

- バージョン6.6における変更点について

1. システム要件の変更
2. 感染経路の可視化
3. Mac OSへの機能強化（スマートスキャン、機械学習型検索など）
4. デバイスコントロール機能の強化
5. ファイルレス攻撃対応
6. バージョン6.6配信のタイミング

1. システム要件の変更

- サポート開始

- Windows Server 2019
- Android OS 9.0
- iOS 12.0

- サポート終了

- Windows

ver6.3でサポートされている下記OSは、ver6.6リリース以降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確認ください。

- 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
- Android OS 4.4.x
- iOS 7

サポートされていないクライアントを確認する方法

- サポート対象外のクライアントが存在する場合、管理者画面上に「サポートされていないオペレーティングシステム」フィルタが追加され、該当の端末を確認することが出来ます。



The screenshot shows a management interface with a sidebar on the left and a main content area on the right. The sidebar contains a search icon and a list of filters, with the last one, 'サポートされていないオペレー...', selected and showing a count of 1. The main content area has a title 'サポートされていないオペレーティングシステム' and a subtitle 'サポートされていないオペレーティングシステムを実行しているビジネスセキュリティクライアントは、最新バージョンにアップグレードできません: 1'. Below this is an 'エクスポート' button and a table with columns for 'エンドポイント', 'オペレーティングシステム', 'クライアントのバージョン', and 'IPv4アドレス'. One row is visible with the endpoint 'Client01-Win7', OS 'Win 7', version '6.3.1297/13.1.2079', and IP address '172.16.5.112'.

エンドポイント	オペレーティングシステム	クライアントのバージョン	IPv4アドレス
Client01-Win7	Win 7	6.3.1297/13.1.2079	172.16.5.112

2. 感染経路の可視化

- 「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。

- 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

The image shows a Windows Security interface. The top part is the 'ログ' (Logs) window, displaying a table of security events. The bottom part is the '拡張脅威分析' (Expanded Threat Analysis) window, which provides a detailed view of a specific threat, including its endpoint, infection path, and detected threat.

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_	New! [Icons]
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_	[Icons]
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_	[Icons]

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 (microsoftedge.exe)
- 検出した脅威: trendx_sign-a.exe

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

microsoftedge.exe → https://doc-0c-...nload → trendx_sign-a.exe

3. Mac OSへの機能強化

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)

※ver6.5でMacをご利用の場合、ver6.6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)



3. Mac OSへの機能強化

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

🍏 macOS

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

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

4. デバイスコントロール機能の強化

- 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!

The screenshot shows the Windows Device Control settings window. The 'Exclusion Settings' tab is selected. A red box highlights the 'Add permission rule' button and a table of existing rules. A callout box provides limits: 1 policy can have up to 20 rules, and 1 rule can have up to 50 user accounts. A red dashed arrow points from the 'Add permission rule' button to a detailed view of a rule.

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

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します。

+ 許可ルールの追加 削除

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:
trendmicroDadmin

追加 "trendmicroDadmin"

- 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
- 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

「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。

4. デバイスコントロール機能の強化

ポイント

- 「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)

The image shows two overlapping windows from the Windows Device Control settings. The background window is 'Endpoint Settings' (エンドポイントの設定) with the 'Exclude Settings' (除外設定) tab selected. It shows permissions for storage devices (CD/DVD, Network Drive, USB Storage) and mobile devices (Storage). The foreground window is 'Permissions Rules' (許可ルール) for the 'Device Administrator' (デバイス管理者) user account. It shows permissions for storage devices (CD/DVD, Network Drive, USB Storage) and mobile devices (Storage). Red arrows point from the 'Full Control' (フルアクセス) setting in the 'Exclude Settings' window to the 'Full Control' setting in the 'Permissions Rules' window. Another red arrow points from the 'Block' (ブロック) setting in the 'Exclude Settings' window to the 'Block' setting in the 'Permissions Rules' window. A blue box highlights the 'Mobile Devices' (モバイルデバイス) section in the 'Permissions Rules' window, with a callout stating that settings in this section are inherited from the 'Endpoint Settings' window. A blue box highlights the 'Permissions Rules' window title bar, with a callout stating that the actions for the settings are as follows. A blue box highlights the 'Permissions Rules' window content, with a callout stating that the permissions for the settings are as follows.

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

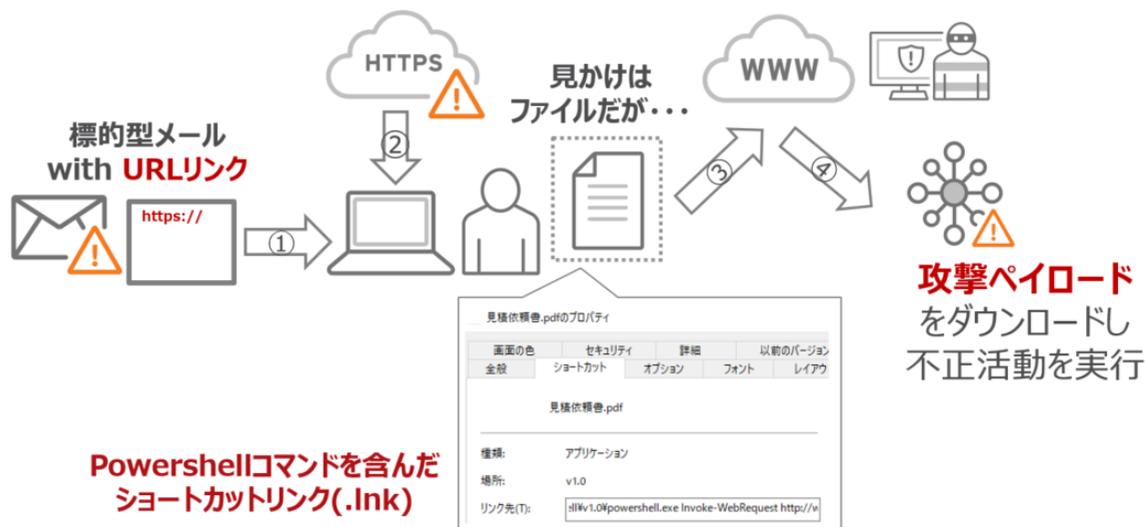
設定がない箇所は「エンドポイント設定」の設定が引き継がれます

5. ファイルレス攻撃対応

- 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で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。

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、メモリ上で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。



ファイルレス攻撃有効化するためには

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

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

機械学習型検索

5. [機械学習型検索] : オン

ポリシーの設定: Group01

The screenshot shows the Windows Group Policy settings for 'Group01'. On the left, under '対象とサービスの設定' (Target and Service Settings), the '脅威からの保護機能' (Threat Protection Features) section is expanded, and '挙動監視' (Behavior Monitoring) is selected. On the right, the '機械学習型検索' (Mechanical Learning Search) policy is shown. The toggle switch is turned 'オン' (On). Below the toggle, a '注意' (Note) section contains two bullet points: '機械学習型検索を使用するには、' (To use Mechanical Learning Search,) and 'インターネット接続を利用できない' (Internet connection cannot be used).

6. バージョン6.6配信のタイミング

- 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わります
- 新機能は、ver6.6エージェント配信開始後より使用可能です

