2012.03

情報セキュリティニュース ＜2011 No.5＞

情報セキュリティに関する脅威の認知と企業の取り組み

2011年、多くの企業や官公庁などがサイバー攻撃を受け、様々な被害を受けることとなった。これら攻撃の中にはシステム部門の過失ではなく、社員のミスに起因して組織のシステムがウィルスに感染するケースも見られ、各組織では、組織内のシステムやネットワークの安全性をいかに確保するか改めて見直しを求められるとともに、社員一人一人が情報セキュリティに関して高い感度を持つことが再認識された。しかしながら、2011年12月に独立行政法人情報処理推進機構（以下、「IPA」と略記）が公表した「2011年度 情報セキュリティの脅威に対する意識調査」の報告書では、一般ユーザーの「情報セキュリティに関する攻撃・脅威の認知」の項目において、企業が注意すべき「標的型攻撃（サイバー攻撃）」、「マルウェア」、「ボット」に関する認知度は低い水準に止まっている。組織を構成する社員についても同様であると推察され、その教育・指導が急務である。そこで本稿では、一般ユーザーの情報セキュリティに関する脅威の認識について俯瞰し、近年多発している標的型攻撃の事例を参考にシステム部門が社員に対して、教育、注意喚起する際のポイントを解説する。

1. 個人の情報セキュリティの脅威と企業の情報セキュリティの脅威

「2011年度 情報セキュリティの脅威に対する意識調査」（表1参照）は、IPA が情報セキュリティに関する対策の情報発信、普及・啓発等の活動の一環として、毎年、継続的に実施している調査である。今回公表された調査報告書には、一般ユーザーの「情報セキュリティに関する攻撃・脅威の認知」の結果（表2参照）が公表されている。それによれば、「ワンクリック請求」、「フィッシング詐欺」といった脅威については、一般ユーザー全体の 9 割以上が認知している（「詳しい内容を知っている」＋「概要をある程度知っている」＋「名前を聞いたことがある程度」）。一方、「標的型攻撃（サイバー攻撃）」、「ボット」、「マルウェア」などの脅威については、認知度が5割を下回る結果となっている。

この認知度の差は、脅威がもたらす被害の違いによるものと考えられる。「ワンクリック請求」や「フィッシング詐欺」による被害は金銭的被害や個人情報の流出など直接的な損害として表れ、一般ユーザーは自分自身が痛手を被ることとなり、メディアをはじめとした周囲からの注意喚起も多い。それに対して、「標的型攻撃（サイバー攻撃）」や「ボット」、「マルウェア」は、不正プログラムの手段を用い、悪意を持った第三者が PC 所有者に見つからないよう PC を遠隔操作し、「迷惑メールの配信」や「PC 内の情報発信」を行うため、一般ユーザーが被害に気づきにくく、メディア等からの注目も集まらない。「標的型攻撃（サイバー攻撃）」については、最近、メディアを通じて多数の被害が報道された。しかしながら、一般ユーザーの認知度が低いのは、報道された「標的型攻撃」の対象が組織であり、個人にとってはあまり関係のない脅威として捉えられたからと考えられる。

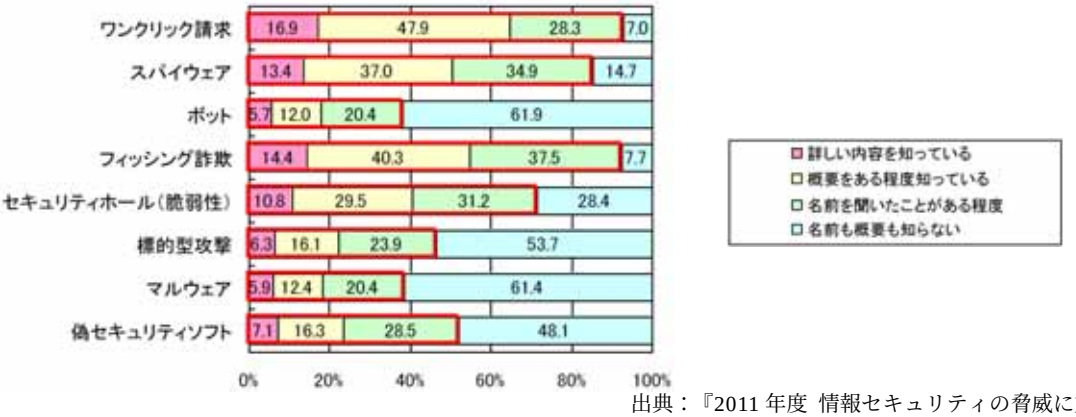
一方で、こうした脅威の中で、企業が留意すべきものは、個人の認知度が高い「ワンクリック詐欺」や「フィッシング詐欺」ではなく、個人の認知度が低い「ボット」や「マルウェア」、「標的型攻撃」などによって組織内のサーバ、ネットワークが攻撃され、機密情報が漏えいしたり、情報が改ざんされたりするケースである。

今日、組織の業務遂行に PC は欠かせない。自ずと PC スキルは十分に高いレベルに達している一方で、調査報告書の結果から、情報セキュリティに関する知識については、システム部門が思っているほどには高くない可能性が考えられる。このため、企業が留意すべき脅威について社員教育を行なう際は、単に社員（ユーザー）が実施すべき対策を説明するだけでなく、その脅威がどういったもので、どういった被害が発生するのか基本的な部分についても教育する必要がある。

表1：調査概要

調査名称：情報セキュリティの脅威に対する意識調査 調査方法：WEB アンケート調査 調査期間：2011 年 10 月 24 日～10 月 31 日 有効回答数：5,240 件

表2：情報セキュリティに関する攻撃・脅威の認知



出典：『2011 年度 情報セキュリティの脅威に対する意識調査　報告書』

【参考】情報セキュリティに関する脅威の主な種類と概要

名称	概要
ワンクリック請求	アニメ、ゲーム、アダルトサイト等で無料の動画を見ようと画像をクリックした利用者に対し、ウェブサイト運営者が利用者の意思に反して『会員登録』を行い、料金を請求する。
スパイウェア	メールの添付ファイルを開くことや悪意のある Web サイトからのダウンロードにより不正プログラムが侵入し、利用者の個人情報やアクセス履歴などの情報を詐取、利用者以外の者に自動的に送信する。
ボット	メールの添付ファイルを開くことや悪意のある Web サイトからのダウンロードにより、コンピュータに感染し、そのコンピュータを、ネットワーク（インターネット）を通じて外部から操る。
フィッシング詐欺	金融機関（銀行やクレジットカード会社）などになりすまして電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する。
セキュリティホール（脆弱性）	ソフトウェア等におけるセキュリティ上の弱点に対して、悪意を持ったスクリプト（命令）を埋め込まれてしまい、偽ページの表示等を行い、個人情報等を詐取する。
標的型攻撃	特定の企業、あるいは組織イントラネット内のパソコンを標的とし、サーバ内の個人情報、および機密情報を詐取する。
マルウェア	悪意を持った不正プログラムで、コンピュータウィルスやスパイウェア、ワームなどユーザーの意図に反した動作を行う。
偽セキュリティソフト	パソコンにウィルス対策ソフトを入れていないのに、突然、ウィルス感染の警告が表示され、指示に従ってパソコンをスキャンすると、有償の対策ソフト購入画面が表示され、クレジットカード決済で偽のセキュリティソフトを購入させる。

2.　標的型攻撃の事例と対策

2011年春以降、企業等の組織のサーバが外部から攻撃され、HP が改ざんされたり、組織の機密情報が窃取されたりする事故が多発している。これらの攻撃は組織の「サーバの脆弱性」をついた攻撃と、社員や組織の構成員に不正プログラムやウィルスを添付してメールを送信するなどの、「クライアントの脆弱性（会社 PC を利用している社員の操作ミスや不正行為）」をついた攻撃に分類できる。近年発生している事故の多くは、後者の「クライアントの脆弱性」をついた攻撃である。この攻撃は組織がファイアーウォールを適切に設定していても容易に突破することも多く、その場合の対応は社員個人にゆだねられる。そして、社員が誤った判断や操作を行うと組織のサーバがウィルス感染してしまうのである。

■事例：大手重工メーカー

2011年秋に大手重工メーカーが受けた攻撃は、悪意のある第三者が実在する団体担当者になりすまして当該企業の社員にウィルス付きのメールを送信していた。即ち、このケースでは悪意のある第三者が組織を攻撃する前に、当該企業と関係のある一般ユーザーの PC を攻撃し、その PC を遠隔操作した上で間接的に当該企業のサーバを攻撃していた。事前に一般ユーザーの PC 内の情報も窃取しているので、メールアドレスはもちろん、メールの内容まで本人からと思わせる内容になっていた。そのため、メールを受け取った当該企業の者は、そのメールが悪意のある第三者からのウィルス付きのメールとは気づかず、開封してしまいウィルスに感染した。当該企業のサーバがウィルスに感染した後は、ウィルスはシステム部門に発見されないよう潜伏し、時間をかけて情報を窃取していた。今回の事件では、結果的に保護すべき情報が漏えいすることはなかったが、組織内の多くのパソコンがウィルスに感染してしまった。

このように、個々のクライアントの脆弱性を狙った攻撃は新しい攻撃（APT：Advanced Persistent Threat）として、今後、対策を講じていくことが求められる。これら攻撃に対する最も良い対策はウィルス付きのメールが送信されても開封しないことであるが、今回のような ART では、上記でも説明したとおり、実在する人物から送られてくることもあるため、見分けることが難しくなる。全ての悪意のある第三者からの攻撃メールに当てはまるとは限らないが、攻撃メールかどうかを判断するポイントを下記に示す。

＜攻撃メールの判断ポイント＞
- 普段やりとりをしていない人から、添付ファイル付きのメールが届いた。
- そのメールがなぜ自分に送ってきたのか心当たりがない。
- ファイルの拡張子が .exe のような実行形式（圧縮ファイルの場合はその中身）になっている。
- ファイル名が文字化けしている。

さらに、このようなメールが社員個人に届いた場合に対応すべき行動を以下に示す。

＜攻撃メール受け取りの際の行動例＞
- メールに連絡先（アドレス、住所、電話番号など）が記載されている場合、連絡先に問い合わせ、そのようなメールを送信したか直接確認する。
- メール送信者がなりすましと判明した場合、組織内の情報システム部門などセキュリティ対策部門に報告し、指示を仰ぐ。
- 組織内のセキュリティ担当部門は、当該メールにウィルス感染の仕掛けがあるか調べるとともに、同様の攻撃メールが組織内の他の人に届いていないか、調査し、注意喚起を行う。

上記は、特別に難易度が高い対応ではなく、一般ユーザーである社員個人にとっても対応可能な取り組みである。システム部門は、サーバ関連のセキュリティについては、コスト対効果を勘案しハード対策を講じていく一方、社員に対しては、実現可能性の高い対策から段階的に実施することをお勧めする。なお、教育方法については、表3に示しており、目的や社員の情報セキュリティの知識レベル、役職、所属・部門等に応じた方法を選択することが望ましい。

表3:教育方法

教育	概要
集合型研修	■講義で情報セキュリティに関する知識全般を教えるだけでなく、グループディスカッション等も行なうことで情報セキュリティに関する知識を深めたり、事故・事件発生時における対応・解決プロセスを学んでもらったりすることで、集中的に幅広く学習することができる。 【メリット】1回で大勢に対して幅広い研修を行なうことができる。 ＜対象者＞　全社員
ロールプレイ形式	■想定される情報セキュリティに関する事故・事件の場面を再現し、参加者に事故・事件発生時の対応・解決プロセスを疑似体験してもらう。 【メリット】現実に近い対応ができ、参加者が緊張感を持って主体的に取り組んでもらえる。 情報セキュリティに関するリスクを再認識してもらえる。 ＜対象者＞　経営層、機密情報を多く取り扱う部署　など
ケーススタディ （クイズ形式）	■想定される情報セキュリティに関する事故・事件の場面で参加者がとるべき行動を問題として出し、事故・事件発生時の対応・解決方法等について解説・議論を行なう。 【メリット】実際に想定される場面を問題としているため、参加者にとって分かりやすく情報セキュリティの対策を教えることができる。 ＜対象者＞経営層、機密情報を多く取り扱う部署
e ラーニング	■パソコンを使って、情報セキュリティに関する知識を学んだり、問題を解いたりすることで、個人のペースで情報セキュリティについて学ぶことができる。 【メリット】参加者が自分のスケジュールで取り組める。 ＜対象者＞全社員

3.　まとめ

組織等の社員は、自分が直接被害を被る脅威以外への興味・関心はどうしても薄くなりがちである。丁寧な教育・啓発活動を通じてＡＰＴ等に対する防衛力を各社員が高めることが、企業の価値を守ることにつながることと肝に銘じて対策を推進させることを切に願っている。

インターリスク総研　コンサルティング第二部　BCM 第一グループ
コンサルタント　笹平　康太郎　（ササヒラ　コウタロウ）

（参考文献）

- 『2011 年度 情報セキュリティの脅威に対する意識調査　報告書』 独立行政法人 情報処理推進機構
- 『標的型サイバー攻撃の事例分析と対策レポート』 独立行政法人 情報処理推進機構

ただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。