- 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
  - 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ションシステム」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。

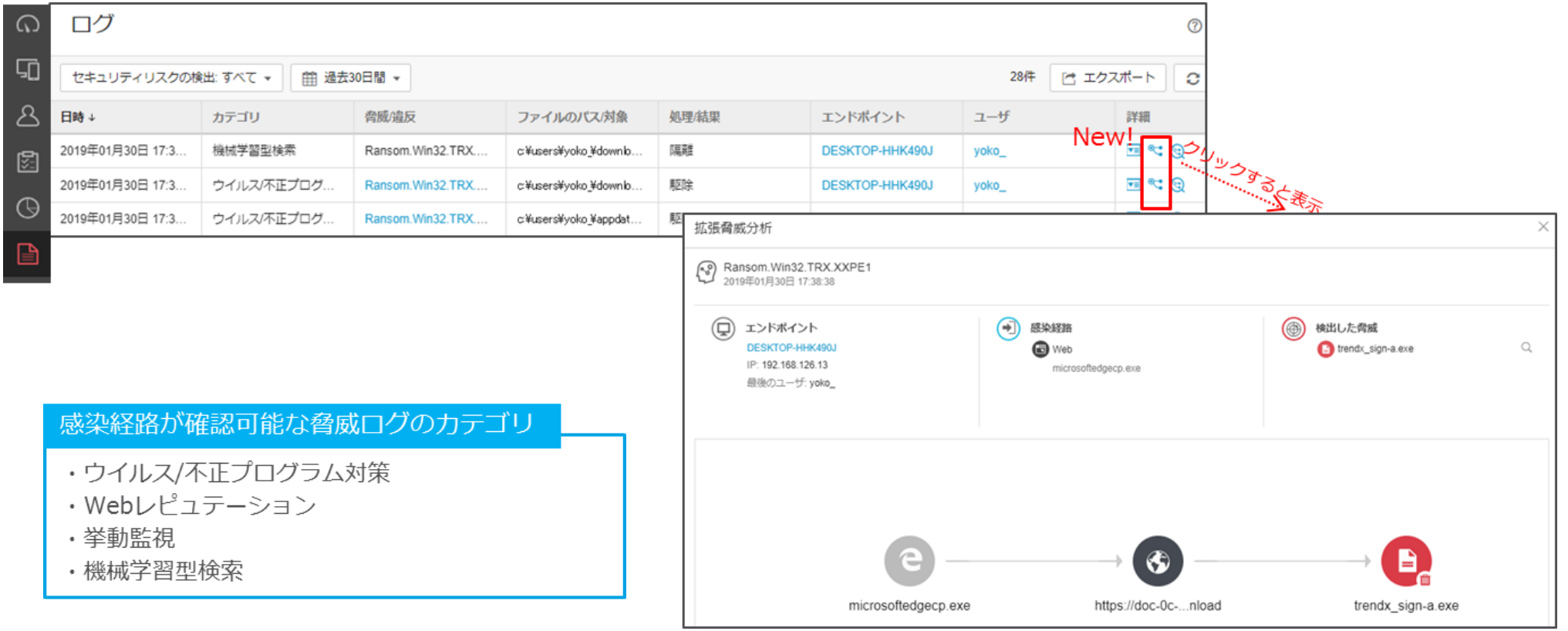
2. 感染経路の可視化

Windows

- 「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



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

大塚商会

3. Mac OSへの機能強化

Mac

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

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

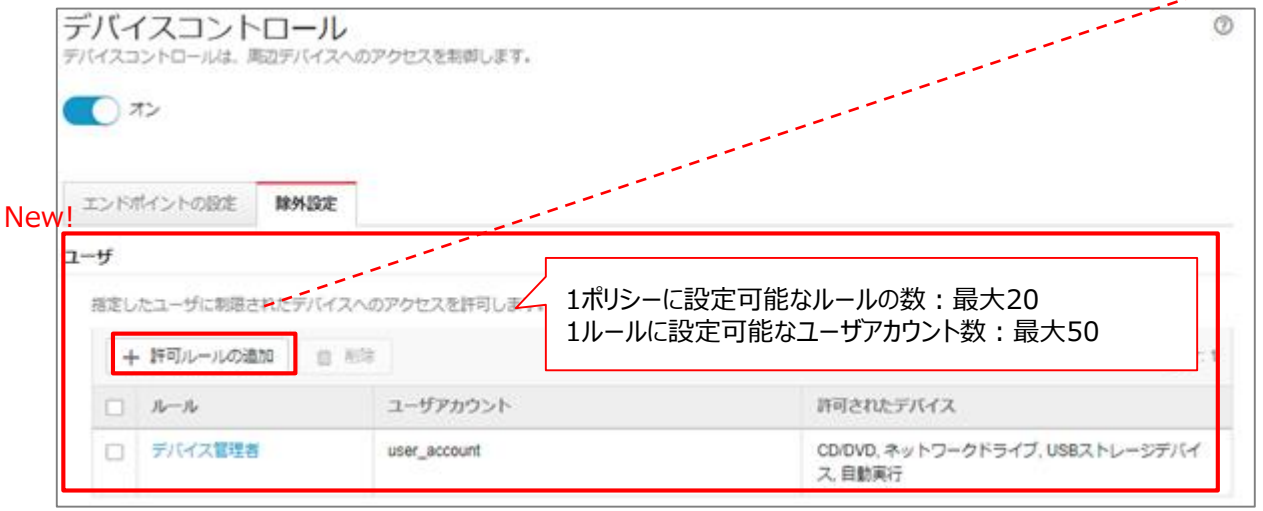
上位
↑
フルアクセス
読み取り　※ネットワークドライブは対象外
ブロック
下位

4. 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ログオンユーザが対象



「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

Windows

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）

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

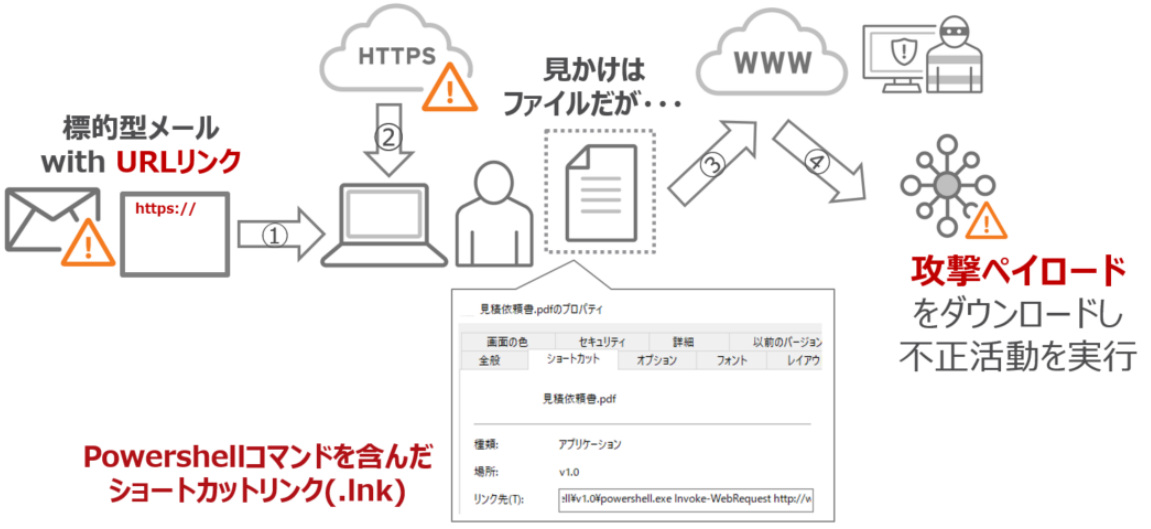
5. ファイルレス攻撃対応

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。

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。



大塚商会

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

大塚商会

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