プライバシー影響評価の重要な役割
―プライバシー保護とパーソナルデータ活用の両立―

「頭隠して尻隠さず」。名前や顔を分からなくするなど法令に形式的に対応するのみで、個人が隠しておきたい肝心なものを守れていないという点で、プライバシーをめぐる昨今の事件にはこのことわざがぴたりと当てはまる。本稿では、消費者への説明責任を果たし、パーソナルデータを円滑に活用するための「プライバシー影響評価」を紹介する。

なぜ非難や反発が相次ぐのか

スマートフォンやソーシャルメディアが普及し、そこから大量に生成される個人に関する情報（パーソナルデータ）を活用して、事業者は以前とは比べものにならないほどの精度で、個人の好みや未来の行動を推し量ることができる時代が到来した。

パーソナルデータには、プライバシーに該当する個人情報もあれば、そうでないデータも含まれている。2005年４月に個人情報保護法が全面施行されて以来、個人情報の保護は日本の社会の隅々にまで浸透し、誰もが個人情報は保護しなくてはならないものと理解するようになった。その一方で、データが個人情報に該当しなければどのような取り扱いをしてもいいという拙速な使い方をして消費者の非難や反発を招くケースも頻発している。また、上記のようにパーソナルデータにはプライバシーに属するのかそうでないのかが明白でない、いわゆるグレーゾーンがあることも、そうした問題の一因になっている。

そもそも、個人情報は何のために保護されなければならないのだろうか。それは、個人情報保護法の第１条に規定されているとおり、「個人の権利利益を保護すること」が目的である。そして、個人の権利利益の中心にプライバシーがある。すなわち、個人情報を保護する目的はプライバシーを守ることであり、個人情報の保護はその手段に過ぎない。しかし、従来型の個人情報保護ではプライバシーを守ることができなくなっており、それがパーソナルデータの活用に関する問題の原因なのである。今はプライバシーを守るための手段を見直さなければならない過渡期といえるだろう。

「プライバシー影響評価」とは

パーソナルデータの取り扱いを開始する前に、発生する可能性のあるプライバシー侵害リスクを評価し、そのリスクを回避・最小化する考え方を「プライバシー・バイ・デザイン（Privacy by Design）」（PbDと略記）といい、近年、世界的に注目されている。一般的なリスクマネジメントにおいても、事前対策は事後対策よりも効果的であると認識されており、その考え方をプライバシー保護分野に応用したものといえる。

PbDの考え方を、実際のプライバシー保護の業務プロセスに落とし込む代表的な手法

野村総合研究所
コンサルティング事業本部
ICT・メディア産業コンサルティング部
上級コンサルタント
小林慎太郎（こばやししんたろう）
専門はICT公共政策・経営

が「プライバシー影響評価（Privacy Impact Assessment：PIA）」である。

PIAそのものはそれほど新しい取り組みではない。すでに1990年代後半から米国、カナダ、オーストラリアなどでは、行政機関が個人情報を取り扱う情報システムを開発する場合に実施されてきた。しかし、PIAの実施方法は国によってさまざまであり、確立された方法はこれまでなかった。また対象は行政機関のみで、民間事業者には直接関係のないものであったため、これまでPIAはあまり普及してこなかった。

しかし、EU（欧州連合）が新しいプライバシー保護ルールである「EUデータ保護規則（案）」にPIAを取り入れたことで、一気に普及が加速する様相を見せている。同案において、一定の条件に当てはまるパーソナルデータを取り扱う行政機関・民間事業者に対して、PIAの実施を義務づけることになったからである。特に民間事業者におけるPIA義務化は世界で初めてとなる。なお、「EUデータ保護規則（案）」では、データ保護影響評価（Data Protection Impact Assessment：DPIA）と呼称しているが、意味するものはPIAと違わない。

日本においても、「社会保障・税の番号制度」（マイナンバー制度）において、「特定個人情報保護評価」という呼称でPIAが行政機関に義務づけられ、すでに運用が開始されている。さらに「パーソナルデータの利活用に関する制度改正大綱」（2014年6月24日IT総合戦略本部決定）ではPIAが継続検討事項となっており、今後検討が深められる見込みである。

PIAの実施手順

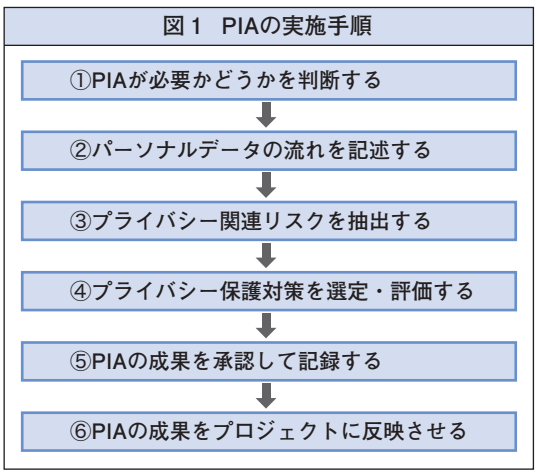
いまだ確立された標準的な方法はないものの、PIAはすでに多くの国で取り組まれ、実施手順の骨格は共通のものとなりつつある。国際標準化団体においても標準化が進められており、筆者もこの作業に日本から参加している。

ここでは、イギリスの第三者機関であるICO（Information Commissioner's Office：情報コミッショナー局）が定めたガイドライン「Conducting privacy impact assessments code of practice」（2014年2月25日公表）に基づいて、個人情報・プライバシー保護に関する筆者のコンサルティング経験や標準化作業の知見を踏まえ、PIAの実施手順の概要を紹介する。

ICOのガイドラインでは、PIAの実施手順を6つのステップに分けている（次ページの図1参照）。以下で順に見ていこう。

①PIAが必要かどうかを判断する

PIAを実施する必要があるのか、実施する場合は、どの程度の規模で実施すればよいのか、最初の段階でふるい分ける。パーソナルデータを取り扱う事案は多く、全てを対象に厳格なPIAを実施することは現実的ではなく



非効率でもあるからである。「予備評価」「しきい値判断（マイナンバー制度の「特定個人情報保護評価」における呼称）」などと呼ばれる。

②パーソナルデータの流れを記述する

このステップでは、誰が、誰から、何のパーソナルデータをどのように取得・利用し、誰と共有し誰に提供するのかといった基本的なデータの流れを整理し、さらにデータフロー図や業務フロー図などを用いてデータの流れを可視化する。この成果は、後続のステップであるリスク抽出のための基礎資料となる。また、データの取得から廃棄までの一連の流れを記述し、データのライフサイクル全般での保護を検討するための資料とする。

③プライバシー関連リスクを抽出する

パーソナルデータの流れが整理できたら、それを基にプライバシー関連リスクを抽出し、その影響を評価する。プライバシーの分野では、特定の領域を除いて、汎用的なリスク参照モデルはいまだ確立されていない。これは、プライバシー保護が比較的新しい分野であり、またパーソナルデータをどのような目的や状況で活用するかに依存する部分が大きいために、一般化できる部分が限られているからである。このため、「OECD（経済協力開発機構）８原則」（OECD理事会で1980年９月23日に採択された「プライバシー保護と個人データの国際流通についての勧告」に記された８つの原則）や「ISO/IEC 29100 Privacy Framework」といったプラバシー保護のフレームワークを用いて、先に整理したデータの流れに沿ってリスクの洗い出し作業を行う。

④プライバシー保護対策を選定・評価する

リスクを抽出した後は、それらがどのくらい影響があるか、発生確率はどの程度あるかを分析し、リスクに応じた対策を講じる。これは、リスクマネジメントにおける一般的なリスク評価手法と同じ考え方に基づいている。すなわち、PIAにおいても一般のリスクマネジメントと同じく、リスクは完全に排除するのではなく、リスクの影響度や発生確率を許容できるレベルにまで低減することを目的に対策を選定することになる。

⑤PIAの成果を承認して記録する

このステップでは、PIAの実施結果として、パーソナルデータの取り扱い、プライバシーリスク、リスクへの対策をレポートにまとめ、プロジェクトの実施責任者やプロジェク

トオーナーによる承認を得る。

先進諸外国の事例を見ると、公的機関の場合、PIAのレポートやその概要を公開することが一般に行われている。民間事業者では営業秘密やセキュリティを理由に、自発的にPIAレポートを公開することはあまりない。ただし、プライバシー保護当局から照会があった際に迅速に開示できるようにレポートを準備しておく事業者もある。

⑥PIAの成果をプロジェクトに反映させる

最後のステップは、PIAの実施結果を確実にプロジェクトに反映させることである。前述したとおり、PbDの思想に基づくPIAでは、事前にリスクへ対処することが目的であるため、サービスや情報システムの設計にPIAの結果を取り込めるタイミングである概念設計が終了するまでの間に行う。

本質はステークホルダー間の合意形成

プライバシー保護に対する意識は個人差が大きい。そのため、多くの消費者がメリットを認めてパーソナルデータの利用を容認する場合であっても、社会的な影響力を持つ企業や公的機関では、保護意識の強い一部の消費者の要求に合わせてデータの利用を控えたり、オプトイン（事前に許可を取ること）で本人同意を得られた場合のみ利用したりする傾向が見られ、パーソナルデータを活用したビジネスに踏み出せない企業もある。PIAは、こうした状況を打開する手段としても期待される。

例えば、行動ターゲティングを活用した新たなサービスを提供するためにパーソナルデータの利用が必要になったとする。このとき、サービス利用者から個別に同意を取得するか、オプトアウト方式（事前に利用者の明示的な同意を取得せずに個人情報を利用し、本人からの求めがあった場合に個人情報の利用を停止するやり方）にするかが問題となっているとする。この場合に、PIAの一環として、サービス利用者へのアンケートやヒアリングを通じてデータ利用に対する受容性を評価し、その結果に基づいて分かりやすい同意取得のインターフェースを開発して簡便にオプトアウト（利用停止の手続き）ができる方法を提供する、といったリスクの回避・軽減措置をステークホルダー（利害関係者）を集めて協議するのである。

このように、PIAは、ステークホルダーとの協議を通じてデータ活用の便益とプライバシー保護とのバランスを追求し、全体最適を求めるプロセスとして有効であり、PIAの実施は説明責任を果たすことになる。

PIAは発展途上にあり、今後もPIAの手法を洗練させる試みが各所で行われると思われる。PIAを義務づけるEUの新しいルールはその強力な追い風になるはずだ。プライバシー保護と両立するパーソナルデータ活用の道を切り開いていくために、今後PIAの役割はますます重要になるであろう。 ■