セキュリティ対策虎の巻（第1回）

# オフィス機器の一元管理で巧妙な攻撃に対抗する

2016.07.27

情報セキュリティー対策には「これで万全」と言えるものがない。攻撃者の手口は巧妙化し、絶えず進化しているからだ。かつて攻撃者の力を誇示する「愉快犯」的な攻撃が目立っていたが、近年は機密情報や金銭の窃取を目的に標的型攻撃メールを仕掛けるなど犯行の動機も変化している。

## 最低限必要な5つのセキュリティー対策

企業が講じるべき情報セキュリティー対策の「基本」を紹介しよう。

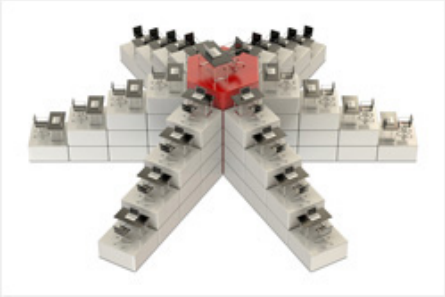
(1)「ソフトウエアの更新」
攻撃者はパソコンにインストールされたソフトウエアの脆弱性を突いて攻撃を仕掛ける。よって、ソフトウエア会社などから提供される修正プログラム（セキュリティーパッチ）を常に更新する。

(2)「ウイルス対策ソフトの導入・更新」
社内のパソコン、システムのウイルス感染を防ぐため、対策ソフトの導入と定義ファイルの更新が不可欠になる。

(3)「パソコン、社内システムへログインするパスワード・認証の強化」
従業員のパスワードが盗まれると、社内システムに不正侵入されるリスクがある。不正侵入を防止するため、推測されにくいパスワードの設定や、アクセスする度に1回限りのパスワード（ワンタイムパスワード）の利用、電子証明書の使用など、複数の認証方法を組み合わせる多要素認証方式を活用する。

(4)「パソコンやサーバーの設定の見直し」
従業員が利用する共有フォルダは部署や役職などに応じてアクセス権限を適正に設定し、異動・退職する社員のユーザーアカウント（ID・パスワード）は確実に抹消する。

(5)「脅威・手口を知る」
最新の脅威、攻撃者の手口、その対策を知り、被害の予防につなげる。



これらの「基本」は、企業活動に最低限必要な取り組みである。自動車運転にたとえれば、「交通ルールを守る」「シートベルトを着用する」といったレベルのものであり、セキュリティー対策の「十分条件」ではないことを理解したい。そして、経営者は「自社の情報は常に脅威にさらされている」との認識に立ち、どのように守るのかを考え、社内に対策を徹底することが重要だ。

## 一元管理をしなければリスクすら分からない… 続きを読む