梅ちゃん先生の法律相談

第15回

「個人情報の保管時の注意点」

公益社団法人日本照明家協会監事　梅本寛人（弁護士）

1　個人情報取扱事業者が守るべき4つのルール

今回も、前回に引き続き、個人情報保護法が定める各種規制内容についてお話を続けたいと思います。

個人情報保護法が定める個人情報の取り扱いについてのルールは、大きく分けて以下の4つにまとめられます（「梅ちゃん先生の法律相談（第13回）」（1月号掲載）参照）。

① 個人情報の**取得・利用時**のルール（個人情報を「**勝手に使わない！**」）
② 個人情報の**保管時**のルール（個人情報を「**なくさない！ 漏らさない！**」）
③ 個人情報の**提供時**のルール（個人情報を「**勝手に人に渡さない！**」）
④ 個人情報の**開示請求等への対応**（個人情報の「**お問合わせに対応！**」）

今回は、以上のうち、個人情報の保管時のルールについて説明いたします。

2　保管時のルール

(1) データ内容の正確性の確保

前回のコラム（「梅ちゃん先生の法律相談（第14回）」）において、個人情報取扱事業者は、個人情報を取り扱うに当たり、その個人情報の**利用目的をできる限り特定**しなければならない（個人情報保護法第15条第1項）と説明しました。

そして、この点も前回のコラムにおいて少し触れましたが、個人情報取扱事業者は、**利用目的の達成に必要な範囲内で「個人データ」を正確かつ最新の内容に保つよう努めなければなりません**（個人情報保護法19条）。この「個人データ」とは、個人情報データベース等を構成する個人情報のことであり（個人情報保護法2条6項）、「個人情報データベース等」とは個人情報を含む情報の集合物で、容易に検索できるように体系的に構成されたものです（例えば「従業員名簿」や「会員名簿」のようなもの。個人情報保護法2条4項）。

すなわち、個人情報取扱事業者は、個人情報データベースの作成の時に、入力の誤りの有無や確認方法を整備し、又、作成後も情報が古くなっていないか、定期的に更新するようにし、そのための具体的な方法を定めておくことが求められます。ただし、個人情報データベース内のすべての「個人データ」を常に最新情報にしておくことまでは求められず、個人情報の利用目的の達成に必要な範囲で、最新の内容にしておけば足ります。例えば、年に1回、新年度の「会員名簿」を作成するという場合、それが個人情報の「利用目的」ですから、その会員の個人データを毎日、常に、最新の内容に保つことまでは不要で、年に1回の「会員名簿」を作成する前には、個人データの正確性を確保しておけば足りるということになります。

(2) 不要になった個人データの消去

個人情報取扱事業者は、**個人データを利用する必要がなくなったときは、その個人データを遅滞なく消去する努力義務を負います**（個人情報保護法19条）。

上記の「利用する必要がなくなったとき」というのは、個人情報の利用目的が達成され、その利用目的との関係では個人データを保有する合理的な理由が存在しなくなった場合や利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合とされています。

例えば、ある商品販売のキャンペーンの懸賞品の送付のために、そのキャンペーンに応募した者の個人データを保有していたところ、懸賞品の発送が終わり、不着対応等のための合理的な期間が経過した場合には、個人データを「利用する必要がなくなったとき」に該当し、集めた個人データを速やかに消去するように努めなければなりません。

なお、別の法令により、保存期間等が定められている場合は、その期間は消去してならず、保管を継続しなければなりません。

(3) 個人情報の安全管理措置

個人情報取扱事業者は、取り扱う個人データの漏えい、滅失、き損の防止等の**安全管理のために必要かつ適切な措置**を講じなければなりません（個人情報保護法20条）。この「安全管理のために必要かつ適切な措置」のことを略して「**安全管理措置**」といいます。

さて、「安全管理措置」とは、具体的にはどのようなことをすればよいのでしょうか？個人情報保護法の条文では「必要かつ適切な措置」としか書かれておらず、これでは具体的な内容は不明ですが、この点は、個人情報保護委員会が策定した「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）」（以下「ガイドライン」と

します）において詳細に定められています。

ガイドラインでは、個人情報取扱事業者が講ずべき安全管理措置について、以下の6つに類型化し、それぞれ、具体的な手法を例示しています。

①基本方針の策定
②個人データの取扱いについての規律の整備
③組織的安全管理措置
④人的安全管理措置
⑤物理的安全管理措置
⑥技術的安全管理措置

それぞれの項目についての具体的内容は、次のとおりです。

①基本方針の策定

個人情報取扱事業者は、個人データの適正な取扱いの確保について組織として取り組むため、「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問及び苦情処理の窓口」等の項目を定めた基本方針の策定が重要とされています。

②個人データの取扱いについての規律の整備

個人情報の取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定するものとされています。

③組織的安全管理措置

a 組織体制の整備（例：個人情報保護管理者の設置、部署や従業者の役割・責任の明確化、監査実施体制の整備など）
b 規程等の整備と規程等に従った運用（例：情報システムの安全管理措置に関する規程等の整備とそれに従った運用、監査証跡の保持など）
c 取扱状況を一覧できる手段の整備（例：個人データ取扱台帳の整備など）
d 安全管理措置の評価、見直し及び改善（例：監査計画の立案・実施など）
e 事故又は違反への対処（例：事故発生時の対応手順の整備など）

④人的安全管理措置

a 会社内で取り扱う個人データについての採用時における従業者との非開示契約の締結、委託契約等における委託元と委託先間での非開示契約の締結など
b 従業者に対する内部規程等の周知・教育・訓練の実施

⑤物理的安全管理措置

a 入退館(室）管理の実施（例：個人データを取り扱う業務を、入退館（室）管理を実施している物理的に保護された室内で実施することなど）
b 盗難等の防止（例：個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止、個人データを含む媒体の施錠保管、氏名・住所・メールアドレス等を記載した個人データとそれ以外の個人データの分離保管など）
c 機器・装置等の物理的な保護（例：盗難、破壊、破損、漏水、火災、停電等からの物理的な保護など）

⑥技術的安全管理措置

a アクセスにおける識別と認証（例：ID/パスワードによる認証、生体認証など）
b アクセス制御（例：アクセス権限を付与するべき者の最小化など）
c アクセス権限の管理（例：アクセスできる者を許可する権限管理の適切 かつ定期的な実施など）
d アクセスの記録（例：アクセスや操作の成功と失敗の記録など）
e 不正ソフトウェア対策（例：ウイルス対策ソフトウェアの導入など）
f 移送・送信時の対策（例：暗号化等の秘匿化など）
g 情報システムの動作確認時の対策（例：情報システムの変更時に、セキュリティが損なわれないことの検証など）
h 情報システムの監視（例：情報システムの使用状況の定期的な監視、アクセス状況の監視など）

個人情報取扱事業者が講ずべき安全管理措置の内容は、以上のとおりガイドラインにおいて詳細が例示されていますが、ガイドラインの内容は**あくまでも例示**であり、**事業者の事業規模や取り扱う個人データの性質や量等に応じ、実情に見合った措置を講ずることが重要**です。

なお、個人情報取扱事業者であっても「中小規模事業者」に該当する場合、具体的には、「従業員の数が100人以下」の事業者（ただし、事業に用いる個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6か月以内のいずれかの日において5000を超える者又は委託を受けて個人データを取り扱う事業者は除かれます）は、先に述べた安全管理措置の具体的内容が軽減されています。

3　従業者と委託先の監督

個人情報取扱事業者は、従業者（正社員、契約社員、嘱託社員、パート・アルバイトなどの雇用関係にある従業員のみならず、取締役、理事、監査役、監事、派遣社員等も含まれます。）に個人データを取り扱わせるにあたり、先ほど述べた**安全管理措置を従業者が遵守するように必要かつ適切な監督**を行わなければなりません（個人情報保護法21条）。

また、個人情報取扱事業者が個人データの取扱いを他の業者等に委託する場合には、**安全管理措置が委託先において遵守されるように必要かつ適切な監督**を行わなければならないとされています（個人情報保護法22条）。個人情報を取り扱う会社や団体によっては、個人データの入力、編集、出力等の業務をアウトソーシングしている場合も少なくありませんが、その場合においても、情報管理をアウトソーシングした委託先に丸投げするのではなく、委託元として、必要かつ適切な監督を行う必要があるのです。