最新セキュリティマネジメント（第6回）

サイバーセキュリティリスクの把握と対応計画の策定

2021.11.16

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、経営者が社内に指示すべきポイントとして示された「重要10項目」。今回は4番目の項目となる「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」について解説する。

リスクの把握と対応を推進

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。

サイバー攻撃を受けて業務が停止したり、商品・サービスの提供に支障が出たりした場合、企業の経営は深刻なダメージを受けることになる。不測の事態を未然に防ぐためには、あらかじめ生じる可能性があるリスクの内容を正確に把握し、計画に基づいた対応を行うことが重要だ。今回はこれらのポイントについて解説する。

セキュリティリスクの種類とは

サイバーセキュリティ対策の必要性について、ほとんどすべての企業が認識していることは言うまでもない。ただし、具体的な対策の内容を見てみると、企業によって差があることが分かる。例えば、現時点で重大なリスクではないものの、将来的にリスクとなり得る事項が見つかった場合、直ちに業務を停止して対策を徹底する企業がある一方、通常業務を継続しながら対策を講じる企業もある。取り組み方には企業それぞれ違いがある。

小さなリスクを見逃さず早急に徹底した対策を行う姿勢は企業として望ましいものだが、その都度業務を停止した場合、生産性が落ち、結果として業績低迷につながる可能性もある。しかし、それを恐れて対策を後回しにした企業が経営危機に陥るケースも少なくない。また、「転ばぬ先のつえ」とばかりに詳細な規則を定めて社員に強いた結果、業務効率が低下して売り上げが減少するケースも考えられる。こうした点から、いかに業務効率を落とさず、リスクに対応するか、その両立が大切だ。

サイバーセキュリティ上のリスクとして代表的なものに、情報漏えい・流出による損害がある。それに対して考えられる対策は「予防」、そして「発生時の対応」となる。さらに他にもリスクを遠ざける「回避」や、影響を最小限にするための「移転」などもある。これらの対策について、進め方を検証してみよう。

対策は「低減・回避・移転」で取り組む… 続きを読む