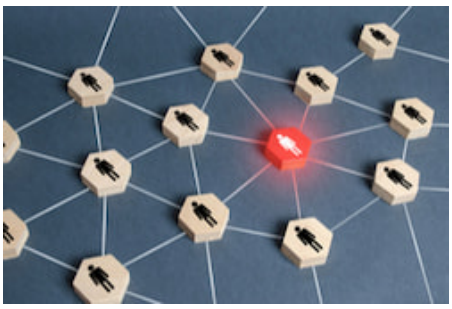
重要情報の扱いを考え直す（第6回）

本当に怖い社員の脅威

2021.09.13



サイバー攻撃の激化が止まらない。その被害は年々深刻さを増し、セキュリティ対策の重要性は一段と高まっている。そんな中、意外に見落とされがちなのが「内部の脅威」への対策だ。外部からの攻撃に備えるのはもちろん、職場内にも存在する脅威を正しく認識し、あらかじめ必要な対策を講じておいたほうがよい。身近な具体例を示しつつ、内部脅威から企業を守る道筋を考える。

激化するサイバー攻撃。だが見落としがちな内部脅威

サイバー攻撃には、さまざまな種類がある。IPA（独立行政法人情報処理推進機構）が発表した「情報セキュリティ10大脅威2021」によると、ランサムウエア、標的型攻撃、ビジネスメール詐欺といった項目と並び、「内部不正による情報漏えい」が6位に挙げられた。サイバー攻撃の加害者は「外部の人間」となる場合が多い。だが、内部不正が原因の場合は加害者、被害者共に同じ職場で働く仲間ということになる。もし不正を発見して被害を最小限に抑えられたとしても、社外の評価は上がるどころか「ダメな会社」の烙印（らくいん）を押されかねない。このため、内部不正による情報漏えいは身内の不祥事的に扱われ、公表されずに終わるケースも少なくないのが実情だ。

サイバー攻撃に備える企業の対策は、「未知の相手から届いたメールの添付ファイルを開かない」「誘導されたWebサイト、サーバーにアクセスしない」など、外部の脅威から身を守る取り組みが中心になっている。しかし、内部不正を防ぐには「勝手にデータを持ち出すな」「このファイルにアクセスするな」といった、ある意味“人を見たら泥棒と思え”的な考えにも捉えられかねない対策を採る必要が出てくる。対策強化で職場がピリピリした雰囲気になるのを恐れて実施を先送りし、結果的に不正の温床になってしまう例も後を絶たない。

もちろん内部脅威は悪意を持った特定の社員だけでなく、悪意のない社員の中にも存在する。「ついうっかりして」「不正だと思わずに」といった理由から発生したケースでも、重大な被害が生じることに変わりはない。内部脅威を考える際には、悪意の有無を問わない姿勢が求められる。

内部脅威あれこれ。ケーススタディーで考える… 続きを読む