

## 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。

**挙動監視**

挙動監視の有効化

**設定**

**不正プログラム挙動ブロック**

不正プログラムの挙動ブロックを有効にする: 既知および潜在的な脅威 ▼

Intuit™ QuickBooks™ Protectionを有効にする ⓘ

**ランサムウェア対策**

すべてのランサムウェア対策機能を有効にする

- 不正な暗号化や変更から文書を保護 ⓘ
- 不審なプログラムによって変更されたファイルを自動的にバックアップして復元 ⓘ
- ランサムウェアに関連付けられていることの多いプロセスをブロック ⓘ
- プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック ⓘ

**脆弱性対策**

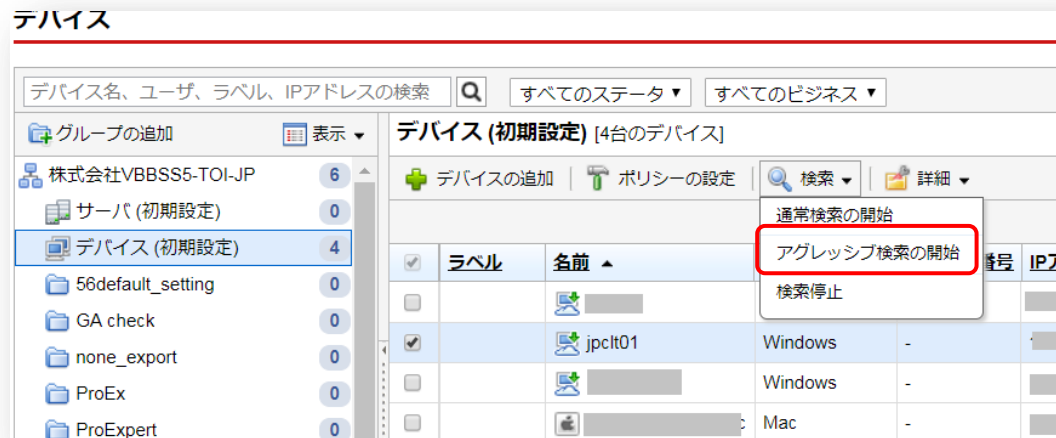
脆弱性攻撃に関連する異常な挙動を示すプログラムを終了

**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。



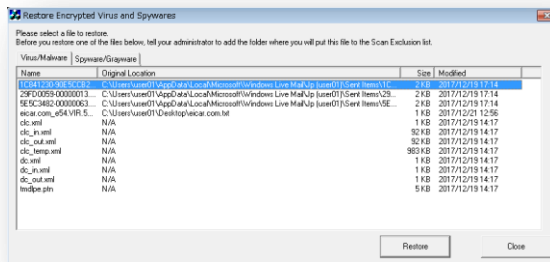
管理者画面上、実行ログは「手動検索」として表示されます。

The screenshot shows the 'デバイス' (Devices) management page with a table of search logs. The table has columns for '手動検索の開始時刻' (Manual Search Start Time) and '手動検索の完了時刻' (Manual Search End Time), which are highlighted with a red box. The log shows two entries for manual searches performed on 2017年12月19日.

ファイル	ウイルスパターン	ウイルス検索エンジン	予約検索の開始時刻	予約検索の完了時刻	手動検索の開始時刻	手動検索の完了時刻	POP3検索	検索方法	クライアントのバージョン	オペレーティングシステム	アーキテクチャ
	-	10.000.1043	-	-	-	-	無効	スマート	6.2.1208/13.1.1318	Win 7 Service Pack 1	x86
	-	10.000.1043	-	-	2017年12月19日 16:59:40	2017年12月19日 18:11:17	無効	スマート	6.3.1117/13.1.2020	Win 7 Service Pack 1	x86

## 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。

