

特集

オンライン利用者保護規制とデータ利活用

I

個人情報保護を越えるプライバシーに関する新たな規制の全体像
～安心安全なデータ利活用に必要なこととは～

一般財団法人日本情報経済社会推進協会 電子情報利活用研究部 主席研究員 寺田 眞治

1. 顕在化した新たなプライバシーの危機

2022年施行の個人情報保護法¹では、「個人関連情報」が新たに定義づけられた。端末の識別子（端末ID）、WEBブラウザのcookieやスマートフォンのOSによる広告ID、またこれら識別子や位置情報等により収集された閲覧履歴、検索履歴、行動履歴、購買履歴などが代表的であるが、これらに限らず広く個人に関連する情報とされている。「個人関連情報」は、それだけでは個人情報保護法では対象とならないが、第三者へ提供された際に当該第三者において個人情報となる場合の規律を定めている。これにより、無法地帯に近かった個人情報以外の個人に関連する情報の利用についても、一定の歯止めがかかることとなった。

また、2022年6月17日に公布され、1年以内に施行される改正電気通信事業法²では、特定利用者情報の適正な取扱いに関する規律、利用者情報の外部送信に関する規律が新たに定められた。電気通信事業法における利用者情報とは、個人情報だけに限られるものではない。PC、スマートフォン、タブレット、その他スマートデバイス等において、機器から外部に送信される利用者に関連する情報全般を指す。端末ID、cookie、広告ID、位置情報、各種履歴だけではなく、WEBブラウザやOSのバージョン情報をはじめ端末の機能や能力を示す情報なども含まれ、個人関連情報と同等以上の広い定義となっている。この規律により、プライバシーを保護する

という観点では、多くの事業者で個人情報の保護だけでは法令遵守とは言えず、電気通信事業法の遵守も必要となった。

規律制定の直接的な原因として、2018年に発覚したケンブリッジ・アナリティカによるFacebookの情報を利用した米大統領選挙への干渉、2019年に起きたリクナビによる内定辞退率データ提供による学生への不利益や差別等が語られることが多い。これらは大規模であったためメディアに大きく取り上げられたが、これまで燻っていたプライバシー侵害への懸念が顕在化した象徴的な事件であると言える。

事件として報道されなくとも、オンライン上の広告やレコメンドに対する消費者の不安が大きくなっていることは、メディアで頻繁に取り上げられている。広告やレコメンドの多くは、個人を特定していない識別子（cookie、広告ID等）を元にさまざまな履歴等を収集し、属性、嗜好性や行動を推測して行っていることから、個人情報保護法の対象外とされてきた。しかし、技術の進化により、大量の情報の分析から精度の高い推測が可能となり、消費者は自身を追跡されていると感じることが増えてきている。それだけではなく、特定のカテゴリに分類され、意思決定を他者により操作されるという事案も顕在化しつつある。選挙に干渉するような社会的影響を与えるためには、ケンブリッジ・アナリティカ事件のように個人を特定する必要はなく、特定のカテゴリにアプローチすれば可能である。

1 <https://www.ppc.go.jp/personalinfo/legal/>

2 <https://elaws.e-gov.go.jp/document?lawid=359AC00000000086>

また、IoT機器の普及により本人が認知できない情報の収集が加速している。今やいたるところにカメラが設置され、防犯用途ではないマーケティング利用として人流、店舗内動線の把握等が一般化しつつある。顔認識も高精度化が進み、画像から年齢や性別を推測して最適なサービスや広告が提供されることも珍しくなくなってきた。個人を特定した場合には個人情報保護法による規律を守らなければならないが、特定せずとも個人に影響を与えることが可能になってきている。消費者にとっては、あたかも本人が特定されてターゲットにされているような不安を感じる場面が増えている。

さらにAIの進化により、これまで想定されていなかった差別や不利益を与えうることがわかってきた。たとえば、過去の人事データでAIの学習を行った場合に、過去に人種的差別や性差別のようなデータが含まれていると、これをそのまま判断材料としてしまうといったことが実際に起こっている。Amazonで採用AIが女性差別を行っていたことが2018年に発覚しているが、このようなことを恣意的に利用すれば、リクナビの内定辞退率データの提供のような事例になる。

このように技術の急速な進化や分析能力の向上により、個人情報保護法だけでは、もはや消費者への差別、不利益を防ぎ、不安を払拭するプライバシーの保護はできなくなっているのが現状である。

2. プライバシー保護の世界の潮流と日本の現在地

EUでは2016年にGDPR（一般データ保護規則：General Data Protection Regulation）³が発行され、2018年に施行されている。欧州連合基本権憲章における基本的人権の保護を目的とするものであり、個人を特定するデータだけでなく、個人に関連し

うるあらゆるデータを対象として、取り扱う場合には同意の取得を原則としている。さらにGDPRの特別法として、電子通信における端末内の情報を保護することを目的としたePrivacy規則⁴の制定に向けた審議も進められている。ePrivacy規則案では、端末内にあるデータ全体を対象としており、GDPRにおける対象データの曖昧さが解消されている。

また、DSA（デジタルサービス法：Digital Service Act）、DMA（デジタル市場法：Digital Market Act）⁵が欧州議会、欧州評議会によって合意がなされ、2023年～2024年に施行される。こちらは主に大規模なプラットフォームやグローバルテックを対象としており、競争法の観点での規制が中心であるが、プライバシーに関する透明性や同意の取得等についても厳しい要求があり、日本の大手の事業者にとっても無縁のものではない。

米国では、プライバシーの保護は消費者保護に含まれると位置付けることが一般化しており、多様な動きが同時に進行している。規制が先行するカリフォルニア州では、2020年にCCPA（カリフォルニア州消費者プライバシー法：California Consumer Privacy Act）⁶が施行され、これをさらに発展させたCPRA（カリフォルニア州プライバシー権法：California Privacy Rights Act）が2023年に施行される予定となっている。これは消費者の権利強化が目的で、本人によるデータのコントロール権を大幅に認めるものとなっている。本人へのデータの開示や削除等だけでなく、特にオプトアウトの義務化が特徴的である。この場合の本人のデータとは特定の個人を識別できるものだけではない。GDPRとほぼ同様に個人に関連するデータはすべて含まれている。

規制の強度の濃淡はあるものの、独自の州法の制定が進められている中、連邦としての法制定についても議論が進められているが、現時点で制定のめどは立っていない。

3 <https://www.ppc.go.jp/enforcement/infoprovision/laws/>

4 <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>

5 <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

6 <https://www.ppc.go.jp/enforcement/infoprovision/laws/CCPA/>

一方で、連邦としての消費者保護の執行機関であるFTC（連邦取引委員会：Federal Trade Commission）は積極的に消費者プライバシーの保護に動いている。FTC法第5条「商取引における又は商取引に影響を及ぼす不公正若しくは欺瞞的な行為又は慣行は、本法により違法と宣言する。」を根拠に、消費者のデータを取り扱う場合のアカウントビリティを強く求めている。この場合のデータも個人を特定するものだけではなく、広く消費者に関連するデータを対象としている。

中国でも2021年に個人情報保護法が施行されるなど、各国で同様のプライバシー保護法制の制定が急速に進んでいるが、その多くがEUのGDPRをベースにしたと思われるものである。必然的に対象としては、特定の個人を識別したものだけではなく広く個人に関連するデータとなっている。

世界のプライバシー保護法制の動向は、プライバシーを保護するために個人に関連するデータあるいは個人が保有する端末内のデータの取扱いを規律することが主流である。これに対し日本の個人情報保護法は、基本的に「特定の個人を識別することができるもの」およびこれより作成される匿名加工情報や仮名加工情報を規律するものであり、対象範囲が狭くなっている。2022年改正で「個人関連情報」

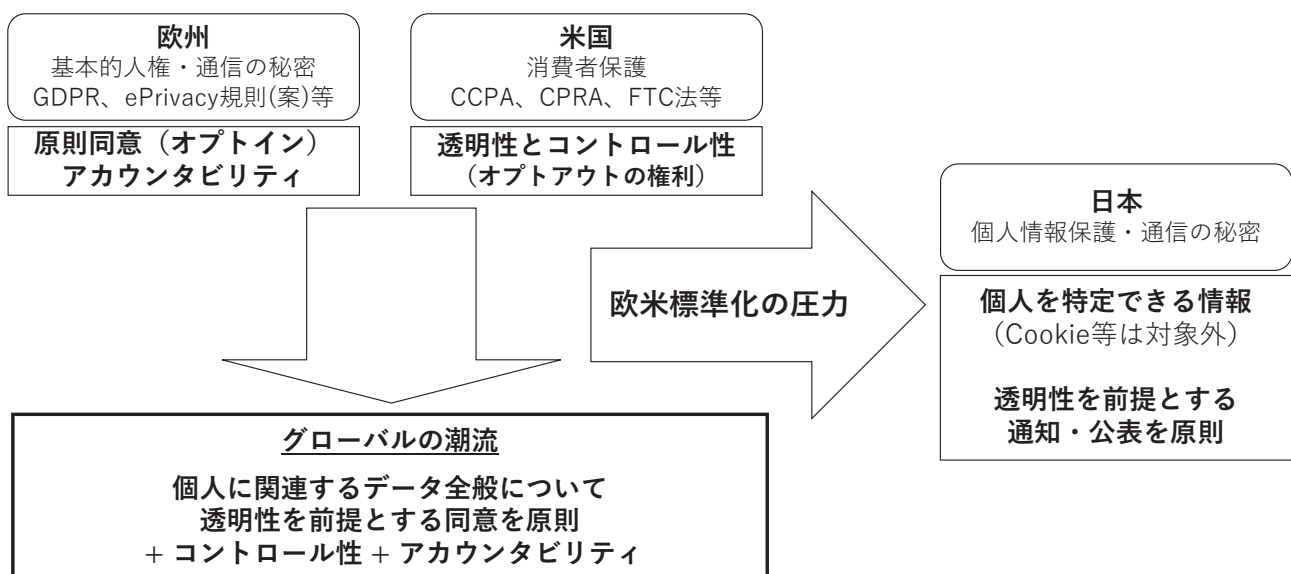
としてこれら以外の個人に関連する情報と定義されはしたが、第三者提供先で個人情報とならない限り対象外とされている。

前項で述べたとおり、プライバシー保護というコンテキストにおいては、個人情報保護法だけでは足りないということが明白になってきている。そのため、日本においてもグローバルと足並みを揃える方向で、さまざまな動きが急激に活発化しているのが現在の状況である。

3. プライバシー保護への多方面からの圧力

プライバシー保護の視点は、必ずしも個人情報保護法の改正という観点だけではなく、下記のようにさまざまな方向から提起されている。

- 1) 個人に関する情報を集積しているプラットフォーム事業者に対する規制
- 2) 個人に関する情報を広範囲に流通させる広告に対する規制
- 3) 利用者の端末からの情報の取得という機能に対する規制
- 4) IoT機器等による消費者の情報収集に対する規制
- 5) 企業活動におけるガバナンスとしてのプライバシー保護



図表 I-1. 世界の潮流と日本

以下、各規制について説明する。

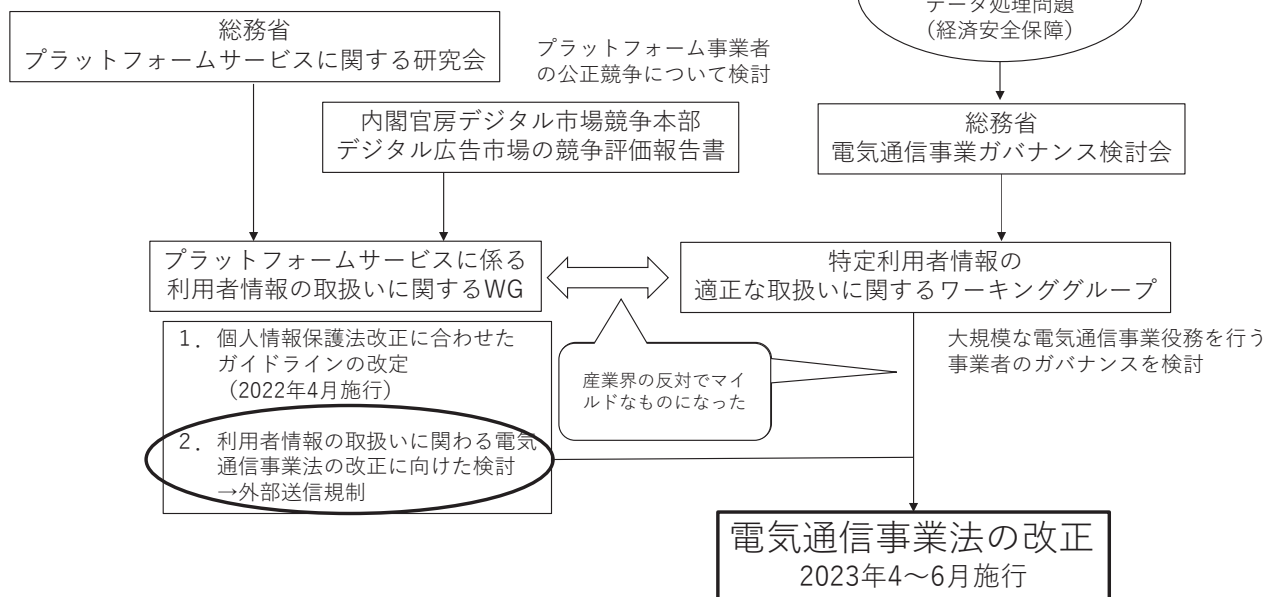
1) のプラットフォーム規制の第一の目的は、公正な市場競争を実現することにあるが、阻害要因の一つとして、大量の消費者のデータを独占的に取り扱っていることにあると考えられている。大量の消費者の嗜好や行動の推測を元にした排他的な事業展開、消費者へのアクセスを独占するゲートウェイ機能による不公正なルール強要等が問題とされている。したがって、優越的な地位の濫用を防ぐためには、消費者の情報の取扱いについての透明性を高めることがまず求められることになる。この場合の優越的地位の濫用の防止は、事業者間だけではなく、プラットフォーム事業者と消費者の間にも適用されるとされている。結果、透明性の確保は、すなわちプライバシーの保護が十分に行われているかも露わにすることになる。これを法制度化したものが、2021年に施行された経済産業省の「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」⁷（デジタルプラットフォーム取引透明化法）⁸である。当初のECのマーケットプレイス、スマートフォンのアプリストアに続いて2022年には

広告のプラットフォームへと対象が拡大されている。

2) 上記1) においても広告プラットフォームについての規制が含まれているが、こちらはプラットフォームという事業形態や規模の大小とは関係なく、差別、不利益や不安感を与える利用者情報を利用した広告を対象とするものである。メディア等ではcookie規制やターゲティング広告規制といった表現が目立つが、これに限られるものではない。2021年に内閣官房デジタル市場競争本部が「デジタル広告市場の競争評価報告書」⁸を発表しているが、この中でデジタル広告における利用者情報の取扱いについては、総務省の「電気通信事業における個人情報保護のガイドライン」にて対応することを指示している。この流れが次の3) に合流し、電気通信事業法の改正へとつながった。

3) 利用者の端末からの情報収集について新たな規制をもたらしたのは、LINEの利用者の個人データが中国の委託先で閲覧可能になっていたことが発

プラットフォーム事業者が大量の利用者情報を活用してサービスを提供していることを踏まえ、利用者情報の適切な取扱いの確保の在り方等について検討



図表 I - 2. 電気通信事業法改正の経緯

7 https://www.meti.go.jp/policy/mono_info_service/digitalplatform/index.html

8 www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai5/siryou3s.pdf

覚したことにある。総務省の電気通信事業におけるガバナンス検討会において、当初は端末の利用者情報を取得する場合には同意を義務化するというEUの規制と同等の厳しいものが提示されたが、産業界の反発が強く、大きく後退している。この流れと2)を検討していた同じく総務省のプラットフォームサービスに関する研究会の検討結果が合流して、2022年6月に電気通信事業法が改正された。PC、スマートフォン、タブレット、スマートデバイス等の端末から送信される情報を個人情報も含めて利用者情報とし、一定の規律を設けるものである。利用者の利益に及ぼす影響が大きいものを特定利用者情報とし、一定数以上の利用者を抱える大手のプラットフォームや電気通信事業者を指定し、ガバナンス強化を義務化した。また、利用者の利益に及ぼす影響が少なくないものとして、規模の大小にかかわらず電気通信を営む者が端末から利用者情報を外部に送信させる場合には、通知・公表、同意、オプトアウトのいずれかを行うことが義務付けられる。いずれも施行は2023年の春から夏にかけてである。

4) のIoT機器については、カメラ画像に関する検討が早くから進められている。特定の個人を識別できる場合には個人情報保護法に従うことになるが、消費者はカメラの存在に気付きにくい、防犯上の監視以外の利用目的について認識されづらく不安感を煽る等のさまざまな課題を抱えている。そのため、経済産業省と総務省によるデータ流通促進ワーキンググループのカメラ画像利活用サブワーキンググループが「カメラ画像利活用ガイドブック」⁹を2017年に発表した。技術革新に伴う問題の複雑化が年々加速していることから、毎年のように更新されている。今後は、同様の課題を抱えるカメラ以外のセンサー機器についても検討が進められる可能性がある。

5) は、個人情報や利用者情報を扱う事業者全般に対してのものとなる。法令違反ではなくともプラ

イバシー侵害への危惧について、メディアやSNSで炎上する事案が増えている。そのため、事業者はどうか対応するべきかといった不安を抱え、消費者は事業者への不信感を高めており、事業者と消費者間での信頼関係が揺らいでいる。これを解決するために、事業者のガバナンスにプライバシーを組み込むことが提唱された。4) と同じくデータ流通促進ワーキンググループの企業のプライバシーガバナンスモデル検討会から「DX時代における企業のプライバシーガバナンスガイドブック」¹⁰が発行されている。こちらも毎年更新されており、プライバシーの課題への対応がますます複雑化、高度化していることが見て取れる証左となっている。

上記以外にも、必ずしも特定の個人を識別できるデータだけではなく、個人に関連する可能性のあるデータの取扱いについて、さまざまな方面から問題提起がされている。たとえば医療分野における匿名加工されたデータのように個人情報でなくなったものの、車載のプロブにより取得されるデータのように直接個人を対象とはしていないが高精度な推測が可能となるもの等、何らかのデータを取り扱う際にはプライバシーに影響を与える可能性が潜んでいることは少なくない。結果的に、ほとんどの事業者や組織は、もはやプライバシーへの対応を検討することから逃れることはできなくなりつつあると言えるだろう。

4. グローバルのプライバシー保護の日本への影響

ここまでは法律や制度の面からプライバシー保護の潮流を見てきたが、この潮流を受けて対応した事業者の影響が、幅広く他の事業者へ影響を及ぼす事例も増えている。特にプラットフォーム事業者によるプライバシーに関するルール策定が、取引事業者に大きな影響を与えている。代表的なものとしては、AppleやGoogleの3rd party cookieの利用制限

9 <https://www.meti.go.jp/press/2021/03/20220330001/20220330001.html>

10 <https://www.meti.go.jp/press/2021/02/20220218001/20220218001.html>

や撤廃の動きである。Appleは広告IDの利用についても、グローバルで同意の取得を義務付けている。いずれもGDPRの規制を受けて、自社のプラットフォームを利用する他の事業者にも同様の規制を強要するものとなっている。日本の個人情報保護法上は、3rd party cookieも広告IDも特定の個人に結びつかない限り規制の対象とはなっていない。したがってこのプラットフォームのルールは、日本国内においては遵守しなくとも法令違反とはならないにも関わらず、プラットフォームを利用する上では必須である。

グローバルでは、日本の個人情報の定義より広い「個人に関連する可能性のあるデータ」を保護の対象としている。そのためこの規律を前提とするグローバル企業によるルールへの準拠は、たとえ日本国内のみを事業の対象とする場合であっても逃れることができない。グローバル企業との取引をする場合には、グローバルの規制が強まるに従って、ますます同様の規制を受けることになるのは間違いないだろう。

このようなグローバルの潮流は、わが国の法制度の改正にも影響を与えつつある。電気通信事業法の改正がもっとも顕著な例であるが、EUのような同意の取得、米国のカリフォルニア州法のようなオプトアウトを原則とするほど厳しいものではない。し

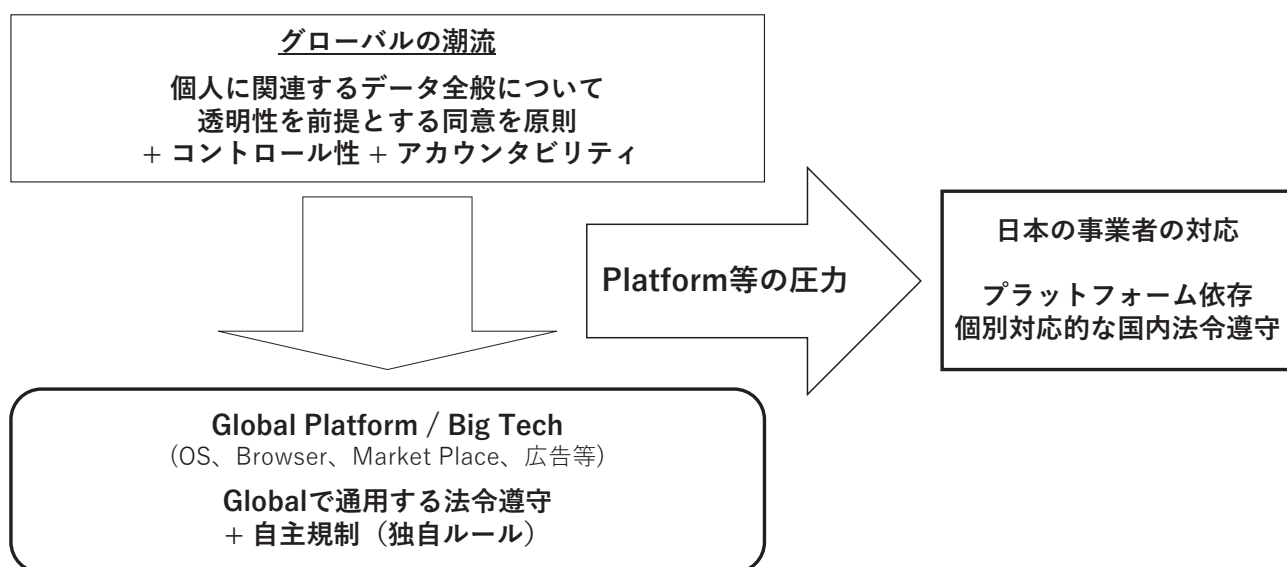
かし、日本の個人情報保護法より、一步グローバルの規律に近づいたことになる。個人情報保護法も電気通信事業法もグローバルの規律との調和を大きな柱として打ち出していることから、規律の強化は今後さらに進むことになるだろう。

では、今後進むであろう規律の方向性、内容の基本的な考え方とはどのようなものであろうか。

まず第1に挙げられるのは透明性の確保である。これに関しては日本、EU、米国で大きな違いはない。日本でも通知または公表すべきとされている情報は細かく指定されている。直近では、2022年施行の改正個人情報保護法において海外へのデータ送信、保存、処理について、当該国の情報の提供が強化されている。

続いて重要となるのがアカウントビリティである。一般にアカウントビリティは説明責任と訳されるが、説明し、それを遵守し、守れなかった場合には責任を取るところまでが含まれる。GDPRでは明確にされており、米国においてもFTC法における「欺瞞的行為を違法とする」という意味に含まれるものである。

本人によるコントロールという考え方を実装することも必須になる。「透明性の確保」「アカウントビ



図表 I-3. プラットフォームの日本への影響

リティ」だけでは、一方的に事業者側のルールに従うような形式になりかねない。EUの基本的人権、米国の消費者の権利といった考え方の中には、差別や不利益を受けないことがベースにあり、消費者はこれを防ぐための権利が与えられている。ダッシュボードと言われる本人のデータの状況を確認し操作できる機能、CMP（同意管理プラットフォーム：Consent Management Platform）という本人が同意や不同意をした内容を事業者間で共有できるツール等、さまざまなツールが開発され普及しつつある。このような本人によるコントロールを実現するためのツールを実装することは、今後必須になってくるであろう。

これに加えて、プライバシーガバナンスの強化が求められている。こちらも米国ではプライバシーリスクを企業のリスクと捉える動きが顕著になっており、コーポレートガバナンス報告書に記載されることが増えている。日本においても前述したガイドブックが発行されており、これに準拠する動きが始まっている。

5. データ利活用への指針

これまで述べてきたとおり、個人情報に限らず個人関連情報、利用者情報はすべてプライバシーに関連する可能性があるデータである。さらに、直接本人に関連しないと思われていたデータも、近年の技術の急激な進化や分析能力の向上により、プライバシーに影響を及ぼす可能性が否定できない状況になってきている。データを利用した事業を行う上では、いかなる場合でもプライバシーへの影響の有無を判断し、影響の可能性がある場合には何らかの対応を考えることが必須となりつつある。コンプライアンスについては法に従えばよいが、プライバシーの保護については法を超えるものがあり、明確な規律は存在しない。では、安全なデータ利活用を実現するためにはどうすればよいのか。それにこたえるものとして、以下のとおり、すでにいくつかの指針

や手法が存在している。

- 1) プライバシーガバナンスのガイドブック
- 2) PIA（プライバシー影響評価）
- 3) PIMS（プライバシー情報マネジメントシステム）認証

以下、指針、手法について説明する。

1) プライバシーガバナンスは前項で触れたとおり、コーポレートガバナンスとしての位置付けが進んでいる。これはプライバシーを事業上のリスクと捉え、事業者が自主的にリスクマネジメントを行うことで確立されるものである。「DX時代における企業のプライバシーガバナンスガイドブック」では、経営者がプライバシーガバナンスの姿勢の明文化、プライバシー保護責任者の指名、プライバシーへの取組みに対するリソースの投入を行い、体制の構築、運用ルールの策定と周知、企業内のプライバシーに関する文化の醸成、消費者とのコミュニケーション、その他のステークホルダーとのコミュニケーションを行うこととされている。これにより消費者との信頼を獲得し、ひいては事業者の価値の向上が図られる。

2) プライバシーのリスクマネジメントの具体的な方法も確立されている。国際標準であるISO/IEC 29134が2021年に「JIS X 9251情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン」¹¹として発行されている。個人情報等の収集を伴う事業の開始や変更の際に、個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法のガイドラインであり、事業の企画・設計段階から個人情報等の保護の観点を考慮するプロセスを事業のライフサイクルに組み込むものである。個人情報保護委員会でも民間の自主的取組みとして紹介されている。消費者の不安や懸念を払拭するために、個人情報保護法の遵守にとどまらない範囲も含めて対応することが重要としている。

11 https://webdesk.jsa.or.jp/books/W11M0090/?bunsyo_id=JIS%20X%209251:2021

3) プライバシーのリスクマネジメントが適切に行われているかを第三者が認証する仕組みの活用も有用である。日本の個人情報保護法への対応としてはプライバシーマークが普及しており、個人情報を超えるプライバシーリスクについても対応が拡大されつつある。

海外での事業展開も想定される場合には、すでに普及が進んでいるISMS（情報セキュリティマネジメントシステム：Information Security Management System）を拡張してPIMS（プライバシー情報マネジメントシステム：Privacy Information Management System）を確立するISO/IEC 27701¹²が2019年に発行されている。すでに日本でも認証が行われているが、その重要性に鑑みてJIS化が進められており、2023年には発行される予定である。プライバシーのリスクがあるものを自ら選定し、リスクに対応する管理策に沿って対策を行うものである。日本における個人情報に限られるものではなく、各国の法規制に沿うことができるものである。

これら3つの指針、手法は、それぞれに関係が深くどれかだけを行えばよいというものではない。事業者自らがリスクを自覚すれば、リスクを可視化して対策を行い、第三者に検証してもらうという一連

の流れの中で、重要なポイントを実装するために必要な事項を抜き出したものであり、どこから始めても、上記の3つをすべて網羅しなければ、十分とは言えないことに気づくはずだ。

プライバシーを保護した安全なデータ利活用を行う上での最上位の概念は、1)のプライバシーガバナンスの確立であるが、事業者の経営レベルを始点とすることからハードルは低くない。したがって、喫緊の実務上のリスク対策として、個人情報保護委員会からも情報発信されている2)のPIAから始めるのは現実的である。あるいは社会的な信頼を得ることを目的として3)の認証取得から始めるといった順番でも何ら問題はない。この場合には結果的に1)や2)の要素も含まれることになる。

プライバシー保護に対する社会的な視線が急速に厳しくなる中、不安を抱えたままデータを取り扱うより、まずは上記のような確立された方法を実行することが有用である。これはリスク対策という消極的な守りだけではなく、消費者や関係するステークホルダーからの信頼獲得という優位性を得るための積極的な経営戦略にも通じる。グローバルのプライバシー保護の潮流は、近いうちに日本にもやってくることは間違いない。早期に、これをキャッチアップして準備しておくことが望まれる。

12 https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=ISO%2FIEC+27701%3A2019