

# 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

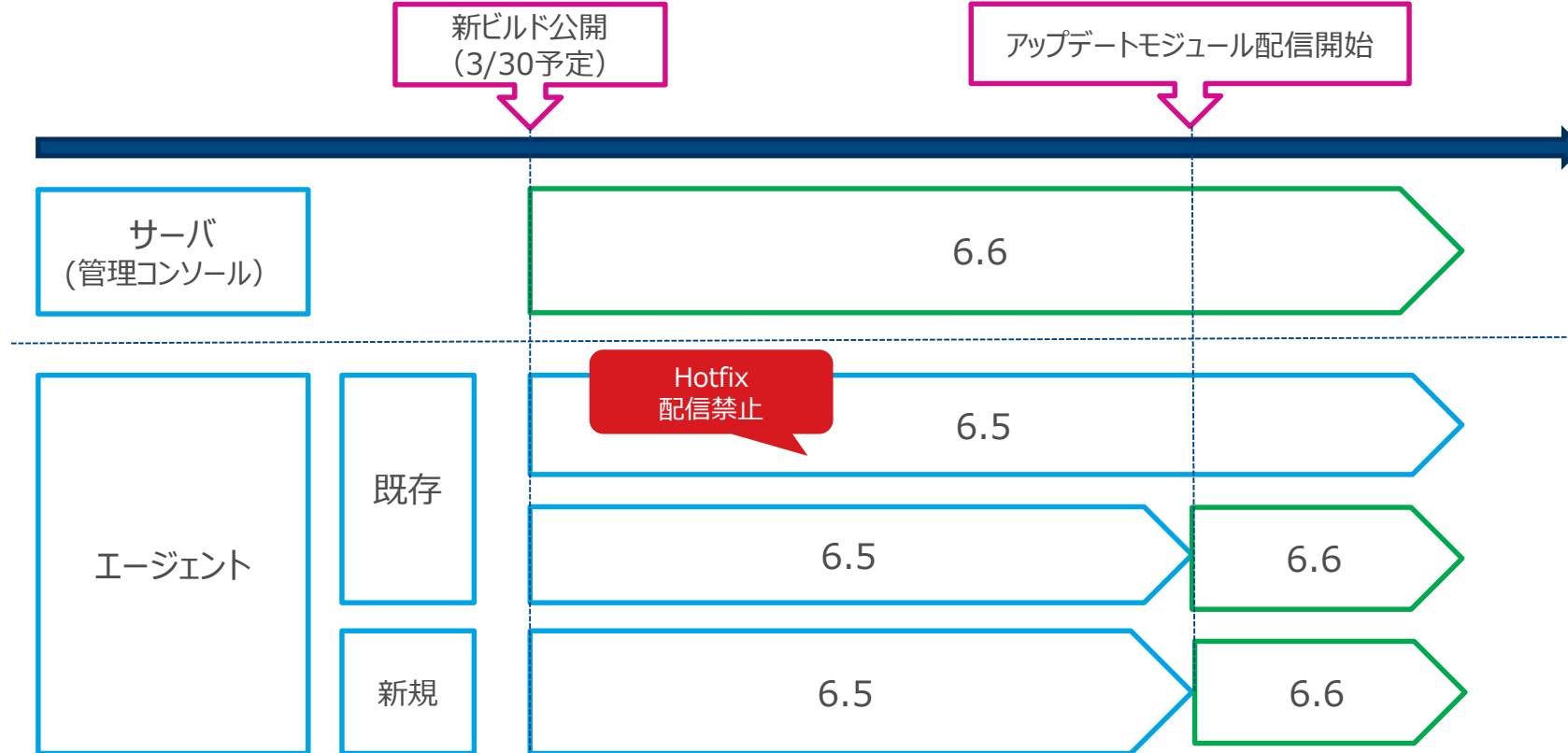
- 感染経路の可視化
- 検索除外リストの登録方法追加
- その他のUI改修

## 4. システム要件の変更

# 1.はじめに

## 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

| 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<br>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<br>Mac |

## 2.セキュリティ対策機能の強化

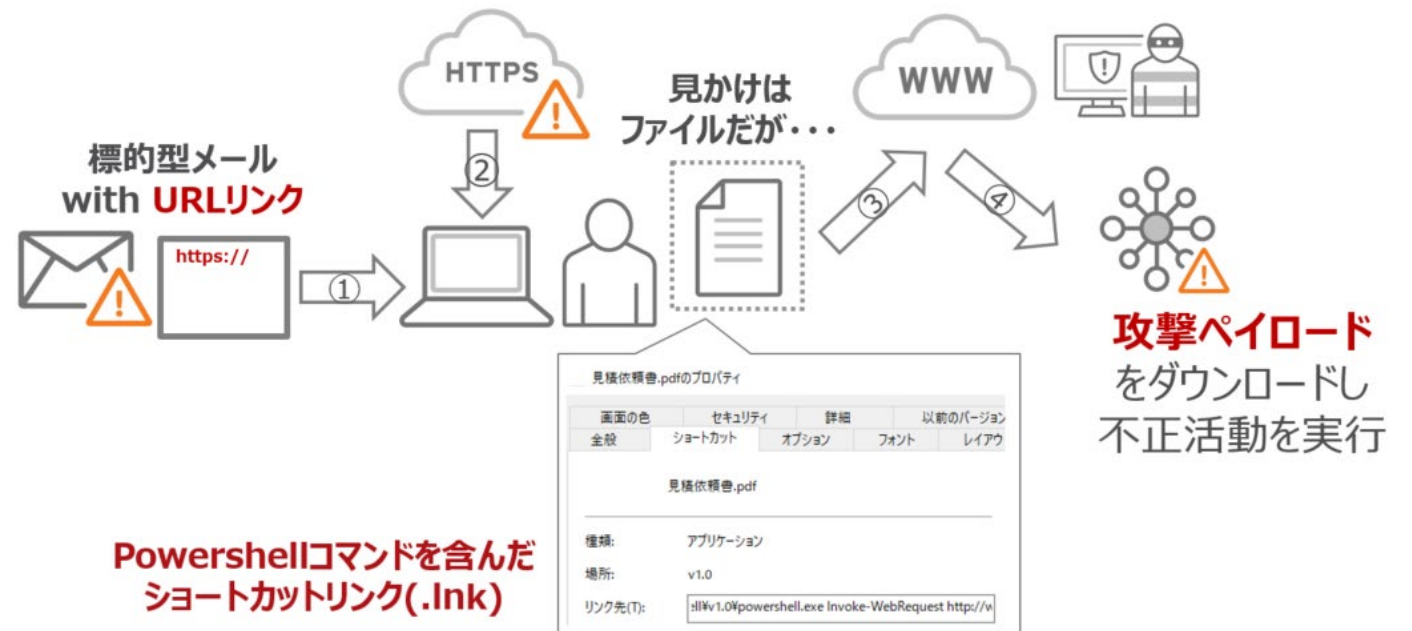
メモリスキャンの機能向上により、ハードディスクに保存されないメモリ上にのみ存在するマルウェアを検出できるようになりました。

- ・ 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。



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)

ポリシーの設定: Group01

### 対象とサービスの設定



### 脅威からの保護機能

- 検索設定
- 挙動監視
- 機械学習型検索

## 機械学習型検索

トレンドマイクロの機械学習型検索は、出します。



注意:

- 機械学習型検索を使用するには、尋
- インターネット接続を利用できない

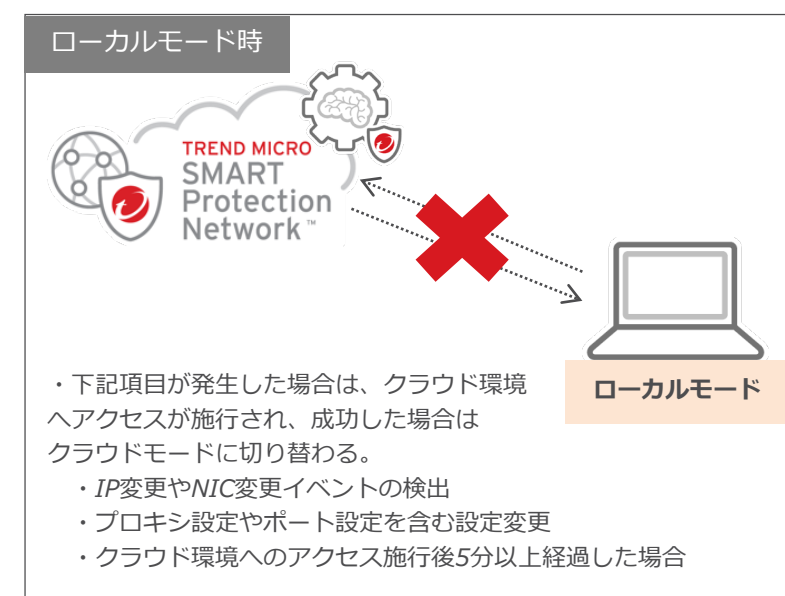
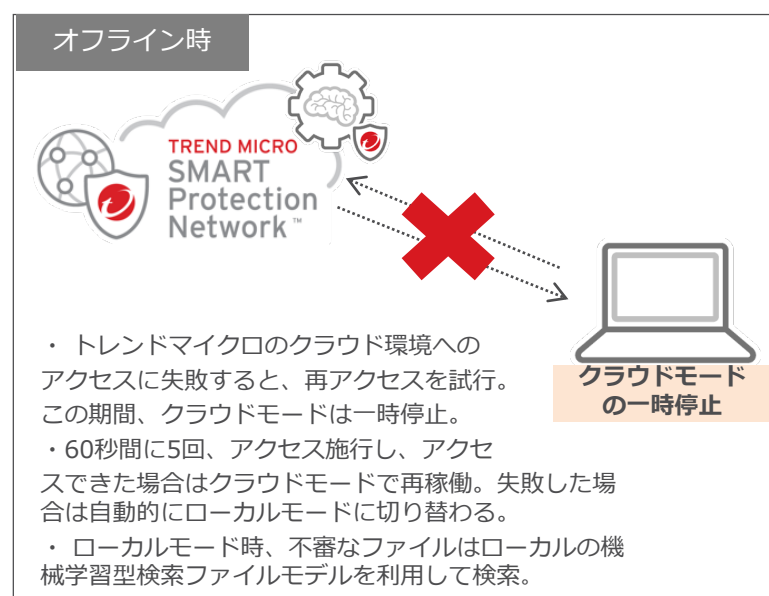
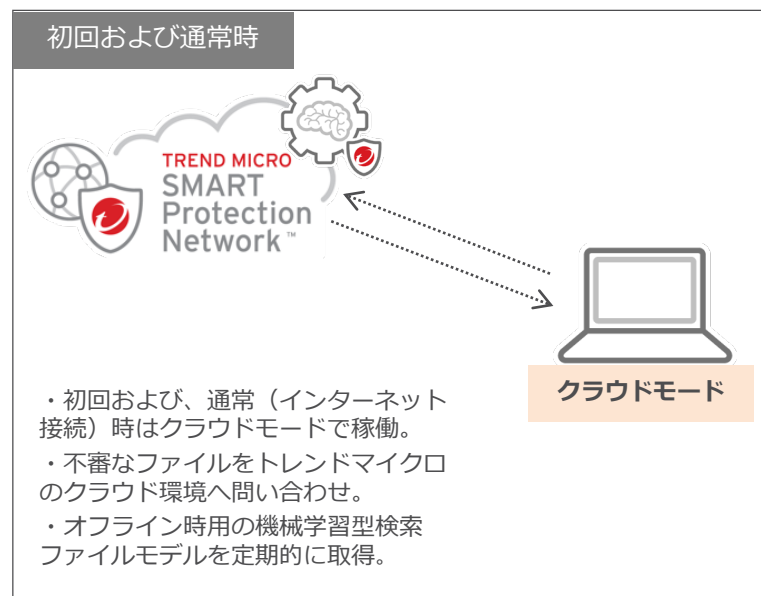


# オフライン時の機械学習型検索対応

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ーを使用)

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)



※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

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ログインユーザが対象

デバイスコントロール  
デバイスコントロールは、周辺デバイスへのアクセスを制御します。

オン

New! エンドポイントの設定 **除外設定**

ユーザ

指定したユーザに制限されたデバイスへのアクセスを許可する。

+ 許可ルールの追加

| ルール                                | ユーザアカウント     | 許可されたデバイス                              |
|------------------------------------|--------------|--|
| <input type="checkbox"/> デバイスマネージャ | user_account | CD/DVD, ネットワークドライブ, USBストレージデバイス, 自動実行 |

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

許可ルール

ルール名:\*  
管理者

ユーザアカウント:  
trendmicro\Dadmin

追加 "trendmicro\Dadmin"

CD/DVD

ネットワークドライブ

USBストレージデバイス

USBストレージデバイスでの自動実行を許可する

モバイルデバイス

ストレージ

ストレージ以外のデバイス

- IEEE 1394インターフェース
- イメージングデバイス
- 赤外線デバイス
- モデム
- COMおよびLPTポート
- プリントスクリーンキー
- Bluetoothアダプタ
- ワイヤレスNIC

「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

## 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)

エンドポイントの設定 **除外設定**

ストレージデバイス

CD/DVD: フルアクセス

ネットワークドライブ: 読み取り

USBストレージデバイス: ブロック

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

モバイルデバイス

ストレージ: フルアクセス

ストレージ以外のデバイス

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

COMおよびLPTポート:  許可  ブロック

プリントスクリーンキー:  許可  ブロック

Bluetoothアダプタ:  許可  ブロック

ワイヤレスNIC:  許可  ブロック

許可ルール

ルール名\*: デバイス管理者

ユーザアカウント: user\_account

ストレージデバイス

CD/DVD 読み取り

ネットワークドライブ 読み取り

USBストレージデバイス 読み取り

USBストレージデバイスでの自動実行機能を許可する

モバイルデバイス

ストレージ

ストレージ以外のデバイス

IEEE 1394インターフェース

イメージングデバイス

赤外線デバイス

モデム

COMおよびLPTポート

プリントスクリーンキー

Bluetoothアダプタ

ワイヤレスNIC

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

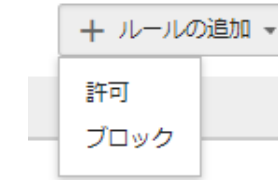
## 設定可能なデバイスコントロールの権限

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

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

## 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。

### アプリケーションコントロールルール

ルールを選択:

すべてのルール ▾

+ ルールの追加 ▾

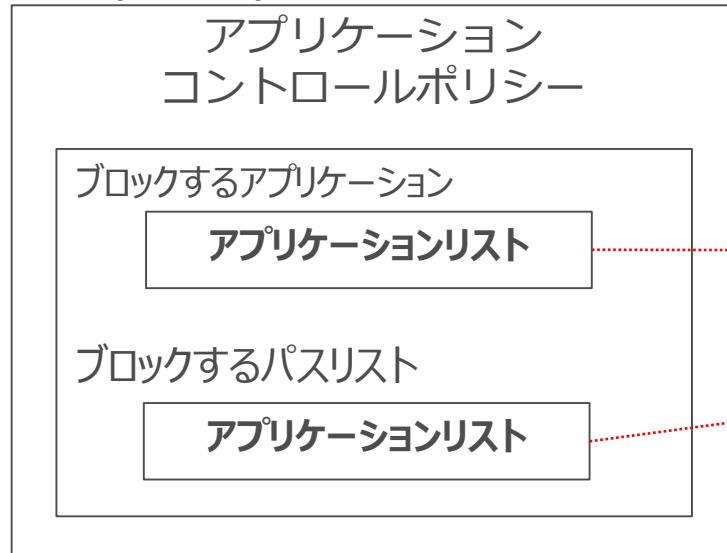
| <input type="checkbox"/>            | 種類 ↑ | ルール    | 概要                  |
|-------------------------------------|------|--------|---------------------|
| <input type="checkbox"/>            | 許可   | 許可フォルダ | ファイルまたはフォルダのパス (1)  |
| <input checked="" type="checkbox"/> | ブロック | グレーウェア | プロキシ匿名化ソフトウェア (all) |

※許可ルールはブロックルールより優先されます

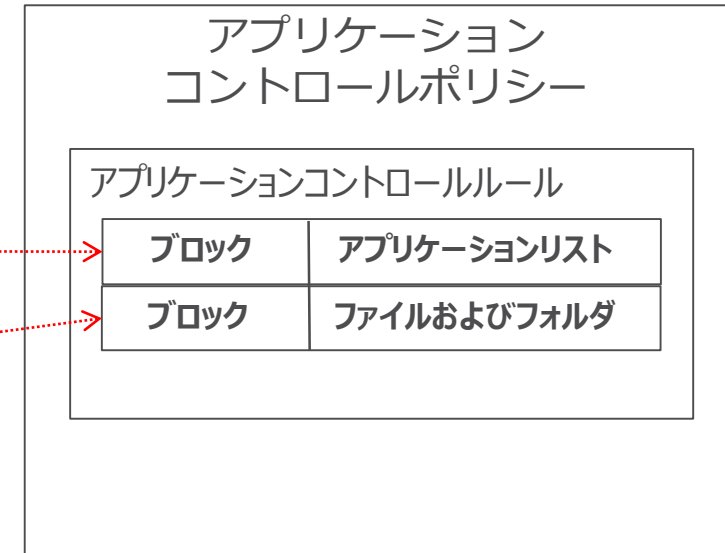
# 参考) アプリケーションコントロールルールの移行

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。

## 6.5 (移行前)



## 6.6 (移行後)



### 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%)

## 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。

## アプリケーションコントロール

エンドポイントでのアプリケーションの実行やインストールを制限するルールを作成します。

オン

規定値は[ブロック]

ブロック: 指定したアプリケーションのエンドポイントでの実行をブロック

New!

**ロックダウン: 前回のインベントリ検索で確認できなかったアプリケーションをすべてブロック** ⓘ

**!!Exclude applications by Trend Micro trusted vendors (Recommended)!!**

Microsoftの署名付きのプログラム (Windows Updateを含む) によるプロセスツリーを除外する

## 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

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

|              |          | アップグレードの延期                   |                                    |                                    |
|--------------|----------|------------------------------|------------------------------------|------------------------------------|
|              |          | 無効                           | 有効[規定値(30)]<br>(現在 > リリース日+設定した日数) | 有効[規定値(30)]<br>(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<br>○マイナーアップグレード | ○メジャーアップグレード<br>○マイナーアップグレード       | ×メジャーアップグレード<br>○マイナーアップグレード       |
|              | 有効       | ○メジャーアップグレード<br>×マイナーアップグレード | ○メジャーアップグレード<br>×マイナーアップグレード       | ×メジャーアップグレード<br>×マイナーアップグレード       |

## スマートスキャン対応

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

### 検索方法

New!

スマートスキャン

スマートスキャンは、クラウドに格納された不正プログラム対策

従来型スキャン

従来型スキャンは、セキュリティエージェントにローカルに格納

## 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

### 手動検索

Webコンソール上の[セキュリティエージェント]シ

設定

スマートスキャンは、

### 手動検索設定

#### 対象

検索するファイル:

New!

検索可能なすべてのファイル

Mach-Oファイルのみ

圧縮ファイルの検索

## 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)

### 対象とサービスの設定



脅威からの保護機能

● 検索設定

New!

● 機械学習型検索

● Web上でのコンピューティング

### 機械学習型検索

トレンドマイクロの機械学習型

オン



## 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)

ポリシーの設定: Group01

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レビュテーション

情報漏えい対策

New! ● **デバイスコントロール**

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

### デバイスコントロール

デバイスコントロールは、周辺デバイスへのアクセスを制御します。

オン

エンドポイントの設定

**除外設定**

ストレージデバイス

- CD/DVD: フルアクセス
- ネットワークドライブ: フルアクセス
- USBストレージデバイス: フルアクセス
- Thunderboltストレージデバイス: フルアクセス
- !!Secure Digital (SD) cards:!!
  - フルアクセス
  - 読み取り
  - ブロック

エンドポイントの設定

**除外設定**

!!USB Devices!!

許可されたUSBデバイスのリスト (グローバル設定) の権限を指定します。  
または [読み取り] を選択した場合に運用されます。

フルアクセス

フルアクセス  
読み取り

### 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

ブロック

下位

※ネットワークドライブは対象外

## 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



管理

一般設定

モバイルデバイス登録設定

通知

Active Directoryの設定

Smart Protection Network

回復キーのパスワード

### Smart Protection Network



TREND MICRO  
SMART  
PROTECTION  
NETWORK

Trend Micro™ Smart Protection Network™は、脅威インテリジェンスセンサのグローバルなネットワークおよびファイルレピュテーションデータベースを継続的にアップデートして、脅威が発生するセキュリティはより高度になります。 [詳細情報](#)

スマートフィードバックを有効にすると、コンピュータで検出された脅威に関する情報（アクセスされたWebアドレス、新たな脅威の迅速な識別や対処に役立てられます。お客さまから収集された情報の取り扱いについての詳細は、<http://jp.trendmicro.com>

**トレンドマイクロスマートフィードバックを有効にする (推奨)**。この機能は、本製品のコンソールでいつでも停止できません。

業種 (任意):  ⓘ

**不審なプログラムファイルのフィードバックを有効にする** ⓘ

# 3.管理コンソールのU I改修

「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。

The screenshot shows the 'ログ' (Log) interface with a table of security events. A red box highlights a 'New!' icon in the '詳細' (Details) column of the first row. A red arrow points to a pop-up window titled '拡張脅威分析' (Advanced Threat Analysis) which displays the infection path for the selected event.

| 日時↓                 | 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01月30日 17:3... | 機械学習型検索       | Ransom.Win32.TRX... | c:\users\yoko\downb...  | 隔離    | DESKTOP-HHK490J | yoko_ |    |
| 2019年01月30日 17:3... | ウイルス/不正プログ... | Ransom.Win32.TRX... | c:\users\yoko\downb...  | 駆除    | DESKTOP-HHK490J | yoko_ |    |
| 2019年01月30日 17:3... | ウイルス/不正プログ... | Ransom.Win32.TRX... | c:\users\yoko\appdat... | 駆除    | DESKTOP-HHK490J | yoko_ |    |

**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

**拡張脅威分析**

Ransom.Win32.TRX.XXPE1  
2019年01月30日 17:38:38

**エンドポイント**  
DESKTOP-HHK490J  
IP: 192.168.126.13  
最後のユーザ: yoko\_

**感染経路**  
Web  
microsoftedgecp.exe

**検出した脅威**  
trendx\_sign-a.exe

microsoftedgecp.exe → https://doc-0c-...nload → trendx\_sign-a.exe

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



ポリシー設定

- 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
- アプリケーションコントロールルール

### グローバルセキュリティエージェント設定

グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定    エージェントコントロール

警告

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、V

### セキュリティエージェントのログ

- WebレピュテーションおよびURLフィルタのログを...
- 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

規定値無効  
本機能が有効の場合、無効の場合に比べてエージェント側のリソースを多く使用するため、パフォーマンスに影響が出る可能性があります。

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

## 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

Windows

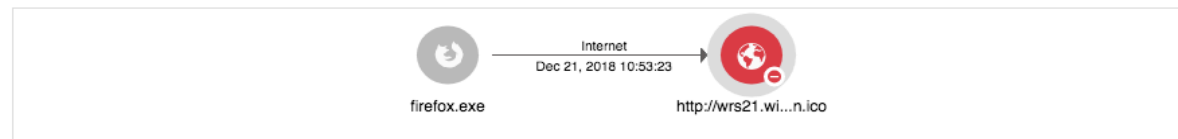
Enhanced Threat Analysis

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**  
rcitest-57.exe



## 機械学習型検索

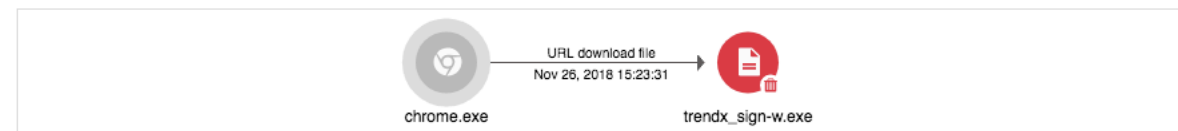
Enhanced Threat Analysis

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

「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 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

Windows

Mac

| 日時 ↓                | 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01月30日 17:3... | 機械学習型検索       | Ransom.Win32.TRX... | c:\users\yoko_\downlo... | 隔離    | DESKTOP-HHK490J | yoko_ | [詳細] |
| 2019年01月30日 17:3... | ウイルス/不正プログ... | Ransom.Win32.TRX... | c:\users\yoko_\downlo... | 駆除    | DESKTOP-HHK490J | yoko_ | [詳細] |
| 2019年01月30日 17:3... | ウイルス/不正プログ... | Ransom.Win32.TRX... | c:\users\yoko_\appdat... | 駆除    | DESKTOP-HHK490J | yoko_ | [詳細] |

クリックすると表示

ウイルス/不正プログラムログの詳細

脅威名: Ransom.Win32.TRX.XXPE1

生成日時: 2019年01月30日 17:38:46

受信日時: 2019年01月30日 17:39:07

エンドポイント

エンドポイント名: DESKTOP-HHK490J

ドメイン: -

ユーザ: yoko\_

グループ名: ベータグループ

**New!** 検索除外リストに追加

検索除外リストに追加

パス:

ファイル  フォルダ

c:\users\yoko\_\downloads\trendx\_sign-a.exe

追加先:

ベータグループ

すべてのグループ

検索の種類:

リアルタイム検索  予約検索  手動検索

追加 キャンセル

## 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

## 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

#### Webレピュテーション

Webレピ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。

オン

#### セキュリティレベル

|   | 危険 | 極めて不審 | 不審 | 未評価 |
|---|----|-------|----|-----|
| <input type="radio"/> 高                   | ✓  | ✓     | ✓  | ✓   |
| <input checked="" type="radio"/> 中 (初期設定) | ✓  | ✓     |    |     |
| <input type="radio"/> 低                   | ✓  |       |    |     |

✓ Webサイトのアクセスをブロックします ⓘ

### 6.6

#### Webレピュテーション

Webレピ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。

オン

#### セキュリティレベル

|   | 危険 | 極めて不審 | 不審 |
|---|----|-------|----|
| <input type="radio"/> 高                   | ⊗  | ⊗     | ⊗  |
| <input checked="" type="radio"/> 中 (初期設定) | ⊗  | ⊗     |    |
| <input type="radio"/> 低                   | ⊗  |       |    |

Webサイトのアクセスをブロックします ⓘ

#### 未評価のURL

トレンドマイクロによる評価が完了していないWebサイトをブロックする ⓘ

規定値無効

New!



## 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)

## Windows OS : Windows Server 2019サポート開始

Windows

| 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)

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