# ソフトウェア制限ポリシー (SRP)

アドウェア、スパイウェア、トロイの木馬
の脅威と危険から企業を保護

XBlock Systems は、意図していないソフトウェアのインストールからコンピュータを堅固に保護する手法を提供しています。この手法を利用するにあたり Microsoft Windows オペレーティング システムの機能以外に特別なソフトウェアは必要ありません。このために、XBlock Systems は ”ソフトウェア制限ポリシー(Software Restriction Policies)または SRP” および “セキュリティ テンプレート(Security Template)” を作成するプロセスを自動化するシステムを開発しました。このシステムを使用すると、デプロイメントの際にユーザーが介入する必要はなく、管理者の負荷も最小限に抑えられます。

## XBlock SRP の戦略

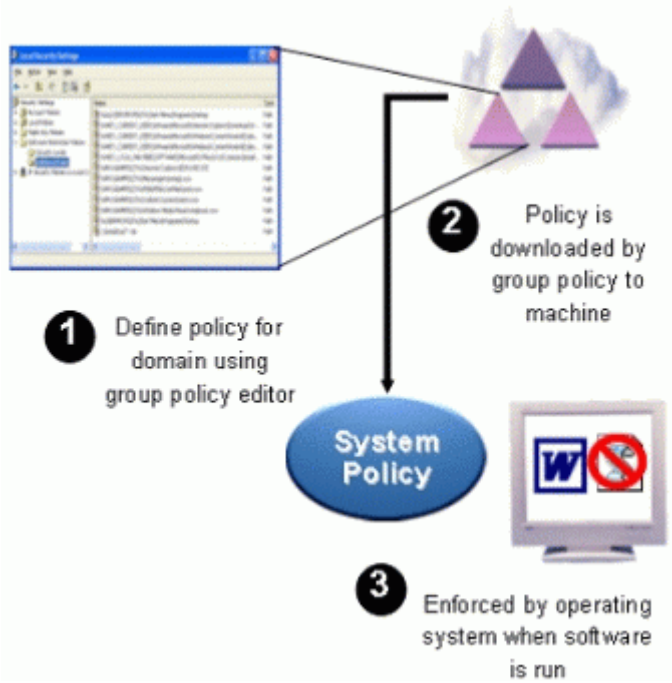
XBlock SRP は、企業コンピュータを狙う不当なソフトウェアや関連するインターネットペストを、大々的なスキャンや除去を行うことなく、簡単かつ迅速に封じ込めたいと考えているシステム管理者向けに作成されました。意図していないプログラムを無効化するプロセスを自動化するために XBlock が確立したアプローチはユニークかつ斬新なものです。

ソフトウェア制限ポリシーは、Microsoft Windows® XP および Windows Server 2003 の新機能です。この機能により、管理者はソフトウェアを特定して、これらのプログラムの実行を制御することができます。

機能的には、この方法により管理者は、実行可能プログラムが実行されることをブロックしたり、許可したりすることができるようになります。

これらの実行可能ファイルは、以下の方法で特定できます。

- 実行可能ファイルのファイル名 (例: MYPROGRAM.EXE)
- 実行可能ファイルが格納されているディレクトリ (例: C:¥Games¥)
- ファイルのチェックサム (MD5 または SHA1)
- 実行可能ファイルがダウンロードされた Web サイトのアドレス (URL)
- 実行可能ファイルの “コード署名者” (ソフトウェア作成者)




## 主な利点

- 標的とされているプログラムの実行に必要な権限を否定することで、マルウェア、スパイウェア、アドウェアなどの意図していないプログラムの機能をネットワーク上で効率的にブロックできる。

- 管理者は、保護範囲全体に渡って詳細レベルの制御が行える。アクティブ ディレクトリおよびグループを使用して管理をシームレスに行うことで、既存の企業ポリシーと簡単かつ迅速に統合できる。

- セキュリティ ポリシーのデプロイメントに既存の Microsoft インフラストラクチャを利用するため、デプロイメントがシンプルである。

- .REG ファイルが用意されているため、複雑なインストール方法はいっさい必要ない。

- 非侵襲的な手法(データを削除する必要のない方法)が採用されているため、管理者はデータの損失に対してリスクなしで実装できる。

- OS レベルで提供される機能を採用しているため、処理にかかるオーバーヘッドがない。

- エンド ユーザーに対して透過的であるため、エンド ユーザーの介在が必要ない。

- Microsoft 認定テクノロジを利用したコスト効率の高い 保護レイヤを採用しているため、あらゆる種類の脅威からワークステーションを堅固に保護する。

- 既に利用中のセキュリティ ポリシー テンプレートとの結合が容易である。

- デプロイメントの前に試験的環境で簡単に検証テストが行える。

- 既に導入済みスパイウェア、ウィルス、トロイの木馬の対策ソフトウェアに影響されない。

## 実装に関する参考資料

**セキュリティ テンプレートのローカル ポリシーへの適用**

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sce_assignpolicy.mspx

**企業全体に渡ってセキュリティ設定を適用する際の手法**

http://support.microsoft.com/default.aspx?scid=kb;EN-US;216735

**ソフトウェア制限ポリシーを使用して不当なソフトウェアからコンピュータを保護する方法**

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx