「情報漏えい、当社に関係なし」の嘘（第3回）

セキュリティー対策を怠ったツケ

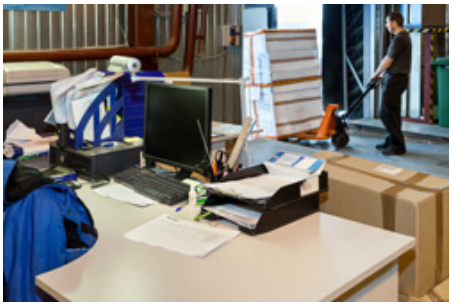
2016.08.24

情報漏えいのセキュリティー事故が後を絶たない。最近も数百万人分の顧客データが流出した大手旅行会社の事件が表面化した。それでもなお、「わが社には、狙われるほどの情報はないから大丈夫」。このように考える中小規模の企業経営者は少なくない。

セキュリティー対策は、経営課題そのものである。経営者にとって、売り上げの拡大や事業の継続が大きな経営目標であるが、万一、情報漏えい事故を引き起こした場合、売り上げの減少どころか事業の存続すら危ぶまれることになる。外部から指摘されるまで情報漏えいに気づかなかったら、取引先からだけでなく、社会的にも情報管理体制の不備を強く責められる。企業イメージは失墜し、経営の危機が訪れる。リスク管理、コンプライアンスの観点から、かつてないほどセキュリティー対策の強化が必須になっている。

手薄な拠点から狙われる「攻撃の連鎖」

本社と主要拠点のセキュリティー対策を徹底していても、ネットワークに接続しているすべての拠点のセキュリティー管理体制を再点検する必要がある。点検の対象には、小規模な営業拠点や遠隔地の工場、倉庫も含まれる。



例えば、在庫管理のため、倉庫にパソコンを置いてインターネットに接続していないだろうか。倉庫のセキュリティー対策に不備があれば、そのパソコンが攻撃される恐れがある。攻撃者は倉庫のパソコンを操って、本社のパソコンやサーバーに保管された機密情報・顧客情報を盗み取る。さらに、攻撃者は本社のパソコンを踏み台にして、取引先のパソコンを攻撃して目的の機密情報を盗み取る。取引先も含めた「攻撃の連鎖」が起こる可能性もある。

被害者ではなく加害者になってしまう… 続きを読む