2015 年 6 月 19 日

株式会社セキュアソフト

日本年金機構の情報漏えい事件にみる標的型攻撃への多層防御システムの必要性

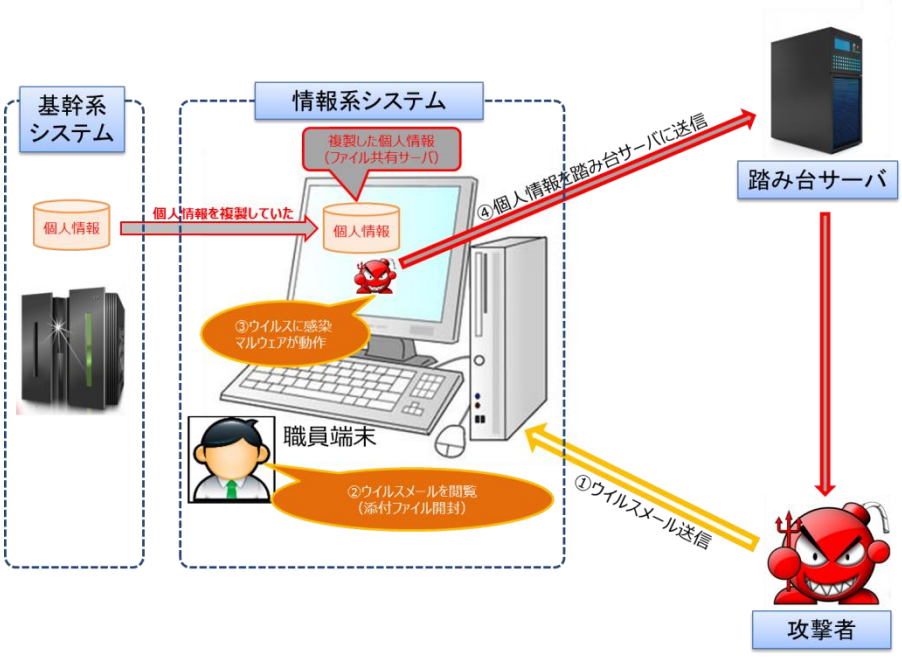
2015 年上半期、国内における情報セキュリティ関連インシデントとして非常に注目された日本年金機構における基礎年金番号などの個人情報漏えい事件がありました。情報セキュリティに対するなお一層の取り組みが必要であることを考える機会となりました。

本資料では事件の概要と対処すべき点について弊社の見解を記載させていただき、弊社が推奨しているネットワークセキュリティシステムの多層防御化も効果があることをご紹介させていただきます。なお、弊社では当事件に一切関与しておりません。

1. 事件の概要

日本年金機構からのプレスリリースおよび各報道機関からの情報によると 5 月に日本年金機構の職員がフリーメールアドレスからの複数種のウィルスメール（標的型メール）を受信し、添付ファイルを開く、あるいはメールに記載された悪性サイトが偽装されている URL をクリックしたことで、ウイルスに感染し、年金関連の個人情報流出が発生しました。

攻撃から情報漏えいの発生までは以下の流れで発生しています。



① 攻撃者は職員宛にウイルスメールを送信します。
② 職員はウィルスメールの添付ファイルを開封し、職員端末がウイルスに感染します。
③ 職員端末でマルウェアが動作し、バックドアをつくり情報収集活動が行われます。
④ 収集された個人情報は踏み台サーバに送信されます。
※今回の場合は本来の運用と異なり情報系システムに個人情報が複製されていたことも重要な問題と言われています。

2. 当該事件から考えられるセキュリティ対策

当該事件をはじめとする標的型攻撃対策についてはセキュリティソリューションベンダー各社から様々な技術、サービスや方策に関する情報がありますが、弊社としても以下の取り組みが必要であると考えます。

（１）事件発生時の対応が組織的に行われる体制作り（事件発生時のエスカレーション体制）
（２）組織のセキュリティに関する教育（今回の場合、事件発生時の対処に関する教育に重点がおかれます。）
（３）エンドポイントセキュリティの徹底（セキュリティソリューションの導入と扱うべき情報に関するルールの徹底）
（４）多層防御システムによる不正通信の可視化、防御（予兆監視、事件発生後の防御、追跡）

多層防御システムとは外部からの不正なアクセスに対して従来からのファイアウォールによる静的防御だけではなく、IDS,IPS、WAF、アプリケーション通信の可視化など複数の観点で検知・防御が可能な仕組みを取り入れたセキュリティ対策です。平時からの定点観測により、有事の際の早期異常検知と迅速な防御が可能となります。

弊社は IPS、DDoS 対策ソリューションを提供する会社として（４）についてお役に立てると考えております。

3. 多層防御システムについて

標的型攻撃を完全に防ぐことは大変困難であると言われています。しかし、被害を最小に抑えるための方策はあります。その１つがネットワーク、サーバ、端末などの各ポイントにおいて様々なセキュリティ対策を施し、その結果、平時の状況との違いを検知することで早期に不正な通信を検知、防御することができる多層防御システムです。
とくにネットワークセキュリティの範囲で考えますと、国内の多くの組織が外部との接続点においてファイアウォールを導入しているものの、IPS や UTM などの不正アクセスを可視化、検知・防御する等の対応についてはまだまだ不足していると弊社では考えています。特に今回のような感染 PC から踏み台サーバとの不正通信を IPS 等の活用で可視化、検知・防御の措置がとれ、被害を受けたときに有効と考えます。

以上

弊社の Sniper IPS では保有している色々なシグネチャを利用してバックドアの監視、C&C サーバとの通信、振舞い検知などが行えます。Sniper IPS の機能を利用することで不正アクセスや内部情報漏えいの対策に役立ちます。ぜひ、この機会にネットワークセキュリティの多層防御について見直しいただき、各種プロトコルの不正通信を検知・防御できる Sniper IPS、Sniper ONE シリーズ等のご検討をいただけますようお願いいたします。