最新セキュリティマネジメント（第3回）

サイバーセキュリティリスクの認識、組織全体での対応方針の策定

2021.08.24

経済産業省が策定した「サイバーセキュリティ経営ガイドライン」の中で、増加するサイバー攻撃から企業を守るため、経営者が担当幹部に指示すべきポイントとして示された「重要10項目」。今回は最初の項目となる「サイバーセキュリティリスクの認識、組織全体での対応方針の策定」について解説する。

「セキュリティは重要な経営リスク」と認識しよう

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「サイバーセキュリティ経営ガイドライン Ver2.0」は、企業がITの利活用を推進していく中で、経営者が認識すべきサイバーセキュリティに関する原則や、経営者のリーダーシップによって取り組むべき項目について取りまとめたものである。

本ガイドラインの冒頭では、経営者が認識すべき3原則として「サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めること」、「ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要」、「サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要」とする項目が挙げられている。

この原則に基づいて、経営者はセキュリティ対策の実務を担当するCISO（最高情報セキュリティ責任者）などの幹部に指示を行うが、ここで大切なのは「有効な施策を具体的に伝える」ことだ。前回では指示すべきポイントとなる「重要10項目」の概要を紹介したが、今回はここで最初に挙げられた項目「サイバーセキュリティリスクの認識、組織全体での対応方針の策定」について解説しよう。

まずは「セキュリティポリシー」の策定から… 続きを読む