最新情報セキュリティ対策総覧（第1回）

保存版！対策が見えてくる「脅威の分類」

2017.09.06

企業のデータを“人質”に身代金を要求するランサムウエアなど新手の攻撃や、特定企業を狙った標的型メール攻撃の被害が深刻化している。企業のリスクはサイバー攻撃だけではない。地震や水害、火災などの災害によって、企業の重要データが消失するケースもある。情報漏えいやデータ消失の影響は自社のみならず、顧客・取引先にも及ぶ。企業を取り巻くさまざまな脅威から情報資産を保護し、ビジネスを継続するためにも情報セキュリティ対策の強化は待ったなしである。

セキュリティ費用を上回る情報漏えい処理費用

企業活動を脅かす情報漏えい。その要因は外部からの攻撃だけではない。内部の犯行もあれば、顧客情報が保存されたノートパソコンを置き忘れたといったうっかりミスもある。情報漏えいの原因がどのようなものであろうとも、企業は被害者ではなく、顧客の個人情報を保護できなかった加害者として社会から非難される。

改正個人情報保護法が2017年5月30日から全面施行され、これまで対象外だった5000人分以下の個人情報を取り扱う事業者も改正法が適用されるようになった。たとえ1件でも個人情報を取り扱っていれば、企業規模にかかわらず改正法の対象となる。中堅中小規模の企業も、これまで以上に個人情報保護の徹底が求められる。

業務の効率化や生産性の向上などの直接的な効果が見込めるIT投資と違い、情報セキュリティ対策は費用対効果が見えにくいという経営者の声も聞かれる。確かに情報セキュリティ対策を強化したからといって、売り上げが上がるわけではない。

だが、これまで情報漏えい事件を起こした企業の例を見ると、被害者に対しておわびの金券を送付するなど、多額の賠償を余儀なくされる。さらに、取引先からの業務停止や社会的な信用失墜の可能性もある。情報漏えいの処理に関わるコストは、情報セキュリティ対策を強化するコストをはるかに上回る。経営者はそのコストの大きさを今一度認識する必要があるだろう。

リスクは環境的脅威と人為的脅威に分ける… 続きを読む