知って納得！
覚えて安心！

個人情報保護法の１～１０まで

個人情報の漏えい・流出に関するニュースや新聞報道を日々、目にされることと思います。
NPO 法人日本ネットワークセキュリティ協会の調査によると、２００９年の個人情報漏えい事故は 1539 件、漏えい人数は約 572 万人ということでした。大企業の数万人規模の情報漏えい事故ともなると、ニュースでも大きく取り上げられます。このような漏えい事故は、企業ブランドの失墜、信用の低下、被害者への損害賠償や訴訟への対応と、物心ともに大きな痛手となり、個人情報保護法の罰則もありえます。また、個人や小規模事業者の場合には、１件のＦＡＸの誤送付が事業の根幹を揺るがす事態にもなりかねません。
とはいえ、個人情報漏えい事故は日々の業務の中で防ぐことが可能ですし、万一事故が起きても落ち着いて的確な対応をすることで、被害を最小限にとどめることができます。今回は「万が一、自社で個人情報漏えい事故が発生したら」の「もしもの時の対応」を考えてみましょう。災害時の避難訓練のようなお気持ちで、自社に照らしながらお付き合いください。

■個人情報漏えい（流出）とは

個人情報の漏えいとは、どのような状態を指すのでしょう。また、いかにして起こるのでしょう。個人情報の漏えいとは、企業や各種団体が保有している個人情報を、その情報に該当する者の意図に反して外部に流出させたり、情報が第三者に渡ったりすることをいいます。かつては名簿やリストなど紙ベースだった個人情報ですが、ＩＴ化の進展により電子データとしても扱われるようになりました。ＵＳＢメモリなどの記憶媒体は、持ち運びしやすく扱えるデータ量も多いので、事故の規模も大きくなる傾向があります。個人情報漏えい事故が起きる原因は、「ＦＡＸや送付物の誤送付やパソコンの誤操作」、「管理不備による誤廃棄や紛失」、「内部犯行による情報の持ち出しや抜き取り」、「窃盗」、「ＰＣや記憶媒体を社外に持ち出した際の盗難や置き忘れ」、「ファイル共有ソフト（Winny など）やコンピューターウィルスの感染による漏えい」、「インターネット上の意図せぬファイルの開示」、「ハッキングによる情報の盗み出し」などがあります。

■個人情報漏えいが発生！その対策のポイント

続いて、個人情報の漏えいが発覚した際の対応のポイントをあげてみます。

●関係者を招集し事実を把握する：日頃から緊急連絡先リストを作っておきましょう。把握すべき情報として「どのような情報が流出したか」「どのくらいの規模か」「どのような漏えい経路か」「現時点で具体的な被害は起きているか、起きうる被害の内容」を把握します。※緊急連絡先は、事故対策責任者、システム管理者、営業責任者、社長、関連委託先やデータセンター、所管の主務大臣、顧問弁護士などが考えられます。

●対応策を検討する：漏えいがシステムやネットワークに関係する場合は、システムの停止や関係するＰＣやサーバーのネットワークを切断しログを保存します。また、問合せに備えて窓口の設置と対応ルールも明確にしておきます。継続して原因や漏えい元を調査し、二次被害や情報の拡散防止を図ります。事件性がある場合には警察へ通報します。監督官庁への報告や関係者への通知の準備も進めます。

●関係者への通知と謝罪：情報漏えいの該当者には文書で速やかに通知します。漏えいした内容や事故の経緯、事故によって想定される二次被害などのリスクとその防止策、問合せ窓口を明記します。被害が発生した場合にはその補償も検討しておく必要があります。

●事故対応の終結：必要に応じて事故を公表し、再発防止策も策定しましょう。訴訟に発展するような場合には証拠資料の準備が必要です。個人情報漏えい事故対応においても、事実の隠蔽、不適切な態度や言動は事態の悪化を招きかねません。迅速かつ的確な対応はもちろん、誠実な企業姿勢を伝えることがより大切です。