中小企業の

セキュリティー対策

―24―

後を絶たない事故

情報漏えいは不注意から

組織や企業において、メールの誤送信や重要情報を保存した情報端末（PCやスマートフォンなど）・記録媒体（USBメモリーなど）の紛失、重要書類（紙媒体）の紛失など、情報管理に対する意識の低さや確認漏れなどによる個人情報や機密情報の漏えい事故が後を絶たない。独立行政法人情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威2019」（https://www.ipa.go.jp/security/vuln/10threats2019.html）でも、「不注意による情報漏えい」が2018年版の12位から返り咲き、10位にランキングしている。

18年も不注意による情報漏えいが多く報道されている。

11月、テレビ局のディレクターが、宗教団体に関する住民インタビュー音声ファイルのダウンロード先情報を含むメールを、誤って宗教団体側に送信した。また、同月、業務委託先のディレクターが、放送素材を入手できる情報を含むメールを第三者に誤送信した。これらメールの誤送信が立て続けに発生したことに対して、テレビ局は謝罪文を掲載し、情報管理の厳格化に努めていくとしている。

12月、大手ガス事業者の業務委託先企業の作業員が、住所や氏名など421世帯分の顧客情報を記録した業務用携帯端末と制服を紛失したことを2日後に公表、その4日後に紛失物を無事発見したことを公表している。

これら不注意による情報漏えいでは、取り扱う情報の重要性に対する認識不足や情報を取り扱う際の本人の状況（体調不良や急ぎの用事など）、組織規定および確認プロセスの不備など、さまざまな要因が考えられる。

しかし、情報漏えいによる影響は、社会的信用の失墜やそれに伴う経済的損失が発生するだけでなく、場合によっては、漏えいした情報が悪用され、二次被害が発生することもある。企業として組織的に対策に取り組む必要があるだろう。

4月は入社シーズン 従業員教育の徹底を

不注意による情報漏えいを減らすためには、例えば企業は次に挙げる項目に取り組む必要がある。

■情報リテラシーや情報モラルの向上

・従業員のセキュリティー意識教育

・組織規定および確認プロセスの確立（特定の担当者への業務集中が発生しないような体制の構築も重要）

■被害の予防（被害に備えた対策含む）

・確認プロセスに基づく運用

・情報の保護（暗号化、認証）

・外部に持ち出す情報や端末の制限

・業務用携帯端末の紛失対策機能の有効化

■被害の早期検知

・問題発生時の内部報告体制の整備

・外部からの連絡窓口の設置

■被害を受けた後の対応

・上司および社内の事故対応チームへの連絡

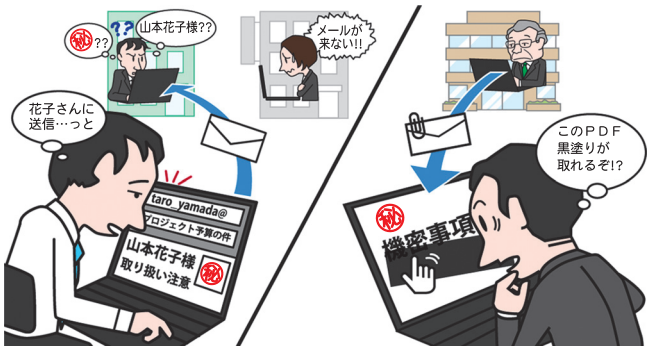
・影響調査および原因の追究、対策の強化

・被害拡大や二次被害要因の排除（ウェブサイトへの誤った情報公開の場合、非公開にするなど）

・必要に応じて、漏えいした内容や発生原因の公表

4月は入社や人事異動のシーズンである。研修などを通して、一度の過失が組織の信用を大きく脅かす可能性があることを従業員に認識してもらい、被害の予防や発見した後の対処の社内ルールを理解してもらうなど、企業として徹底した対策を取ることが望まれる。

（独立行政法人情報処理推進機構・江島将和）



不注意による情報漏えい