北近畿の中小企業のための情報セキュリティー相談室

㈱マルテツ（福知山市）代表取締役社長
個人情報保護士／情報セキュリティアドバイザー　原田正大

㉑「被害と復旧」前提に経営者主体で指示を

経済産業省は昨年11月16日に「サイバーセキュリティー経営ガイドライン ver 2」を発表した。これは、中小企業も適用可能なサイバーセキュリティーの基本的な方針で、まず経営者が基本理念と方針を定めて、対策基準と現場に展開させるべき項目やポイントが記載されているものである。

ガイドラインにはもともと「経営者が認識すべき3原則」として①経営者のリーダーシップによる対策②自社だけでなく取引先やパートナーを含めた対策③平時からのステークホルダーや関係者とのコミュニケーション円滑化―に触れた上で、「サイバーセキュリティー経営」の重要10項目が定められていた。

しかし今回の改訂では、この重要10項目が変更され、これまでの侵入されないための対策ではなく、被害を受けてしまうことを前提とした対策に重点が置かれるようになったのが大きな特徴である。

「攻撃の検知」を含めたリスク対応体制と、「サイバー攻撃を受けた場合の復旧の備え」を取るよう記載されているが、これは国家としても、増え続けるサイバーセキュリティーの問題・被害に関する各種ソフトウェアのバージョンを最新の状態にアップデートしておく③データを復元するバックアップ体制を整えておく④パソコンやインターネットを使う社員全員に対して、定期継続的セキュリティー教育を行う―といったところだろう。

今一度、経営者が主体となって社内の情報セキュリティー対策を見直すべきとすすめてきた重要になってきている。

ずっと申し上げていることだが、お勧めの情報セキュリティー対策方法は、①スパムメールや不正サイトをブロックするためにウイルス対策ソフトとUTM（統合脅威管理）を導入する②使用していることが分かる。

サイバーセキュリティー経営の10項目

① サイバーセキュリティーリスクの認識、組織全体での対応方針の策定
② サイバーセキュリティーリスク管理体制の構築
③ サイバーセキュリティー対策のための資源（予算、人材等）確保
④ サイバーセキュリティーリスクの把握とリスク対応に関する計画の策定
⑤ サイバーセキュリティーリスクに対応するための仕組みの構築
⑥ サイバーセキュリティー対策におけるPDCAサイクルの実施
⑦ インシデント発生時の緊急対応体制の整備
⑧ インシデントによる被害に備えた復旧体制の整備
⑨ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
⑩ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供