最新情報セキュリティ対策総覧（第6回）

会社を救う「社員教育×データ集中管理」

2017.12.06

情報セキュリティの脅威は偶発的なものと意図的なものに分かれる。偶発的なものは障害と人為的なものにさらに分かれる。今回は人為的なミスが引き起こす脅威への対策について考えたい。

社内の情報資産を洗い出し、脅威から情報を保護する情報セキュリティ対策を進めていく中で、難しいのが「人」の問題だ。いくら情報保護のためのルールを策定しても、それが守られなければ「絵に描いた餅」となる。ルールを守らない社員がいると、そこが全社的な情報セキュリティ上の弱点にもなりかねない。メールの誤送信や、顧客情報が保存されたスマホの置き忘れといったうっかりミスが個人情報漏えい事件に発展する時代である。情報セキュリティ対策を強化するITサービスの検討とともに、忘れてはならないのが社員教育だ。

疑似メールを送って社内訓練を実施

メールやWebサイトを悪用した標的型攻撃の被害が後を絶たない。毎年、情報セキュリティの脅威を公表しているIPA（情報処理推進機構）の「情報セキュリティ10大脅威
2017」では、組織向け脅威として「標的型攻撃型による情報流出」が前年に続いて1位となった。

標的型攻撃では、「つい、うっかりしてメールや添付ファイルを開き、ウイルスに感染」するケースが多い。こうした手口は周知のはずだが、それでも引っかかるのは攻撃者の手口が巧妙化しているからだ。例えば、攻撃者が正規のアカウント情報（ユーザーID・パスワード）を盗み、本人になりすましてウイルスを埋め込んだ偽のメールを取引先に送信する。取引先は何の疑いもなくメールの添付ファイルを開いて感染する。標的型攻撃の対策としては、社員に対する情報セキュリティ教育の実施が欠かせない。

メールを悪用する標的型攻撃に備えた社員教育、訓練を実施する企業もある。ある企業ではIT部門が中心となり、会社のメールアドレスを持つ社員を対象にセキュリティ研修を実施。脅威の傾向を学ぶeラーニングに加え、定期的に社員に疑似メールを送り、標的型メール攻撃に対する訓練を行っている。

迷惑メールはフィルタリングをかけて隔離していても、標的型攻撃では送信元を偽装しており、隔離されないケースもある。不審メールを不用意に開かないように、日ごろから社員の訓練が必要だ。また、新入社員の研修時にセキュリティ教育を実施するのも有効だろう。入社時から徹底して社員のセキュリティ意識を高める狙いがある。

不審メールを受信したら担当部門に連絡… 続きを読む