中小企業の

セキュリティー対策

改正個人情報保護法に対応を

チェックすべき基本5事項

改正個人情報保護法が5月30日に全面施行される。改正法により、取り扱う個人情報の数が5000人以下の事業者を適用除外とする例外規定が廃止され、中小企業・小規模事業者も個人情報保護法の適用対象となる。中小企業・小規模事業者が対応を進める上では、個人情報保護委員会による「個人情報保護法の五つの基本チェックリスト」を活用して対応状況の確認から始めるとよいだろう。チェックリストの内容は次のようになっている。

①取得のルール

個人情報を取得する時は、例えば、購入商品の発送のため、購入商品のサポート情報を提供するためなど、あらかじめ何に使うか利用目的を決めて、本人に伝える必要がある。

②利用のルール

取得した個人情報は決めた目的以外のことには使うことはできない。例えば、賞品を発送するために取得した個人情報を使って、自社の商品の宣伝を行ってはいけない。

③保管のルール

取得した個人情報をパソコンで管理したり、名簿などにまとめたりする場合は、安全に管理する必要がある。例えば、電子ファイルであればパスワードを設定する、紙媒体であれば施錠できるところに保管するなど、自社の状況に応じた安全管理措置（情報セキュリティー対策）を講じる必要がある。

④提供のルール

個人情報を本人以外の第三者に提供する場合は、原則、本人の同意が必要になる。ただし、法令に基づく場合、人命に関わる場合で本人から同意を得ることが困難なとき、業務を委託する場合などは本人の同意を得なくても、個人情報を第三者に渡すことができる。

⑤開示のルール

会社が保有する個人情報について本人から開示や訂正などを請求されたら、企業は対応しなければならない。また、その個人情報の利用目的を問われた場合に、しっかりと答えられるようにしておく必要がある。

データ管理で漏えい防止

個人情報取扱事業者は、その取り扱う個人データ（個人情報データベースなどを構成する個人情報）の漏えい、滅失または毀損（きそん）の防止その他の個人データの安全管理のため、「組織的」「人的」「物理的」「技術的」の四つの側面から安全管理措置を講じなければならない。

「組織的安全管理措置」とは、安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況の確認を行うことをいう。

「人的安全管理措置」とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育などを行うことをいう。

「物理的安全管理措置」とは、入退館（室）の管理、個人データの盗難の防止など、個人データに対する物理的な措置をいう。

「技術的安全管理措置」とは、個人データおよびそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視など、個人データに対する技術的な措置をいう。

なお、個人情報保護委員会が発行する「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）」では、別添として講ずべき安全管理措置の内容を具体的な手法の例示も交えて解説しているので参考にするとよいだろう。また、独立行政法人情報処理推進機構（IPA）が発行する「中小企業の情報セキュリティ対策ガイドライン」も安全管理措置を規程化する上で有用であるため参考にしてほしい。

（独立行政法人情報処理推進機構・江島将和）

個人情報保護法の５つの基本チェックリスト

その１ 個人情報を取得するときのルール 個人情報を取得する際、何の目的で利用されるかご本人に伝わっていますか？	□
その２ 個人情報を利用するときのルール 取得した個人情報を決めた目的以外のことに使っていませんか？	□
その３ 個人データを保管するときのルール 取得した個人データを安全に管理していますか？	□
その４ 個人データを他人に渡すときのルール 取得した個人データを無断で他人に渡していませんか？ ※委託の場合は除きます。	□
その５ 本人から個人データの開示を求められたときのルール 「自分の個人情報を開示してほしい」とご本人から言われて、断っていませんか？	□

※個人情報保護委員会の冊子より抜粋