# セキュリティの最初の防衛線

**相次ぐ不正アクセス、止まないサイバー攻撃、猛威をふるう標的型攻撃。ITセキュリティ対策は、今や企業の重要な施策の一つであるといえる。しかし、システム的な対策だけでは、完全に脅威を防ぐことは難しい。セキュリティの脅威における最初の防衛線は、「従業員（人）」という一番身近なところに存在している。**

## 無防備な“人”の隙を突く標的型攻撃

2011年に三菱重工で起きたサイバー攻撃による情報漏洩事故を契機に、特定の企業や組織を狙った「標的型攻撃」が国内でも注目を集めている。このきっかけは、従業員に送りつけられた標的型メールだった。標的型メールの本文内に記載されたURLにアクセスしたり添付ファイルを開いたりすると、ウイルスに感染し、情報漏洩やネットワークへの侵入などにつながってしまう。

こうした攻撃の被害を防ぐには、システム的な対策だけでは不十分である。いかに高度なセキュリティ機能を搭載したシステムを導入したとしても、残念ながら標的型攻撃を完全に防ぐことは困難だ。それは、たとえ玄関に最新鋭のカギを設置していても、「そのカギを自分で開けてしまう」のが個々の従業員、つまり「人」だからである。標的型メールは無防備な従業員の隙を突くように送られてくる。システムを扱う人にセキュリティの観念が備わっていないという「人が脆弱な状態」では、いくら強固な砦を建設しても、抜け穴はいくらでもあることになる。まさに「人」が企業のセキュリティでウィーケストリンク[1)]となってしまうのである。

## セキュリティアウェアネスとその重要性

昨今の情報システムは様々な機能が複雑に絡み合った集合体であり、安全に使用するには一定のセキュリティの知識が必要となる。標的型攻撃とはどういうものか、標的型攻撃に対する心構え、といったセキュリティ教育を従業員に施す、“人”を対象としたセキュリティ対策の重要性が年々高まっている。

もちろん、こうした「知識」を中心としたセキュリティ教育が重要であることは間違いない。しかし、まずその前段階として最も大事なのが、従業員の「意識をセキュリティに向けること」――すなわち「セキュリティアウェアネス（Security Awareness）」である[2)]。

なぜセキュリティ「教育」の前に「アウェアネス（意識を向けること）」が必要なのか。企業のシステム管理やリスク管理等とは関連のない一般従業員について考えてみればよくわかる。企業が定めたセキュリティポリシーやルールを守るには、従業員は少なからず面倒な手続きを踏まなければならず、「できればこんな手続きは避けたい」と思うかもしれない。また、これを遵守しても、自身に直接的な利益が生まれるわけではないため、「セキュリティは重要ではない」と考える従業員も少なくないだろう。実際、ある調査[3)]で様々な企業の従業員にセキュリティに対する意識を尋ねたところ、「セキュリティポリシーを守り、会社全体として常に気をつけることが重要」という回答は全体の約4割にとどまり、実に過半数はセキュリティポリシーを気にしていないという回答だった。

このような状態で自社のセキュリティポリシーやルールを説いたところで、（誤解を恐れずに言えば）大多数の従業員にとっては馬耳東風であろう。従業員は、何が重要か、何を優先するべきかという自身の基準によって行動している。セキュリティに価値を見出しておらず、それより効率を優先すべきという基準が従業員の中にあれば、企業がセキュリティの重要性をいくら説いたところでまったく伝わらないだろう。だからこそ、まず企業はその従業員である“人”の意識を変え、セキュリティに対する優先順位を上げさせることが必要なのである。


野村総合研究所　金融ITイノベーション研究部

NOTE

1) "The strength of the chain is in the weakest link." 鎖の全体の強度は最も弱い輪によって決まるという諺。
2) 米国立標準技術研究所（NIST：National Institute of Standards and Technology）がまとめたNIST SP800-16『情報技術セキュリティトレーニングの要件：役割および実施ベースモデル』には、「アウェアネスとはトレーニングではなく、単にセキュリティに注意を向けることを目的としたものである」と述べられている。
3) 出所：Avira社
http://www.avira.com/en/press-details/nid/532/news/corporate+security
4) 出所：内閣官房情報セキュリティセンター（NISC）政府機関における情報セキュリティ対策の取り組み状況について
http://www.nisc.go.jp/press/pdf/torikumi_press.pdf
5) ENISA：欧州ネットワーク・情報セキュリティ機関 "How to Raise information security awareness"
http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide

## 効果的なアウェアネスとは？

従業員に効果的に作用するアウェアネスにはどのようなものがあるだろうか。まず思いつくのは、実際の情報漏洩事故事例を挙げ、「こんな事故がもし自社で起きたら？」と考えさせることだろう。具体例を用いてイメージを膨らませるわけである。しかし残念ながら、「事故事例」と「企業（自社）」を関連付けて説明しても、「まさか自分には起こらない（関係ない）だろう」と思われてしまうことが多い。そこで、「事故事例」を「企業」ではなく「従業員」自身と関連付け、より身近な設定にする。例えば、「業務中に受け取ったメールに記載されていたURLにアクセスしたところ、知らぬ間に自分のPCがウイルスに感染し、それが原因で自社の機密情報が外部に漏れてしまった。自分の何気ない行動が、世間を騒がせる大ニュースになってしまった」といった事例である。こうすると、各従業員の意識をセキュリティにぐっと引き寄せることができる。「事故事例」と「従業員」を疑似体験という形で関連付け、自分にも起こりうる脅威として強烈な印象を与えるのである。

また、政府機関等で実施されている標的型メールの訓練[4]もアウェアネスの取組みの一つである。当社でも2011年より標的型攻撃を疑似体験できるサービスを提供しており、擬似的に標的型メールを対象企業の従業員に送付し、添付ファイルの開封／リンクURLへのアクセス状況等を企業に報告している。述べ17万人が訓練に参加したが、訓練後のアンケートを見ると、「サイトを閲覧するだけで、マルウェアに感染するとは思っていなかった」「自宅のPCだったら開封しないが、自社のセキュリティは万全と思っていたので開いた」と、怪しいと感じつつも"問題無い"と自己判断していた従業員が実に多い。マルウェア感染に繋がる行為をよく理解していない、企業のセキュリティシステムを過信している"人"が、まさに企業の情報セキュリティの最初の防衛線を危うくしているという実態が見える。一方、訓練を経験した後の感想を聞くと、「自分とは関係ないと思っていた」「何気なく添付ファイルを開封していたが、件名や本文を確認するようになった」など、意識の変化に繋がったという回答が多かった。訓練はアウェアネスの喚起に一定の効果を持つと考えられる。

ただ、アウェアネスの効果は永続的ではない。同じ内容を繰り返すだけでは、人は慣れてしまうものである。このため、アウェアネスの活動は継続的に、なおかつ形を変えながら行うべきであるとの見解が定説となっている。官公庁を始め多くの組織、企業が標的型メールの訓練を行っているが、継続的な実施と、新たな要素を加え続けていくことが重要である。新たな要素に困ったら、外部サービスの利用も検討していいだろう。

「アウェアネスがセキュリティの最初の防衛線となる。」これはENISA[5]からの引用である。従業員に対するセキュリティ教育はもちろん重要だ。しかし、まず彼らの意識をセキュリティに向けないことには、企業のセキュリティポリシーや情報システムのセキュリティ、セキュリティに関わるルールも有効に機能しないのである。

Writer's Profile
**西田 助宏** Sukehiro Nishita
NRIセキュアテクノロジーズ　テクニカルコンサルティング部
主任セキュリティコンサルタント
専門はサイバーセキュリティ
focus@nri.co.jp