VBBSS バージョン6.6
新機能と改善点のご紹介

1. はじめに

- Ver6.6公開スケジュールと新ビルド配信のタイミング
- Ver6.6 新機能/改善点一覧

2. セキュリティ対策機能の強化

- ファイルレス攻撃対応
- オフライン時の機械学習型検索対応
- デバイスコントロール機能の強化
- アプリケーションコントロール機能の強化
- バージョンアッププログラムの配信設定
- Mac OSへの機能強化

3. 管理コンソールのUI改修

- 感染経路の可視化
- 検索除外リストの登録方法追加
- その他のUI改修

4. システム要件の変更

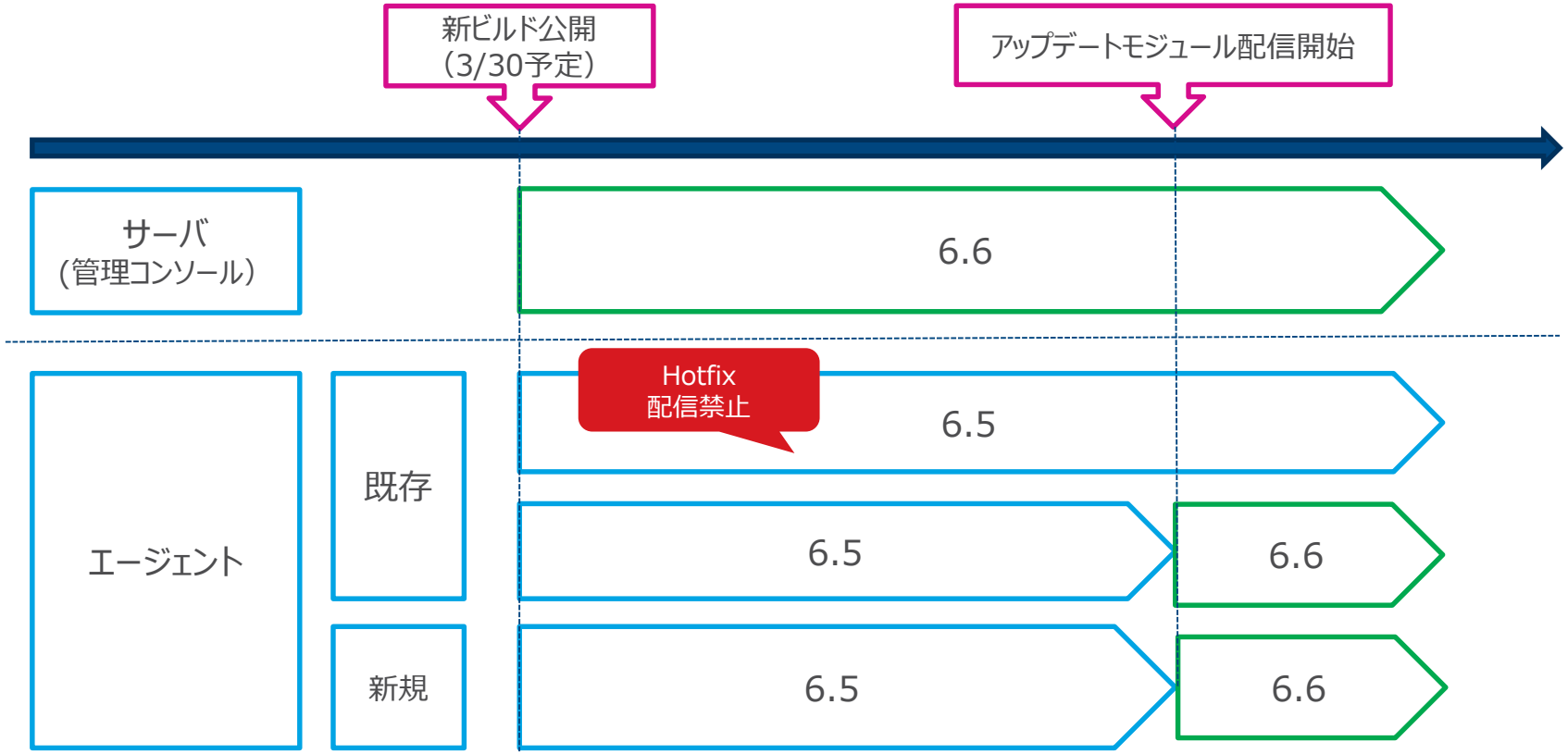
1.はじめに

Ver6.6公開スケジュールと新ビルド配信のタイミング

DAIWABO INFORMATION SYSTEM CO., LTD.

VBBSS Ver6.6 公開スケジュール： 2019年3月30日　公開(予定)

- リリース後、一定期間を経過(*)後にエージェント側へ配信します
- Hotfix配信禁止を設定している場合は配信されません
- 新規インストーラはアップデートモジュール配信開始と同時に置き換えます
- 新機能は6.6エージェント配信開始後より使用可能です



VBBSS Ver6.6 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	ファイルレス攻撃対応	ファイルレス攻撃の手段およびメモリスキャンの機能改善にファイルレス攻撃の検出に対応しました	Win
	オフライン時の機械学習型検索対応	エージェントオフライン時にも機械学習型検索が可能になりました	Win
	デバイスコントロール機能の強化	除外設定としてユーザに対するデバイス制御設定機能が追加されました	Win
	アプリケーションコントロール機能の強化	ホワイトリスト型の登録やロックダウンモード機能が追加されました	Win
	バージョンアッププログラムの配信設定	バージョンアップ時、エージェントへのプログラム配信を延期する設定項目が追加されました	Win
	Mac OSへの機能強化	スマートスキャン対応 /手動検索時間の短縮化機能追加/ 機械学習型検索対応 / デバイスコントロール機能の追加および強化されました	Mac
管理コンソールのUI改修	検索除外リストの登録方法追加	「ログ」画面から、ファイルやフォルダを検索除外リストに追加できるようになりました	Win Mac
	感染経路の可視化	セキュリティイベントが検出されるまでの簡易的なルート確認画面が追加されました	Win
	その他のUI改修	未評価のURLに対する設定項目の切り出し / Site Safety CenterのURLリンク追加 / ダッシュボードからのアグレッシブスキャン が追加されました	Win Mac

2.セキュリティ対策機能の強化

ファイルレス攻撃対応

DAIWABO INFORMATION SYSTEM CO., LTD.

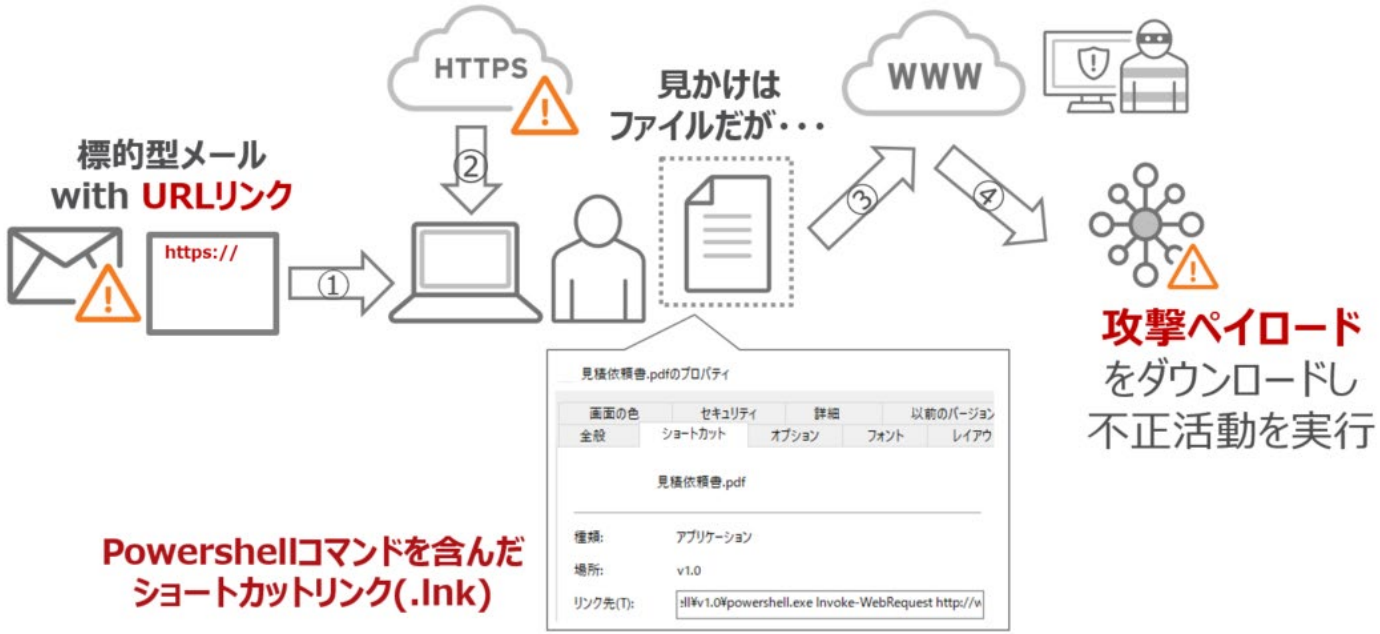
Windows

メモリスキャンの機能向上により、ハードディスクに保存されない
メモリ上にのみ存在するマルウェアを検出できるようになりました。

・WMI(Windows Management Instrumentation)やレジストリを応用した攻撃への対応
・メモリスキャンの強化による一見正常とみられるプロセスの監視機能追加

ファイルレス攻撃とは

通常のマルウェアがハードディスクに保存
され実行されるのに対し、メモリ上にのみ
保存され実行されるファイルレスマルウェア
を使った攻撃。
一般的に、Windows OSに搭載された
power shellで実行可能なコードとして、
不正なスクリプトやコードがメモリ上に
配布実行される。



ファイルレス攻撃対応

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

下記5項目すべてを設定することで、ファイルレス攻撃対策機能が有効になります。

検索設定

1. 「リアルタイム検索」 ： オン
2. 「リアルタイム検索」 -「設定」-「対象」タブ ：
   ☑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(規定値有効)

挙動監視

3.「挙動監視」 ： オン
4. [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] ： オン(規定値有効)

機械学習型検索

5. [機械学習型検索] ： オン(規定値無効)

オフライン時の機械学習型検索対応

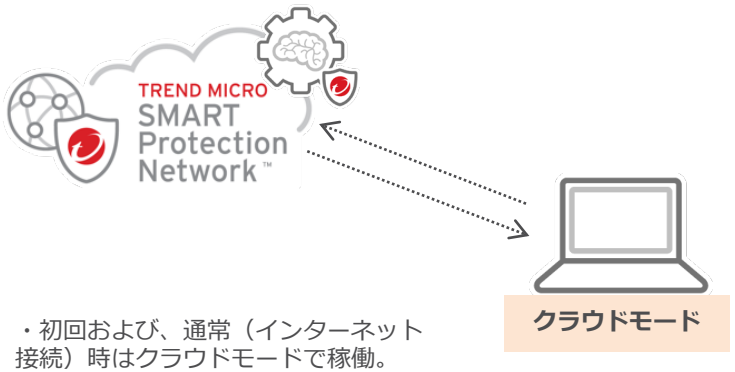
DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

機械学習型検索の利用には、インターネット接続が必要でしたが、
Ver.6.6にて、オフライン時でも機械学習型検索が可能になりました。

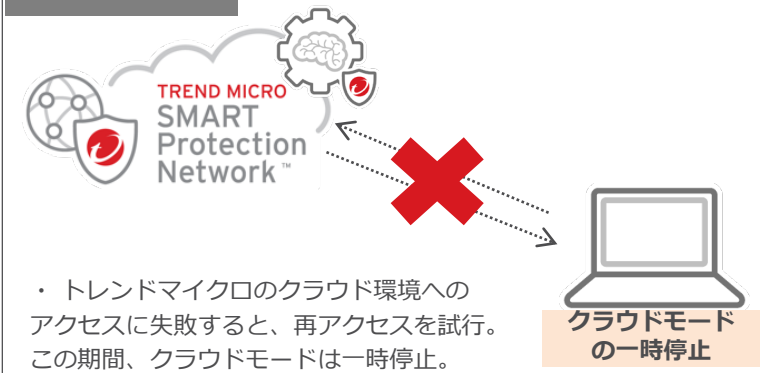
オンライン時（インターネット接続可）　：クラウドモード(弊社クラウドテクノロジを使用)
オフライン時　（インターネット接続不可）：ローカルモード(ローカルの機械学習型検索ファイルモデルを使用)

初回および通常時



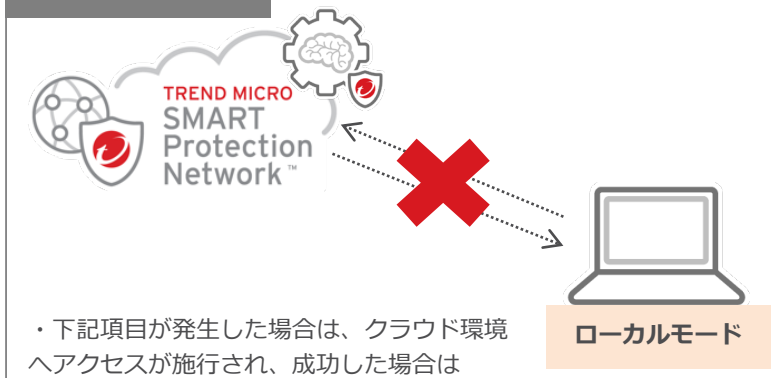
・初回および、通常（インターネット接続）時はクラウドモードで稼働。
・不審なファイルをトレンドマイクロのクラウド環境へ問い合わせ。
・オフライン時用の機械学習型検索ファイルモデルを定期的に取得。

オフライン時



・トレンドマイクロのクラウド環境へのアクセスに失敗すると、再アクセスを試行。この期間、クラウドモードは一時停止。
・60秒間に5回、アクセス施行し、アクセスできた場合はクラウドモードで再稼働。失敗した場合は自動的にローカルモードに切り替わる。
・ローカルモード時、不審なファイルはローカルの機械学習型検索ファイルモデルを利用して検索。

ローカルモード時



・下記項目が発生した場合は、クラウド環境へアクセスが施行され、成功した場合はクラウドモードに切り替わる。
・*IP*変更や*NIC*変更イベントの検出
・プロキシ設定やポート設定を含む設定変更
・クラウド環境へのアクセス施行後*5*分以上経過した場合

※オフライン時は、管理者への通知などなく自動的にローカルモードへ切り替わります。
※クラウドモード/ローカルモードの、モードの選択はできません。適したモードが自動的に適用されます。
※オフライン時用の機械学習型検索ファイルモデルは、パターン同様にダウンロードやアップデートが必要です。

デバイスコントロール機能の強化

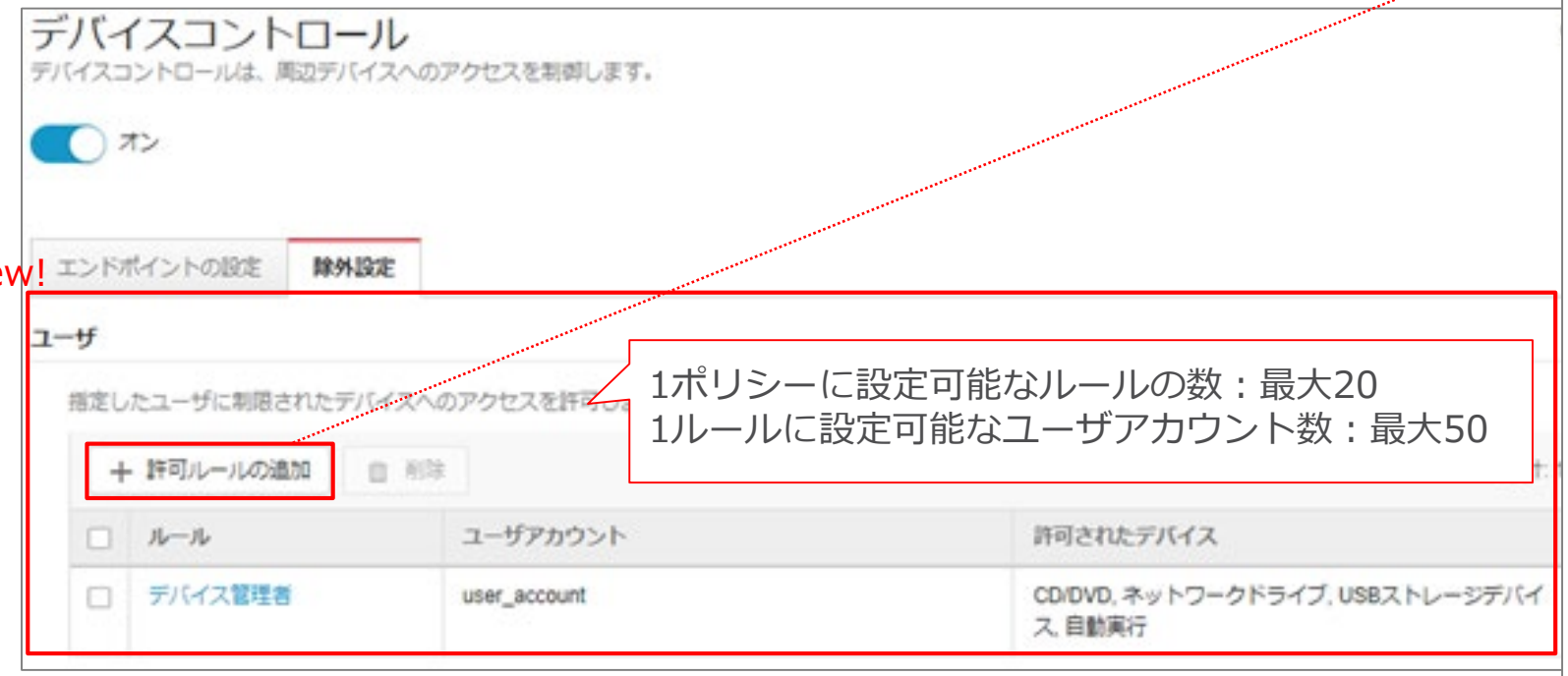
DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

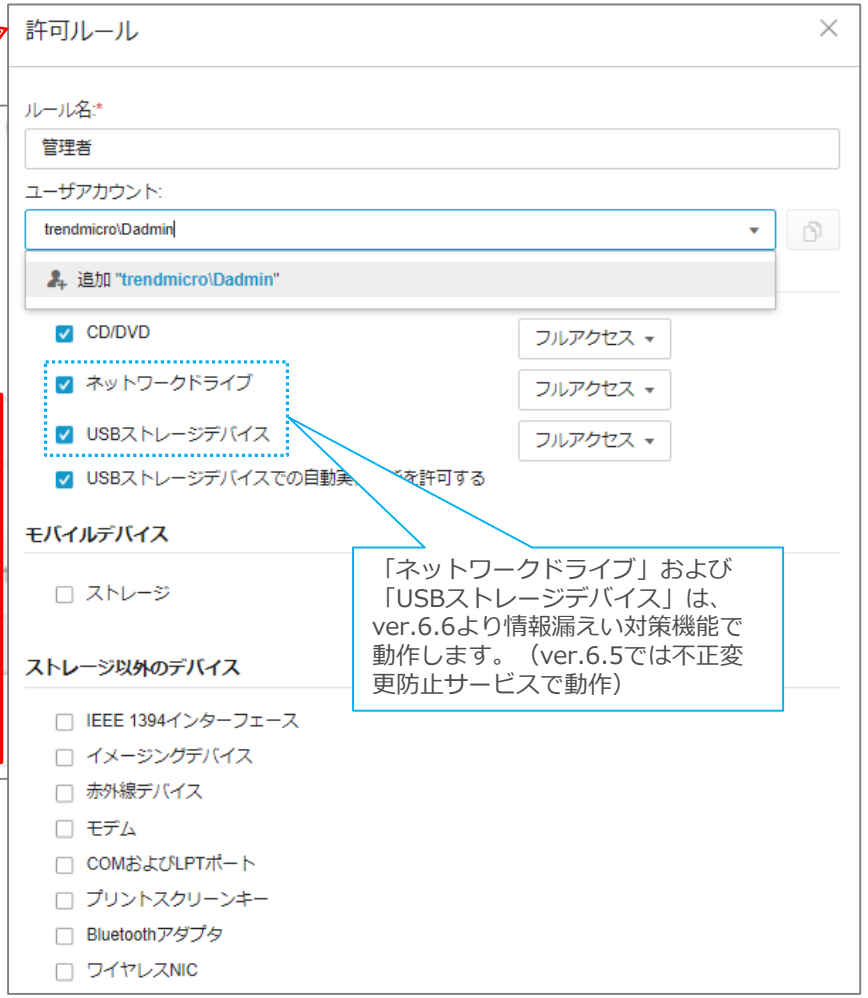
デバイスコントロール設定画面にてタブが追加され、
「除外設定」タブにてユーザごとのデバイス制御設定が可能になりました。

※Windowsログオンユーザが対象

New!



1ポリシーに設定可能なルールの数：最大20
1ルールに設定可能なユーザアカウント数：最大50



「ネットワークドライブ」および「USBストレージデバイス」は、ver.6.6より情報漏えい対策機能で動作します。（ver.6.5では不正変更防止サービスで動作）

「エンドポイントの設定」タブにてデバイス制御設定を行います。設定した制御ポリシーから除外したいユーザがいる場合は、「除外設定」タブにて対象ユーザとそのユーザに対するデバイス制御設定を行います。

デバイスコントロール機能の強化

DAIWABO INFORMATION SYSTEM CO., LTD.

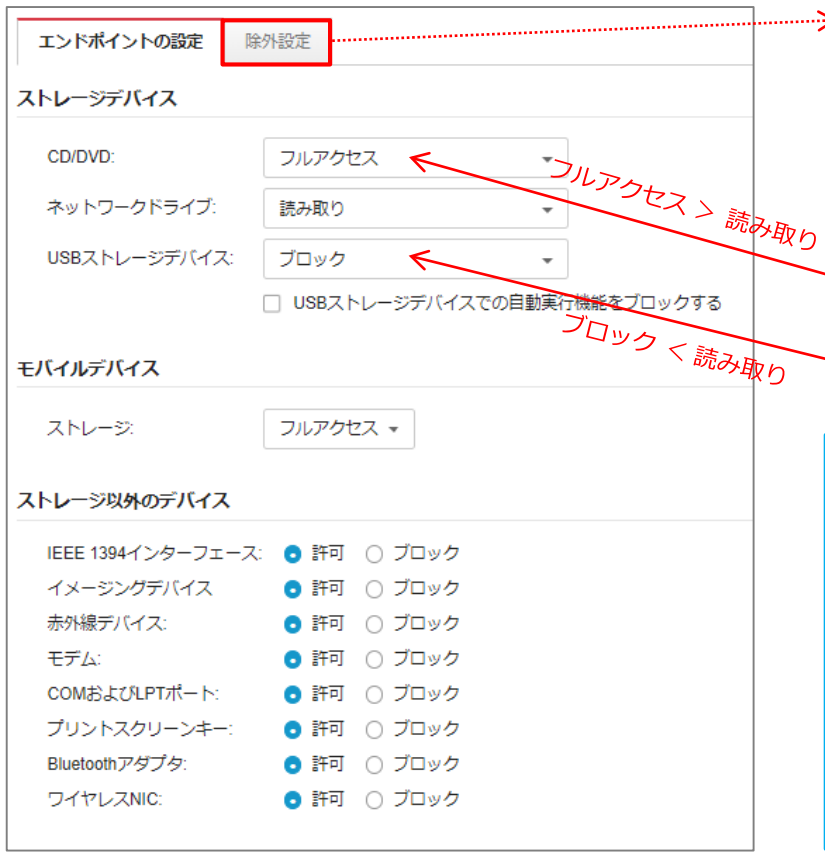
ポイント

Windows

・「除外設定」タブのデバイスコントロール権限が、「エンドポイントの設定」タブのデバイスコントロール権限よりも上位の場合に「除外設定」で設定した権限が有効になります。

・同じ端末に複数ユーザがログオン中の場合は、最後にログオンしたユーザのポリシーが全ログオンユーザに適用されます。

設定例）



フルアクセス ＞ 読み取り

ブロック ＜ 読み取り

設定がない箇所は「エンドポイント設定」の設定が引き継がれます

例のように設定した場合の動作は下記です

Windowsログオンユーザがuser_accountの場合
CD/DVD：フルアクセス
USBストレージデバイス：読み取り

Windowsログオンユーザがuser_account以外の場合
CD/DVD：フルアクセス
USBストレージデバイス：ブロック

設定可能なデバイスコントロールの権限

上位　フルアクセス
↑　変更
読み取りと実行
読み取り
下位　デバイスの内容のみリスト表示 ※ネットワークドライブは対象外

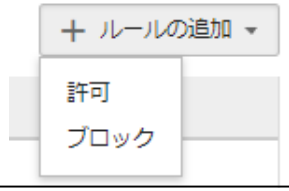
アプリケーションコントロール機能の強化

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

許可するアプリケーション(ホワイトリスト)に対応

Ver.6.5ではブロックするアプリケーションの登録のみでしたが、
Ver.6.6では許可するアプリケーションの登録も可能になりました。



ルールベースのポリシー設定

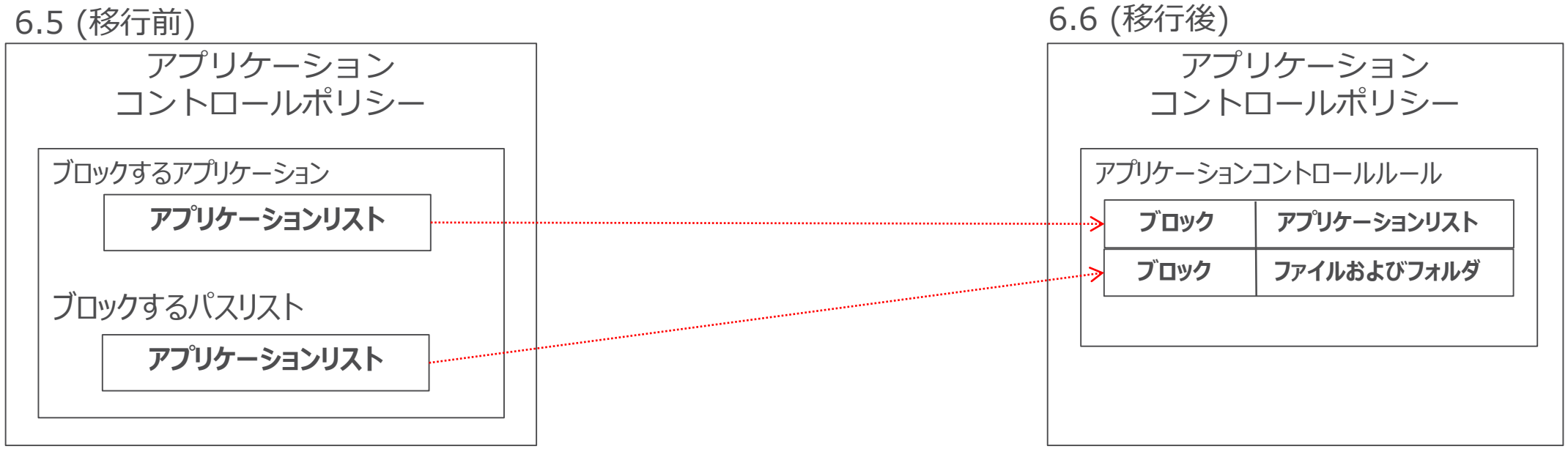
「アプリケーションコントロールルール」として許可/ブロックルールをまとめました。
複数のポリシーで同じような制御設定をする場合、1度ルールを作成すれば、複数のポリシーで同じルールを割り当てることができます。

※許可ルールはブロックルールより優先されます

参考）アプリケーションコントロールルールの移行

DAIWABO INFORMATION SYSTEM CO., LTD.

ver.6.5で設定済みのアプリケーションコントロール設定は、アプリケーションコントロールルールに移行されます。



移行後のルールの名前について

・ブロックするアプリケーション ： Blocked applications_%グループ名%
・ブロックするパスリスト： Blocked paths_%グループ名%
※異なるActive Directoryで、同じ名前のグループがある場合は、親グループ名が追加され下記の通りとなります
・ブロックするアプリケーション ： Blocked applications_%グループ名%(%親グループ名%)
・ブロックするパスリスト： Blocked paths_%グループ名%(%親グループ名%)

アプリケーションコントロール機能の強化

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

ロックダウンモードの追加

ロックダウンモードが追加されました。

ロックダウンモードを適用すると、インストールされているアプリケーションの一覧が確認されます。（インベントリ検索）以降、インベントリ検索で確認していないアプリケーションをすべてブロックします。

※ロックダウンモードはインストールや変更が禁止されているような環境可でのご利用を想定しています。

※アプリケーションコントロールは規定値無効です。有効にした場合、規定値はブロックモードです。

アプリケーションの指定方法追加

設定可能なアプリケーション照合方法が追加されました。

- ファイル/フォルダのパス
- ソフトウェア安全性評価リスト

New! ・ファイルハッシュ値(SHA-256)　※手動入力またはファイルのインポート

New! ・グレーソフトウェアリスト　※トレンドマイクロが保持するソフトウェア安全性評価リストから選択

バージョンアッププログラムの配信設定

DAIWABO INFORMATION SYSTEM CO., LTD.

バージョンアップの際、エージェントへのプログラムの配信を延期する設定項目が追加されました。

Windows

【アップグレードの延期】 ： メジャーアップグレードに関する設定
（ver.6.6→ver.6.7など）
・規定値有効 30日
・リリース日の翌日から数えて設定した日数を経過するとアップデートプログラムが配信されます
例）リリース日2019/1/1で、延期日数[30]の場合、2019/2/1から配信

【HotFixを適用しない】 ：マイナーアップグレードに関する設定
（ver.6.6.1001 →　ver.6.6.1002など）
・規定値無効

		アップグレートの延期		
		無効	有効[規定値(30)] （現在 ＞ リリース日＋設定した日数）	有効[規定値(30)] （現在 ＜ リリース日＋設定した日数）
HotFixを適用しない	無効 [規定値]	○メジャーアップグレード ○マイナーアップグレード	○メジャーアップグレード ○マイナーアップグレード	×メジャーアップグレード ○マイナーアップグレード
	有効	○メジャーアップグレード ×マイナーアップグレード	○メジャーアップグレード ×マイナーアップグレード	×メジャーアップグレード ×マイナーアップグレード

Mac OSへの機能強化

DAIWABO INFORMATION SYSTEM CO., LTD.

スマートスキャン対応

Mac

スマートスキャンに対応しました。(規定値有効)

※ver.6.5でMacをご利用の場合、ver.6.6にアップデート後、規定値としてスマートスキャンが適用されます

手動検索時間の短縮化機能追加

手動検索設定にて、「Mach-Oファイルのみ」を検索できるようになりました。

「Mach-Oファイルのみ」を選択することで検索時間が短縮されます。

※「検索方法」がスマートスキャンの場合のみ有効です

機械学習型検索対応

機械学習型検索による未知のセキュリティリスク検出に対応しました。(規定値有効)

Mac OSへの機能強化

DAIWABO INFORMATION SYSTEM CO., LTD.

Mac

デバイスコントロール機能の追加

デバイスコントロール機能が追加されました。「エンドポイントの設定」タブにて各デバイスへの権限を設定します。

「除外設定」タブでは、グローバル除外リストに登録されているUSBデバイスへの権限設定が可能です。
（「エンドポイントの設定」タブでUSBデバイスが [ブロック] または [読み取り]の場合に適用されます）

設定可能なデバイスコントロールの権限

上位
↑
フルアクセス
読み取り　※ネットワークドライブは対象外
ブロック
下位

Mac OSへの機能強化

DAIWABO INFORMATION SYSTEM CO., LTD.

Mac

スマートフィードバック対応

Macエージェントがスマートフィードバック機能に対応しました。
※ver.6.5の設定が、ver.6.6よりMacエージェントにも適用されます

3.管理コンソールのＵＩ改修

感染経路の可視化

DAIWABO INFORMATION SYSTEM CO., LTD.

「ログ」画面に、セキュリティイベントが検出されるまでの簡易的な経路の確認画面が追加されました。

Windows

感染経路が確認可能な脅威ログのカテゴリ

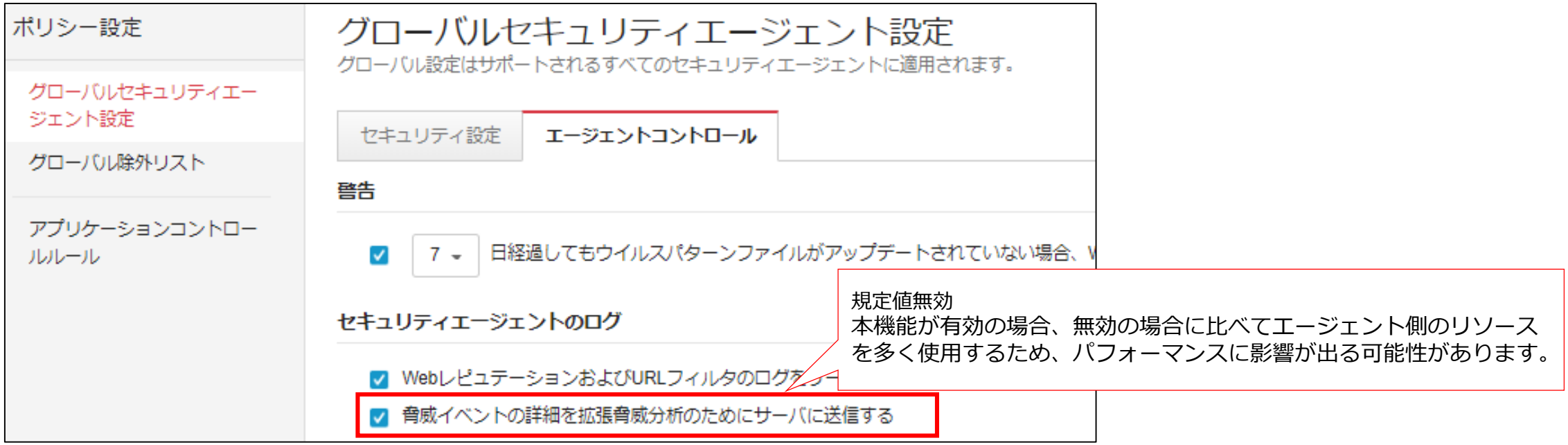
- ウイルス/不正プログラム対策
- Webレピュテーション
- 挙動監視
- 機械学習型検索

感染経路の可視化

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

下記を設定することで有効になります。
「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
[脅威イベントの詳細を拡張脅威分析のためにサーバに送信する]：有効



設定が有効になった以降の検出ログが対象です。有効にする前のログに関する感染経路は確認できません。

参考）感染経路の可視化　脅威カテゴリ別画面サンプル

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

ウイルス/不正プログラム対策

Enhanced Threat Analysis

Eicar_test_1
Dec 25, 2018 14:24:16

Endpoint
joe_tsai-PC
IP: 172.16.5.233
Last user: joe_tsai

Infection Channel
Email
outlook.exe

Detection
eicar.txt

Webレピュテーション

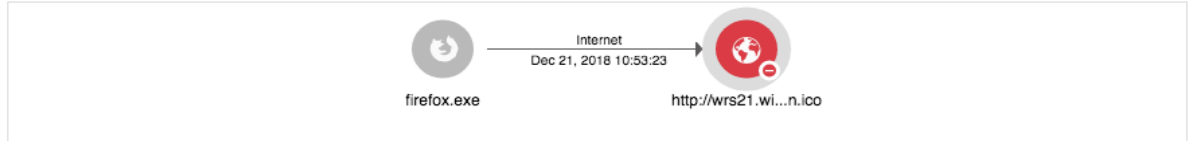
Enhanced Threat Analysis

http://wrs21.winshipway.com/favicon.ico
Dec 21, 2018 10:53:00

Endpoint
DESKTOP-K1S0MCP
IP: 192.168.181.159
Last user: kitto_hong

Infection Channel
Web
firefox.exe

Detection
http://wrs21.winshipway.co…



挙動監視

Enhanced Threat Analysis

Newly encountered program
Dec 7, 2018 14:21:28

Endpoint
VCAC-Window-210
IP: 10.201.172.26
Last user: Administrator

Infection Channel
Web
chrome.exe

Detection
rcltest-57.exe

機械学習型検索

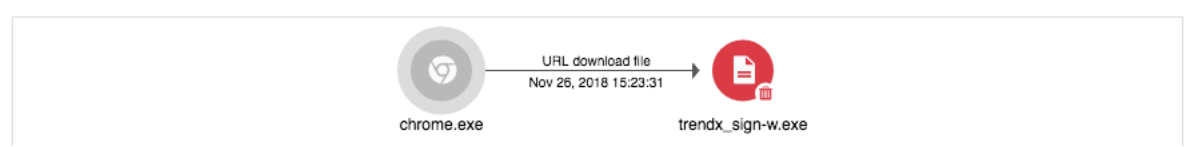
Enhanced Threat Analysis

Ransom.Win32.TRX.XXPE1
Nov 26, 2018 15:23:32

Endpoint
IP: 192.168.175.141
Last user: Kenmin Lin (RD-TW)

Infection Channel
Web
chrome.exe

Detection
trendx_sign-w.exe



検索除外リストの追加方法の改善

DAIWABO INFORMATION SYSTEM CO., LTD.

「ログ」画面から、ファイルやフォルダを検索除外リストに追加できるようになりました。

Windows
Mac

※Windows Server OSは対象外(Windows クライアントOSは対象)

※「ログ」画面の「エンドポイント」欄が“削除されたクライアント”の場合は対象外

※脅威の種類はファイル

クリックすると表示

対象のログのカテゴリ

- ウイルス/不正プログラム対策
- 挙動監視
- スパイウェア/グレーウェア

その他のUI改修

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows
Mac

未評価のURLに対する設定項目の切り出し

「ポリシーの設定」-「webレピュテーション」にて、未評価URLに対する設定が高/中/低のセキュリティレベルから独立しました。

6.5

6.6

その他のUI改修

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

Site Safety Centerへのリンク追加　※Windowsのみ

「ポリシーの設定」-「URLフィルタ」画面に、トレンドマイクロ Site Safety CenterへのURLリンクが追加されました。

※ Site Safety Center：トレンドマイクロが公開しているwebサイト安全性確認サイト

ダッシュボードからのアグレッシブスキャン　※Windowsのみ

ダッシュボードのアクションセンター「解決されていない脅威」画面に、対象エージェントへのアグレッシブスキャン実行ボタンが追加されました。

※アグレッシブスキャンの動作自体は「セキュリティエージェント」タブから実行するものと同じです

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(Windows)

DAIWABO INFORMATION SYSTEM CO., LTD.

Windows

Windows OS　：　Windows Server 2019サポート開始

OS	6.6からサポートされるバージョン	6.6ではサポートされなくなるバージョン	備考
Windows	Windows Server 2019	―	

※現在6.3でサポートされている下記は、6.6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。OSサービスパックの適用などをご検討ください。

- Windows 7 Ultimate/Enterprise/Professional/Home/Premium/Home Basic SPなし
- Windows Server 2008 Foundation/Standard/Enterprise/Datacenter SP1
- Windows Server 2008 R2 Foundation/Standard/Enterprise/Datacenter SPなし
- Windows SBS 2008 Standard/Premium SP1
- Windows EBS 2008 Standard/Premium SP1
- Windows Storage Server 2008 Workgroup/Standard/Enterprise SPなし/SP1
- Windows Storage Server 2008 R2 Workgroup/Standard/Enterprise SPなし
- Windows SBS 2011 Standard SPなし

サポート開始OSとサポート終了OS(Android・iOS)

DAIWABO INFORMATION SYSTEM CO., LTD.

Android
iOS

Android OS　：　9.0サポート開始、4.4.xサポート終了
iOS　：　12.0サポート開始、7.xサポート終了

OS	6.6からサポートされるバージョン	6.6ではサポートされなくなるバージョン	備考
Android	9.0	4.4.X	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。
iOS	12.0	7.X	

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