

個人データ漏えい時の対応

Q

昨今、企業において、事務ミスや外部からの不正アクセス等により、個人情報が入部漏えいしたという事例に関する公表や報道をよく目にします。当社でも、雇用する従業員情報や、お客様情報等を保有しています。が、万一、このような情報が外部に流出してしまった場合には、どのような対応をとるべきでしょうか。

A

1. 個人データの漏えい

後述するとおり、現行の「個人情報の保護に関する法律」（以下「法」）および「個人情報の保護に関する法律施行規則」（以下「規則」）は、個人データの漏えいが生じた場合に、事業者が一定の対応を講じ、ることを義務付けています。ここにいう「個人データ」とは、法の定める個人情報のうち、

個人情報データベース等（個人情報を含む情報の集合物であつて、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成したもの、又はコンピュータを用いずに個人情報を一定のルールに従って整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であつて、目次、索引その他検索が容易にされたもの）を構成する情報を指します（法16条1項・3項）。具体的には、企業が保有するデータベースや名簿に含まれる個人情報、原則として、いずれも「個人データ」に当たります。また、「漏えい」とは、個人データが外部に流出した事態全般を指す概念であり、例えば、個人データを記載した電子メールを第三者に誤送信した場合、クラウド上のストレージに保管

した個人データが設定ミス等によってインターネット上で一般に閲覧された場合、第三者による不正アクセスにより個人データが窃取された場合等は、いずれも「漏えい」に当たります（個人情報保護委員会^{（注）}「個人情報の保護に関する法律についてのガイドライン（通則編）」令和8年6月一部改正。以下「ガイドライン通則編」3・5・1・2参照）。

2. 漏えい時の対応

（1）漏えい等の報告（速報、確報）

個人データの漏えいが生じた場合で、以下の①から④のいずれかに該当するときは、個人の権利利益を害するおそれがある個人情報保護委員会に報告する義務が生じます（法26条1項、規則7条）。

①要配慮個人情報が含まれる個人データ（高度な暗号化その

虎門中央法律事務所
（商工研相談業務委嘱先）
弁護士

高橋泰史

他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下、②から④の類型において同じ）の漏えいが発生し、又は発生したおそれがある事態

②不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

③不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であつて、個人データとして取り扱われることが予定されているものを含む）の漏えい等が発生し、又は発生したおそれがある事態

④個人データに係る本人の数が1000人を超える漏えい等が発生し、又は発生したおそれがある事態

れがある事態

例えば、事業者が管理する顧客のクレジットカード番号を含む個人データが漏えいした場合、②に該当する事態に当たるとして、また、事業者の保有するデータベースに対して第三者から不正アクセスが行われ顧客の氏名・住所が漏えいした場合は、③に当たるものとして報告対象となると考えられます（ガイドライン通則編3・5・3・1参照）。

このような場合、個人データの漏えいが発生した事業者は、速やかに（個別事案によるものの、事業者が事態を知ってから概ね3～5日以内とされます）、個人情報保護委員会ウェブサイトに上の報告フォームに所定の事項を入力して報告を行う必要があります。

これは、いわゆる「速報」といわれるものであり、事態の概要（発生日、発覚日、事実経過等）、漏えいした（おそれのある）個人データの項目、当該個人データに係る本人の数、原因、本人に対して行った措置、公表実施状況等について、事業者が、

報告時点で把握している内容を報告することが求められます（規則8条1項）。

その上で、事業者は、報告対象となる事態を知ったときから30日以内（対象となる事態が③に該当する場合は60日以内）に、改めて確定的な報告をすることが義務付けられます（規則8条2項）。これは、いわゆる「確報」といわれるものであり、原則として、この期限までに、速報の対象とされているのと同様の事項の全てについて報告する必要があります。

(2) 本人に対する通知

個人データの漏えいを生じた事業者は、漏えいに関する事案が、前述(1)の①から④の報告対象となる事態のいずれかに該当する場合、原則として、当該個人データに係る本人に対し、事態の概要、漏えいした（おそれのある）個人データの項目、原因、二次被害又はそのおそれの有無及び内容等を、速やかに通知する必要があります（法26条2項、規則10条）。

この点、通知方法については、法令上、特定の様式が定められ

ているわけではありませんが、文書の郵送や電子メールの送信など、本人にとってわかりやすい形で行うことが望ましいといえます。

また、本人の連絡先が不明であるなど、個別の連絡が困難である場合には、通知に代えて、本人の権利利益を保護するために必要な措置をとることが認められています（法26条2項）、そのような場合、当該事業者のウェブサイト等において漏えいに係る事案の公表が適切であることが多いと思われます。

3. まとめ

事業者において個人データの漏えいが発覚した場合には、前記のスケジュールに沿って、個人情報保護委員会に対する速報を行った上、遅くとも確報の期限までに事態を詳細に把握しなければならず、これと併行して場合によっては多人数に及ぶ本人への通知を実行することが必要となります。

また、漏えいの態様や情報の性質によっては、法律上の義務の履^{りせん}践とは別途、本人に対する

情報提供や注意喚起のため、事業者が積極的に事案を公表することを検討すべきケースもあります。

さらに、第三者による不正アクセス等の事案においては、事業者自身による調査には限界があり、詳細な原因や影響範囲を分析するために専門業者へ委託してデジタル・フォレンジック^{（注2）}を実施することが必要になるなど、限られた期間内に多くの事項に対応する必要性に直面することが想定されます。

事業者においては、個人情報の漏えいが生じた場合に必要に対応について、平時から整理しておくことにより、万一の事態に、速やかな初動対応がとれるように備えておくことが望ましいでしょう。

（注1）個人情報（特定個人情報を含む）の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報の適正な取り扱いの確保を図ることを任務とする独立性の高い機関（個人情報保護委員会ウェブサイトから抜粋）

（注2）パソコンやスマートフォンなどのデジタルデバイスに残されたデータを分析し、サイバー犯罪や不正アクセスの証拠を収集する技術とその手続き

