最新セキュリティマネジメント（第8回）

セキュリティ対策におけるPDCAサイクルの実施

2022.01.18

経済産業省が策定した「セキュリティ経営ガイドライン」で、経営者が社内に対して指示すべきポイントとして示された「重要10項目」。今回は6番目の項目「サイバーセキュリティ対策におけるPDCAサイクルの実施」について解説する。

「PDCA」を回してセキュリティを改善

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」では、企業のIT活用を推進する上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、経営者がリーダーシップをもって取り組むべき項目がまとめられている。

サイバーセキュリティ対策の効果を高めるためには、個々の問題にその都度対処するだけでなく、取り組みの「継続」が重要になる。継続的な改善方法として知られているものの一つが「PDCAサイクル」だ。P（Plan：計画）、D（Do：実行）、C（Check：評価）、A（Act：改善）という4段階を繰り返し行うことで改善の効果を高めるPDCAサイクルは、業務効率化につながる手法として多くの企業がさまざまな分野で導入している。今回はセキュリティ対策にPDCAサイクルを取り入れるメリットと、効果を最大限に引き出すためのポイントを紹介する。

PDCA実施に必要な体制整備

PDCAの実施に当たっては、それぞれの段階に対応する体制を整備する必要がある。具体的な構築方法を考えてみよう。

・P（Plan：計画）
現在の課題や今後の予測を基に目標を設定し、実行計画を作成する。立案に際してはテーマを明確にするとともに、解決までの道筋が描けるプランを構築する必要がある。

・D（Do：実行）
作成した計画に沿って業務を実行する。進捗状況を詳細に記録し、以後の段階で個別に分析できるようにすることが重要。

・C（Check：評価）
実行した業務が計画に沿ったものかどうかを確認し、評価する。もし計画通りに進まなかった業務が見つかった場合は原因を分析し、改善すべきポイントを明らかにする。

・A（Act：改善）
判明した結果に基づいて、今後の改善策を検討する。その中で作成された改善案を次回の「P」作成に役立てる。

サイバーセキュリティ対策を目的としたPDCAサイクルを実行するためには、さまざまなリスクに継続して対応可能な体制（プ

ロセス）を整備する必要がある。セキュリティ対策は「終わりのない旅」とも例えられるように、一度の対策で完結する類いのものではない。ある課題に対するPDCAサイクルが一旦完了しても、そこには新たな「P」がすでに存在し、休むことなく次のサイクルに取り組む必要がある。常に登場する新しい脅威（リスク）に対応するためのさらなる改善に向けて、らせん状に続くPDCAサイクルを「回していく」ことが欠かせない。

不適切なPDCAは「改善の妨げ」に… 続きを読む