Z!Shield3.10

SEP12.1のプロアクティブ脅威防止機能が無効になる

この度、Z!ShieldとSymantec社製Symantec Endpoint Protectin 12.1
(以下、SEP12.1)との共存環境で、次の問題が見つかりました。

つきましては、回避方法をご案内いたします。

【発生する環境】
・SEP12.1 のプロアクティブ脅威防止機能を有効にしている。
・Z!Shieldのバージョンは 3.10.007～3.10.029のいずれかである。
・ファイルフォルダ単位でUserモード運用する。

【発生する現象】
上記環境において、LiveUpdate等を使用してSEP12.1 のプロアクティブ脅威防止機能に関するアップデートを実施後、OSを再起動すると、プロアクティブ脅威防止機能が無効となる。
また、システムイベントログにエラーが記録される。

【問題発生時のリカバリー方法】
次の手順にて現象をリカバリーすることができます。

1) Z!ShieldをAdominモードに変更する。
2)OSを再起動し、SEP のプロアクティブ脅威防止機能が有効であることを確認する。
3)確認後、Userモードに変更する。

【現象の回避方法】
予め次の設定変更を実施してください。

1.Z!ShieldをAdminモードに変更する。

2.SEP12.1 の改変対策を変更する。

1)SEPの管理コンソールを開き、「設定の変更」を選択する。
2)クライアント管理の「オプションの設定」ボタンを押す。
3)「改変対策」タブを選択する。
4)「シマンテック製セキュリティソフトウェアを改版または終了から保護する」
チェックボックスのチェックを外す。
5)「OK」ボタンを押す。

3.レジストリエディタにて次の設定を行う。

レジストリキー HKEYLOCALMACHINE\SYSTEM\CurrentControlSet\Services\BHDrvx86
に対して、次の設定を実施する。

(c) 2025 SONJ FAQ Master <sjsa@son.co.jp> | 2025-07-31 02:33
URL: https://faq.son.co.jp/index.php?action=faq&cat=29&id=113&artlang=ja

・Start エントリの値(初期値1)を 2 に変更する。
・DelayedAutoStart エントリ(値の種類はDWORD)を追加し、値に 1 を設定する。

4.2.で設定したSEP の改変対策設定を変更前の設定に戻す。

5.Userモードに変更する。

※上記設定を行うと、Windows起動直後にログオンした場合、SEP12.1 のアイコンにプロアクティブ脅威防止機能のプログラム起動が遅れていることを示すマークが暫く表示されることがあります。

一意的なソリューション ID: #1112
製作者: FAQ Supporter
最終更新: 2012-07-05 13:50

(c) 2025 SONJ FAQ Master <sjsa@son.co.jp> | 2025-07-31 02:33
URL: https://faq.son.co.jp/index.php?action=faq&cat=29&id=113&artlang=ja