最新セキュリティマネジメント（第40回）

認識すべき3原則と指示すべき重要10項目

2024.09.17

経済産業省と独立行政法人情報処理推進機構（以下、IPA）は、企業経営者やCSIO（最高情報セキュリティ責任者）向けにサイバーセキュリティ対策をどのように実践していくかを解説した「サイバーセキュリティ経営ガイドライン」を発行している。併せて、実際に行われている事例を紹介した「実践のためのプラクティス集」も発行している。どちらもセキュリティ強化を考える上で参考になるものだが、ここでは、経営者が認識すべき3原則と経営者が指示すべき重要項目について取り上げる。

対策強化は経営者の3つの原則への認識から

「サイバーセキュリティ経営ガイドライン」は、経営者が認識すべき3原則を挙げている。1つ目は「経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要」としている。

ビジネスのデジタルへの依存度が高まっている今、サイバー攻撃が事業活動に与える影響は大きくなり、被害も深刻化している。経営者はこの事実を認識し、サイバーセキュリティ対策を必要不可欠な投資と捉え、自らリーダーシップをとって必要に応じた対策の推進を主導するよう求められる。

2つ目は「サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要」という点だ。

サプライチェーンというとモノの調達と捉えがちだが、取引にはデータのやり取りも含まれる。サプライチェーンのどこかでサイバー攻撃への対策が不十分だった場合は、そこが侵入口となり重要情報が流出したり、サプライチェーン全体が機能停止に追い込まれたりして、甚大な被害を受ける場合がある。経営者はこれらを常に意識しなければならない。

3つ目に「平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要」としている。ポイントは、平時における積極的なコミュニケーションだろう。平時からサイバーセキュリティリスクや対策に関する気づきや課題を共有しておけば、万が一サイバー攻撃による被害が発生しても互いを信頼し、迅速な対応が可能になるので、転ばぬ先の杖として考えておきたい。

経営者が実施させるべきセキュリティの重要10項目… 続きを読む