルのアップデートの通知を受け、ダウンロードを行います。

❖ IA からの AA への接続の管理

IA から、AA へのアップデートをダウンロードするためのタイミングは、クライアント負荷を分散するためにランダムになっています。これにより、AA の CSMVB のシステムリソースの使用率が極端に大きくなることはありません。

付録 B:プロキシサーバご使用のお客様へ

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、同様にユーザ名、パスワードを入力してください。

付録 C: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。

通信	使用ポート	説明
定期的なアクセス	443	クライアントのステータスの更新 最新設定の取得
インストールパッケージの ダウンロード	80	ブラウザからインストール用のパッケージをダウンロードします。

接続先	URL
CSMVB サーバ(管理サーバ)	http://wfbs-svc-nabu-aal.trendmicro.com https://wfbs-svc-nabu-aal.trendmicro.com http://wfbs-svc-nabu.trendmicro.com https://wfbs-svc-nabu.trendmicro.com

❖ 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(Google Cloud Messaging)を利用してデバイスへ通知を送信します。

通信	使用ポート	説明
GCM (Google Cloud Messaging)	5228 5229 5230	CSMVBサーバからのコマンドの通知

付録 D:AA と IA 間の通信について (Windows OS、 Android OS)

AA と IA 間の通信において使用されるポートは以下のとおりです。

サービス	プロトコル	ポート番号
Agent send command to Client	TCP	21112
Local http server	TCP	61116
Broadcast for electing AA	UDP	61117
WhoisAA tool communication	UDP	61118
Downloader	UDP	61119

■各 CSMVB クライアント(AA/IA)と CSMVB サーバ間の定期的な通信について

各 CSMVB クライアントとサーバ間の通信には、AA のみが行う通信と AA/IA 双方が行う通信があります。

❖ AA が CSMVB サーバと行う通信について

以下の通信はすべて 5 分間隔で実施します。

- オンライン/オフラインの確認
- Hotfix の確認
- サーバから発行されるコマンドの確認
- ポリシー設定の確認

❖ 各 AA/IA が CSMVB サーバと行う通信について

- クライアント環境情報(クライアントインストール後 1 回のみ)
- コンポーネントのアップデート情報(コンポーネントのアップデートがあった場合:1 分毎)
- ウイルスログ等の各種ログの送信(ログの種類により 30 秒～50 分毎)

付録 E:クライアントのアイコン一覧

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。 ・リアルタイム検索が無効です ・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 ・エンジンがアップデートされたため再起動が必要です ・アップデートが必要です （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 ・ファイアウォール ・Web レピュテーション ・URL フィルタ ・挙動監視 ・デバイス制御		オン
		オフ