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

PDCAサイクルを継続し、改善を積み重ねることで得られるメリットは、業種・業界を問わず広く知られているのは言うまでもない。ただし、進め方によってはPDCAがむしろ改善を妨げる要因になってしまうケースもある。各段階で発生しうるトラブルの例を挙げてみよう。

・P「目標設定は適切か?」
長期的なPDCAサイクルを考えた場合、課題解決に向けた目標は1サイクルごとに設定することになる。ここで大切なのは「その目標は適正か?」という部分だ。ハイレベルな目標は当然達成が困難で、関係者の意欲をそいでしまう。ただし、あまりに簡単に達成できる目標ばかりでは「慣れ」が生じ、結果的に改善が進まないという結果につながることも考えられる。現状をしっかり把握しつつ、最大限の改善効果が望める目標を定めよう。

・D「活動の記録範囲」
計画に基づく活動を進めることは当然だが、その結果だけを記録している場合は注意が必要だ。例えば目標を達成できなかったケースであっても、内容に触れない「○×」的な記録では、達成までにどの程度の改善が必要なのか不明で、次回のサイクルに向けた検討が難しくなる。特に長期的な取り組みでは、詳細な記録を心掛けよう。

・C「評価基準は公正か?」
PDCAにおける評価は、一般的な業務で行われるものに比べて厳しいといえる。その理由は、評価に何らかの揺らぎや曖昧さが生じた場合、活動全体の失敗につながる恐れがあるからだ。「熱心に取り組んでいた」「一定の成果が認められる」といった評価では具体的な成果を知ることは不可能。このような評価を継続しても改善は望めないだろう。公正で客観的な評価を行い、可能な限り数字で達成度を示す必要がある。

・A「改善に対する意欲」
改善を進める上で重要なのが「意欲」。明らかになった課題を解決するまでの道のりは長く、種類によっては数年以上を費やすことも少なくない。どこまで達成すれば解決とするかは個々のケースによるが、活動に対する慣れが生じ、「この程度でいいだろう」という雰囲気が出てしまうと、PDCAが「掛け声倒れ」の活動になってしまう恐れもある。常に意欲を持って取り組めるよう、必要に応じて課題の見直しや再設定も検討すべきだろう。

「開示」が重要

PDCA継続によるセキュリティ対策を実現するために、もう一つ重要なポイントとなるのが「(情報の)開示」だ。開示対象は組織内(社員・経営層)をはじめ、顧客、取引先、株主、金融機関、行政機関など「ステークホルダー」全般にわたる。

実施した対策の内容は情報セキュリティ報告書、CSR報告書、サステナビリティレポートや有価証券報告書などへの記載を通じて開示を検討しよう。もし適切な開示を行わなかった場合、社会的責任の観点から、事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失うとともに、インシデント発生時に企業価値が大きく低下する恐れがある。

また、PDCAの対象となる脅威は常に変化している。最新の脅威への対応ができているかといった視点も踏まえ、組織のサイバーセキュリティ対策を定期的に見直さないと環境変化に対応できず、新たに発生した脅威に対応できないという事態に陥りかねない。新たなサイバーセキュリティリスクの発見などにより追加で対応が必要な場合には、速やかに対処方針を修正し、状況に応じてセキュリティ診断や監査を受けてシステムやサイバーセキュリティ対策の問題点を検出し、継続的な改善を行う必要があるだろう。

業種、職種を問わず、現代のビジネスシーンで広く使われているPDCAは、セキュリティ分野でも効果が期待できる取り組みの一つだ。業務効率化とともに「大切な情報資産を守る」というテーマに沿ったPDCAサイクルを継続的に回し、企業の成長につなげることの価値は大きい。