セキュリティ脅威を招く落とし穴（第4回）

知られざるセキュリティ3つの要件と3つのステップ

2017.12.06

情報セキュリティ対策は経営者の責務である。これは強調してもし過ぎることはない。企業が保有する情報は幅広い。経営資源となる業務情報をはじめ、顧客・取引先の情報、マイナンバーなど従業員の情報がある。技術情報やノウハウといった知的財産である無形の情報もある。また、サーバーやネットワーク機器のハードウエア、USBメモリーの記憶媒体、紙文書といった有形の情報もある。無形、有形にかかわらず、情報をどう守っていくのかを検討し、適切に判断を下すのが経営者の役割となる。

3要件を基本にセキュリティ対策を検討

これらの守るべき情報を扱うに当たり、情報セキュリティのあるべき3つの要件として「機密性」「完全性」「可用性」がある。機密性は、利用が許可された人だけが情報にアクセスできる状態にしておくこと。完全性は、情報そのものや、情報の処理方法が常に正確である状態を保持すること。可用性は許可された人が必要なときに必要な情報にアクセスできること。この3つの要件を基本に、さまざまな脅威から情報を保護するための情報セキュリティ対策を検討する。

例えば機密性の確保では、システムを利用する際に本人確認を行うユーザー認証や、役職や権限に応じてシステムを利用できるアクセス制御などがある。完全性を維持するには外部からの不正アクセスを防御するファイアウォールやウイルス対策、迷惑メール対策などが必要だ。そして、可用性を担保するには、消失や改変に備えたデータバックアップ、停電に備えた電源バックアップなどの対策がある。これら3つに加え、利用履歴を保存するログ管理も情報セキュリティの要件になる。いつ、だれが、何をしたのか履歴を残しておくことで、問題発生時の原因究明や不正行為の抑止が可能になる。

情報資産洗い出し、脅威の想定、そして対策の3ステップ… 続きを読む