サイバーセキュリティ 経営の重要項目

サイバーセキュリティ経営の重要 10 項目

経営者は、サイバー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 等）に対して以下の重要１０項目を指示すべきである。

指示 1 ：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
指示 2 ：サイバーセキュリティリスク管理体制の構築
指示 3 ：サイバーセキュリティ対策のための資源（予算、人材等）確保
指示 4 ：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示 5 ：サイバーセキュリティリスクに対応するための仕組みの構築
指示 6 ：サイバーセキュリティ対策における PDCA サイクルの実施
指示 7 ：インシデント発生時の緊急対応体制の整備
指示 8 ：インシデントによる被害に備えた復旧体制の整備
指示 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
指示 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

（経済産業省 独立行政法人 情報処理推進機構　サイバーセキュリティ経営ガイドライン　Ver2.0 より）

経済産業省より、企業の経営者、セキュリティ対策責任者、およびセキュリティ担当者に向けて、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、取り組むべき項目について取りまとめた「サイバーセキュリティ経営ガイドライン」が策定され、その解説書も IPA（独立行政法人 情報処理推進機構）より公開されています。
このガイドラインでは、経営者は 3 原則を認識して、対策を進めることが重要だとしています。
（1）経営者は、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が必要
（2）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
（3）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
そして、経営者が具体的に CISO（Chief Information Security Officer ）等のセキュリティ対策の実施に責任を持つ立場の人に対し、どのような指示を与えるのかを 10 項目あげています。
まず、経営者がリーダーシップをとったセキュリティ対策の推進をするための、セキュリティリスクの管理体制の構築、リスクの特定と対策の実装、インシデント発生に備えた体制構築までが 1 ～ 8 の指示で、残り 2 つが、サプライチェーンセキュリティ対策の推進と、ステークホルダーを含めた関係者とのコミュニケーションの推進の指示になります。
IPA では、「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集」も公開しており、具体的な例をもとに実践のステップ、実践内容を各指示に照らし合わせ、多くのプラクティスとして解説しています。このプラクティス集では、ページごとに一番上に読むべき対象者が色分けされているので、効率的に活用できます。
また、「インシデント発生時に組織内で整理しておくべき事項」も、エクセルのファイル形式で公開されているので、セキュリティインシデントが見つかった場合に、チェックすべき項目として再確認ができます。
サイバーセキュリティ経営ガイドラインでは、Ver2.0 への改訂に伴い、経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えてしまった場合、経営責任のみならず、法的責任が問われる可能性があるとしています。
企業の経営者は、サイバー攻撃の脅威は、経営課題として経営層が率先して取り組む必要があることを、このガイドラインを通じて再認識すべきでしょう。