中小企業の

セキュリティー対策

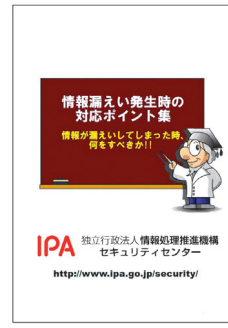
事故後の対応 検討を

適切な処置で被害を最小限に

マイナンバー法や改正個人情報保護法が施行され、情報セキュリティー対策の重要性はますます強く認識されるようになったが、民間企業、公的機関を問わず情報漏えいなどの事故や事件の報道が後を絶たない。

企業として十分な情報セキュリティー対策を行うことにより、情報漏えいを未然に防ぐことが重要ではあるが、いかに対策を行なっていても情報漏えいを完全に防ぐことは難しい。そのため、情報漏えいが発生してしまったときに、速やかに適切な処置を行うことによって被害を最小限に留めることが重要だ。しかし、情報セキュリティーの専門家がいない中小企業においては、インシデント対応マニュアルや対応ノウハウを持っていない場合が多く、いざそのような事故や事件が起きてからどうしたらよいか苦慮することが多いというのが現状といえる。

独立行政法人情報処理推進機構（ＩＰＡ）では、情報漏えいが発生した時に参考となる小冊子「情報漏えい発生時の対応ポイント集」をウェブサイト（https://www.ipa.go.jp/security/awareness/johoueiji/）で公開している。情報漏えい対応の作業ステップと、ウイルスや誤送信、紛失・盗難など情報漏えいタイプごとの留意点、個人情報や公共性の高い情報など流出した情報の種類ごとの留意点、通知・報告・届け出における留意点などについて分かりやすく解説しているので情報漏えい対応の参考にしてほしい。



情報漏えい発生時の対応ポイント集

押さえておくべき五つの原則

「情報漏えい発生時の対応ポイント集」では、情報漏えい対応に当たって五つの原則を掲げている。

原則1：被害拡大防止・再発防止の原則

情報漏えいが発生した場合に最も重要なことは、情報漏えいによって引き起こされる被害を最小限にとどめることである。また、一度発生した事故・事件は二度と起こることのないよう再発防止を図る。

原則2：事実確認と情報の一元管理の原則

情報漏えい対応において、憶測や類推による判断や不確かな情報に基づく発言は混乱を招くこととなる。企業内の情報を一カ所に集め、外部に対する情報提供や報告に関しても窓口を一本化し、正しい情報の把握と管理を行う。

原則3：透明性・開示の原則

被害拡大防止や類似事故の防止、企業の説明責任の観点から必要と判断される場合には、企業の透明性を確保し情報を開示する姿勢で臨むことが好ましい。情報公開により被害の拡大が見込まれるような特殊なケースを除いては、情報を公開することを前提とした対応が企業の信頼につながる。

原則4：チームワークの原則

情報漏えい対応においては、さまざまな困難な判断を迅速に行わなければならず、精神的にも大きな負担がかかる。また、経営、広報、技術、法律など、さまざまな要素を考慮する必要があるため、組織として対応していくことが重要である。

原則5：備えあれば憂いなしの原則

情報漏えいなど事故・事件が発生した時のことを想定し、あらかじめ緊急時の体制や連絡要領などを準備しておく。また、緊急時にどう対応するべきか、方針や手順を作成し、日頃から訓練しておく。

このように、技術や法務の担当を選任することが難しい中小企業こそ、情報セキュリティー対策の一環として、情報漏えいなどの事故や事件の対応についても検討しておくことが望まれる。

（独立行政法人情報処理推進機構・江島将和）