2022 年 11 月

マンスリー・ハイライト　拝啓社長殿

マネジメントのための経営財務情報

今回のテーマ：　サイバーセキュリティとインシデント対応計画

増加するインシデント報告数

2021 年 10 月の本稿では、組織における IT 環境を狙ったサイバー攻撃が、高水準で推移していることをお伝えしました。一般社団法人 JPCERT コーディネーションセンター公表の「インシデント報告対応レポート」によると、2022 年 7 月から 9 月の 3 か月間におけるインシデント件数は 2021 年の 12,723 件から 10,656 件に減ったものの、依然として高い水準であるといえます。またその内訳はフィッシングサイトに分類されるインシデントが 71%、システムの弱点を探索するインシデントが 18%を占めています。

インシデント対応とインシデント対応計画

このインシデントの検知から封じ込め、復旧、さらにはその予防策を含めた体系的な取り組みを「インシデント対応」と呼びます。そしてインシデントが発生した際、適切なインシデント対応を講じるために「インシデント対応計画」を策定しておくことが有効です。

インシデント対応計画

「インシデント対応計画」を定めるには、まず組織内の方針（基本方針の作成と組織内への周知）と役割（責任者や対応チーム構成）を定め、インシデント発生時における指揮系統や責任範囲を明確にする必要があります。次に具体的な取組みとなる「インシデント対応」の基本的フローである

① 報告（見慣れない URL へのアクセス、メール誤送信等、速やかな社内窓口へ連絡）
② 初動対応（情報漏えいの可能性を含めた二次被害防止の応急措置）
③ 調査対応（いつ・どこで・誰が・何を・なぜを整理し、事実の確認とログ情報保全）
④ 復旧対応（早期の暫定措置）
⑤ 事後対応（根本的対策、最終報告書の提示）

について、「インシデント対応計画」に落とし込むことが求められます。「インシデント対応計画」があらかじめ定められていることで、万が一のインシデント発生時においても冷静な対応を実施することが可能となります[i]。

お見逃しなく！

「中小企業活性化パッケージ NEXT」は、経済産業省のホームページで全文を確認することができます（https://www.meti.go.jp/press/2022/09/20220908001/20220908001.html）。また、伴走型特別保証の概要については、中小企業庁のホームページで確認することができます。是非ご一読ください。

---

[i] 情報処理推進機構(IPA)から、「中小企業の情報セキュリティ対策ガイドライン」として経営者が実施すべき指針などが公開されており、情報セキュリティ対策を構築する際には必要な検討事項を学ぶ上でも有用です。

https://www.ipa.go.jp/security/keihatsu/sme/guideline/