ＬＭ　ニュースレター　Vol. ２１　　平成２９年５月

平成 29 年 5 月 30 日施行　改正個人情報保護法
～中小規模事業者が留意すべき安全管理措置について～

個人のプライバシー保護の必要性が高まったことを受け、「個人情報の保護に関する法律」（以下、「個人情報保護法」）が平成 17 年に施行されてから 12 年が経ちました。多くの事業者がその対応に追われたのは記憶に新しいところですが、この間も、個人情報の流出のニュースが世間を騒がせたことも多くあり、プライバシー・個人情報の要保護性は高まるばかりでした。

平成 27 年に個人情報保護法について大きな改正がなされ（以下、「平成 27 年改正」）、その施行は平成 29 年 5 月 30 日とされています。本ニュースレターでは、この改正個人情報保護法のうち、比較的小規模の事業者にとって影響が大きい部分を中心に、重要となるポイントについて簡潔に説明を致します。

第１　平成 27 年改正により原則としてすべての事業者が対象に

１　平成 27 年改正以前の取扱い

個人情報保護法は、「個人情報を取り扱う事業者の遵守すべき義務等を定めることにより」「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする法律」とされています（同法 1 条）。そして、同法の条文の多くは、「個人情報取扱事業者は・・・しなければならない。」として、「個人情報取扱事業者」に該当する者が、個人情報を取り扱うに当たっての各種義務を定める形式をとっています。

そして、平成 27 年改正以前は、当該事業者が管理する、個人情報によって識別される特定の個人の数が、過去 6 か月以内に 5000 件を超えていなければ、「個人情報取扱事業者」には該当しないこととされていました（改正前個人情報保護法施行令 2 条）。これは、簡単に言うと、保有する個人情報の件数が 5000 件未満である場合には、個人情報取扱事業者に該当しなかったことを意味します（5000 件要件）。

すなわち、保有する個人情報の件数が 5000 件未満の小規模の事業者は、「個人情報取扱事業者」に該当しないことから、個人情報保護法の規制を遵守することは法的義務とはされていなかったのです。

2　平成27年改正による対象事業者の拡大

しかし、平成27年改正及びこれに伴う個人情報保護法施行令の改正により、この5000件要件が撤廃されることとなりました。

すなわち、個人情報の取扱いが5000件以下である、比較的小規模の事業者であっても、個人情報保護法が定める、情報の安全管理措置等を遵守すべき義務を負うこととなります。「個人情報取扱事業者」は、民間部門において、個人情報を検索することができるように体系的に構成して事業活動に利用している者をいうところ（個人情報保護法2条5項）、例えば、個人で通販サイトを運営する方や、不動産業を営む方、さらに、我々弁護士ももちろんこれに含まれることになります。

5000件要件が撤廃され、管理する個人情報の件数を問わず、個人情報保護法の規律に服することとなった以上、これまで、どちらかというと個人情報の取扱いに留意をしてこなかった事業者の皆様も、その取扱いについて改めて確認をしておく必要があります。

第2　新たに個人情報保護法の適用対象となる事業者が理解しておくべきポイント

1　個人情報保護法のポイントは4つ

個人情報保護法が事業者に課している義務は、大きく、①個人情報を取得する際の義務、②個人情報を利用する際の義務、③個人情報の安全管理措置に関する義務、④個人情報を第三者に提供する際の義務に分けることができます。

このうち、①、②及び④に関する個人情報保護法の規律は以下のとおりです。

① 個人情報を取得する際の義務＝個人情報取得時の利用目的の公表・通知

「個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。」（個人情報保護法18条1項）

② 個人情報を利用する際の義務＝取得した個人情報の目的外利用の禁止

「個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。」（同法16条1項）

④ 個人情報を第三者に提供する際の義務＝本人の同意を得ずに、第三者に提供することの原則禁止

「個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。」

これら①、②及び④は、いずれも、個人情報保護法の条文上、個人情報取扱事業者がなすべきことが一義的に明確であり、対象となる事業者の規模によって取り扱いを区別する条文上の根拠がありません。そのため、小規模な事業者であっても、5000件をはるかに上回る個人情報取扱事業者と同様に遵守をしなければなりません。

もっとも、これら、個人情報を取得する際の義務等は、条文上も何をすべきか明確であり、かつ、対応がそれほど困難なものでもないため、これまで個人情報保護法の適用対象外であった事業者であっても、既にその多くが遵守しているのではないかと思われます。

では、③個人情報の安全管理措置に関する義務はどうでしょうか。

2　個人情報の安全管理措置　総論

③個人情報の安全管理措置を講ずべき義務は、法文上、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データ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らない」（個人情報保護法20条）と規定されています。

「必要かつ適切な措置」というものが、具体的に何をすべきであるのか一義的に明確ではないため、各業種に応じて、監督官庁等がガイドラインを定め、具体的に何をすべきかを明らかにしています。例えば、高度に秘匿性の高い個人情報を取り扱う金融機関であれば金融庁が、また、医療機関であれば厚生労働省が、それぞれ個別にガイドラインを定め、具体的にいかなる安全管理措置をとるべきかを明確にしています。

また、すべての事業者が遵守すべき総則的なものとして、「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、「通則」）が、個人情報保護委員会により定められています。

もっとも、新たに平成27年改正により、原則としてすべての事業者が個人情報保護法の「個人情報取扱事業者」に含まれることとなった一方、比較的規模の小さな事業者について、従前の個人情報取扱事業者と同様に高度な安全管理措置義務を課すことは必ずしも現実的ではないと考えられます。そこで、新たに義務を課されることとなるこれら比較的規模の小さな事業者に混乱が生じないよう、個人情報保護委員会は、平成29年3月に通則を改正し、一定の事業者については緩やかな、特例的な対応で足ることを明らかとしています。

3　個人情報の安全管理措置　各論（「中小規模事業者」に求められる具体的な対応）

（1）対象となる事業者

改正された通則により、特例的な取り扱いが許容される事業者は、通則において「中小規模事業者」とされ、従業員の数が100人以下の個人情報取扱事業者のことをいう

とされています。

従業員の数が 100 人以下の事業者というと、相当多くの事業者がこれに該当することになりますが、①個人情報の取扱い件数が 5000 件を超える者、及び②第三者から委託を受けて、個人データを取り扱う者は除外されています。

（２）中小規模事業者が実施すべき具体的な安全管理措置

ア　組織的安全管理措置

通則は、個人情報取扱事業者が講ずべき、組織的な安全管理措置として、大きく分けて、①組織体制の整備、②個人データの取扱いに係る規律に従った運用、③個人データの取り扱い状況を確認する手段の整備、④漏えい等の事案に対応する体制の整備、⑤取り扱い状況の把握及び安全管理措置の見直しをすべきことを規定します。

これらの措置に関して、通則は、中小規模事業者について、以下のとおり、具体的な例を挙げ対応方法を規定しています。

（ア）①組織体制の整備

個人データを取り扱う従業者が複数いる場合に、取扱いの責任者（以下、「取扱責任者」）と、その他の者（例えば、単純に事務作業を行う者）とを区分する。

（イ）②個人データの取扱いに係る規律に従った運用、及び③個人データの取り扱い状況を確認する手段の整備

あらかじめ整備された基本的な取扱方針に従って、個人データを取り扱う運用がなされているか、取扱責任者が確認をする。

（ウ）④漏えい等の事案に対応する体制の整備

漏えい等の事案が発生した場合に備え、従業員から取扱責任者に対する報告連絡体制・フローをあらかじめ定めておく。

（エ）⑤取り扱い状況の把握及び安全管理措置の見直し

取扱責任者が、個人データの取り扱い状況について、定期的に点検を行う。

イ　人的安全管理措置

通則は、講ずべき人的安全管理措置として、「従業員の教育」を挙げ、その具体的な手法として、①個人データの取扱いに関する留意事項について、従業者に定期的に研修等を行うこと、②個人データについての秘密保持に関する事項を就業規則等に盛り込むことを挙げています。

この人的安全管理措置に関しては、中小規模事業者とその他の事業者とで取扱いは異なりません。

ウ　物理的安全管理措置

通則は、物理的安全管理措置として、大きく分けて、①個人データを取り扱う区域

の管理、②機器及び電子媒体等の盗難等の防止、③電子媒体等を持ち運ぶ場合の漏えい等の禁止、④個人データの削除及び機器、電子媒体等の廃棄をすべきことを規定します。

この物理的安全管理措置として求められる内容は、中小規模事業者とそれ以外の事業者とで大きく異なっており、以下に概説する中小規模事業者のものに比べて、それ以外の事業者のものは非常に細かく、かつ、厳格なものとされています。

（ア）①個人データを取り扱う区域の管理、及び②機器及び電子媒体等の盗難等の防止

個人データを取り扱うことのできる従業員及び本人以外が、容易に個人データを閲覧等することができないような措置を講ずる。

具体的には、個人情報が出力された紙媒体資料について、施錠できるキャビネットに保管し、取扱責任者がそのキーを管理したり、紙媒体資料あるいは機器を、特定の作業区域から持ち出してはならないことを周知することなどが考えられます。

（イ）③電子媒体等を持ち運ぶ場合の漏えい等の禁止

個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。

具体的には、会社が管理する USB メモリー（パスワード付）及びモバイル PC（同様にパスワード付）による場合以外に、社外に個人情報を持ち出すことを許容しないことや、個別のワード・エクセルのファイル等にも都度パスワードを設定することが考えられます。

（ウ）④個人データの削除及び機器、電子媒体等の廃棄

個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄したことを、取扱責任者が確認する。

不要になった個人情報は都度削除をしていく必要がありますが、紙媒体の個人情報を廃棄する場合には、常にシュレッダーで処理することや、パソコンを廃棄する場合には、物理的に破壊する、あるいは専門業者に委託する（廃棄証明書の交付を受ける）等、取扱責任者の管理の下で方針を確立する必要があります。

エ　技術的安全管理措置

最後に、通則は、技術的安全管理措置として、大きく分けて、①アクセス制御、②アクセス者の識別と認証、③外部からの不正アクセス等の防止、④情報システムの使用に伴う漏えい等の防止をすべきことを規定します。

（ア）①アクセス制御

個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確にし、

個人データへの不要なアクセスを防止する。

社内で使用する、個人情報が記載されたデータファイルにパスワードを設定し、これにアクセスすることができる従業員以外がパスワードを知ることができない体制をとる等の対応が必要となります。

（イ）②アクセス者の識別と認証

機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。

（ウ）③外部からの不正アクセス等の防止

個人データを取り扱う機器のオペレーティングシステムを最新の状態に保持し、セキュリティ対策ソフトウェアを導入して自動更新機能等の活用により、同様に最新状態とする。

（エ）④情報システムの使用に伴う漏えい等の防止

メール等により、個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

第３　おわりに

本稿では、個人情報の安全管理措置を中心として、平成 27 年改正により新たに個人情報保護法の適用対象となる中小規模事業者が確認をすべき事項を概観しました。

安全管理措置のうち、例えば、データファイルへのパスワード付与や、パソコンのセキュリティ対策ソフトの常時のアップデート等、通則が例示する内容をすでに実施している事業者の方も多くおられると思います。しかし、平成 27 年改正法の施行のタイミングで、改めて、自社の安全管理措置として、最低限通則が例示している事項が遵守できているか、チェックをしてみることが必要であると思います。

（執筆者　弁護士　上野　尚文）

LM法律事務所
LM Law Offices

東京都千代田区永田町２－１１－１
山王パークタワー２１階
ＴＥＬ　０３－６２０６－１３１０