中小企業のセキュリティー対策

－6－

経営者主導で効果実感

サイバー攻撃は他人事ではない

テレビや新聞などでサイバー攻撃による情報漏えい事件などが報道されているが、これは大企業に限った話ではない。先頃、独立行政法人情報処理推進機構（IPA）が発表した「中小企業の情報セキュリティ対策の実態調査－事例集－」（以下、事例集）では、全国の中小企業の被害事例や取り組みが紹介されており、サイバー攻撃はもはや他人事ではないことが理解できる。いくつか掲載事例を紹介させていただきたい。

事例1　□　□

「従業員がメールに添付されていたファイルを不用意に開いたためウイルス感染し、基幹システムの設定が書き換わる障害が発生した。システムベンダーの協力を得て障害対応を行なったが、復旧するまでの1週間ほど基幹システムの一部が使用できなくなった（静岡県・製造業）」

同社ではウイルス対策ソフトを導入していたがウイルスを検出できず被害を受けた。これを教訓に、メールのフィルタリング製品の導入や従業員に対するセキュリティー教育を実施しており、以降は被害が発生していないという。

事例2　□　□

「自社で運営しているCMS（コンテンツマネジメントシステム）で作成したウェブサイトが改ざんされてしまい、閲覧者が有害なサイトへ誘導されるようになってしまった。実害はなかったが、セキュリティー被害は身近なものであると感じた（宮崎県・運輸業）」

サイバー攻撃を受けることで「被害者」になるだけではなく、「加害者」になることもある。同社はメールやウェブのフィルタリングができ一元的なレポーティング機能を備えたUTM製品を導入することで対策強化と監視業務の効率化に取り組んでいるという。

これらを対岸の火事と考えず、セキュリティー対策に取り組む際の参考としてほしい。

一方、事例集では前向きな取り組みも多く紹介されている。

事例3　□　□

「同業他社の情報漏えい事件をきっかけに、自社のセキュリティー対策の見直しとIT人材育成に取り組んでいる。セキュリティー認証取得にも取り組んでおり、行政、金融機関、取引先からの信頼獲得を実感している（北海道・金融業）」

セキュリティー対策は費用対効果が明確ではないためコストとして考えられることが多い。しかし、事例集では、取り組みを対外的にアピールすることで信頼獲得につながった、従業員のセキュリティー意識向上など人材育成につながったという経営者の声も多い。経営者がリーダーシップを発揮して対策を推進した企業ほど効果を実感しているようだ。

ロゴマーク取得し取り組みPR

中小企業がセキュリティー対策を進めるに当たってはIPAが公開する「中小企業の情報セキュリティ対策ガイドライン」（以下、ガイドライン）が指針となるだろう。

また、セキュリティー対策の取り組みを対外的にアピールするに当たってはIPAが4月から募集開始した「SECURITY ACTION」制度を活用してほしい。

SECURITY ACTIONのロゴマーク

「SECURITY ACTION」とは、中小企業自らが、セキュリティー対策に取り組むことを自己宣言する制度で、ガイドラインの実践をベースに2段階の取り組み目標を用意している。また、取り組み目標に応じたロゴマークを使用することができ、ウェブサイトや名刺などに表示することで、情報セキュリティーに自ら取り組んでいることをアピールすることが可能だ。

1段階目は、OS・ソフトウエアの更新やウイルス対策ソフトの導入、パスワードの強化など、あまりお金をかけなくても実施できる効果的な5つの対策に取り組むこととなっている。これまで組織として対策に取り組んでこなかった小規模企業でも容易に取り組める内容であるため、まずはここから取り組んでほしい。

利用手数料は無料。具体的な手続きはIPAのホームページ（https://www.ipa.go.jp/security/security-action/）を確認してほしい。

（独立行政法人情報処理推進機構・江島将和）