サイバー被害 通知義務化
個人情報漏洩の全員に　企業の対応不可避

2020/7/16付 | 日本経済新聞　朝刊

政府の個人情報保護委員会はサイバー攻撃で個人情報が漏洩した企業に対し、被害が発生した全員への通知を義務付ける。違反には最高で1億円の罰金を科し、悪質な場合は社名も公表する。2022年春にも実施する。対応を誤れば訴訟リスクも高まり、企業は厳密な対応が必要になる。

東京商工リサーチによると12～19年に上場企業とその子会社で個人情報漏洩・紛失を公表した企業は372社で、事故数は685件あった。漏洩・紛失した可能性のある個人情報は累計8889万人分に上る。

3504万件が流出した14年のベネッセホールディングスのような大規模な例がある一方、事故数の約8割は漏洩・紛失件数が1万件未満だ。

欧米では通知・報告が義務

	本人への通知	当局への報告	義務の対象・内容
日本（現在）	×	×	努力義務
日本（2022年春）	○	○	①サイバー攻撃による被害 ②病歴などの要配慮情報 ③大量に漏洩した場合
米国（カリフォルニア州）	○	○	社会保障番号や免許証、クレジットカードの情報など
欧州	○	○	72時間以内に報告義務。権利侵害が大きい場合は通知

個人情報の流出を一人ひとり通知する企業はあるものの、現時点で法律上、個人への通知は企業の判断に委ねられている。国際大学GLOCOM客員研究員の楠正憲氏は「情報流出の確認は難しく、可能性があっても企業が公表していない場合もありうる」とする。

6月に成立した**改正個人情報保護法（総合2面きょうのことば）**では、個人への通知義務は「個人の権利に害を与える恐れが大きい場合」とした。個人情報保護委は厳密なルールを運用規則に明記し企業があいまいな対応で済ませられなくする。

サイバー攻撃などの不正アクセスが原因の場合には例外なく通知を義務付ける。サイバー攻撃は個人情報の闇サイトへの転売や詐欺など悪用が目的の場合が多く、米ベライゾンによると企業のデータ漏洩の7割は外部からの攻撃が原因だ。

サイバー被害が原因でなくても、個人の病歴など影響が深刻な場合や、人数が膨大な場合などは通知義務の対象にする。

一人ひとりへの通知には詳細な調査が必要になる。現在はホームページへのおわびの掲載で済ませたり、漏洩の発生だけをメールで伝えたりするケースも多い。今後は個別に詳細な情報を伝えることが求められる。

企業はデジタルフォレンジックと呼ぶ解析作業を通し、通信記録からメールアドレスや銀行口座、商品の購入履歴など流出データの種類を調べる。パソコン1台あたり100万円以上かかるとされ被害の範囲が広がればコストが膨らむ。

ルールが明確になれば不備があった場合の訴訟リスクも高まる。米国では集団損害賠償請求への対応やシステム改修、クレジットカードの再発行などを含めて推定損害額が10億ドルにのぼったり経営破綻に追い込まれたりしたケースもある。

米カリフォルニア州はデータ侵害通知法で個人への通知を義務にし、欧州の一般データ保護規則（GDPR）は72時間以内の報告を求める。杉本武重弁護士は「欧米は不正アクセスによる情報漏洩への対応が厳しい。日本も今回の義務化でグローバルスタンダードに近づく」と指摘する。

欧米では原因調査や通知の費用を補償するサイバー保険の市場規模が35億ドルを超える。国内ではサイバー保険を提供する東京海上日動火災保険がTMI総合法律事務所系のコンサルティング会社と提携し、フォレンジック調査や通知の支援業務も始める。国内のサイバー保険の加入率は1割程度で、規制強化に対応するサービスの市場が広がる可能性がある。