資料コーナー

情報セキュリティにおける１０大脅威「脅威の“見えない化”が加速する」

出典：独立行政法人　情報処理推進機構　情報セイキュリティ白書 2007 版
（http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html）より抜粋

1.　はじめに

数年前は，ウイルスに感染するなどの被害を受けると，ソフトウェアの挙動が不安定になったり，通信が遅くなるなど，目に「見える」影響が多くありました。このため，一般の利用者であっても脅威に気づくことができ，対策に結びつけることができました。しかし，近年ではスパイウェアやボットなど，一般の利用者だけではなく，ネットワーク管理者であっても事前の対策なしには気づくことすらできない「見えない」脅威が増えています。

2.　2006 年の傾向

昨年から引き続き情報漏えいは多発しており，減少の傾向は見られません。安易なパスワードを狙ったウェブシステムへの不正侵入や，ウェブサイトのデータベースを狙った SQL インジェクション攻撃など，攻撃は増え続けており，更に金銭目的化にも拍車がかかっています。また Winny においては，利用者が意図せず情報流出の被害を拡大させる点が問題になっています。また，攻撃手法に関しては，ソフトウェアの脆弱性によってシステムを狙う手法と，フィッシング詐欺によって人間の心理を狙う手法を組み合わせた，より巧妙な攻撃が行われています。本来であれば，利用者はウェブブラウザのアドレスバー等を確認することで，フィッシング詐欺から身を守ることができますが，対象のウェブサイトや利用中のソフトウェアに脆弱性がある場合には，画面をいくら注意深く確認しても，フィッシング詐欺の被害に遭ってしまいます。その他にも，スパイウェアやボットなど，一般の利用者だけではなく，ネットワーク管理者であっても事前の対策なしには気づくことすらできない脅威が多くなっています。例えば，このボットを拡散させる手法の一つとして，ゼロディ攻撃を利用されるような，利用者が攻撃を受けたことに気づきにくい巧妙な手口がみらえるようになりました。特に，これらが標的型攻撃との組み合わせで行われた場合，気づくことはさらに困難です。また，ボットを利用してスパムメールが大量ばらまかれたり，ボットネットワークを利用して不適切な設定の DNS サーバを踏み台とした大規模な攻撃がおこなわれたりしました。

3.　ま と め

対策を行う際には，場当たり的な対策ではなく，意識して適切な準備と行動をおこなうことが重要です。利用者は安易なパスワードを使わない，開発者は設計時からセキュリティを意識して行動する，管理者はポリシーを定めて PDCA サイクルで徹底させるなど，それぞれの立場で，セキュリティを意識して行動する必要があります。セキュリティ上，脅威を単独で知っているだけでは不十分です。脅威は組み合わされ，見えにくい形で攻撃に使われるようになりました。脅威同士の関係を理解し，対策がどこまでなら有効なのかという対策の限界をしっかり認識したうえで対策をおこなって下さい。

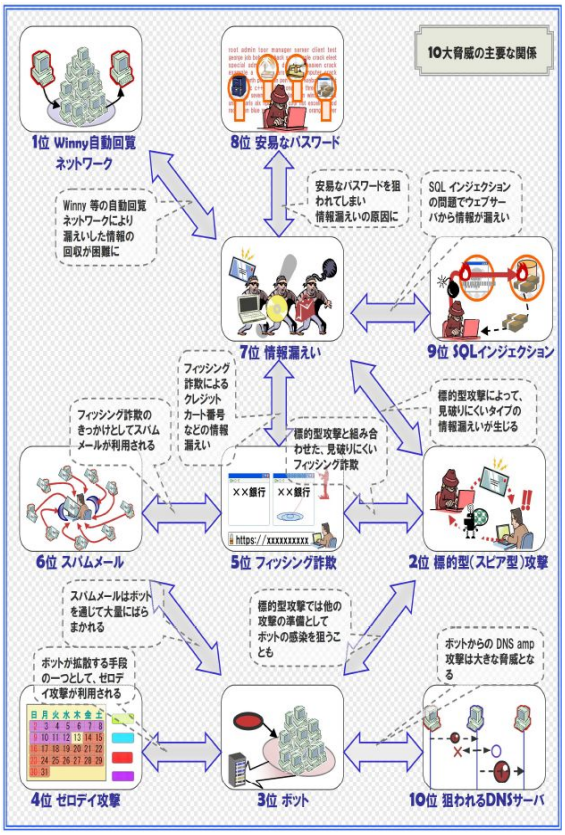

図１　10 大脅威の主要な関係概念図

富樫　一顯（㈱日立製作所）