プライバシー保護をめぐる日米欧の制度面の動向

寺田 眞治 ●一般財団法人日本情報経済社会推進協会 客員研究員

日本では個人情報保護制度の在り方が転換期に、世界では子どものプライバシー保護規制強化や各国共通の認証制度に向けた議論が進行。国境を越えたデータ流通に向けグローバルな調和が求められる。

■日米欧の動向の概要

日本の個人情報保護法は欧米に比べて規制が緩いものと見なされている中、3年ごと見直しの議論で規制強化が検討されている。一方、個人情報には該当しないパソコンやスマートフォンなどの利用者情報については総務省の電気通信事業法で外部送信規律が制定され、法的義務はないもののスマートフォン プライバシー セキュリティ イニシアティブ（SPSI）では欧米の規制に近い内容が議論されている。また、2025年末施行の、アップルとグーグルによる支配市場を開放するための「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律（スマホ新法）」においても、これら2社によるプライバシー保護対策を下回らないようにガイドラインの策定が進められている。

EUでは、2018年施行の一般データ保護規則（General Data Protection Regulation：GDPR）以降、2023年と2024年に相次いで成立したデジタル政策・データ政策の法制度整備において、それぞれの法律の中にプライバシー保護の条項が規定され、社会の変化に則した規制の適用が進んでいる。偽・誤情報規制を含むオンライン上の安心・安全を目指したデジタルサービス法（Digital Service Act：DSA）、市場競争環境の公正性を獲得するためのデジタル市場法（Digital Market Act：DMA）では、特に大規模なデジタルプラットフォームに対して、利用者保護の観点から広告の透明性の確保などを義務化している。また、データ法（Data Act）、サイバーレジリエンス法（Cyber Resilience Act：CRA）、AI法（AI Act）等においても、プライバシー保護を前提条件としていることが明文化されている。これは、EUにおいてプライバシー保護は市民の基本的権利とされているからだが、特にデジタル社会への移行に際して想定されるあらゆる場面においてプライバシーの毀損（きそん）を防止することを目的としており、事前規制的な要素が強い。

米国では2024年4月に米国プライバシー権法（American Privacy Rights Act：APRA）が議会に提出されたが、ドナルド・トランプ大統領が率いる共和党は伝統的に規制に消極的であり、成立は困難とみられている。現在の連邦全体の規制としては、連邦取引委員会（Federal Trade Commission：FTC）がFTC法第5条の商取引における不公正・欺瞞（ぎまん）的な行為または慣行の禁止を根拠に、消費者保護の観点からプライバシー保護の取り締まりを行っている。

一方でFTC法の商取引という限定を超えるために、州ごとやセクターごとにプライバシー保護に関する法律の制定が進むことになり、乱立する様相を呈している。州法ではカリフォルニア州消費者プライバシー法（California Consumer Privacy Act：CCPA）とこれを拡張するカリフォルニア州プライバシー権法（California Privacy Rights Act：CPRA）が包括的な規制法として代表的で、各州がこれに倣う方向で次々と法律を成立させている。基本的な規制内容は、おおむね情報の取り扱いの透明化とオプトアウトの義務化となっている。

セクター別では、2024年に子どもの保護を目的として制定された児童オンラインプライバシー保護法（Children's Online Privacy Protection Act：COPPA）が、対象年齢を上げるなど新たに規制を強化して児童および青少年のオンラインプライバシー保護法（Children and Teens' Online Privacy Protection Act：COPPA 2.0）となった。同時に、デジタルプラットフォームに対して青少年を守るための合理的な措置を求めた、子ども安全オンライン法（Kids Online Safety Act：KOSA）も成立している。他にも、医療関係やセキュリティ関係など多方面でプライバシー保護の強化が進んでいる。

日米欧ではプライバシー保護の法制度の構造が異なり、それに伴って個別の法律の対象や目的も異なっている。グローバルで俯瞰すると、ブリュッセル効果といわれるEU法が世界へ広がり法規制のスタンダードとなる流れが強まっている。また、カリフォルニア効果ともいわれるカリフォルニア州法が米国のスタンダードとなって、米国との取引実務においては大きな影響を与えるようになっている。一方で、規制の重要な論点や内容は似たようなものになりつつあり、相違点は縮小される方向にある。

■個人情報の定義

最も基本的な前提となるプライバシー保護に関する情報の定義は、日本と欧米で異なっている。日本語に翻訳するといずれも「個人情報」とされるが、欧米ではPersonal Data、日本ではPersonal Informationとなっている。日本では、一般的な理解としては特定の個人に関するものであるが、欧米のPersonal Dataは特定することができる可能性のある情報も含まれ、対象となる情報の範囲が非常に大きい。一方、国際標準規格ではPersonally Identifiable Information（PII）といわれ、Personal Dataと同様に広く個人に関する情報を意味している。いずれも日本では個人関連情報と定義されているものを含んでいる。

日本の個人情報保護法の3年ごと見直しでも、個人関連情報の取り扱いについて議論されている。単独では個人情報でなくとも特定の個人に対する働きかけが可能となるものについて、一定の規律を設けようという議論である。代表的なものとしてはメールアドレス、ウェブブラウザーを識別するcookie、端末などの識別記号、広告IDなどである。欧米では、これらの取り扱いについて説明などの透明性確保が義務付けられている。EUでは個人情報として扱わなければならないことから大半の場面で同意が必要であり、米国においてもオプトアウトできることが事実上義務化されている。

■オンラインにおける利用者情報

利用者情報は、日本では電気通信事業法において端末から外部に送信できる情報全般とされている。日本法でいう個人情報も含まれる広範囲なものとなっており、欧米ではPersonal Dataに含まれるものである。つまり、欧米では個人情報の中に利用者情報が含まれる構造であり、日本においては利用者情報の中に個人情報が含まれる構造と

なっている。これにより、欧米では利用者情報に対する規制は個人情報と変わらないが、日本では個人情報が含まれない利用者情報は異なる取り扱いとなる。例えば、電気通信事業法で電気通信役務を営む者が端末から外部に利用者情報を送信する場合には、情報の項目や利用目的を公表するなどが義務化されている。

個人情報保護法の3年ごと見直しでは、対象事業者を電気通信役務を営む者に限定せず、前述の通り個人関連情報のうち特定の個人に働きかけが可能となる情報などを規制することが検討されている。

■個人情報保護の基本的な考え方

EUのGDPRでは、個人情報の取り扱いは原則禁止であり、一定の条件を満たすことで取り扱いを許可するものとなっている。条件の中には合理的な理由も含まれるが、その要件が厳しいこともあり、事前にデータ主体から同意を取得することが一般的となっている。米国では、消費者観点で取り扱いに関する透明性の確保とデータ主体（本人）がコントロールできること、特にオプトアウトできることが基本となっている。

対して日本の個人情報保護法は、プライバシーに影響を与える重要な情報に一定の規律を与えるというデータ法的な考え方になっている。そのため情報の区分が細分化し、取り扱いによる結果的な影響よりも取り扱い自体を規律する傾向が強くなっている。例えば、コロナ禍の際に罹患者の情報を集めて対策を行おうとしたが、要配慮個人情報に当たることによる手続きの煩雑さから支障を来したことが挙げられる。そこで3年ごと見直しでは、個別の個人の権利利益への直接的な影響が想定されない個人データの利用に対する規律の考え方が検討されている。さらに、中長期的には「より包括的なテーマや個人情報保護政策全般として、個人情報保護政策が踏まえるべき基本的事項について検討を深めていく」といったことから、社会のデジタル化に対応した見直しが進められている。

■エンフォースメント

エンフォースメントとは、課徴金や差し止め請求などの法律の罰則を執行することを指す。このエンフォースメントに関して、欧米では法令違反に対する制裁が日本よりもはるかに厳しい。EUのGDPRでは、最大で全世界年間売り上げの4％または2000万ユーロのいずれか高い方が制裁金として課される。例えば、2023年にメタ（旧フェイスブック）が12億ユーロの制裁金を課されている。米国では、被害の回復と懲罰的制裁が科される。例えば、エピックゲームズは5億2000万ドルの制裁金を課され、メタは単独の州法違反にもかかわらずテキサス州と14億ドルで和解するなど、極めて巨額なものとなっている。

日本においては、個人情報保護法による指導・助言、勧告、命令などにより是正されることで解決したものとする。一部で民事訴訟による賠償金の判例はあるものの、懲罰的な制裁は非常に限定的で、違反によって得た不当な利益もそのままであることから、抑止効果に疑問があるとされている。これに対して消費者や欧米からの圧力により、課徴金や差し止め請求の導入についての議論が進められている。本稿執筆時点では導入の是非から、どのような違反に対してどのような手続きを行うかへと議論は移っている。2025年の改正で導入されることにはなりそうだが、執行要件や金額も抑制的であり、引き続き欧米との差は大きい。

■共同規制

規制の在り方としては、政府や公的な規制機関

がすべての規律を決定して執行する方法、民間が自主的・自律的に行う方法、その中間で官民が協力して行う方法があり、欧米と日本ではここにも違いがある。EUでは民間による自主規制が法執行における考慮事項となることが明示されており、米国においては消費者団体による監視や提訴が大きな抑止効果をもたらしている。日本においても認定個人情報保護団体の規定があるが、インセンティブもエンフォースメントも極めて小さいため、実態として機能しているとは言えない状況にある。

官民の協力による共同規制とは、業界や領域ごとに異なる事情、進化や変化が速い状況にある場合などに、規制機関による法律の策定や改正の遅れとリソース不足を解決する方法として有効とされている。また、後述するプライバシー強化技術や認証制度を活用するためにも重要と考えられている。欧米では民間の自主規制に対して一定のエンフォースメント権限を与え、法の執行を緩和するタイプの共同規制の活用が進んでいる。一方、日本では行政法の考え方として民間がエンフォースメントを行使することについては否定的な意見が主流で、議論が活性化していない。しかし、規制機関である個人情報保護委員会も限界を認識して課題としており、議論も始まっている。

■子どものプライバシー保護

子どもや青少年の保護については、プライバシーに限らず社会のデジタル化に伴う変化を受けてあらゆる領域で議論が進められている。プライバシー保護については、グローバルで詳細や強弱について多少の違いはあるものの、おおむね一致した方向性となっている。ここで注意したいのは、プライバシーの保護と誹謗中傷を含む犯罪や教育上の悪影響防止は必ずしも同じ視点ではないということだ。例えば、オーストラリアにおける16歳未満のSNS利用禁止は後者が目的であり、プライバシー保護の法制度としてのものではない。この区別ができていない中で、プライバシー保護制度において安易に特定のサービスなどの禁止が検討されるのは危険であると考えられている。

一般的に子どもや青少年のプライバシー保護は、成長過程での判断能力の不足を補うものとして考えられている。つまり、プライバシーに関するリスクの排除や低減が目的である。そのため、対象とする年齢とその年齢においてどのようなリスクに対処するかに焦点が当てられ、低年齢化するほど保護の度合いが強く、年齢が上がるに従いリテラシーの向上に重点が移っていく。ただし、各国・地域において子ども、児童、青少年、ティーンエージャー、未成年といった区分の法的あるいは社会的通念が異なっており、特に13〜18歳における取り扱いが異なっている。一方で、特に保護を必要としているのはおおむね13歳未満としている点では、ほぼ共通している。プライバシーに関する情報の取り扱いについて親権者等の同意が必要とされ、プロファイリングによる広告が禁止されるのが一般的だ。

欧米で議論されているのは、この年齢を引き上げることや、大人の子どもへの干渉に一定の規制を設けることなどで、特に米国ではCOPPA 2.0やKOSAといった法律が審議中である。日本にはこれまで子どもを対象とする明確な規制はなかったが、個人情報保護法の3年ごと見直しや総務省のSPSIにて検討が進められており、2025年にはグローバルに近い規制が導入されることになるだろう。

■ダークパターン

総務省のSPSIでは、ダークパターンを「サービスの利用者を欺いたり操作したりするような方法又は利用者が情報を得た上で自由に決定を行う能

力を実質的に歪（ゆが）めたり損なったりする方法で、ユーザインタフェースを設計・構成・運営すること」と定義している。一言で表すとデジタルにおける「欺瞞（ぎまん）的な方法」による行為全般がダークパターンと言える。

欧米では明確に禁止されており、日本でも消費者取引において禁止されているが、プライバシー保護の観点では十分とは言えない状況にある。例えば、個人情報の第三者提供や要配慮個人情報取得などの同意取得が必要な場面で、同意をデフォルトにしたり拒否を目立たなくしたりする、オプトアウトの手続きを煩雑にしたりすることはダークパターンに当たるが、明確に違法とされているとは言えない。この点が問題視されており、ガイドライン等で具体的な指針を示すことが検討されている。

■プロファイリングとサードパーティーcookie

グーグルのChromeがサードパーティーcookieの廃止を取りやめたことは2024年の大きなトピックの一つであったが、これにより、プロファイリングが従来通り行えると考えるのは早計である。前述の通り、欧米ではサードパーティーcookieをはじめとするプロファイリングに必要となる識別子は個人情報であり、EUでは同意取得、米国ではオプトアウトが前提となっている。日本でも、前回の個人情報保護法改正においてプロファイリングを行う場合には、利用目的を具体的に説明することが義務化されている。

さらに、前述の通り、個人関連情報のうち規制強化が検討されているものは、大半がプロファイリングに利用される識別子である。検討半ばではあるが、少なくともサードパーティーcookieや広告ID、さらにはユニバーサルID作成の基となるメールアドレスなどへの規制は強まると同時に、これらの情報を利用したプロファイリングは目的を具体的かつ明確にすることが求められることになるだろう。その際には、前項のダークパターン規制も順守することが求められる。

■プライバシー強化技術

データを暗号化したまま分析する秘密計算、一定の偽の情報を追加するなどの差分プライバシーなど、データの秘匿性を高めたり個人特定の可能性を低減したりするプライバシー強化技術（Privacy Enhancing Technologies：PETs）が数多く開発され、進化が加速している。これに伴って、欧米ではこれを活用できるようにする法制度の整備が進められている。EUでは官民での研究が進められていると同時に、事故が起こったときにPETsを正しく利用していた場合には一定の考慮、つまり罰則の軽減が行われるようにしようとしている。

日本では、暗号化などを行った場合でも実体は個人情報という前提であることから、PETsを活用するインセンティブが働かず、普及の妨げとなっている。これに対して、安全管理措置の手段として活用すべきという意見が高まっており、対応の検討が始まっている。

■認証制度

世界各国のプライバシー規制機関などが集まる2024年10月の世界プライバシー会議（Global Privacy Assembly：GPA）にて、プライバシー保護の認証制度について、以下の通り決議された。「多くの国・地域のデータ保護法に認証制度の活用に係る規定があることや、認証制度の活用が効果的な執行を可能にする点等に鑑み、①認証制度の活用をデータ保護の一般原則とみなすこと、②適切な場合に認証制度への遵守を規制の緩和要因として考慮する等、法の範囲内で制度活用を奨励

すること、③国際フォーラムを通じ認証制度に関する国際協力を推進することについて、提唱し、標榜するもの」[1]

EUでは既に、ユーロプライバシーと呼ばれる認証制度が上記の内容に沿った形で実現しており、EU以外への展開も進められている。国際標準規格でも、いわゆる情報セキュリティマネジメントシステム（Information Security Management System：ISMS）認証であるISO 27001にプライバシー情報マネジメントシステム（Privacy Information Management System：PIMS）を上乗せするためのISO 27701が発行されており、認証も始まっている。APEC（アジア太平洋経済協力会議）においても越境プライバシールール（Cross Border Privacy Rules：CBPR）をグローバル化することが進められており、英国が準会員として参加している。これらを軸に、各国で共通に通用する認証制度の構築が進むことが想定される。

■今後の動向

日本では中長期での個人情報保護法の在り方についての議論が始まったが、その場合に最も重要な前提となる、社会のデジタル化に対応した他省庁も含めた政策デザインが立案半ばである。そのため、当面は個別の懸案事項の解決が優先される状態となっている。立法根拠が明確で構造化されているEUにおいても、また個別事案に対して事後的な立法となっている米国においても、懸案事項は日本と大きく変わらず、解決の方向性は極めて似たものとなっている。ただし、個人情報の定義が異なる罰則の在り方など、日本と欧米の制度運用における実態の相違は小さくはない。

デジタル社会では国境を越えたデータ流通が常態化するため、プライバシー保護もグローバルでの調和、いわゆるスタンダード化へと向かわざるを得ない。現在の日本のプライバシー保護制度は、決して意図して欧米のまねをしようとしているわけでも、日本独自の道を目指しているわけでもない。デジタル社会のグローバル化の潮流から遅れまいとしている状況であり、その結果として先行している欧米に近づくものとなるのは必然である。日本のデジタル政策が信頼性のある自由なデータ流通（Data Free Flow with Trust：DFFT）をベースとする限り、グローバルスタンダード化は避けて通れない。従って、先行者優位のデジタル市場形成が進んでいる欧米の制度設計とハーモナイズさせることは必須事項である。その結果、差分の解消が進み、ますます欧米の規制に近づくこととなる。さらに、社会のデジタル化が加速していることから、プライバシー保護制度の改正も加速することになるだろう。

1. 個人情報保護委員会、「第308回個人情報保護委員会」、資料2-2、2024年12月4日
https://www.ppc.go.jp/aboutus/minutes/2024/20241204/

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および株式会社インプレスが1996年～2025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および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 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp