バージョン6.3における変更点について

1. 挙動監視機能の強化
2. アグレッシブ検索機能の追加
3. プログラム配信タイミングについて

2018年1月19日

1. 挙動監視機能の強化

・挙動監視機能の強化

- 脆弱性を悪用した攻撃との疑いのある挙動を検知すると、その挙動を示すプロセスを停止します。

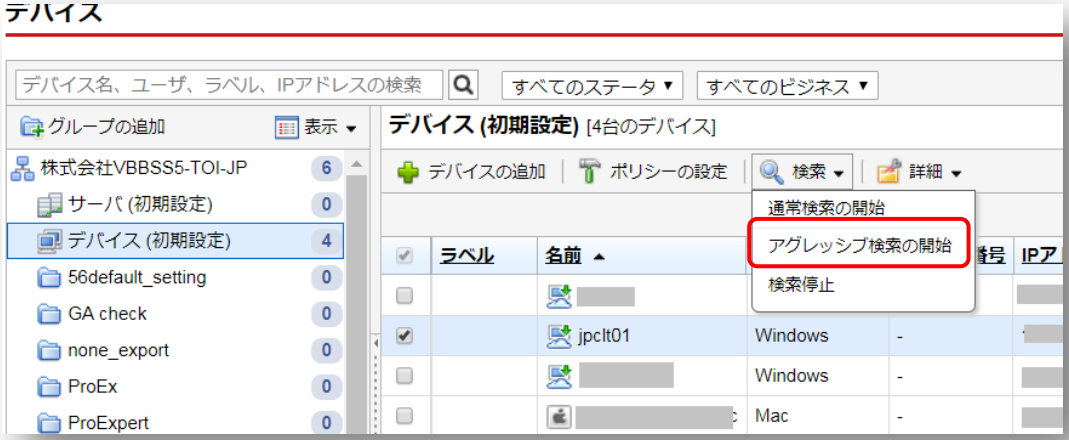
※本機能を利用するには、挙動監視機能が有効である必要があります。

プログラム検査と同じモジュール用いて検知するため、脆弱性対策を有効にすると、プログラム検査も有効になります。（初期値：無効）

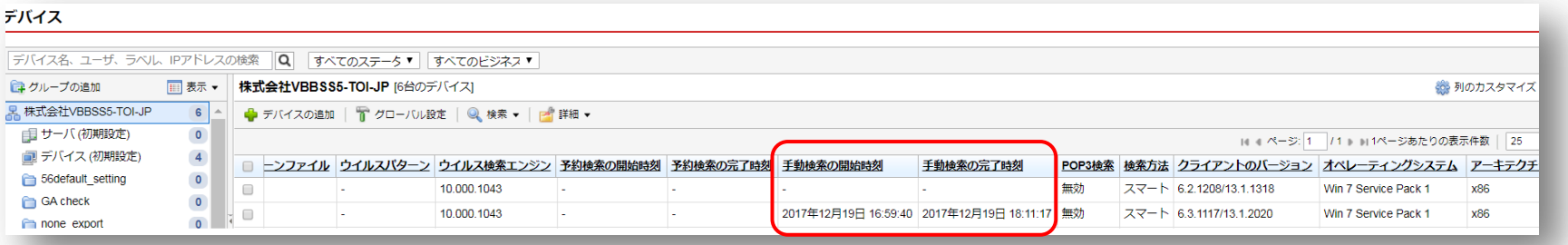
2. アグレッシブ検索機能の追加（1/2）

・アグレッシブ検索機能の追加

- 手動検索の方法として、従来の「通常検索」に加え、通常運用の中で感染が疑われる際に、より詳細な検索および感染端末のクリーンアップを行うことができる「アグレッシブ検索」が追加されます。



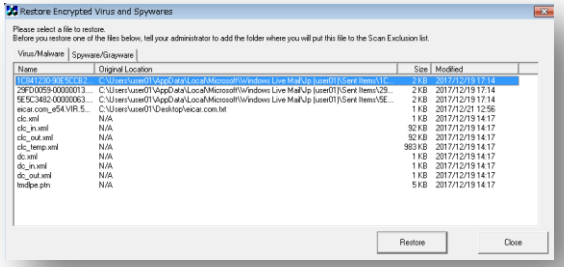
管理者画面上、実行ログは「手動検索」として表示されます。



2. アグレッシブ検索機能の追加（2/2）

- Read Onlyのメディアに対しては、アグレッシブ検索においても削除処理ができません。
  (クライアント側のログ上、結果は[処理が必要]になります。)

- 検索により見つけた脅威は削除されますが、下記フォルダにバックアップされます。また指定のプログラムを用いてリストアが可能です。
  - バックアップ先：<インストールディレクトリ>¥Client Server Security Agent¥Suspect ¥Backup folder
  - バックアップファイルリストアのためのプログラム：<インストールディレクトリ>¥Client Server Security Agent¥VSE¥VSEncode.exe



※通常のスキャンで駆除されたファイルも含まれます。
事前にファイルの安全性や除外設定など運用上問題がないことをご確認の上リストアを行ってください。

- 管理者画面から端末/グループを指定していつでもアグレッシブスキャンの実行が可能ですが、端末リソースへの負荷や過検出の観点から、疑わしい端末の検索を実施する場合のみ利用することを推奨します。

3. プログラム配信タイミングについて

- 管理者画面については、2018年1月27日のメンテナンス後、新バージョンの画面に変わりますが、各端末へのプログラム配信は一定期間経過後に開始されます。
  （現時点では3月頃を予定しています）
  - 新機能は、端末にプログラムが配信されてから利用可能となります。
  - プログラム配信を開始した以降にインストールした端末は、はじめからバージョン6.3でインストールされます。
  - Hotfix配信禁止設定を施している場合は、配信されません。