ワンポイント会計基準

vol.300 サイバーセキュリティリスクへの対応について

１．はじめに

ランサムウェア被害を中心とした、サイバーセキュリティ・インシデントの発生が近年増加しています。サイバーセキュリティ・インシデントの発生が、決算・開示実務に影響を与える事例も少なからず見受けられます。

このような状況を受けて、日本公認会計士協会テクノロジー委員会から、2024 年 5 月 30 日に「サイバーセキュリティリスクへの監査人の対応（研究文書）」が公表されました。

2024 年 4 月以降適用されている改訂された内部統制報告制度においても、サイバーリスクの高まり等を踏まえた情報セキュリティ確保の重要性が記載されています。

今回は、研究文書に記載された、財務報告に関連するサイバーセキュリティリスク、サイバーセキュリティリスクに関連する内部統制システムについてご紹介します。

２．財務報告に関連するサイバーセキュリティリスク

サイバーセキュリティ・インシデントには様々な種類がありますが、代表的な手口としては、フィッシングメール、不正アクセス、ランサムウェアをはじめとするマルウェア、ビジネスメール詐欺（BEC）・メールアカウント侵害（EAC）などがあります。

サイバー攻撃により、データ漏えい、データ改ざん、システム停止及びデータ暗号化などの被害が生じた場合、財務報告への影響として損失の見積りが必要になったり、財務諸表を適時かつ正確に開示できなくなるリスクがあります。

財務報告に関連するサイバーセキュリティリスクは企業環境により影響を受けると考えられます。

研究文書では、サイバーセキュリティリスクに関連する企業環境として、以下のものが例示されています。該当するものが多いほど、財務報告に関連するサイバーセキュリティリスクが高い傾向にあると思われます。

・ 企業のビジネスは、ＩＴに強く依拠する傾向にあるか。

・ 企業は多数のＩＴアプリケーションを利用しているか。
・ ＩＴを利用した内部統制に強く依拠しているか。
・ 企業自身がサイバーセキュリティリスクを重要なリスクと識別しているか。
・ 過去にサイバーセキュリティ・インシデントが発生しているか。
・ サイバーセキュリティリスクに関する体制や責任者が明確になっているか。
・ 漏えい時に多額の損失が想定される、個人情報や、企業機密、顧客情報等の機密情報を保有しているか。

３．サイバーセキュリティリスクに関連する内部統制システム

財務報告に関連するサイバーセキュリティリスクは関連する内部統制システムにより低減されます。

研究文書では、サイバーセキュリティリスクに関連する内部統制システムとして以下のものが例示されています。該当するものが多いほど、財務報告に関連するサイバーセキュリティリスクが低く抑えられている可能性が高いと思われます。

・ サイバーセキュリティリスクに関する対応方針があるか。
・ サイバーセキュリティリスクを定期的に再評価しているか。
・ セキュリティに関する教育を実施しているか。
・ 標的型メールに関する注意喚起又は訓練を実施しているか。
・ 子会社のインシデント情報を把握する仕組みがあるか。
・ 定期的な情報資産の見直し及び重要な情報資産がないかを確認しているか。
・ 個人情報や、企業機密、顧客情報等の機密情報の保管に関する統制があるか。
・ 不正なアクセスやインシデントを監視・発見する仕組みがあるか。
・ セキュリティの脆弱性に関する情報を収集する仕組みがあるか。
・ 適時のセキュリティパッチの適用を実施する仕組みがあるか。
・ 物理的媒体への保管、改変不可能な媒体へのバックアップ等、サイバーセキュリティリスクに対応したバックアップを取得する仕組みがあるか。
・ サイバーセキュリティ・インシデントを想定した事業継続計画を策定しているか。
・ サイバーセキュリティリスクやインシデントを開示・報告する仕組みがあるか。

以上