

Topics

経済トピックス

個人情報保護法に対する金融機関の望まれる対応

主席研究員

田邊敏憲



個人情報保護法の趣旨

2003年5月に成立した個人情報保護法が、本年4月から金融機関を含めた個人情報を取り扱う事業者にも対象を拡大し、完全施行されている。

そもそも本法の趣旨は、個人情報を取り扱う事業者に対して、その適正な取得、利用、管理のための制限や義務を課し、一方で情報を提供する個人に対しては自己情報の開示や訂正などを事業者に求める権利を保障するものである。

公的機能も帯びる金融機関は、以前から金融規制法や金融庁検査マニュアル、証券・銀行・保険等の各業界の事務ガイドライン等に沿って、顧客情報の保護に努めてきている。本法施行によって、本質的な面で抜本的な改革を迫られるものではないが、従来なかった新たな制度も設けられる。

規制面と活用面

業務遂行上規制を受ける主な面として、①利用目的の制限、②センシティブ（機微）情報の取得禁止、③第三者提供の制限、④委託先の監督、⑤開示請求への対応があげられる。

①「利用目的の制限」とは、金融機関が取得した個人情報はその利用目的を特定し、本人に通知または公表することとし、特定した利用目的を超えて利用してはならないというものである。

②「センシティブ情報の取得禁止」とは、政治的見解、信教、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報を取得、利用、第三者への提供を禁止するものである。

この条項は当該情報漏洩時に被る被害度合いが極めて大きいことから情報提供主体である個人の立場に配慮し定められたものであるが、裏返せば金融機関にとっても漏洩時には深刻な危機に直面することになる。

③「第三者提供の制限」とは、金融機関は本人の事前の同意を得ずに個人データを第三者に提供してはならないというものである。従来から金融機関に対しては、金融庁検査マニュアルや金融規制法などで、本人の同意を得ない第三者提供を原則禁止してきた経緯もあり、大半の金融実務でのインパクトは限定的である。

④「委託先の監督」とは、金融機関が個人データの全部ないしは一部を委託する場合は、その個人データの安全管理が図られるよう、委託先に対し必要かつ適切な監督を行わなければならないというものである。過去、大手コンビニ等で起こった大規模な個人情報流出はいずれも委託先から情報が漏洩したもので、社会的にも委託先の監督は重要視されてきている。

Topics

経済トピックス

⑤「開示請求への対応」とは、金融機関は本人から当該本人が識別される保有個人データの開示を求められたときには、本人に対し遅滞なく当該データを開示しなければならないというものである。金融機関にとっては新たな負担が発生する。

一方、経営資産の「活用」という側面で、「オプト・アウト制度」「共同利用制度」が新設されていることに着目したい。本法は、あくまで個人情報保護のための「規制」が中心であるが、「活用」する条件も示しているのである。

「オプト・アウト制度」とは、第三者への提供を利用目的とする、その個人データ項目、提供の手段・方法、本人の求めに応じて提供を停止する、という4点を本人に通知していれば、別の法人格の企業に対し、本人の同意を得ずに個人データを第三者提供できる。また「共同利用制度」とは、特定の者との間で共同利用すること、その個人データの項目、利用の範囲、利用者の目的、当該個人データの管理責任者の名称、の5点を本人に通知していれば、同様の扱いができる。

両制度とも、金融機関にとっては機動性に富んだ制度となる。

本法施行への対応措置で直接的に生じるコストは、金融庁ガイドラインの定める安全管理措置等も含めて対処した場合、大手金融機関であれば200億円前後の対策費用と想定される。個人情報漏洩時に負担するコストは、仮に100万人規模の漏洩事件を一度起こしてしまうと、150億円～500億円程度の損害賠償という計算になる（因みに都市銀行は個人情報を最低でも1,000万人程度保有）。更に社会的信用・ブランドイメージの失墜、マーケットシェア低下、重要顧客の取引停止、従業員の不安、不満、モラル低下などを招く可能性もあり、経営を揺るがす恐れがある。

米国の実情とインプリケーション

ここで、IT先進国、米国の個人情報保護への取組みをみよう。個人情報保護に関する深刻な問題がIT化の最も進んだ分野の金融で多く発生し、また90年代半から急速にIT化が進んでいる医療分野でも厳格な個人情報保護策が急ピッチで構築されている。

膨らむ被害を踏まえ、企業や政府・議会も動き始めたが、金融機関等のコスト増加につながることもあって実効性は疑問視される。

また米国でGDPの15%強を占めるダントツに大きな医療産業では、医療過誤の多発への対応もあって、ITによる医療行為及び医療情報の標準化が推進されてきた。今や世界で最もIT活用が進んだ医療産業となり、「医療情報ほど厳格な個人情報管理が必要な分野はない」との認識の下、個人情報保護に膨大なエネルギーが投入されている。96年にHIPAAという法律が制定され、「情報漏洩は100%完全には防げない」とみて、罰則も従来の懲役1年から10年に引上げられた。同時に病院、保険会社、薬局など医療情報を共有する関係者が多岐にわたる中、個人が特定される情報を徹底的にガードできるような、金融機関のそれをはるかに上回る、現在技術的に考えられる最高レベルのIT化に向けた投資が実行されている。

こうした米国の動向をも踏まえると、今次個人情報保護法の施行を契機に、「100%完全な情報漏洩防止は不可能」としても、日本のIT産業をユーザーサイドでリードする立場でもある金融機関においては、防戦一方の発想ではなく、オペレーショナルリスク管理体制の整備に務めると同時に、新たなイノベーションの模索が求められる。新しい個人情報管理システムの創出自体が、新しいビジネスチャンスを生み出すとの発想も重要である。