人に語れるようになる“ITのツボ”（第12回）

本当に不安はない？改めて考える多拠点のセキュリティ対策

2024.06.28

情報処理推進機構（IPA）は毎年、情報セキュリティの10大脅威を選出している。2024年版の「組織」向けの脅威としては、「ランサムウェアによる被害」「サプライチェーンの弱点を悪用した攻撃」「内部不正による情報漏洩などの被害」が上位3位に並んだ。

これらを含めて、10大脅威の多くは5年～10年近くにわたり継続して選出されているものが多い。すなわち、組織の側で脅威に対策をしていても、攻撃者側はそれを上回る悪知恵を働かせて被害が続出しているというわけだ。

多拠点展開の企業で、IT担当者が本社にしかいないケースも

こうした状況では、組織側の事前対策はもちろん、万が一のトラブル時にも迅速で適切な対応が求められる。情報システム部門が手厚い大企業であれば、対応についてシステム的に守りを固めると同時に運用管理体制を整えて備えているケースが少なくない。一方で、中小企業では情報システム部門の社員やIT担当者の人材確保そのものが難しく、業務システムなどの維持管理で手一杯になってセキュリティ対策まで目が届かないこともある。

さらに、多拠点展開している中小企業では、状況はより深刻になる。数少ない情報システムやIT担当者が本社などにしか配置されていないと、多くの店舗や支店の状況を逐一把握して対応することができない。日常的なシステムトラブルや端末機器の故障などへの対応が求められる中で、多拠点のセキュリティ対策まで手が回らないのが現実だ。

セキュリティ体制と生産性向上を同時に実現するには？現状の棚卸とリスク把握が大切… 続きを読む