

VBBSS バージョン6.7 新機能と改善点のご紹介

1. はじめに

- Ver6.7公開スケジュールと新ビルド配信のタイミング
- Ver6.7 新機能/改善点一覧

2. セキュリティ対策機能の強化

- 除外リストへのIPv6アドレス追加対応
- Mac OSへの機能追加

3. 管理コンソールのUI改修

- 「ダッシュボード」画面のウィジェット改修
- インストーラのダウンロード
- 検出されたUSBデバイスの許可
- 「ログ」画面のUI改修

4. システム要件の変更

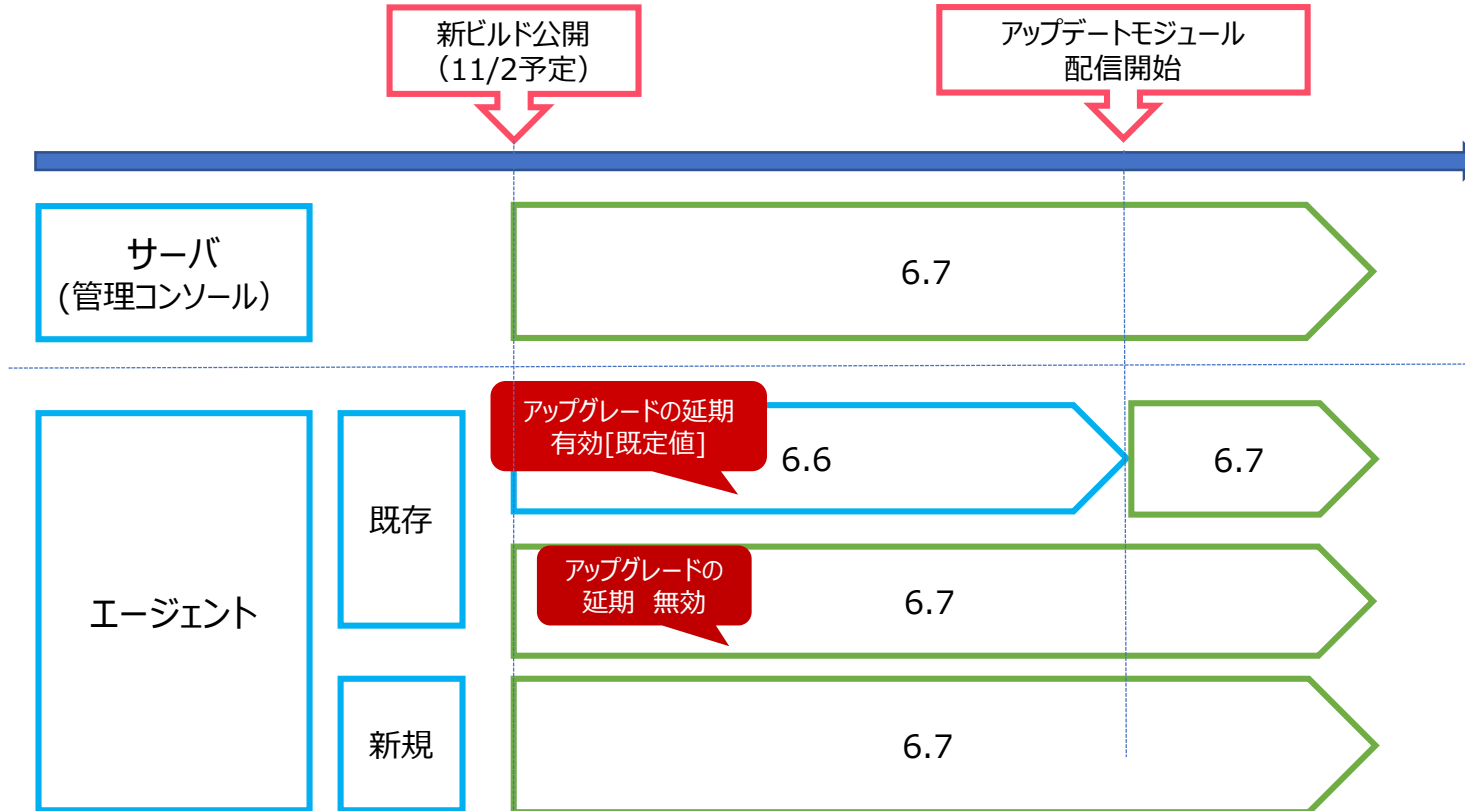
5. appendix

- GUIDリセットツール
- Macコンポーネントバージョン画面の表示情報変更（エージェント側）
- 初期値の変更

1.はじめに

VBBSS Ver6.7 公開スケジュール：2019年11月2日 公開(予定)

- 既定値では、新ビルド公開後30日経過(*)後、順次エージェント側へ配信します。アップグレードの延期設定を無効にしている場合は、新ビルド公開後、順次配信されます
- 新規インストーラは新ビルド公開と同時に置き換えます



*既存エージェントへの配信は、下記の設定値に依存します
「ポリシーの設定」-「権限およびその他の設定」-「その他の設定」タブの
「アップグレードの延期」設定



VBBSS Ver6.7 新機能/改善点一覧



DAIWABO INFORMATION SYSTEM CO., LTD.

分類	項目	概要	
セキュリティ対策機能の強化	除外リストへのIPv6アドレス追加対応	グローバル除外リストの承認済みIPアドレスリストおよびファイアウォール除外リストへ、IPv6アドレスの登録が可能になりました。	Win
	Mac OSへの機能追加	URLフィルタ機能が追加されました。	Mac
管理コンソールのUI改修	「ダッシュボード」画面のウィジェット改修	ダッシュボードの「ランサムウェアの概要」ウィジェットが、「感染経路別の検知数」ウィジェットに変更されました。プルダウンより [すべての脅威] または [ランサムウェア] から表示する脅威の種類を選択できます。	Win Mac
	インストーラのダウンロード	「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」にて、インストーラのダウンロード時、OS種類を選択してダウンロードできるようになりました。	Win Mac
	検出されたUSBデバイスの許可	許可されたUSBデバイスのデバイス追加方法に、[検出されたデバイスを選択]が追加されました。これによりデバイスコントロールで検出されたUSBデバイスを選択しリストへ追加できるようになりました。	Win
	「ログ」画面のUI改修	ログの日時情報指定 / ログからのアプリケーションコントロール許可ルールへの追加画面が追加されました	Win Mac

2.セキュリティ対策機能の強化

除外リストへのIPv6アドレス追加対応①

Windows

グローバル除外リストの承認済みIPアドレスリストおよびファイアウォール除外リストへ、IPv6アドレスの登録が可能になりました。

- ・「ポリシー」 - 「グローバル除外リスト」 - [承認済みIPアドレスリスト]

ポリシー設定

追加の設定

- グローバルセキュリティエージェント設定
- グローバル除外リスト

ポリシーリソース

- アプリケーションコントロールルール

グローバル除外リスト

ポリシー設定を使用するために必要な除外設定を構成します

Webレピュテーション / URLフィルタ

- 承認済みURLリスト (15)
指定されたWebサイトへのアクセスを許可します。(Windows Defender SmartScreen)
- ブロックするURLリスト (0)
指定されたWebサイトへのアクセスをブロックします。
- 承認済みIPアドレスリスト (1)**
指定された宛先IPアドレスへのアクセスを許可します。
- 許可されたプロセスのリスト (0)
指定されたプロセスがWebサイトにアクセスすることを許可します。

承認済みIPアドレス

宛先IPアドレス:

fe80::d52a:2f8d:adc9:fb38%6 × IPv4またはIPv6アドレス **New!**

例: 192.168.2.1; 192.168.1.0

追加 キャンセル

除外リストへのIPv6アドレス追加対応②

グローバル除外リストの承認済みIPアドレスリストおよびファイアウォール除外リストへ、IPv6アドレスの登録が可能になりました。

- 「ポリシーの設定」 - 「ファイアウォール設定」 - [詳細モード]

ポリシーの設定: Test_Group

対象とサービスの設定

Windows Apple Android iOS

脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索
- Webレピュテーション
- 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
- 情報漏えい対策

アクセスコントロール

- URLフィルタ
- アプリケーションコントロール

除外リスト

- 検索除外
- 承認済みブロックするURL

エージェントの設定

- 権限およびその他の設定

ファイアウォール設定

ファイアウォールは、エンドポ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、一時的にエンドポ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、設定の変更を行ってください。

簡単モード 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

セキュリティレベル

	受信トラフィック	送信トラフィック
<input type="radio"/> 高	ブロック	ブロック
<input type="radio"/> 中	ブロック	許可
<input checked="" type="radio"/> 低	許可	許可

IDS (侵入検出システム)

IDS (侵入検出システム) を有効にする

除外リスト

+ 追加

クリックすると表示

ファイアウォール除外

名前: IPv6

処理: ネットワークトラフィックを拒否

方向: 受信
 送信
 両方向

プロトコル: TCP/UDP

ポート: すべてのポート
 指定ポート
 範囲

IPアドレス: すべてのIPアドレス (IPv4/IPv6)
 単一IP

New! fe80::d52a:2f8d:adc9:fb38%

IP範囲

URLフィルタ機能が追加されました。

Windows用のURLフィルタ機能と同様に、カテゴリごとのフィルタルールや業務時間の設定が可能です。

「ポリシーの設定」 - 「URLフィルタ」：既定値有効

※ver.6.6でMacをご利用の場合も、ver.6.7にアップデート後既定値としてURLフィルタが有効になります

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

Windows Apple Android iOS

脅威からの保護機能

- 検索設定
- 機械学習型検索
- Webレピュテーション

情報漏えい対策

- デバイスコントロール
- マカサスコントロール
- URLフィルタ**

除外リスト

- 承認済みURL
- 検索除外

エージェントの設定

- 権限およびその他の設定

URLフィルタ

URLフィルタを有効にすると、管理者は、1日のさまざまな時間帯でブロックする特定の種類のWebサイトを設定することができます。

オン

フィルタ強度

- 高 既知または潜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、生産性または帯域幅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
- 中 既知のセキュリティ上の脅威および不適切なコンテンツをブロックします
- 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
- 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

URLカテゴリ	<input checked="" type="checkbox"/> 業務時間	<input type="checkbox"/> 業務時間外
田 アダルト	<input type="checkbox"/>	<input type="checkbox"/>
田 ビジネス	<input type="checkbox"/>	<input type="checkbox"/>
田 コミュニケーションメディア	<input checked="" type="checkbox"/>	<input type="checkbox"/>
田 一般	<input type="checkbox"/>	<input type="checkbox"/>
田 インターネットのセキュリティ	<input checked="" type="checkbox"/>	<input type="checkbox"/>
田 ライフスタイル	<input type="checkbox"/>	<input type="checkbox"/>
田 ネットワーク	<input type="checkbox"/>	<input type="checkbox"/>

URLのカテゴリや安全性の評価を確認するには、次のWebサイトにアクセスしてください。 <http://sitesafety.trendmicro.com/>

対応webブラウザ

下記webブラウザのHTTP/1.1通信

- Google Chrome
- Mozilla Firefox
- Safari

※詳細は最新のシステム要件をご確認ください

3.管理コンソールのU I改修

「ダッシュボード」画面のウィジェット改修

Windows

Mac

ダッシュボードの「ランサムウェアの概要」ウィジェットが、「感染経路別の検知数」ウィジェットに変更されました。プルダウンより [すべての脅威] または [ランサムウェア] から表示する脅威の種類を選択できます。

6.6(ランサムウェアの概要)



6.7(感染経路別の検出数)



[すべての脅威] 選択時に表示される脅威ログのカテゴリ

- ・ ウイルス/不正プログラム対策
- ・ Webレピュテーション
- ・ 挙動監視
- ・ 機械学習型検索

インストーラのダウンロード

「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」にて、インストーラのダウンロード時、OS種類を選択してダウンロードできるようになりました。

Windows
Mac

セキュリティエージェントのインストール方法

インストール方法の選択: セキュリティエージェントの追加先: 初期設定

インストーラリンクの送信
インストールのダウンロード
このエンドポイントにインストール

メールコンテンツの表示
リンクの有効期限の設定

配信スクリプト、インストール方法の
MSIパッケージを使った
の手順

クリックすると表示

New!

ダウンロードされるファイル名

Windows : WFBS-SVC_Downloader.exe
Mac : WFBS-SVC_Agent_Installer.pkg.zip

セキュリティエージェントのインストーラ

Windows Mac

ダウンロード

ダウンロードユーティリティ (WFBS-SVC_Downloader.exe) をダウンロードして実行し、セキュリティエージェントのインストーラ (WFBS-SVC_Agent_Installer.msi) を取得します。

ファイルの実行は適したOSや条件のもと実施してください。

※Windows端末上でダウンロードしたMac用ファイルをMac端末へコピーして実行しないでください。

正常にインストールできない可能性があります。

検出されたUSBデバイスの許可

許可されたUSBデバイスのデバイス追加方法に、[検出されたデバイスを選択]が追加されました。これによりデバイスコントロールで検出されたデバイスを選択しリストへ追加できるようになりました。

「ポリシー」 - 「グローバル除外リスト」 - 「許可されたUSBデバイスのリスト」

New!

許可されたUSBデバイスのリスト

+ 追加 - 削除 エクスポート

検出されたデバイスを選択
インポート

機種/製品ID シリアルID/番号 メモ

検出されたデバイス

許可されたUSBデバイスのリストに追加するデバイスを選択します。

過去7日間 ① ベンダ 検索

<input checked="" type="checkbox"/>	ベンダ	機種	シリアルID	エンドポイント	ユーザ	日時↓
<input checked="" type="checkbox"/>	buffalo	026D	200078230708565e2c20bd10	■ ■ ■ ■ ■ ■ ■ ■	Trend-DEMO	2019年08月29日 16:29:07

1 - 1 / 1 | 100件/ページ* 1 / 1 < >

追加 キャンセル

デバイス情報を取得する方法

「ログ」画面のUI改修

ログの日時情報指定項目の追加

「ログ」画面にて表示するログの日時情報を、受信日時/生成日時から選択して表示できるようになりました。

受信：サーバがログを受信した日時 (既定値)

生成：エージェントがログを生成した日時

ログ

New! 日時: 受信

受信	カテゴリ	脅威/違反	ファイルのパス対象	処理/結果	エンドポイント	ユーザ	詳細
2019年08月21日 14:49:13	ウイルス/不正プログラム	Eicar_test_1	C:\Users\User01\Downloa...	隔離	win10PC	user01	
2019年08月21日 14:46:32	Webレピュテーション	http://wrs41.winshipway....	-	ブロック	win10PC	user01	

ログ

New! 日時: 生成

生成	カテゴリ	脅威/違反	ファイルのパス対象	処理/結果	エンドポイント	ユーザ	詳細
2019年08月21日 14:48:49	ウイルス/不正プログラム	Eicar_test_1	C:\Users\User01\Downloa...	隔離	win10PC	user01	
2019年08月14日 18:00:00	Webレピュテーション	http://wrs41.winshipway....	-	ブロック	win10PC	user01	

※6.6管理コンソールで表示されていたのは受信日時です。

※[エクスポート]からエクスポートするCSVファイルには、受信日時と生成日時の両方が記載されます。

アプリケーションコントロールログからの許可ルール追加対応

アプリケーションコントロールログのログ詳細画面から、アプリケーションコントロールの許可ルールへ追加できるようになりました。

アプリケーションコントロールログの詳細

プログラム: MicrosoftEdge.exe
生成日時: 2019年08月29日 15:03:37
受信日時: 2019年08月29日 15:22:12

エンドポイント

エンドポイント名: [REDACTED]
ドメイン: -
ユーザ: Trend-DEMO
グループ名: 本社

検出した脅威

ファイルパス:	C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe
SHA-256:	4ac713b9902eeeac3090e033f67fce7eefb23fda013cf6ad69fe817c3d3364d1
ポリシールール:	(ブロック) ブラウザ
処理結果:	ブロック
件数:	4

New!

許可ルールに追加

クリックすると表示

許可ルールに追加

パス:

ファイル フォルダ

C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe

追加先:

許可するフォルダ

追加 キャンセル

ログに記載のパスが自動入力される (編集可)

プルダウンより、追加先の許可ルールを選択する

追加先の許可ルールとして選択可能なルールは、照合方法が[ファイルまたはフォルダのパス]のルールです。
[ファイルまたはフォルダのパス]の許可ルールがない場合は、事前に作成してください。

※[ファイルまたはフォルダのパス]の許可ルールとして追加されます。

4. システム要件の変更

サポート開始OSとサポート終了OS(Mac・Android・iOS)

Mac : 10.15サポート開始、10.10サポート終了
Android OS : 10.0.xサポート開始、5.xサポート終了
iOS : 13.xサポート開始、8.xサポート終了



OS	6.7からサポートされるバージョン	6.7ではサポートされなくなるバージョン	備考
Mac	10.15	10.10	例外を除き、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。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。その際、サポート対象にできない状況がある場合には、別途情報を記載します。
Android	10.0.x	5.0.x, 5.1.x	
iOS	13.x	8.x	

※Mac 10.15対応は、6.7リリースより遅れる可能性があります

※現在6.5でサポートされている下記は、6.7リリース以降すべてのVBBSSバージョンでサポートされなくなります。

- Windows Server 2008 Foundation/Standard/Enterprise/Datacenter SP2
- Windows SBS 2008 Standard/Premium SP2
- Windows EBS 2008 Standard/Premium SP2
- Windows Storage Server 2008 Workgroup/Standard/Enterprise SP2

5.appendix

本ツールを使うことで、複数端末への展開用ディスクイメージ作成前にVBBSSエージェントのGUIDをリセットすることができます。

「管理」 - 「ツール」 からダウンロード可能です。



The screenshot shows a management interface with a sidebar on the left containing menu items like '管理', '一般設定', 'モバイルデバイス登録設定', 'ユーザアカウント', '通知', 'Active Directoryの設定', 'Trend Micro Remote Manager', 'Smart Protection Network', '回復キーのパスワード', and 'ツール'. The main content area is titled 'ツール' and contains several tool entries:

- ログインスクリプトのセットアップ**: Description of adding batch files to server login scripts. Includes links for 'ツールのダウンロード' and '詳細情報'.
- 配信スクリプトのサンプル**: Description of using sample scripts for security agents. Includes links for 'ツールのダウンロード' and '詳細情報'.
- アンインストーラ (Mac)**: Description of using the tool to uninstall agents from Mac OS. Includes links for 'ツールのダウンロード' and '詳細情報'.
- オンプレミスサーバ移行ツール**: A tool for migrating on-premise servers.


A red box highlights the 'Image Cloning Setup Tool' section, which contains the following text:

!!Image Cloning Setup Tool!!
!!Use the tool to prepare necessary registry key values used for the Security Agent program before creating a cloned image for mass deployment!!
ツールのダウンロード | 詳細情報

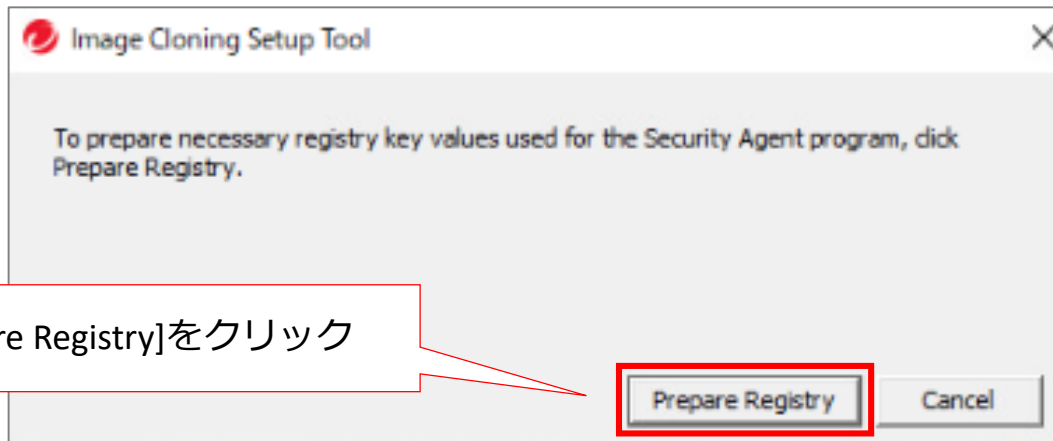
・本ツールに関する詳細は、製品Q&Aおよびオンラインヘルプを公開予定です。

参考) GUIDリセットツールの実行イメージ

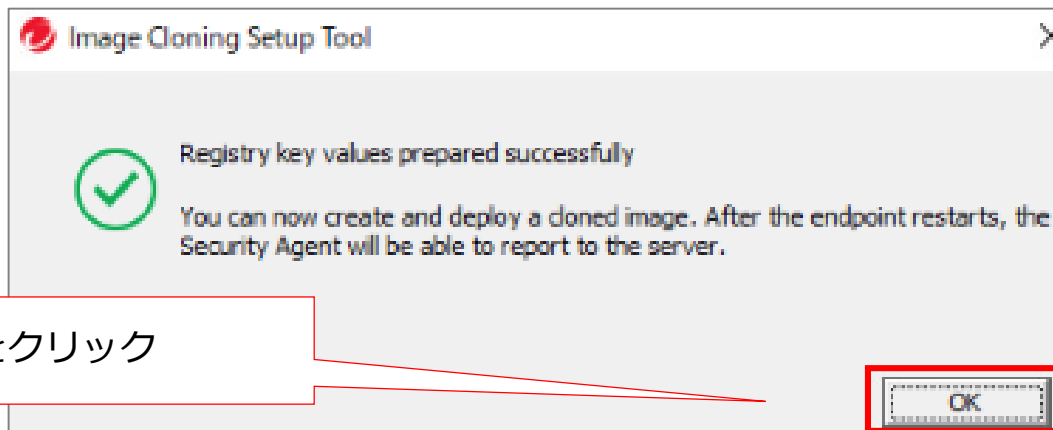
1. ダウンロードした本ツールをマスターPC上で実行

名前	更新日時	種類	サイズ
 ImageCloningSetupTool	2019/09/03 15:19	アプリケーション	2,512 KB

2. [Prepare Registry]をクリック



3. [OK]をクリック



GUIDはエージェント側の「コンポーネントのバージョン」より確認可能です



Mac コンポーネントバージョン画面の表示情報変更 (エージェント側)

エージェント上の「コンポーネントバージョン」画面が下記のように変更されました。

ファイルレピュテーションサービスおよびwebレピュテーションサービス情報を削除

6.6

Trend Microセキュリティエージェント

コンポーネントバージョン

前回のアップデート: 2019/09/02 14:02
エージェントバージョン: 3.5.1134
エージェントGUID: 7F1CFA1A-EEB7-4883-AC61-320137C971E7
サーバ: wfbs-svc-nabu-aal.trendmicro.com
ファイルレピュテーションサービス: <https://wfbsvc65-mac-jp.icrc.trendmicro.com/ss> (使用可能)
Webレピュテーションサービス: <http://wfbs-svc65-jp.url.trendmicro.com> (使用可能)
ポリシー名: Test_Group ⓘ

コンポーネント	バージョン	前回のアップデート
ウイルス検索エンジン	10.000.1040	
スマートスキャンエージェントパターンファイル	15.337.00	2019/09/02
ダメージクリーンナップエンジン	1.500.1033	
ダメージクリーンナップテンプレート	0.011.11	
Macヒューリスティックパターン	1.420.00	2019/09/02

戻る

6.7

Trend Microセキュリティエージェント

コンポーネントバージョン

前回のアップデート: 該当なし
エージェントバージョン: 3.5.1227
エージェントGUID: D808B46F-19D6-47D2-9D10-47E7BABB83CE
サーバ: wfbs-svc-nabu-aal.trendmicro.com
ポリシー名: Test_Group ⓘ

コンポーネント	バージョン	前回のアップデート
ウイルス検索エンジン	10.000.1040	
スマートスキャンエージェントパターンファイル	14.485.00	
ダメージクリーンナップエンジン	1.500.1033	
ダメージクリーンナップテンプレート	0.011.11	
Macヒューリスティックパターン	1.322.00	

戻る

初期設定値の変更

ポリシーの初期設定値が一部変更されます。

対象：6.7公開後に作成した新規ドメインのすべてのポリシー、既存のドメインで新規に作成するポリシー

Windows

Mac

Windows

項目	設定項目	6.6 初期値	6.7 初期値	備考
「検索設定」 - 「リアルタイム検索」 - 「設定」 - 「対象」	メモリで検出された不正プログラムの変種/亜種を隔離する	[サーバ(初期設定)]：無効	[サーバ(初期設定)]：有効	
「デバイスコントロール」	-	無効	有効	[サーバ(初期設定)]は無効のまま
「デバイスコントロール」 - エンドポイントの設定	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	無効	有効	[サーバ(初期設定)]は無効のまま
「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」	行われなかった予約検索を翌日の同じ時刻に実行	無効	有効	

Mac

項目	設定項目	6.6 初期値	6.7 初期値	備考
「検索設定」 - 「リアルタイム検索」 - 「設定」	圧縮ファイルの検索	無効	有効	

ウイルスバスター™  Powered by DIS
ビジネスセキュリティサービス