AMS Z!Shield

Z!Shieldとシマンテック社製品のウイルス対策ソフト連携時の注意点

シマンテック社のSymantec Endpoint Protection(以下、SEP)に関する注意事項について記載します。

1.1 Symantec Endpoint Protection との共存について

Z!ShieldクライアントとSymantec Endpoint Protection（以下SEP）を共存させ、ファイルフォルダ単位のUSERモードで運用した場合、Windows のシステムイベントログに以下のようなエラーが記録される場合があります。

・ ソース：SRTSP 内容：Error loading virus definitions.

・ ソース：SRTSP 内容：Error loading Symantec real time Anti-Virus driver.

これは、Z!Shieldの瞬間復元ドライバと、SEP のドライバの組み合わせによって発生するものですが、その後以下の情報が記録されSEPのドライバは正常に動作いたします。

・ソース：SRTSP 内容：Symantec Antivirus minifilter successfully loaded.

このイベントログは、SEP の設定を変更することで記録されないようにすることが可能です。SEP の設定変更法はシマンテック社の次のサイトを参照ください。

ファイルシステムAuto-Protect をロードするタイミングを変更する方法
シマンテック社の情報を参照する

1.2 Symantec Endpoint Protection 12.1とZ!Shieldクライアント共存時の注意

Symantec社製 Symantec Endpoint Protection 12.1 とZ!Shieldクライアントを共存する環境において、次の注意事項があります。

1.2.1 SymantecEndpoint Protection 12.1 のプロアクティブ脅威防止機能のエラーについて

プロアクティブ脅威防止機能を使用する場合は、事前に下記の設定変更を行って下さい。

Z!ShieldクライアントとSymantec Endpoint Protection 12.1（以下SEP）を共存させた環境において、SEP

(c) 2024 SONJ FAQ Master <sjsa@son.co.jp> | 2024-04-27 14:32
URL: https://faq.son.co.jp/index.php?action=faq&cat=3&id=162&artlang=ja

のプロアクティブ脅威防止機能に関するエラーが発生する場合があります。

【発生条件】

次の条件を両方満たす場合に発生します。

・ SEP のプロアクティブ脅威防止機能を有効にしている。

・ Z!Shieldクライアントをファイルフォルダ単位のUSERモードで運用している。

【発生する現象】

LiveUpdateを使用してSEP
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クライアントをADMINモードに変更する。

② もう一度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、Z!ShieldクライアントをUSERモードに変更する。

【回避方法】

次の設定変更を実施してください。

① Z!ShieldクライアントをADMINモードに変更する。

② Symantec Endpoint Protection 12.1 の改変対策を変更する。

(1)Symantec
Endpoint Portection 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。

(c) 2024 SONJ FAQ Master <sjsa@son.co.jp> | 2024-04-27 14:32
URL: https://faq.son.co.jp/index.php?action=faq&cat=3&id=162&artlang=ja

レジストリキー

【32 ビットOS の場合】

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BHDrvx86

【64 ビットOS の場合】

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BHDrvx64

に対して、次の設定を実施する。

・ 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。

④②で設定したSymantec Endpoint Protection の改変対策設定を変更前の設定に戻す。

⑤Z!Shieldクライアントを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、SEP 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。

1.2.2 次の手順にてSymantec Endpoint Protectionの手動スキャンを実行すると、「スキャンエンジンを初期化できませんでした」というメッセージを出力し、スキャンに失敗する。

Z!ShieldクライアントとSymantec Endpoint Protection 12.1（以下SEP）を共存させた環境において、次の手順の操作を実施することによりSEP の動作に異常が発生します。

【手順】

① Z!Shieldクライアントの復元タイプがファイルフォルダ単位であり、かつ、動作モードがUSERモードの状態において、初めてWindows にログオンするユーザ(注1)でログオンする。

② その後コンピュータを再起動し、①のユーザで再度ログオンする。

【発生する現象】

- 上記操作後、SEP の手動スキャン(注2)を実施すると、「スキャンエンジンを初期化できませんでした」というメッセージが出力され、スキャンに失敗する。
- 上記操作後、「新しいスキャンの作成」を実行しようとすると、「スキャンエンジンを

(c) 2024 SONJ FAQ Master <sjsa@son.co.jp> | 2024-04-27 14:32
URL: https://faq.son.co.jp/index.php?action=faq&cat=3&id=162&artlang=ja

初期化できませんでした」というメッセージが出力され、新しいスキャンの作成ができない。

(注1)一般ユーザの場合はUAC(ユーザーアカウント制御)の有効/無効に関わらず発生します。管理者権限ユーザの場合は、UAC が有効の場合に発生します。

(注2)「アクティブスキャン」「完全スキャン」「右クリックメニューでのウイルススキャン」を指します。AutoProtect には影響ありません。

【組合せ製品】

SEP12.1(2012 年10 月10 日現在リリースされている SEP 11.x では発生しません)

【対象OS】

- Windows 8(32 ビット版、64 ビット版)
- Windows 7(32 ビット版、64 ビット版)

【原因】

SEP12.1 より、SEP 11.x 以前にはなかったユーザ情報の持ち方となったため。

【回避方法】

次の手順により回避することができます。

①Z!ShieldクライアントをADMINモードにする。

②SEP の改変対策を無効に変更する。

③レジストリエディタにて次のレジストリにeveryone
フルコントロールのアクセス権を追加する。

【32 ビットOS の場合】

HKLM\SOFTWARE\Symantec\SymantecEndpoint Protection\AV\Scheduler

【64 ビットOS の場合】

HKLM\SOFTWARE\Wow6432Node\Symantec\SymantecEndpoint Protection\AV\Scheduler

④SEP の改変対策を有効にする。(注3)

⑤Z!ShieldクライアントをUSERモードにする。

（注３）SEP 自身の改変対策機能によってレジストリの改変等は保護されます。

(c) 2024 SONJ FAQ Master <sjsa@son.co.jp> | 2024-04-27 14:32
URL: https://faq.son.co.jp/index.php?action=faq&cat=3&id=162&artlang=ja

1.2.3 Symantec Endpoint Protection 12.1 のサービスタイムアウトについて

Z!ShieldクライアントとSymantec Endpoint Protection（以下SEP）を共存させ、ファイルフォルダ単位のUSERモードで運用した場合、Windows
のシステムイベントログに以下のようなエラーが記録され、SEP
のサービスが正常に動作しない場合があります。

「Symantec Management Client サービスの接続を待機中にタイムアウト (30000 ミリ秒) になりました。」

このエラーは前述の「3.6.5 SymantecEndpoint Protection との共存について」と「3.6.5 SymantecEndpointProtection との共存について」に記載の対処を行うことで回避が可能です。

一意的なソリューション ID: #1161
製作者: FAQ Supporter
最終更新: 2013-11-12 15:53

(c) 2024 SONJ FAQ Master <sjsa@son.co.jp> | 2024-04-27 14:32
URL: https://faq.son.co.jp/index.php?action=faq&cat=3&id=162&artlang=ja