企業経営における個人情報の保護について⑦

企業における個人情報保護法への対策（上）

佐藤典文 司法書士
text by Sato Norifumi

これまで6回にわたり、個人情報保護法（以下「本法」）の内容について見てきました。そこでこれから2回にわたり、個人情報取扱事業者としての企業における本法への対策について検討していきたいと思います。まず今回は、本法の特徴と注意点を確認した上で、本法への対策の手順について概括的に検討していきたいと思います。

個人情報保護法の特徴と注意点

本法への対策について検討する前提として、本法の特徴と注意点について確認しておきましょう。

まず第1に、本法の目的は、個人情報の適正な取り扱いによる個人の権利利益の保護とそれを利用する企業（個人事業主を含む）の活動との調和を図ることとされていますが、実際には前者の保護が確保されることを前提にその利用が可能とされるようになったと考えられます。従来の「個人情報はそれを収集した企業の財産で自由に利用できる」という発想は180度変更されたと考えるべきでしょう。

第2に、本法は個人情報取扱事業者の義務を定めた行政上の取締法規であり、企業と個人間の法律関係に対する直接的な効果はありません。しかし、個人情報について本法に違反した取り扱いがされれば、実際の被害の有無にかかわらず、本人からの損害賠償の請求を受ける可能性が高くなったと言えます。

第3に、本法が直接規制の対象としている個人情報取扱事業者は5,000人を超える個人データを保有する企業ですが、それ以外の事業者にも影響が及ぶ可能性があります。その企業が保有する個人データの量は外部の一般個人には分かりませんから、たとえ自社は本法の規制の対象外であると主張しても、本法と同一水準の管理を要求されたり、取引先が個人情報取扱事業者であれば、やはりその取引先から本法に則した管理を要求されたりすることが考えられます。

第4に、本法は全事業者を対象にした個人情報保護に関する一般法規であるため、実務上は本法だけでなく、各監督官庁や認定個人情報保護団体がその業界ごとに作成するガイドラインや基本方針等をよく検討し、それに則した対策を立てることが必要となります。

ところで、対策の立案に当たっては、平成16年4月2日に閣議決定された「個人情報の保護に関する基本方針」内の個人情報取扱事業者が講ずべき措置に関する基本的な事項の規定が参考となるでしょう（右頁・資料参照）。

個人情報保護法への対策の手順

それでは、具体的にどんな手順で、どのような対策をとる必要があるのか検討していきましょう。企業規模や個人情報の利用量などによって異なる部分もあると思いますが、一般的には次のような手順が必要となるでしょう。

(1) 個人情報保護責任者の選任

企業で保有する全ての個人情報が本法の対象となり、従業者が個別管理する個人情報等まで一元管理する必要がありますので、全社が一丸となって取り組まなければ、対策を立案し実施していくことはできません。そこで、相応の権限を持った人材を責任者＝チーフ・プライバシー・オフィサー（CPO：Cheif Privacy Officer）に任命し、その指示・管理のもとで計画的な対策を実施していく必要があります。できれば、本法について学んだ人材を集め、対策プロジェクトチームをつくりましょう。

(2)個人情報の洗い出しと利用目的の明確化

「個人情報」と思われる情報をすべていったんリストアップし、その利用目的を明確にして、不要な情報は廃棄し、情報を整理していきます。そして、保有を継続する情報については保管場所、保管方法、取得項目、利用目的、アクセス権限を持つ者、利用期限などを記載した個人データ取扱台帳を作成していきます。

(3) プライバシーポリシー制定と対外公表

プライバシーポリシーとは、その企業の個人情報保護に関する考え方や基本方針に関する宣言のことです。これを策定し公表することにより、社内的には従業者の取り組み意識を啓発・統一するとともに、対外的には自社の企業活動に対する信頼の確保を図ります。具体的には個人情報の収集、処理および管理方法についての基本方針を宣言し、自社のインターネットのホームページや社内外の広報誌にその内容を公表していきます。

(4) 業務フローの見直しと社内規定の策定

保有している個人情報を確認し、その利用に関する基本方針が決定したら、現在の

個人情報の取り扱いに関する業務の流れを把握・検討し、問題点は改善し、その見直した業務を個人情報保護規定として社内の各業務規程の中に落とし込んでいきます。コンプライアンス規程の中にはプライバシーポリシーを盛り込むとともに、新たに独立した個人情報保護基本規程を策定したり、各種の業務規程の中にそれを補完するかたちで保護規定を追加したりして社内規程を整備していきます。そして、これらの保護規定の違反に対する従業者の懲戒に関しては、就業規則の懲戒規定を改定し、その中に明記するようにすべきでしょう。

(5)個人情報保護管理の体制の構築

いくら立派な社内規程が整備されても、それがきちんと運用されなければ何にもなりませんので、個人情報保護の推進には法的観点からのコンプライアンス体制と個人情報管理の体制の構築が必要となります。各部門に管理責任者を配置するとともに、それを取りまとめる管理部署を定め、自社のCPOへの通報および指揮命令系統を明確化しておきます。特に、対外的苦情受付窓口や従業者からの相談窓口は必ず設置する必要があります。また、監査部門や人事部門との連携体制も整備しておく必要があります。

(6)情報セキュリティ対策の導入

個人データやそれを取り扱う情報システムのセキュリティをより厳格化するため、新しい機器・装置の導入等の物理的対策や不正アクセスからの防御・不正ソフトウェアの排除等の技術的対策を導入し、常に更新していく必要があります。

(7)従業者教育の充実と監督

過去の個人情報の流出事件からも分かるように、その原因の多くは個人情報を取り扱う「人」の問題ですので、個人情報保護に関する意識の向上、モラルの維持、安全管理(セキュリティー技術等含む)に関する知識の習得など、継続的かつ計画的な教育プログラムを作成し、実施していくことが重要となります。また、本法は「個人情報取扱事業者は従業者に対し必要かつ適切な監督をしなければならない」と定めています(本法第21条)ので、従業者が個人情報保護に関する社内規程を遵守しているかどうかを、企業は定期的に監督していく必要があります。

資料　個人情報の保護に関する基本方針(抜粋)(平成16年4月2日閣議決定)

6.個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項

(1) 個人情報取扱事業者に関する事項

個人情報取扱事業者は、法の規定に従うほか、各省庁のガイドライン等に則し、個人情報の保護について主体的に取り組むことが期待されているところであり、事業者は、法の全面施行に向けて、体制の整備等に積極的に取り組んでいくことが求められている。各省庁等におけるガイドライン等の検討及び各事業者の取組に当たっては、特に以下の点が重要であると考えられる。

① 事業者が行う措置の対外的明確化

事業者の個人情報保護に関する考え方や方針に関する宣言(いわゆる、プライバシーポリシー、プライバシーステートメント等)の策定・公表により、個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である。

また、事業者において、個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することが重要である。

② 責任体制の確保

事業運営において個人情報の保護を適切に位置づける観点から、外部からの不正アクセスの防御対策のほか、個人情報保護管理者の設置、内部関係者のアクセス管理や持ち出し防止策等、個人情報の安全管理について、事業者の内部における責任体制を確保するための仕組みを整備することが重要である。

また、個人情報の取扱いを外部に委託することとなる際には、委託契約の中で、個人情報の流出防止をはじめとする保護のための措置が委託先において確保されるよう、委託元と委託先のそれぞれの責任等を明確に定めることにより、再委託される場合も含めて実効的な監督体制を確保することが重要である。

③ 従業者の啓発

事業者において、個人情報の漏えい等の防止等、その取り扱う個人情報の適切な保護が確保されるためには、教育研修の実施等を通じて、個人情報を実際に業務で取り扱うこととなる従業者の啓発を図ることにより、従業者の個人情報保護意識を徹底することが重要である。

出所:内閣府国民生活局ホームページ「個人情報の保護に関する基本方針」(http://www5.cao.go.jp/seikatsu/kojin/kihonhoushin-kakugikettei.pdf)

(8)外部との個人情報の受け渡しの見直し

本法は、「個人情報の取扱い業務の全部又は一部を外部に委託する場合には、委託側である個人情報取扱事業者が必要かつ適切に管理しなければならない」と定めています(本法第22条)ので、委託先の見直し、委託契約の内容の変更及び委託先業者への監督の強化等が必要となります。また、第三者への提供については、事前に本人の同意のない提供は原則できないと認識し、従来のグループ企業や取引先との慣行を見直すとともに、新たに個人情報に関する規定を盛り込んだ提携に関する業務規程を締結する必要があります。

(9)外部機関による個人情報保護認定の獲得の検討

個人情報保護体制が整備されていることを外部にアピールする手段として、プライバシーマーク制度等の外部機関による個人情報保護認定の付与を受けることも有効です。ただし、認定の獲得と維持には相当なコストがかかる等のデメリットもありますので、そのメリットとデメリットをよく認識した上で取り組むべきこととなります。

(10)事故発生時の対策の検討

個人情報流出等の事故発生時に落ち着いて対応できるよう事前に想定対応マニュアルを作成しておき、通報および指揮命令系統を明確にしておく必要があります。特に、大量の顧客情報が流出した場合などには、その事実と対策についての対外公表が必要となる場合があり、危機管理対策の優劣がその企業の命運を左右することも想定されます。また、事故発生時の損害賠償費用等の負担に備えて、それを補償する損害保険をかけておくことも考えられます。

次回は、いくつかの新たに必要となる対応をテーマとして取り上げ、より具体的に企業における本法への対策について検討していきたいと思います。

1957年生まれ。1981年3月東京都立大学法学部卒業。同年4月横浜銀行に入行。2000年11月横浜銀行在職中に司法書士試験合格。2002年12月横浜銀行退職。2003年6月司法書士登録。2004年3月神奈川県横須賀市に「佐藤典文司法書士事務所」開設。現在、司法書士業務を行うかたわら、企業向けの法務コンサルティングを行う。