自然災害と同等の備えを

セキュリティインシデントが多発

近年、サイバー攻撃による工場停止や医療機関の診療受け付け停止などの報道が相次いでいる。セキュリティインシデント（情報漏えいや情報システムの機能停止、またはこれらにつながる可能性のある事象など）の発生は自社のみならず、顧客や取引先へ影響を及ぼすケースが少なくない。そのため、地震や水害、パンデミックへの対応と同様、情報セキュリティにおいても、事業継続の観点から被害を最小化し、早期に復旧するために、インシデントを想定した備えを行う必要性がある。

そこで、独立行政法人情報処理推進機構（IPA）では、中小企業の情報セキュリティ対策ガイドラインの改訂に合わせて、新たに「中小企業のためのセキュリティインシデント対応の手引き」を公表した。手引きでは、インシデント発生時の対応について、三つの段階に分けて検討事項を説明している。

被害の最小化へ3段階の対応説明

①検知・初動対応

インシデントが疑われる兆候や実際の発生を検知したり、外部からの通報を受けたりした場合は、速やかに情報セキュリティ責任者に報告する。情報セキュリティ責任者は、対応すべきインシデントであるか判断を行い、速やかに経営者に報告する。経営者は、インシデントが事業や顧客に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げ、対応方針を指示する。

初動対応においては、被害の拡大防止を意識する。対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を行う。

②報告・公表

インシデントの被害拡大を防ぐために、二次的な被害が想定される場合などは、本人にその事実を報告する。本人への報告が困難な場合や、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトやメディアを通じて公表する。公表によって被害の拡大を招かないよう、時期、内容、対象などは考慮する必要がある。

インシデント対応後は、被害者や、影響を及ぼした取引先、顧客など関係者に対して、インシデントの対応状況や再発防止策などについて報告する。また、必要に応じて監督官庁などへ報告を行う。

③復旧・再発防止

インシデントからの復旧に当たって、原因を調査し、対応を検討する際は、発覚・発生日時や表面化している事象・被害・影響、発覚から現時点までの時系列での対応経過、現時点で想定される原因などの情報を整理しておくようにする。原因に応じて必要な対応を行うが、自社で調査や対応が難しい場合は、IT製品のメーカー、保守ベンダーなどの外部専門組織や公的機関の相談窓口などに支援や助言を依頼する。

インシデント対応後は、停止したシステムやサービスを復旧し、経営者に対応結果を報告する。また、インシデントを再発させないために根本原因を分析し、抜本的な再発防止策を検討して実施する。

◇　◇　◇

手引きでは、「ウイルス感染・ランサムウエア感染の場合」「情報漏えいの場合」「システム停止の場合」といった場合ごとの解説や、相談窓口、報告先も紹介している。インシデント発生時だけではなく、インシデント発生に備えるために手引きを活用していただきたい。

（独立行政法人情報処理推進機構・江島将和）

「中小企業のためのセキュリティインシデント対応の手引き」はこちら