プライバシー規制の動向

寺田 眞治 ●一般財団法人日本情報経済社会推進協会主席研究員
柊 紫央璃 ●一般財団法人日本情報経済社会推進協会客員研究員

EUのGDPRや米国のCCPAなどプライバシー保護の規制が強まる。国際標準的な規格の動きも。日本の改正個人情報保護法も2020年に改正法が成立予定。

2017年に施行された改正個人情報保護法は、3年ごとに見直すことになっており、2020年は新たな改正法が成立する予定だ。このわずか3年の間に個人情報の取り扱いを巡る環境は大きく変化しており、メディアを賑わす事件や事故にも事欠くことはなく、次々と新たな課題が浮上している。海外に目を向けてみても、EUではGDPR（一般データ保護規則）が2018年5月に、中国ではサイバーセキュリティ法が2017年6月に、米国でもCCPA（カリフォルニア州消費者プライバシー法）が2020年1月に施行されるなど、各国でプライバシー保護に関する規制が強まっている。

■個人情報保護からプライバシー保護へ

個人情報の保護とプライバシーの保護は異なるものである。法律で定義された個人に関するデータを守るのが個人情報の保護であるのに対して、個人の私生活について知られたくないことという、より広い概念を守るのがプライバシーの保護である[1]。「知られたくないこと」の定義は難しく、個々人ごとに大きく異なるものでもある。これを定量的なものに置き換えるために、特にプライバシーに影響がある個人に関するデータに注目し、これの取り扱いを規定したものが個人情報保護法である。ちなみにGDPRもGeneral Data Protection Regulationであり、プライバシーとは表現していない。

ところが最近、ルールに従って個人情報の取り扱いに関する同意を取っていればどんな使い方をしてもよいのか、という問題を提起する事例が目立ち始めている。「データ」の取り扱いルールとしては違法ではないが、利用者に不利益を与える、もたらされる結果が予想外である、不安や不快感を与えるといった事例である。2019年に発覚したリクルートキャリアによる内定辞退率予測の企業への提供が、典型的な事例のひとつであろう。個人情報保護委員会の勧告は同意取得の不備を指摘しているが、たとえ問題がなかったとしても、個人情報の使い方として許されるのだろうかという問題である。米国では、貧困者が多いと思われる地域を除外して住宅広告を行うことは、差別的であり機会均等の原則に反するとしてFacebookが訴えられている。なお、その後Facebookは住宅広告では年齢、性別、郵便番号に基づいてターゲティングできないようにするとして和解している。

これらのような場合、データを分類して取り扱いの規則を作るルールベースの考え方では対応で

きない。本来、最終的な目的は「個人情報」を守ることではなく「プライバシー」を守ることであり、利用者が不利益や差別を受けないようにするための規制はどうあるべきかが問われている。

■ルールベースからゴールベースへ

EUのプライバシー保護法制は、プライバシーという基本的人権を守ることがベースであるため、GDPRの基本原則では最初に「適法性」「公正性」が謳われている。つまり、人権を蔑ろにしたり不公正であったりした場合には、違法となる。

米国では、プライバシーの保護は消費者の保護に含まれるという考え方で、連邦取引委員会法第5条にある「不公正・欺瞞的な行為又は慣行を禁止する」という規定がベースとなっている。これにより不利益や差別となることを知らせていなければ違法とされる。

また、個人データの取扱いを含むサービスや業務を導入する場合に、その設計段階からプライバシーリスクの低減策を組み込むという、プライバシーバイデザインという考え方が国際的に定着しつつある。その実現方法の基本はリスクベースで対策をするということである。このリスクには、漏洩や炎上といったものだけではなく、消費者に不利益を与えることも含まれている。つまり、プライバシーに何らかのインパクトを与えるものは、すべてリスクと捉えて対策を行うということである。このように、プライバシーを保護するというゴールに対してのアプローチはさまざまであるが、いずれもルールの上位にゴールがあることを示唆している。

一方、日本の個人情報保護法は厳格に対象を決めたデータの取り扱いのルールであるため、ルール通りに取り扱っている限り、差別や不利益となる利用方法であっても法として取り締まることが難しいという側面がある。そのため、2019年には大きく2つの動きが見られるようになった。一つは、本筋である個人情報保護法の改正でカバーしようとする動きであり、3年ごと見直しの制度改正大綱に見ることができる。もう一つは、既存の他の法制度によるものである。

■国内動向

2020年は個人情報保護法の改正以外にも、特にDX（デジタルトランスフォーメーション）の進展に伴って生じるサイバー空間における個人情報やプライバシーに関する問題への対応について、各省庁でも様々な動きが出ている。

●個人情報保護法改正の動向

執筆時点では制度改正大綱の意見募集が締め切られた段階であり、法案とそれに続く政令、規則、ガイドラインがどのようなものになるかについては未定である。ここでは制度改正大綱に見られる改正の意図や方向性について簡単に解説する。

まず、従来からの規制の延長として、個人の権利の拡大（利用停止等の請求権を拡大など）と、事業者の責務の拡大（漏えい等報告の義務化など）がある。プラットフォーム事業規制にも通じるところであるが、海外の事業者に対する法の域外適用（イコールフッティング）と越境移転（移転先の情報提供など）は、実効性をどう担保するかは課題であるものの一歩踏み込んだものとなっている。一方で、漏えい報告については共同規制から直接規制に変更し、企業単位での自主規制スキームだけではなく事業単位の自主規制スキームも可能となるように変更、課徴金を含むペナルティについては見送るなどグローバルの流れとは異なる方針も見られる。仮名化情報（仮称）の創設は、一見するとGDPRに合わせたようにも見えるが、実際には企業内部での利用に限定されるため、単語としては同じものの異なる性格を含んでいる。

前項で触れたゴールベースへのアプローチとしては、不適正な方法により個人情報を利用してはならない旨を明確化する方針が示されている。ただし、現時点では「不適正な方法」とは何を意味しているのかが明らかにされていないので、どこまで踏み込んでいけるのかは不明である。

一部ではクッキーが規制されると報道されているが、そのような内容は含まれていない。リクルートキャリア事件を受けて、提供先において個人データとなることが明らかな場合は第三者提供を制限するという方針について、クッキーの突合が禁止されると早合点したものと思われる。

一方で、データマーケットプレイスや広告におけるDMP（データマネジメントプラットフォーム）等では大量のデータが複雑に行きかうことから、どこかで個人情報となる可能性は否定できない。そのため、データ流通に関するビジネスが委縮するのではないかと危惧される側面もある。その他、名簿屋対策として、個人データの第三者提供を受けた者への開示請求の義務化、保有個人データとならないと定めた6か月という期間の撤廃など、事業者への負荷が想定されるものが少なくない。

今後の予定としては、2019年3月頃の法案提出が予定されているが、具体的な内容はその後の規則やガイドラインで規定されることになると考えられている。したがって、上述の内容が実際にどの程度実装されるかは不明で、今回の募集意見や今後の各関係者との折衝による振れ幅は大きそうだ。

●各省庁の動向

一方、個人情報保護委員会以外の省庁でもプライバシー保護に関する動きは活発になっている。その多くはデジタルプラットフォーム事業の規制という形で表に出てきている。

総務省は「プラットフォームサービスに関する研究会」の最終報告書案（執筆時点ではパブリックコメント中）において、利用者情報の適切な取扱いの確保として、電気通信事業法やガイドラインの改正を視野に入れた方向性を示している。

プラットフォーム事業者の国内外のイコールフッティングに注目が集まっているが、ベースとなる考え方はEUのePrivacy規則に近いもので、端末情報の「通信の秘密」「プライバシー保護」の強化が含まれている。すでに個人情報保護委員会から権限を委任されて策定されている「電気通信事業における個人情報保護に関するガイドライン」では、通信履歴や発信者情報などの通信に関わる利用者情報、位置情報などが保護すべきものとして規制されているが、そこから対象が大幅に拡大される可能性がある。

公正取引委員会は2019年12月に「デジタル・プラットフォーム事業者による消費者に対する優越的地位の濫用に関するガイドライン」を発表している。利用目的を知らせずに、あるいは利用目的の達成に必要な範囲を超えて消費者の意に反し、さらに安全管理のために必要かつ適切な措置を講じずに、個人情報を取得、利用することが濫用行為の類型として例示されている。また、サービスの対価として提供している個人情報等とは別に、個人情報等その他の経済上の利益を提供させることも例示されており、これはリクルート事件を受けて追加されたようだ。

消費者庁も12月に「デジタル・プラットフォーム企業が介在する消費者取引における環境整備等に関するプロジェクトチーム」を発足した。この中で新たな問題として、プロファイリングが示されている。議論は始まったばかりであるが、消費者保護の観点から、説明責任の強化以外に何らかの規制がかかる可能性がある。

プロファイリングは、オンライン広告において

も問題視されている。2019年9月に発足した内閣官房デジタル市場競争本部は、2019年12月からの「デジタル広告市場の競争状況の評価」について提案を公募する中で、パーソナルデータの取得・利用の透明性を主な論点の一つとしている。こちらも議論の初期段階で2020年春ごろに中間整理がされる予定であるが、こちらも少なくとも説明責任の強化は避けられないだろう。

さらに経済産業省でも、Society 5.0やDFFT（Data Free Flow with Trust）の実現に向けた検討の中でプライバシー保護が取り上げられている。概観するとプライバシー保護は企業のガバナンスとして取り組むものであり、その際に重要となるのはゴールベースでの考え方であり、アカウンタビリティが求められるというものである。アカウンタビリティは説明責任と翻訳されることが多いが、説明し、それを証明し、誤っていた場合には責任を取るところまでが含まれるものである。同省では最近「コンプライ＆エクスプレイン」と置き換えている。

■国際動向

EUでは、GDPRの補完となる電気通信事業領域のePrivacy規則が未だ議論が収束しておらず、認証システムの構築についても遅々として進んでいない。各種ガイドラインは精力的に発表されているが、全体としては大きな動きはなく、GDPRの浸透に注力している状態だ。

米国では、州法の制定が活発化しているが、分断を嫌って連邦法の制定を進めようという機運が高まっている。しかしながら直近で成立する状況ではない。

一方で、法規制ではなく自主的かつ国際標準的な規格を構築しようという動きが成果を見せ始めている。実質的に米国の標準規格策定を主導してきたNIST（国立標準技術研究所）によるプライバシーフレームが、2020年1月に発行された。また、国ごとにバラバラに独自のプライバシー保護法制が成立してグローバルでのデータ流通に支障をきたすことを懸念し、それを望まない国々や産業界による国際標準規格制定も進んでいる。さらに国家間でのデータ流通を推進するための枠組みも急激に立ち上がりつつある。これらの代表的なものについて、以下に紹介する。

●ISO/IEC 27701

2019年8月に発行されたISO/IEC 27701は、ISMS（情報セキュリティマネジメントシステム）の実装を前提としたPII（Personally Identifiable Information）の保護を目的とした規格である。ISO/IEC 27001に基づくISMSはリスクベースで情報管理を行うものだ。これまでもプライバシーリスクがある場合には、ISMSがプライバシー保護の規格としても機能していた。これに追加し、PII保護に特化した要求事項として新たに策定されたものがISO/IEC 27701である。

ISO/IEC 27701は、ISMS認証を取得した上で、プライバシー情報に関するセキュリティをマネジメントしたい組織が、PIMS（個人情報保護マネジメントシステム）を構築する際に求められる追加の要求事項になる。PIMSは個人情報そのものを保護するものではなく、その情報が取り扱われた際にプライバシーの侵害が起きないようにするというリスク管理の考え方のものだ。そのため組織がPIMSを導入する際には、情報セキュリティマネジメントの適用範囲を指定するほか、自組織が考えているプライバシー情報とは何かを定義する必要がある。

●ISO/IEC 29314

今回の個人情報保護法改正の制度改正大綱においてもPIA（プライバシー影響評価）の重要性が

強調されている。そのPIAの国際標準規格がISO/IEC 29314である。

PIAとは、個人情報およびプライバシーに係るリスク分析、評価、対策検討を行う手法である。2008年にISO/IEC 22307として金融関係を対象としたものが発行されている。それを踏まえた拡張として、公的機関、民間企業、政府機関、および非営利団体を含むあらゆる種類、および規模の組織に適用することができる新しい規格ISO/IEC 29314が、2017年に発行された。

ISO/IEC 29314では、PIAの実施プロセスおよびPIA報告書の構成と内容についてのガイドラインを提供している。実施プロセスは、大きく「PIAの必要性の決定」、「PIAの実行」、「PIAのフォローアップ」の3項目に分かれ、プロセスごとの「目標」、「インプット」、「期待されるアウトプット」、「アクション」、「実施のガイダンス」が具体的に説明されている。

プライバシーバイデザインの考え方が国際的に定着し、GDPRを始め各国制度にもその思想が盛り込まれている。GDPRでは、大規模の特別な個人情報の取扱いなど、一定の要件においてPIAの実施が必須となっている。これに対応する動きとして、EUだけでなく米国でもISO/IEC 29314に準拠した認証が始まっている。日本でも国内外を横断したデータ利用における共通の国際規格が求められていることから、JIS原案の作成が進められており、2020年半ば頃の発行を目指している。

●NIST Privacy Framework

2020年1月に、NISTのPrivacy Frameworkが発行された。2014年にNISTが発行したCyber Security Framework（以下CSF）が、米国だけではなく世界的に広く用いられるようになっていることから、Privacy Frameworkへの注目度や期待度は非常に高い。両フレームワークはリスク管理を考え方のベースとする密接な関係があり、それぞれのリスクの関係は、資料4-2-1のような図で説明される。

またPrivacy Frameworkは、コア、プロフィール、ティアの3つの要素によって構成されており、概念的にも構造的にもCSFを襲踏していることが分かる（資料4-2-2）。

NISTのPrivacy Frameworkは、米国においてプライバシー保護規制を担う主要機関であるFTC（連邦取引委員会）が支持を示唆していることから、CSFのようにガイドラインでありながらも業界のデファクトスタンダードになる可能性は低くないだろう。CSFを実装している組織や、大量または複雑な個人情報を取り扱っている組織は、今後の動向に注目する必要があるだろう。

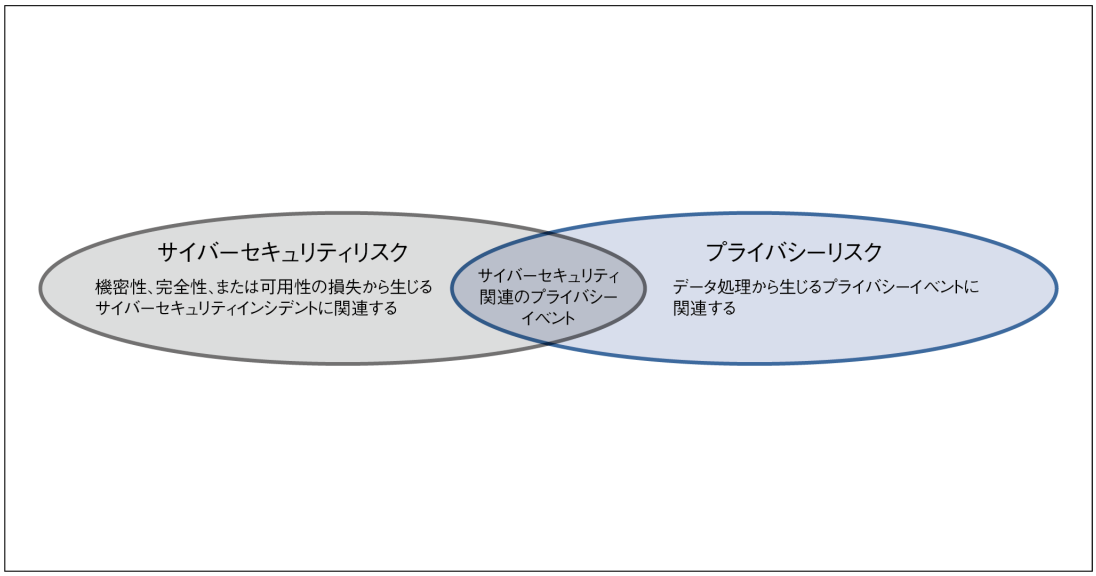
●APEC CBPR

APEC（アジア太平洋経済協力）における個人データの越境移転の保護に関する取り組みは、2004年から始まり、2011年のCBPR（APEC越境プライバシールール）の策定によって確立された。日本の個人情報保護法第24条では、「第三国の提供事業者がCBPRを取得している場合」は「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要はないとしている。

CBPRは、適切な情報プライバシー保護策の策定を奨励し、アジア太平洋地域での情報の自由な移動を保証する際の重要な手段を具体化するための仕組みとして位置付けられている。APEC Cross-border Privacy Enforcement Arrangementに参加しているエコノミーで運用する。50項目に及ぶ質問書で事業者等がAPECプライバシー原則に適合した個人情報の取り扱いを行っていることを認証するシステムである。

ASEAN諸国をはじめとしたアジア太平洋地域の経済活性化にともなうデータの越境流通が拡大

資料4-2-1　サイバーセキュリティリスクとプライバシーリスク



出典：NIST Privacy Framework Version1.0（筆者訳）

資料4-2-2　Privacy Framework の３つの要素

要素	機能	詳細
コア	特定	組織のプライバシーリスクの把握
	統制	組織のガバナンス構造の開発
	管理	適切なデータ管理の手法の開発
	通知	データ処理に関するコミュニケーション活動
	対応	プライバシー侵害の対応策
プロフィール	組織の現在のプライバシー活動または望ましい結果	5 つの機能にそれぞれ定義されたカテゴリーおよびサブカテゴリーに従い自己評価し、現状と目標を比較して改善策を特定する
ティア	組織のプライバシー対応の効果を評価する基準	ティア 1：部分的な ティア 2：リスク情報を生かした ティア 3：反復可能な ティア 4：適応性のある（層 4）

出典：筆者作成

したことにより、プライバシー保護のフォーカスも、国内法令の遵守（コンプライアンス）から国際間で通用する共通のアカウンタビリティへと移行している。CBPR は情報の越境流通の拡大とプライバシー保護方針の地域分断化との乖離を緩和するために効果的な仕組みであると考えられている。米国と日本が普及に力を入れており、この２か国に加えてシンガポールと韓国での認証が始まり、オーストラリアが手続きを進めている。

1. プライバシーの定義は諸説あり定まっていないが、本稿では「データの保護」という狭義なものではないという趣旨で使っている。

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2020年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp