最新セキュリティマネジメント（第10回）

インシデントによる被害に備えた復旧体制の整備

2022.03.15

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8番目の項目「インシデントによる被害に備えた復旧体制の整備」について解説する。

速やかな復旧を可能にするために

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、マルウエア感染、不正アクセス、情報漏えいといったインシデントに見舞われた際、当事者である企業にとって最も気になるポイントは「早期の復旧と事業継続」といえるだろう。安全確保のため、インシデント発生後に業務を停止して被害状況を把握し、さらなる拡大防止を図ることは、セキュリティ対策として正しい方法だ。ただし、停止期間の長期化は経営に深刻なダメージを与えるため、可能な限り速やかに復旧させる必要がある。本ガイドラインでは経営者が先頭に立ってサイバーセキュリティ対策を進める重要性を指摘しているが、今回はインシデントからの復旧体制をどのように整備すべきかについて紹介する。

体制構築の進め方

インシデントが発生すると社内は混乱に陥り、業務に何らかの支障が出ることは避けられない。もちろん、その時点の応急措置で無事に復旧するケースも考えられるのだが、サイバーセキュリティ経営をめざす企業の心構えとしては、常に業務停止という最悪の事態を想定し、あらかじめ復旧・業務再開を進めるための体制を構築しておくことが望ましい。

復旧作業の進め方はインシデントの種類や被害状況など、個々の企業により異なるが、コンピューター、ネットワーク関連の問題は情報システム部門が中心的な役割を果たしているケースが多い。ただし、インシデントによる混乱で現場からの問い合わせが殺到したり、社外ベンダーなどとの交渉対応に追われたりする結果、本来優先して取り組むべき復旧作業が進まず、時間を要してしまう場合がある。これによって長時間業務が停止するような事態に陥ってしまうと、企業の経営そのものが深刻なダメージを受けることは明らかだ。復旧体制の構築に当たっては、速やかに復旧するため、担当者が的確に関係機関との連携や復旧作業を実施できるよう指示することが求められる。

また、日ごろから復旧手順に従った演習を実施し、復旧までの時間を短縮するとともに、インシデント発生時の混乱を最小限に抑えるための取り組みも重要だ。この演習については前回解説した「サイバーセキュリティ経営ガイドライン Ver2.0」の指示7「インシデント発生時の緊急対応体制の整備」の付録Cに掲載されている項目を参照し、組織内であらかじめ手順を確認しておきたい。

一方、早期復旧に向けた作業を開始するとともに、取引先など関係者にも現在の状況を説明する必要が生じる。その内容

を挙げてみよう。

①インシデント発生の事実
発生日時、インシデントの具体的な内容、業務停止に至った経緯などを説明する

②被害状況
現時点で判明している被害、および今後発生する恐れのある事柄について説明する

③復旧予定
業務再開に向けた作業の内容、判明している復旧予定日時を提示する

これらの項目はインシデントの種類、被害程度にかかわらず速やかに発表する必要があることは言うまでもない。復旧作業に追われて発表が遅れてしまうと、最悪の場合「(インシデント発生を)隠ぺいした」と捉えられ、社会的な信頼を失う恐れがある。発生を確認したら直ちに担当部署に報告し、営業時間外であっても発表できる体制を整備しておく必要がある。

整合のとれた計画策定を

業務停止状態からの復旧時期は「速やかに」と発表されるケースが多いが、「明日の営業開始時間までに」「本日〇〇時までに」というように明確な期限、目標を示すことは、全ての関係者にとってメリットがある。

目標策定に当たっては、災害など緊急事態発生時の被害を抑えて事業継続、復旧をめざすBCP(事業継続計画)と整合させることが大切だ。例えば、地震で工場が被災した際には操業を停止し、被害を免れた他の工場で事業が継続できるようにするのだが、このような計画はサイバーセキュリティ分野の「災害」であるインシデントでも必要になる。データの保護、バックアップ活用、予備システム運用など、復旧までのプロセスを計画に織り込み、組織全体として整合のとれた目標策定が可能になる。

すでにBCPを策定している企業では、事業継続を困難にする脅威、リスクの1つとしてインシデントを捉え、他の災害と同様の考え方・手順で対策を進めることで復旧にかかる時間を効率よく短縮できる。まだBCPが整備されていない状態であっても、インシデント対応を契機に経営リスクの全体像を把握し、サイバーセキュリティを含めた事業継続計画を策定する価値は大きいといえる。

演習で対応力をアップしよう

インシデントへの対応力を高めるための演習、訓練は有効な方法だ。その実施に当たって注意点を示しておく。まず挙げられるのは、「業務停止に陥る状況の再現は難しい」ということ。多くの企業にとって、たとえ一時的であっても全社のシステムを完全停止することは困難なことから、演習は停止した前提(設定)で行われるケースが多い。しかし、実際に発生したインシデント事例では、予備システム自体の不具合やバックアップデータの消失といった予期せぬ出来事が大きく影響し、早期復旧を妨げているのが実情だ。演習では可能な範囲で実際にシステムを停止するなど、「想定外の状況」を減少させる取り組みが求められる。

また、演習実施に際しては、できるだけ多くの関係者が参加できるよう工夫することがポイントになる。インシデントは部署や役職を問わず、あらゆる場面で発生する可能性がある。アルバイト、派遣のスタッフや、非常勤、在宅勤務の社員を含めた大規模な演習は対応力を高めるとともに、関係者のモチベーション維持にも有効だ。

なお、本ガイドラインで提示されている復旧体制は、社内に情報セキュリティ担当部門を持つ企業をモデルに構成されている。担当部門を置かず、外部ベンダーなどにセキュリティ業務を委託している企業では、必要に応じて委託業者に対して、インシデント対応に関するヒアリングを行い、有事の際の対応や業務の役割分担などを協議しておき、混乱しないよう取り決めておくべきだろう。