最新セキュリティマネジメント（第2回）

サイバーセキュリティ経営の重要10項目

2021.07.20

IT活用はビジネスの成長に欠かせない要素だ。しかし、サイバー攻撃で深刻な被害を受けるケースの増加など、セキュリティ面の不安が広がりつつある。経営者はセキュリティ関連のリスクを最小限に抑え、高まる脅威から企業を守る必要に迫られている。そこで今回は、サイバーセキュリティ経営（経済産業省がガイドラインを策定している）のポイントとされる「重要10項目」について解説する。

セキュリティ対策推進のカギは「リーダーシップ」

これまで、サイバー攻撃から企業を守るための対策は「コスト」と捉えられることが多く、経営者にとっては長年悩みの種として扱われてきた。その中で2015年に経済産業省と独立行政法人情報処理推進機構（IPA）が共同で策定したのが「サイバーセキュリティ経営ガイドライン Ver2.0」である。

本ガイドラインは、セキュリティ対策を将来の事業活動、成長に必須なものとして位置づけ、経営者が有効な「投資」として認識することを求めている。ITに関するシステムやサービスを供給する企業、および経営戦略上ITの利活用が不可欠な企業の経営者を対象に、経営者のリーダーシップの下で対策を推進するのが目標だ。

具体的な取り組みの進め方として、サイバー攻撃から企業を守る観点で経営者が認識する必要がある「3原則」、および経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO／Chief Information Security Officer／最高情報セキュリティ責任者）などに指示すべき「重要10項目」がまとめられている。本記事ではこのうち、実務責任者である幹部への指示となる重要10項目について、それぞれの要素を挙げて紹介する。

10項目の指示内容をチェック… 続きを読む