データ保護からプライバシー保護へ
―パーソナルデータ活用の前提となる行動規範―

個人情報保護法改正の方向性を示す「パーソナルデータの利活用に関する制度改正大綱」が発表された。「大綱」は、これまでの形式的な「データ保護」から、個人への実質的な影響を重視する「プライバシー保護」へ向けた一歩を踏み出している。本稿では、「大綱」の概要と、プライバシー保護の枠組みとしての国際規格を紹介する。

パーソナルデータの活用に向けた検討

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）は、2013年12月20日に「パーソナルデータの利活用に関する見直し方針（案）」を発表した。これは、いわゆるアベノミクスの３本目の矢である成長戦略の１つとして、パーソナルデータ活用の重要性と、そのための制度見直しを訴えるものである。

具体的には３つの方向性を打ち出している。第１に挙げられたのが「ビッグデータ時代におけるパーソナルデータ利活用に向けた見直し」で、「個人データを加工して個人が特定される可能性を低減したデータに関し（中略）第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所要の法的措置を講ずる」としている。これは、一定の条件の下で本人の同意がなくてもデータの活用を可能とするべく制度を見直そうということである。

これを受けて、IT総合戦略本部に設置された「パーソナルデータに関する検討会」では、「準個人情報」と「個人特定性軽減データ」（いずれも仮称）を定義し、後者については同意がなくても流通できるようにしようという検討が開始された。なお「準個人情報」とは、個人が特定されていないものの特定される恐れのある情報、「個人特定性軽減データ」とは、個人が特定される蓋然（がいぜん）性が低くなるようにデータを加工して個人の特定を困難にしたものである。いずれも、個人情報でも非個人情報でもない「グレーゾーン情報」として定義し、取り扱い義務の内容を変更しようというわけである。

だがこのアプローチは委員からも、民間からの意見を通じても多くの批判を受けることになる。検討会でも、検討が始まって４回目の５月20日に行われた第９回会合あたりから、データを分類しそれに基づいて法規制を行う「データ種類別規制」一辺倒から、（これから始める）データの活用がどのようにプライバシーに影響を及ぼすかを勘案して事例ごとに扱いを決めていく「行為規制」（事業者の行為に対する規制）を取り入れる方向へ変わったように思われる。

制度改正に向けた「大綱」の決定

こうした検討を経て、法案作成の指針を示

野村総合研究所
IT基盤イノベーション事業本部
オープンソースソリューション推進室
上席研究員
崎村夏彦（さきむらなつひこ）
専門はID管理・プライバシー技術に関する国際標準化

した「パーソナルデータの利活用に関する制度改正大綱」が2014年6月24日に決定された。そこでは、制度改正に当たって以下の4つの課題が挙げられている。

①法解釈や事業者ルールの曖昧さが生じさせているグレーゾーンを解消して「利活用の壁」を取り払うこと。同時に、個人の権利利益の侵害を未然に防止すること。
②法律で定めるべき範囲と政省令や規則、ガイドラインなどで対応すべき範囲を分けるとともに、機動的な対応のための民間の自主的な取り組みを促進すること。
③確実な制度執行（公平な執行主体、公的機関による認定や普及啓発など）を担保すること。
④国際的に調和の取れた制度にすること。

そして、これらの課題を解決するための枠組みとして「本人の同意がなくてもデータの利活用を可能とする枠組みの導入等」「基本的な制度の枠組みとこれを補完する民間の自主的な取組の活用」「第三者機関の体制整備等による実効性ある制度執行の確保」を挙げている。以下、これを簡単に解説していこう。

(1)本人同意なしでのデータの活用

これは上記の1つ目の課題に対応するもので、「大綱」では「現行法の規律に加え、新たに一定の規律の下で原則として本人の同意が求められる第三者提供等を本人の同意がなくても行うことを可能とする枠組みを導入する」とし、具体的には「個人データ等から個人の特定性を低減したデータへの加工と、本人の同意の代わりとしての取扱いに関する規律を定める」としている。すなわち、現行法の本人同意原則をベースとして、その上でプライバシー侵害の実質的大きさを見積もり、所定の条件を満たした場合には同意原則の例外として扱おうということである。

このような枠組みは珍しいものではなく、英国の「データ保護法」でも、個人の同意がなくても個人データの活用が認められる5つのケースを定めている。

米国においては、連邦取引委員会（FTC）が2012年3月に公表した報告書の中で、企業が消費者のデータを利用する際の3つの条件（「FTC3要件」と呼ばれる）を挙げている（FTC「急速に変化する時代における消費者プライバシーの保護」）。

①当該企業は、データを合理的に非識別化（de-identify）するための措置を取ること。
②当該企業は、そのデータを再識別化（re-identify）しないことを公に約束すること。
③委託先・第三者にかかわらず、そのデータの移転を受ける者が再識別化することを当該企業が契約で禁止すること。

ここで重要なのは、「非識別化」は技術的対策というよりも、条件②および③を記述するための準備であるということだ。重要なのは条件②および③で、当該企業とデータを受け取る企業に「再識別しない」と宣言させること、すなわち「個人のプライバシーを侵害

するようなことはしない」と宣言させることが重要なのである。米国の場合、いったんこのように宣言すると、それに背くことをした場合にはFTC法第５条によって取り締まりの対象になる。そういう意味で、「FTC３要件」はプライバシー保護のための行為規制であり、データの種類による規制ではないことに注意する必要がある。

(2)基本的な制度の枠組みと自主的な取り組みの活用

プライバシー侵害のリスクの大きさは、人々のプライバシーに対する考え方や攻撃手法の巧妙化などによって変わっていく。そのため、プライバシー侵害を防ぐ手法に至るまで事前に法律で規定することは不可能である。従って、前述した「大綱」が挙げる２つ目の課題で示されているように、要件や執行体制などの大枠を法律で規定して、具体的内容は政省令や規則、ガイドラインなどで機動的に決めていく形にならざるを得ない。

また、制度の趣旨に則して「本人同意なしの利用」を考えるのであれば、それによって本人ないし社会が得られる利益が、プライバシー侵害による損失を上回ることを検証しなければならない。そのためには、当該業務に対する深い知識を基にケースバイケースで吟味することが必要で、業界ごとの検討が必要になる。「大綱」ではこれを「消費者等も参画するマルチステークホルダープロセス」によって実現するとしている。

(3)実効性ある制度執行の確保

制度や枠組みを考える際に重要なことは、それらの外側で何かをしようとする「悪者」にどう対処するかということである。「大綱」が挙げる３つ目の課題はこうしたことを指している。この課題を解決しないと、不良事業者の存在が優良な事業者の負担を大きくしてしまい、その結果「悪貨が良貨を駆逐する」ことになってしまう。

「大綱」ではこの対策として、現行の「特定個人情報保護委員会」を改組して、第三者機関として「パーソナルデータの保護及び利活用をバランスよく推進することを目的とする委員会」を設置し、立ち入り検査などの機能・権限を与えるとしている。

「プライバシーフレームワーク」の重要性

「大綱」が掲げる以上のような枠組みに従ってパーソナルデータの取得・利用・保持・開示をしようとした場合に、まず行わなければならないのが本人への影響を測ることである。それは具体的にはどうしたらよいだろうか。場当たり的な方策が役に立たず、全てを包括的に規定した仕組みが必要なのは自明である。それが「プライバシーフレームワーク」と呼ばれるものである。

プライバシーフレームワークは、言葉を定義し、行為者間のやり取りを整理し、プライバシーを尊重するためにはどのような原則に従い、どのような管理を行わなければならな

いかを整理するものだ。

国際標準規格としては2011年に制定された「ISO/IEC 29100 Privacy Framework」がある。ISO/IEC 29100は言葉の定義、プライバシー保護要件を定め、プライバシーリスク管理を行うことを求めている。そして、これは①法規制要因②契約要因③業務要因④本人のプライバシー選好などその他の要因－の４つの要因によって影響されるとしている。個人情報保護法といった単一の法律よりも広い範囲の考慮を求めていることに注目すべきであろう。

加えて、ISO/IEC 29100はパーソナルデータの取り扱いに関して満たすべき下記の11の原則を挙げている。

①同意と選択
②目的の正当性と規定
③収集の制限
④データ最小化
⑤利用、保持、開示の制限
⑥正確性と品質
⑦オープンさ、透明性、通知
⑧個人の参加とアクセス
⑨説明責任
⑩情報セキュリティ
⑪プライバシー法令の順守

詳細は誌面の都合で紹介できないが、ぜひ原文に当たっていただきたい。データを新しい目的で使い始める前に本人にその目的を知らせなければならないなど、何をすべきかが具体的に書かれている。ISO/IEC 29100を基本として、後続の「プライバシーアーキテクチャー（ISO/IEC 29101）」などの国際規格が生まれた。「大綱」に４つ目の課題として挙げられた「国際的に調和の取れた制度」とするためには、日本独自の規則を作るのではなく、各国の代表が集まって何年もかけて練り上げたこうした国際規格を取り入れていくべきであろう。

「プライバシー影響評価」から始める

プライバシーは、日本国憲法が規定する基本的人権の一部であり、第13条には「立法その他の国政の上で最大の尊重を必要とする」と書かれている。

従って、パーソナルデータの活用を正当化するには、まずそれが個人にどのような負の影響を与えるかを吟味し、プラスの影響がそれを上回ることを立証し、負の影響が上回ってしまう人にはどのように補償するかを決めなければならない。

このための第１ステップは、国際的に認められたプライバシーフレームワークに基づいた「プライバシー影響評価（Privacy Impact Assessment：PIA）」を行うことである。現在ISO/IECでは、PIAの手法の規格化が進行している（ISO/IEC WD 29134）。パーソナルデータの活用を目指した制度改正に当たっては、これらを参照しながら行っていくことが肝要である。 ■