2015 年 9 月 29 日
株式会社セキュアソフト

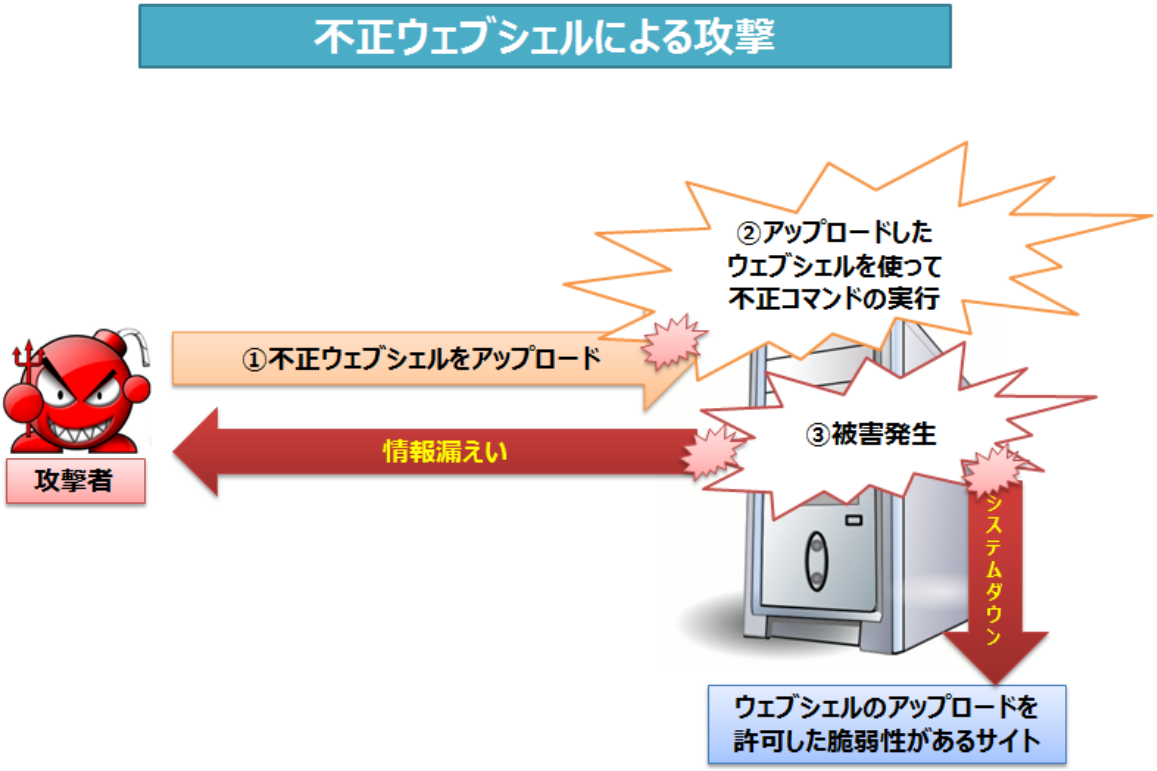
注意喚起：ウェブシェルを利用した攻撃について

1. はじめに

ウェブシェル（Webshell）を利用した攻撃は以前より多数確認されています。対策も行われていますが、まだまだ被害が発生し続けている状況です。今回はウェブサイトのアップロード機能を利用し、攻撃についてご説明します。

2. 攻撃方法

ウェブシェルはウェブサイト上で動作するシェルプログラムです。攻撃者は Web スクリプト言語を利用して不正ウェブシェルを作成します。攻撃者はウェブサイトで提供している掲示版などのアップロード機能を利用して悪意のあるウェブシェルファイルをアップロードし、アップロード後にリモートでウェブシェルを使ってウェブサーバ上で任意のコマンドを実行します。コマンド実行の結果、サーバ内部の情報漏えいやサーバ停止などの被害が発生します。



4. 注意が必要なサーバ

①任意の Web スクリプトの実行ができるウェブサイト
②アップロードの制限が設定されていないウェブサイト

5. 対策方法

1) ウェブサイト側での対策

① 任意のウェブシェルが動作しないようにサーバを設定。
② 掲示版などで任意のウェブシェルのアップロードを禁止。

2) ネットワーク側の対策（Sniper よる対策）

Sniper IPS ではウェブシェルを利用した攻撃に対し、100 を超える多数のシグネチャを提供しています。Sniper IPS を使用することでサーバからの情報漏えいやサーバ停止などの被害を未然に防ぐことが可能となり、安心・安全な運用が可能となります。

以上