最新セキュリティマネジメント（第9回）

インシデント発生時の緊急対応体制の整備

2022.02.15

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7番目の項目「インシデント発生時の緊急対応体制の整備」について解説する。

インシデントによる被害を食い止めるには

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。

今回のテーマ「インシデント」とは、出来事・事件を意味する英単語。情報セキュリティ分野では「望まない単独もしくは一連の情報セキュリティ事象、または予期しない単独もしくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（ISO 27000）」と定義されている。

具体的にはサイバー攻撃、マルウエア感染、不正アクセス、情報漏えいなど、重大な結果につながりかねない出来事。これらのインシデントは当然ながら起きないことが望ましいのだが、実際にはどこかで毎日のように発生しているというのが現状だ。その被害を最小限に食い止めるためにどのような体制を整備すべきか、本ガイドラインで示された内容を紹介する。

対応は「初動」がカギに

インシデント発生時に最も重視・優先すべきなのが「初動対応」だ。具体的には発生事実の確認、被害状況の把握、影響範囲の特定といった項目が挙げられる。これらの初動対応に遅れが生じることは被害拡大に直結するため避けなければならない。

企業において情報セキュリティに関する初動対応の役割を担うのは、多くの場合情報システム部門となる。何らかのインシデントが発生した際、当事者もしくは関係者からの知らせを最初に受ける窓口は、基本的に365日、24時間体制で運用するのが原則だ。サイバー攻撃に備えてシステム、ネットワークを常時監視するSOC（Security Operation Center）や、インシデント発生時の対応に特化したCSIRT（Computer Security Incident Response Team）は世界各国で多くの組織が設立されており、最近では企業内に自社のCSIRTを設置する動きも加速している。

緊急事態に即応する体制が整備されていない場合、発生後に下記のようなさまざまな問題が生じてくる。

・コミュニケーション：
原因特定のための調査作業において、組織の内外の関係者間のコミュニケーションが取れず、速やかな対処ができない。

・情報開示:
速やかな情報開示が行われない場合、顧客や取引先などにも被害が及ぶ恐れがあり、損害賠償請求など責任を問われる場合がある。

・報告:
法的な取り決めがあり、所管官庁などへの報告が義務付けられている場合、速やかな通知がないことにより、罰則などを受ける場合がある。

などが挙げられる。即応体制が整備されておらず、こうした問題を生じさせた企業はインシデント後の対応が不十分とみなされ、最悪の場合は社会的信頼を失う事態にも陥りかねない。

インシデント発生後の対応項目

では、インシデント発生後に企業が行うべき対応項目をいくつか挙げてみよう。

・証拠保全、調査の指示
被害原因の特定および解析を速やかに実施するため、速やかな各種ログの保全や感染端末の確保などの証拠保全が行える体制を構築するとともに、関係機関との連携による調査が行えるよう指示する。

・再発防止
インシデント収束後の再発防止策の策定、所管省庁などへの報告手順も含めて演習を行う。再発防止策の検討に当たっては、必要に応じて外部の専門家の知見を活用することも検討する。

・連絡網の整備
緊急連絡網(システム運用、セキュリティベンダーなどの連絡先)、社外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく。

・協力体制の構築
初動対応時にはどのような業務影響が出るか検討し、緊急時に組織内各部署(総務、企画、営業など)が速やかに協力できるよう、あらかじめ取り決めておく。

・諸手続きの確認
関係法令を確認し、法的義務が履行されるよう手続きを確認しておく。

・経営者への報告
インシデントに関する被害状況、他社への影響などについて経営者に報告する。

これらの対応を円滑に進めるためには、当然ながらインシデント発生前にあらかじめ社内の体制を整備し、テストや演習を繰り返してスキルを高めておくことが求められる。また、インシデントの原因調査に当たって参考にすべき事項として、本ガイドラインでは付録として基本項目、情報漏えい、ウイルス感染、不正アクセス、DoS攻撃の5項目について、組織内で整理しておくべき事項を示している。

対応の進め方

初動対応が完了し、インシデントによる被害が確定した後には、そのインシデントがなぜ発生したかを探る「原因調査」を実施する。原因には外部の攻撃者によるもののほか、社員の不注意や不正行為、さらにはシステムの脆弱性などさまざまな種類があり、簡単には特定できないケースもある。本ガイドラインでは被害を受けた人に対する周知を徹底するほか、他組織が同様の攻撃による被害を受けないための情報共有を行う目的で、報告書を作成することを求めている。

その後、対応の締めくくりとなるのが「事後対策」だ。被害に対する対応と、その後の再発防止策を含めた事後対策の実施などについて周知を行うことで、関係者の安心と、他組織の参考となる知見を提供することができる。

なお、これらの対応に関する演習は情報セキュリティに関わる人だけでなく、経営者以下すべての社員が参加して行う必要がある。独自にCSIRTを立ち上げている企業などでは、「専門性の高いメンバーに任せておけば大丈夫」と考えてしまうケー

スもあるようだが、インシデントの発生を防ぐには「(インシデントを)起こさない・見逃さない」という意識を全社員が持つことが重要だ。

また、本ガイドラインの付録C で、インシデント発生時に組織内で整理しておくべき事項をまとめているので参考にしたい。その中ではすべてのインシデントに共通する「基本項目」以外に、「情報漏えい」「ウイルス感染」「不正アクセス」「(D)DoS攻撃」といった主なインシデントについてより詳細な項目を列挙している。例えば「情報漏えい」の項目では、発覚の経緯、原因および経路、情報漏えいの有無、漏えいしたデータの項目および件数、二次被害など、詳細な部分を個別にリストアップして初動対策を考えている。

企業がパソコンやネットワークを利用する上で、インシデントは避けて通れない問題だ。不測の事態に備え、日ごろから情報収集と訓練を欠かさない体制を構築しよう。