2022 WINTER

IT-REPORT

特集

▽「オンライン利用者保護規制とデータ利活用」

Contents

【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～ 01
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

Ⅱ．欧米のプライバシー保護とデータ利活用の動向 09
一般社団法人Privacy by Design Lab
代表理事　栗原 宏平

【JIPDECレポート】

本人に資するPHRサービスの在り方
ー民間PHRサービスの品質と評価の観点からの考察ー 19
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
上河辺 康子

【コラム】

• 個人情報管理のためのデータマッピング・ツールキット 25
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
グループリーダ　松下 尚史

• 海外のプライバシー動向に係る日本への影響 26
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
主査　石井 美穂

• ISMS認証基準（ISO/IEC 27001）の改訂 27
一般財団法人日本情報経済社会推進協会
セキュリティマネジメント推進室 室長　成田 康正

• デジタルトラストと電子証明書の役割 28
一般財団法人日本情報経済社会推進協会
デジタルトラスト評価センター主査　成田 ミキ

• 準天頂衛星システムの今後 29
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
グループリーダ　松下 尚史

〈資料編〉国内外の主な個人情報保護関連の年表 30
情報化に関する動向（2022年4月～2022年9月） 34

JIPDEC
一般財団法人日本情報経済社会推進協会

2022年４月の改正個人情報保護法の全面施行後、６月に電気通信事業法の改正やガイドラインの改正検討が進められており、利用者データを扱う事業者への規制が厳しくなってきています。

改正電気通信事業法は特定の通信事業者ではなくとも、たとえばオンラインサービス関連事業に携わっていたりインターネット検索サービスやSNSの運営、広告収入を得ている事業者なども規制対象となる可能性があることから、規制内容や自社の事業内容を把握し、必要に応じて対応する必要があります。

そこで、本誌では、国内外で新たに検討、成立されたプライバシー保護法規制の動向と、利用者保護をしつつ、データの利活用を図るために、事業者がどう対応すべきか、「オンライン利用者保護規制とデータ利活用」として、特集を組みました。

また、「PHRサービス」「データマッピング」「海外のプライバシー動向の日本に係る影響」「ISO27001 改訂」「デジタルトラスト」「準天頂衛星」の最新動向をテーマに、当協会職員によるレポート、コラムも掲載しています。

あわせて、2022年４月から2022年９月の国内外の情報化動向をとりまとめていますので、今後のIT環境整備の参考にしていただければ幸いです。

2022年12月
一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2022 Winter

Contents

【特集】オンライン利用者保護規制とデータ利活用 …… 01
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～ …… 01
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
Ⅱ．欧米のプライバシー保護とデータ利活用の動向…… 09
一般社団法人Privacy by Design Lab　代表理事　栗原 宏平

【JIPDECレポート】…… 19
本人に資するPHRサービスの在り方
－民間PHRサービスの品質と評価の観点からの考察－　…… 19
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
上河辺 康子

【コラム】…… 25
・個人情報管理のためのデータマッピング・ツールキット…… 25
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
グループリーダ　松下 尚史
・海外のプライバシー動向に係る日本への影響…… 26
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
主査　石井 美穂
・ISMS認証基準（ISO/IEC 27001）の改訂…… 27
一般財団法人日本情報経済社会推進協会　セキュリティマネジメント推進室
室長　成田 康正
・デジタルトラストと電子証明書の役割…… 28
一般財団法人日本情報経済社会推進協会　デジタルトラスト評価センター
主査　成田 ミキ
・準天頂衛星システムの今後…… 29
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
グループリーダ　松下 尚史

〈資料編〉国内外の主な個人情報保護関連の年表 …… 30
情報化に関する動向（2022年4月～2022年9月）…… 34

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よう。

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=359AC0000000086

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き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はなく、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タ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。

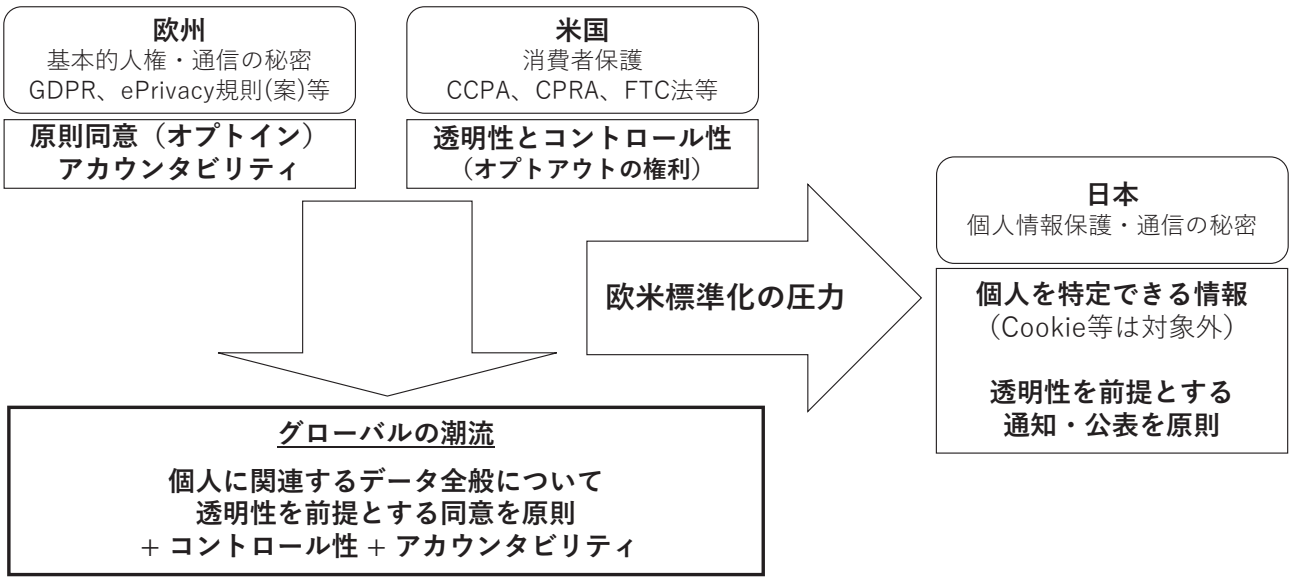
世界のプライバシー保護法制の動向は、プライバシーを保護するために個人に関連するデータあるいは個人が保有する端末内のデータの取扱いを規律することが主流である。これに対し日本の個人情報保護法は、基本的に「特定の個人を識別することができるもの」およびこれより作成される匿名加工情報や仮名加工情報を規律するものであり、対象範囲が狭くなっている。2022年改正で「個人関連情報」としてこれら以外の個人に関連する情報と定義されはしたが、第三者提供先で個人情報とならない限り対象外とされている。

前項で述べたとおり、プライバシー保護というコンテクストにおいては、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取集に対する規制
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



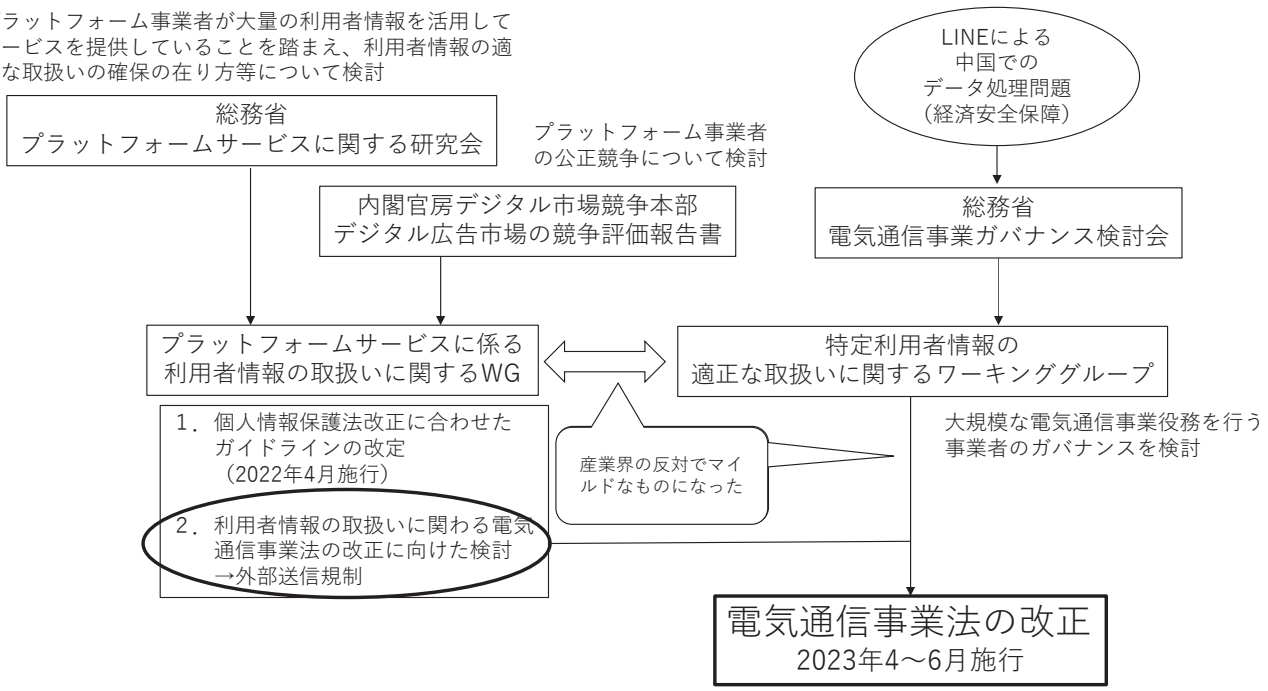
図表Ⅰ－1．世界の潮流と日本

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）」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



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、車載のプロー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　http://www.iotac.jp/wg/data/camera/
10　http://www.iotac.jp/wg/data/govenance/

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。

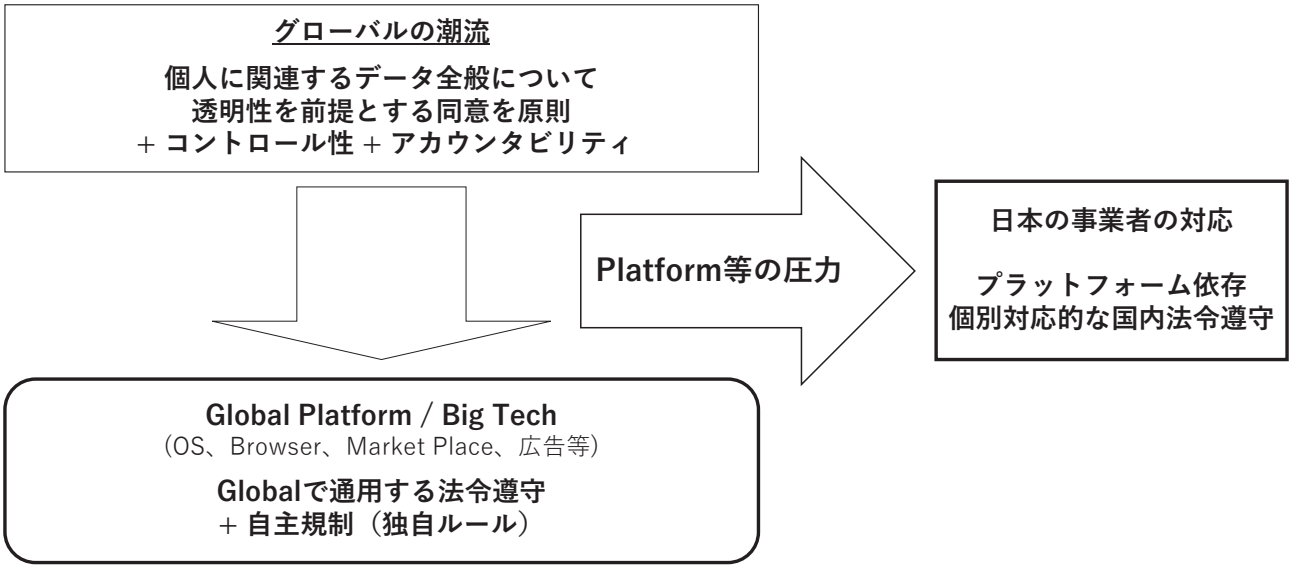
このようなグローバルの潮流は、わが国の法制度の改正にも影響を与えつつある。電気通信事業法の改正がもっとも顕著な例であるが、EUのような同意の取得、米国のカリフォルニア州法のようなオプトアウトを原則とするほど厳しいものではない。しかし、日本の個人情報保護法より、一歩グローバルの規律に近づいたことになる。個人情報保護法も電気通信事業法もグローバルの規律との調和を大きな柱として打ち出していることから、規律の強化は今後さらに進むことになるだろう。

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ういうものであろうか。

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タビリティである。一般にアカウンタ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」「アカウンタビ



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 27701[12]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

Ⅱ 欧米のプライバシー保護とデータ利活用の動向

一般社団法人Privacy by Design Lab　代表理事　**栗原 宏平**

Ⅱ－1　はじめ

本年はわが国で４月１日に施行された改正個人情報保護法に限らず、各国でデジタル規制の進展が著しい一年だった。特に欧州のデータ保護規制については、GDPR（欧州一般データ保護規則）の下で執行件数が大幅に増加している。IT-Report 2020執筆時にはGDPR施行後の２年半で435件（2020年11月８日時点）の制裁が行われていると紹介したが、2022年には1,439件（2022年10月16日時点GDPR Enforcement Trackerより）まで拡大しており、約２年間で1,000件近くの制裁事例が増加したことになる。

デジタル規制については、欧州に限らず、米国、英国でも２年前のレポート寄稿以降に大幅な議論の進展があり、各国が新しい制度設計に向けて議論を進めている。今回のレポートでは2020年以降からの欧米各国の動向も踏まえつつ、2023年に向けて事業者が注目すべきポイントを整理してお伝えする。

Ⅱ－2　2022年までに議論されているプライバシー保護に関する議論の整理

2.1　欧州

欧州では2022年に入るまで主に４つの重要なデジタル関連の制度設計について議論が行われてきた。１つ目が2018年に施行されたGDPRに関する内容、２つ目が主にDSA（デジタルサービス法）、３つ目がDMA（デジタル市場法）、そしてAI法案についてである。

GDPRに関しては、2021年以降各国のデータ保護機関による制裁内容よりも、主に欧州域内の越境データ移転における適切な執行が議題に上がることが多く、GDPR第56条に定められている、代表のデータ保護機関（LSA）による執行（ワンストップショップ制度）が法の下で適切に行われているのかを検討する議論がさかんに行われている。

特に大手テクノロジー企業に対する制裁に関しては、税制上の理由からアイルランドにテクノロジー企業の欧州本社が集中していることもあり、アイルランドのデータ保護機関に対して適切な制裁を行うように、他国のデータ保護機関から強く要求が行われるケースも数多く見られるようになった。

代表のデータ保護機関による執行が適切に行われないケースに対して、各国のデータ保護機関が参加し意思決定を行う機関である欧州データ保護委員会は、アイルランドのデータ保護機関に代わって制裁を要求するような動きを見せている。具体的には2021年の夏のWhatsAppに対する制裁である。この手法は包括的な制裁と呼ばれ、欧州データ保護委員会が各国のデータ保護機関で行われている議論に介入して制裁を実施するケースである。

GDPRに加えてDSAおよびDMAが欧州委員会から提案されている背景としては、大手テクノロジー企業に対する欧州域内での執行が適切に実施されていないのではないかという懸念が大きく関わっている。GDPRとの執行体制を両法案で比較すると、各国のDPAに執行を依存する分散型の体制をもとに設計されたGDPRに対して、DSAおよびDMAに関しては欧州委員会が域内での紛争解決に当たる中央集権型の体制の整備を進めている[1]。

1　https://www.youtube.com/watch?v=vcBG99pi2F0

AI法案に関しても同様の方向性で議論が進められており、今後はデジタル規制がそれぞれ相互に連携し、適切な執行を行うための体制と制度作りに注力することを念頭に置いている。

2.2　米国

米国では2022年に入るまで、連邦プライバシー法を軸にした議論が継続して行われてきた。加えて、米国内の各州で独自のプライバシー法が数多く制定され、特にカリフォルニア州では2020年に施行されたCCPA（カリフォルニア州消費者プライバシー法）に加えて、2020年に住民投票で可決したCPRA（カリフォルニア州プライバシー権法）が2023年に施行されることから、施行に向けた準備が進められている。CCPAの下での執行事例も数多く報告されるようになってきており、施行から８月24日時点のアップデートで40件が紹介[2]されている。

さらに、これまでプライバシー事案については慎重であったFTC（連邦取引委員会）による制裁件数も徐々に増加し始めており、米テキサス州の中絶禁止法に関する議論が始まって以降、デジタルサービスに対するプライバシー強化の声が高まってきており、政府による民間企業への要請がより強く求められるように変わってきている。

越境データ取引に関しては、2020年に欧州司法裁判所によって不当であると判決が下された米欧のプライバシーシールドの問題を受け、バイデン政権へ移行して以来、両国の代表者が水面下で交渉を進めており、円滑に越境データ移転を行うことができる対策を足元で検討してきている。

2.3　英国

英国では2020年のブレグジット以降、英国と欧州間でデータ移転を行うための十分性認定の取付けと、英国内でのGDPRに類似した法律をもとに運用を進めてきている。一方で、英国事業者からはGDPR基準が事業者へ過度な負担を強いることになるという声もあり、欧州基準のデジタル規制に対して独自の改革案提出の検討を進めている。

Ⅱ－3　2022年の欧米各国によるデータ保護制度の動き

2022年は欧米各国のデジタル規制がより強化され、具体的な法律の解釈も含めて大きな進展があった年になった。

3.1　欧州

欧州では前段で紹介したようにGDPRの下での制裁が引き続き各国で行われている。2021年まで問題視されていたアイルランドデータ保護機関による制裁は、欧州データ保護委員会による包括的な決定通知により、メタプラットフォーム社に対する580億円の制裁金を９月に発表した。2021年から問題に上がっている欧州域内の越境データ移転への適切な執行を行うため、各国のデータ保護機関は欧州データ保護委員会の呼びかけの下でオーストリアのウィーンで開催された“ウィーン会議”と呼ばれる会合に出席し、今後の執行体制について議論を行った。

欧州各国のデータ保護機関によって“ウィーン会議”で話し合われた内容は“ウィーン宣言”[3]として４月28日に発表された。宣言内容を要約すると、３つのテーマに注力していくことがうかがわれる。

①戦略的な執行ケースに注力するために協力体制を推進
②効率的かつ実効性のある執行のための戦略的なケースの決定

2　https://oag.ca.gov/privacy/ccpa/enforcement
3　https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf

③国ごとの異なる法制度を前提とした執行実務における救済措置

これまでは巨額の制裁金を始めとして、GDPR自体を広く周知するような動きを中心に進めていたが、データ保護戦略を周知から実務的な執行体制へと転換したことが2022年に決定された最も大きな動きである。

ウィーン会議で話し合われた執行手続きに関する課題は、10月10日に欧州委員会のディディエ・レンデルス司法委員へ、欧州委員会より一覧リストとして通達され[4]、欧州データ保護委員会（EDPB）が、現存の課題を踏まえつつ欧州全域での執行体制の強化を欧州委員会に報告している。欧州委員会に通達された執行手続きの課題は以下の５つの点について言及している。

①関連組織による管理手順
②手続きの締切り
③申立てに対する認可および拒否の要求範囲
④執行機関による調査能力
⑤実務的な協力手順

この決定に加えて、欧州データ保護委員会および欧州データ保護監察機関（EDPS）は９月12日に欧州議会、および欧州評議会に対して追加人員に対する予算要求[5]を行い、以下の３点の強化を行うと公表している。

①欧州データ保護委員会の人員を現在の40人から８名増やして、より強固な執行体制を強化する
②テクノロジー領域での執行のための十分な知見を強化する
③GDPRに適応するための法的なガイダンスの発行を強化する

欧州全域の動きとしては、2022年は“ウィーン会議”を起点とし、域内での執行および協力体制の強化へと戦略を大きく変化させ始めている。

2020年12月に欧州委員会によってデジタルパッケージ法案として提出されたDSA、DMAについては、DMAが３月24日、DSAが４月23日に欧州議会および欧州評議会によって暫定合意に至った[6, 7]。この暫定合意によって、大規模プラットフォーム事業者および、大規模検索エンジン提供事業者への要求がより厳しくなる動きが進んでいる。今後は、欧州議会および評議会の代表者によってそれぞれ署名が行われたのちに欧州連合官報が発行され、15カ月の期間を経て有効化される予定である。

4 https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf
5 https://edps.europa.eu/system/files/2022-09/22-09-12_edps-edpb-open-letter-budget-2022_en.pdf
6 https://www.consilium.europa.eu/en/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/
7 https://www.consilium.europa.eu/en/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/

	デジタル市場法	デジタルサービス法
目的	欧州域内での公正な競争環境を整える	小規模プラットフォーム企業やスタートアップ、中小企業が競争力を持ち、開かれた環境でイノベーションに向けて活動できる環境を整える
対象１	ソーシャルメディア、メッセンジャー、ブラウザ等を展開し、月間4,500万人以上が欧州で利用し、かつ１万以上のビジネス利用者が存在し、過去３年間で欧州域内において7.5ビリオンユーロの売上を上げている事業者[8]	ネットワークインフラ等を提供する中間事業者
対象２	ソーシャルメディア、メッセンジャー、ブラウザ等を展開し、月間4,500万人以上が欧州で利用し、かつ１万以上のビジネス利用者が存在し、75ビリオンユーロの時価総額を記録している事業者[8]	クラウドサービス等を提供するホスティングサービス事業者
対象３		4,500万人以上にサービスを提供する大規模検索エンジンサービス提供事業者
対象４		マーケットプレイス等を提供するプラットフォーム事業者
対象５		4,500万人以上の月間アクティブユーザーを欧州域内で抱える大規模プラットフォーム事業者
罰則	最大前年度の全世界売上の10%、もしくは違反が繰り返される場合には20%上限に加え、全世界の日毎売上高の５％を上限にした周期的な罰金が課される[9]	オンラインプラットフォームおよび検索エンジン事業者に関しては最大全世界の売上の６％が課され、大規模プラットフォームに対してはより強固な制裁が課される[10]

図表１：デジタル市場法（DMA）およびデジタルサービス法（DSA）の比較

	要求事項	禁止事項
項目１	必要な場面で第三者と対象事業者のサービスが接続できるようにしておく	対象事業者のプラットフォーム上で、第三者が類似の商品やサービスを告知している場合に、対象事業者の意図によってランキング等で好意的な対応を行わない
項目２	対象事業者のプラットフォーム上でビジネス利用者が自身のデータにアクセスできるようにしておく	対象事業者のプラットフォーム外の第三者ビジネスに消費者が接続することを妨げない
項目３	対象事業者が提供する広告システムにおいて、広告主やパブリシャーが独立して広告内容を確認できるように情報やツールの提供を行う	消費者がすでにインストールしているアプリやソフトウェアをアンインストールすることを妨げない
項目４	対象事業者のプラットフォーム外で、ビジネス利用者が顧客と契約を結ぶことができるようにしておく	効果的な同意なく、プラットフォーム外で消費者をターゲティング目的のためにトラッキングしない

※ The Digital Markets Act: ensuring fair and open digital marketsの情報を下に日本語で作成[11]

図表２：デジタル市場法（DMA）の下での事業者に対する責務

8 https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users

9 https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment

10 https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment

11 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

	ネットワークインフラ等を提供する中間事業者	クラウドサービス等を提供するホスティングサービス事業者	マーケットプレイス等を提供するプラットフォーム事業者	4,500万人以上の月間アクティブユーザーを欧州域内で抱える大規模プラットフォーム事業者
透明性レポート	○	○	○	○
基本的な権利を考慮した利用規約	○	○	○	○
政府機関の指令に対する協力	○	○	○	○
法的業務に必要な代表者の設置	○	○	○	○
利用者に対して責務や行動に関する情報の提供		○	○	○
犯罪性のある攻撃を受けた場合の報告		○	○	○
是正、申立に対する対応および裁判所外での和解			○	○
オンライン上での違法コンテンツへの対応			○	○
虐待性のあるコンテンツの評価と異議申立て対応			○	○
マーケットプレイスに限定し、第三者サプライヤーが適切な法的対応を実施しているか評価検証（KYBC）			○	○
子供を含む特定の利用者に対するターゲティング広告の禁止			○	○
レコメンドシステムへの透明性			○	○
利用者にわかりやすい広告システムの採用			○	○
リスクマネジメント対策と危機管理対応				○
外部の独立した監査および公共へのアカウンタビリティ、内部コンプライアンス対応				○
プロファイリングを前提としない利用者による選択				○
政府機関や研究者へのデータ共有				○
行動規範の設定				○
危機対応および協力				○

※ What are the key goals of the Digital Services Act?の情報を下に日本語で作成[12]

図表３：デジタルサービス法（DSA）の下での事業者に対する責務（○は該当範囲）

12 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

2021年４月に欧州委員会によってAIパッケージとして提出されたAI法案は、欧州議会内で2020年９月に発足した「デジタル時代の人工知能に関する特別委員会」（AIDA）からの最終提案内容を欧州議会が３月５日（土）に採用を発表[13]し、９月末にAI法案に関するとりまとめを内部市場および消費者保護に関する委員会（IMCO）および市民の自由・司法・内務委員会が共同で実施すると発表している。欧州委員会は欧州議会からの要請を受けて、９月28日に「AI責任指令」[14]のホワイトペーパーを公開しており、指令の中では、想定されるAIによって発生した問題に対する被害者救済の観点や法規制の対象を明確にすることを前提に、法的責任を求めることが発表されている。

3.2　米国

米国では2022年に入り連邦プライバシー法に関する議論が活発に行われている。６月14日に下院エネルギー・商業委員会で実施されたヒアリング[15]で、非公式なディスカッション用ドラフトとして米国データプライバシー保護法（ADPPA）案が委員メンバーによって連邦法への提案として支持されたことが発端になり、連邦プライバシー法に関する議論がさかんに行われるようになった。

連邦法への提案に関しては、上院および超党派の委員から支持[16]を受け、消費者保護を中心として以下の３点を軸に議論が行われた。

①簡潔でわかりやすい英語を用いたプライバシーポリシーやプライバシー通知の採用
②米国データプライバシー保護法の専占規定
③私的な権利行使の範囲

米国データプライバシー保護法案はフランク・パロン下院議員を議長とし[17]超党派議員からの支援を受けながらも、一部民主党議員からは提案に対して反対する意見も上がっている。カリフォルニア州選出のナンシー・ペロシ下院議長は自身のHPで９月１日にステートメント[18]を発表し、提出されている法案はカリフォルニア州のプライバシー関連法と比較すると消費者保護を保証できるものではないと反対する意見を述べている。

子供や金融等の特定の分野に囚われない一律の連邦プライバシー法の制定のためには、各州で異なるプライバシー州法の基準を一定数揃えていくことが必要になるため、各論で議論が止まっている状況である。

一方、2020年に欧州司法裁判所で不当であると判決が下された欧州と米国間での越境データ移転フレームワークであるプライバシーシールドに関しては、バイデン政権へ変わった後に水面下の交渉が始まり[19]、新たな進展があった。

３月25日に米国ホワイトハウスはプライバシーシールドに代わるTrans-Atlantic Data Privacy Frameworkについて、欧州委員会とともに両国間で事業者が円滑にデータ移転を行うことができるように協力して取り組むと発表[20]した。ホワイトハウスが発表した内容では、以下の３点について米国政府は積極的に取り組むと明言している。

①米国政府による通信などの傍受に基づく諜報活動

13　https://www.europarl.europa.eu/news/en/press-room/20220429IPR28228/artificial-intelligence-meps-want-the-eu-to-be-a-global-standard-setter
14　https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf
15　https://energycommerce.house.gov/committee-activity/hearings/hearing-on-protecting-americas-consumers-bipartisan-legislation-to
16　https://www.lexology.com/library/detail.aspx?g=3b04d868-9061-457a-9b9a-a3ca6ea2bc83
17　https://energycommerce.house.gov/newsroom/press-releases/bipartisan-ec-leaders-hail-committee-passage-of-the-american-data-privacy
18　https://www.speaker.gov/newsroom/9122
19　https://iapp.org/news/a/biden-appoints-chris-hoff-to-oversee-privacy-shield-talks/?fbclid=IwAR1vFKRQDS8LPA35IdBCvEHrUV_5vXf4jreI4IeP8oUdHyLyItR4DyhB8Sk
20　https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

（SIGINT）[21]を統制し、プライバシーと市民の自由を強化
②独立して包括的な是正の仕組みを設置
③既存の通信などの傍受に基づく諜報活動に対する階層型で厳格な監督体制をより強化

10月７日にはバイデン大統領によって米国による通信などの傍受に基づく諜報活動への安全性強化に対する大統領令に署名が行われたとホワイトハウスが発表[22]した。この署名によって、米国欧州間でのデータ移転のフレームワークに対する米国の姿勢が明確になり、欧州委員会は米国に対する十分性認定に向けたドラフトの発行を進めると公表[23]した。今後は、欧州データ保護委員会および各国のデータ保護機関、そして欧州議会による審査を経て欧州委員会による十分性認定の発行が認められることになる。

米国国内各州の動きに目を向けると、CPRA（カリフォルニア州プライバシー権法）の施行を2023年に控えたカリフォルニア州では州独自の取組みが活発に議論されている。中でも子供のプライバシーに関する議論が進展し、９月15日にカリフォルニア州知事ギャビン・ニューサム氏の署名[24]により年齢適正デザインコード法（Age-Appropriate Design Code Law）が成立[25]した。

この法律は英国GDPR内の規定で2021年９月に有効になったAge-Appropriate Design Codeを参考に設計されており[26]、CCPA（カリフォルニア消費者プライバシー法）を拡張するものであるとされている。米国内では2022年までに５つの州でプライバシー法が制定され、６つの地域で法制度について議論が行われており[27]、引き続き各州でプライバシー法に関する議論が続いていくと考えられる。

FTCは、５月19日に声明を発表[28]し児童オンラインプライバシー保護法（COPPA）[29]による執行を昨今の状況を鑑みて、強化する方針であると発表した。特にデジタル広告市場ではあたり前になりつつあるターゲティング利用に対する制限等の動きが強化されるのではないかと考えられる。さらに、医療情報や正確な位置情報等に関しても強固な姿勢を見せて対応していくと発表しており、来年にかけても具体的な執行例が出てくるのではないか[30]と考えられる。

3.3　英国

英国ではICO（情報コミッショナーオフィス）の代表に、ニュージーランドで2014年２月から2021年12月までプライバシーコミッショナーを務めたジョン・エドワード氏が就任し、１月４日より新代表として活動[31]を行っている。各国との連携に関しては、７月にはICOと韓国個人情報保護委員会との連携に関する覚書を締結[32]したことに加えて、英米２国間での犯罪抑止の観点からデータアクセスへの合意が７月21日に声明として発表[33]され、10月３日

21 https://digitalforensic.jp/2015/10/05/column382/
22 https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/
23 https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045
24 https://www.gov.ca.gov/2022/09/15/governor-newsom-signs-first-in-nation-bill-protecting-childrens-online-data-and-privacy/
25 https://evalian.co.uk/keeping-children-safe-online-the-california-age-appropriate-design-code-act-vs-the-uk-age-appropriate-design-code/#:~:text=With%20the%20aim%20of%20protecting,1st%20of%20July%202024.
26 https://evalian.co.uk/keeping-children-safe-online-the-california-age-appropriate-design-code-act-vs-the-uk-age-appropriate-design-code/#:~:text=With%20the%20aim%20of%20protecting,1st%20of%20July%202024.
27 https://www.huschblackwell.com/2022-state-privacy-law-tracker
28 https://www.ftc.gov/system/files/ftc_gov/pdf/P155401KhanStatementCOPPA.pdf
29 http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim
30 https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal
31 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/01/new-uk-information-commissioner-begins-term/
32 https://ico.org.uk/media/about-the-ico/mou/4020864/ico-pipc-mou-202207.pdf
33 https://www.gov.uk/government/publications/data-access-agreement-joint-statement-by-the-united-states-and-the-uk/data-access-agreement-joint-statement-by-the-united-states-and-the-united-kingdom

に有効となった。この合意内容に関しては、英国と米国２国間でのデータ取引の合意が、英国を経由して米国へとデータが流通するオンワードトランスファーに該当するのではないかという懸念[34]も表明されており、英国と欧州間での十分性認定に関しては引き続き議論が行われていくと考えられる。

英国内では英国デジタル・文化・メディア・スポーツ省を中心として、2020年12月に公表された英国の国家データ戦略[35]をもとに2021年９月10日から同年11月19日まで英国のデータ保護法の見直しについて議論が行われており[36]、研究開発でのデータ利用等より開かれたデータ利用[37]に向けた内容を軸に検討が進められている。2022年９月のトラス政権発足後に、欧州の規制との整合性を踏まえて一時的に議論が中断している[38]が、現スナク政権において、今後の英国データ保護法制度がどう進んでいくのか、欧州との十分性認定に対する影響を含め、注目が集まっている。

Ⅱ－４　2023 年に向けて事業者として注視していくべきデータ保護制度のポイント

2022年は欧米各国でデジタル関連規制について大きな動きがある１年であった。特に欧州政府による戦略変更は欧州域内で事業を展開する事業者にとっては大きな動きの一つであると考えられるため、引き続き注視していく必要があると考えられる。ここからは各地域の状況に合わせて、2023年度に事業者が取り組むべきポイントについて解説していきたい。

４．１　欧州

2023年は引き続きGDPRの下で欧州域内での執行が積極的に行われるであろうと考えられる。各国のデータ保護規制への対応に加えて、越境データ移転への制裁強化をウィーン会議では発表し、欧州データ保護委員会イサベル・ベレッケン氏への弊社インタビュー内では公共分野でのクラウドコンピューティング利用について調査も実施していくと回答している。欧州域内でのクラウド利用は拡大する一方、フランス政府がMicrosoft365の利用を禁止する等[39]、国独自のクラウドサービスを採用する等の動きが来年度も加速するのではないかと考えられる。一方でドイツでは、サイバーセキュリティ法の下でクラウドサービスへの認証制度[40]を検討する等の動きも出てきており、事業者としては欧州全域での動きと国ごとの対応を並行して理解する必要性が高まってきている。さらに欧州域内での認証制度に関しても議論が始まっており、欧州データ保護委員会は６月22日に越境データ移転の認証ツールに関するガイドラインを発表[41]しているので、十分性認定の範囲外で越境データ移転を実施している事業者については、欧州データ保護委員会の動向に関しても注視することが望ましい。

DSAに関しては、15カ月の期間もしくは2024年１月[42]に欧州全域で施行されることになるため、2023年は対象となる事業者の施行までの対策や動向が大きなテーマになると考えられる。対象事業者のサービス仕様やポリシーの変更等の動きが出る可能性もあるため、すでにDSAの対象になる事業者との取引がある場合は動向に注目する必要がある。

その他のデジタル法案に関しては引き続き動向を

34　https://www.europarl.europa.eu/doceo/document/E-9-2022-002790_EN.html
35　https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy
36　https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation
37　https://www.gov.uk/government/news/new-data-laws-to-boost-british-business-protect-consumers-and-seize-the-benefits-of-brexit
38　https://techcrunch.com/2022/10/03/uk-data-reform-bill-replace-gdpr/?guccounter=1
39　https://prednyslm.eu/en/french-government-has-banned-the-use-of-microsoft-365/
40　https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/?fbclid=IwAR2WEJN6d7sJZ7Z97oZUmyf5m5dQFoQ-Zr2wQ7yAoH3gfAcl_5Lzd2funOs
41　https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf
42　https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

注視していく形になると思うが、９月22日に欧州委員会フォン・デア・ライエン委員長より発表された“STATE OF THE UNION 2022[43]”の中で、メタバース等のデジタル空間における新しい取組みを推進していくとも発表されているため、データ保護規制を含めた動きに関しては、メタバース関連の事業を取り組む事業者も注視していく必要があると思われる。

4.2　米国

2023年は欧州との越境データ移転フレームワークおよび十分性認定についての具体的な回答が出ると考えられるため、日本の事業者への直接的な影響は少ないと考えられるが、米国政府による諜報活動を容認する法律へどこまで影響があるかは今後注目される。欧米越境データ移転フレームワークが欧州政府、もしくは欧州司法裁判所によって再度不採用になる可能性もある。その場合に、米国政府が代替案として何を交渉材料にするのかは注目である。

米国国内では引き続き各州でプライバシー法についての議論が進んでいくと考えられるが、中でもカリフォルニア州に関してはより厳しい制裁が行われると考えられる。８月24日にはフランスのLVMHモエ・ヘネシー・ルイ・ヴィトン傘下セフォラに対し、CCPA違反による和解がカリフォルニア州司法長官より公表され120万ドルの支払いで合意する[44]ことになった。今回は利用者の要求に基づいて情報公開を行うオプトアウト権に反して個人データを販売したことが問題になったケースであり、司法長官のロブ・ボンタ氏はカリフォルニア州の事業者に対してCCPAへの対応を強く求めると発表している。

各州での制裁はカリフォルニア州だけに止まらず、イリノイ州のBIPA（生体情報プライバシー法）を下にした集団訴訟ケースも増加しており、各州で行われている集団訴訟の判決内容について調査しておくことも事業者にとっては重要である。

年齢適正デザインコード法については2024年７月１日施行予定であるが[45]、公表された法案では子供の利益（18歳以下）を守るデータ保護影響評価を求めており、児童オンラインプライバシー保護法（COPPA）で定められている13歳未満[46]よりも対象が広いため注意が必要である。日本の個人情報保護法での対象とは異なる要素が求められる点もあるため、ゲーム系の事業者を始めとして、子供のデータを取り扱う事業者は事前対策が必要になると考えられる。FTCの対応に関しても、医療や正確な位置情報に関する利用に対してこれまで以上に対策を強化していくと発表しており、個人データを取り扱うことを前提としたビジネスモデルを米国全土で展開する際には、これまで描いていたプライバシーコンプライアンス対策を見直していくことも必要になると考えられる。

4.3　英国

英国国内のデータ保護法の改正案が、欧州の十分性認定を満たすものになるのか否かが非常に重要なポイントである。データ保護制度に加えて、英国内ではプライバシー強化技術に関する調査も積極的に行っており、９月７日に情報コミッショナーオフィスはプライバシー強化技術に関するガイダンスを発表[47]した。ガイダンスの中では、プライバシー強化技術を導入することによる影響を事前に評価することを求めており[48]、導入ケースに合わせて適切な技術評価を実施することが必要になる。

43　https://state-of-the-union.ec.europa.eu/system/files/2022-09/SOTEU_2022_Letter_of_Intent_EN_0.pdf
44　https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement
45　https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273
46　http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim
47　https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/?fbclid=IwAR2Z1n66zxou4W22ShvUASGLku4L9HbY08J8fOclCFZt1EZfrt6VcUKKx9g
48　https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

Ⅱ－5　最後に

2022年は欧米各国で新たな動きが始まる重要な１年になった。事業者にとっては、データ保護法の下で求められる対応がより厳しくなることに加えて、国ごとの対応は依然として異なるため、コンプライアンスコストが増加することが見込まれる。

2020年に不当であると判決が下ったプライバシーシールドに関しても、ここに来て新しい動きが始まってきている。各国の法制度に加えて、越境データ移転の問題はより深刻になっていくと考えられるため、事業者内でデータマッピング等の施策を行い適切なデータ管理が実施されているかどうかを早期に把握することが必要になる。

さらに今年からデータ保護規制の強化に加えて、プライバシー強化技術の導入に向けた議論も前進しつつある。９月８日にドイツのボンで開催されたＧ７プライバシー機関ラウンドテーブル[49]では、プライバシー強化技術についても議論[50]が行われ、各国のデータ保護機関の連携のもと技術的な対策についても具体的な指針が示されていくのではないかと考えている。

49　https://www.ppc.go.jp/enforcement/cooperation/international_conference/g7_roundtable_202209/
50　https://www.ppc.go.jp/files/pdf/G7roundtable_202209_communique_jp.pdf

JIPDEC
レポート

本人に資するPHRサービスの在り方
－民間PHRサービスの品質と評価の観点からの考察－

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　**上河辺 康子**

1．PHRを巡る動向

保険医療分野のデータ利活用が進みつつある。信頼性のある自由なデータ流通“Data Free Flow with Trust”（DFFT）の重要性が国際的に認識される中、欧州委員会が2022年５月３日“European Health Data Space”（EHDS）の設立を提案、これにより、自身の健康に関するデータを自国に限らずEU加盟国内で管理し利用する（一次利用）とともに、EUのデータ保護水準に則り研究開発等へのデータ利活用（二次利用）のための枠組みが提供されるという。EUのデータ戦略は“European Common Data Spaces”構築を掲げており、重点分野のうちヘルスケア分野が先行して進められていると考えられる。日本においてはデジタル田園都市国家構想の下、マイナポータルを通じて自身の健康診断結果や服薬履歴等の健康保険データを閲覧する仕組みが構成され、データヘルス改革が示す工程表に則り、マイナポータルを通じて閲覧可能な情報は今後拡大することが期待される。また、マイナンバーカードと健康保険証の一体化による医療機関等との情報共有が推進されている。これらを含む医療分野でのDXを通じた保健医療の向上を目指し、医療DX推進本部が設置された（2022年10月11日閣議決定）。さらにこのような公的な基盤整備と並行して、民間事業者が健診等の情報を取り扱う場合の指針[1]が整備され、PHR（Personal Health Record）を利用したサービスを提供する民間事業者が業種の垣根を越えて業界団体の設立宣言を行う[2]など、民間事業者がPHRの利活用を通じて提供するサービス（民間PHRサービス）が着目されている。

2．PHRサービスとは何か

PHRは、健康に関する個人情報を、生涯にわたり本人が電子的に閲覧し管理することにより、本人の健康に関する意思決定に資する仕組みまたは仕組みを通じて管理されるデータを指す[3]。本人の健康に関する意思決定に資する仕組みとは、具体的には、本人が自ら医療機関を受診した際の情報を閲覧したり、本人が健康に関する情報（ライフログ（歩数、運動、活動量　等）、食事、睡眠　等）を取得し管理したりすることにより、本人が健康に関する取組みを行うことを支援する仕組みである。この本人の健康維持や疾病予防を、本人を含む「顧客」のニーズに応じて何らかの形で支援するサービスがPHRサービスである。先述のマイナポータルを通じて自身の保健医療データを閲覧する仕組みは、公的なPHRサービスであるということができる。

3．民間PHRサービスの特徴

3.1　対象

民間PHRサービスで取り扱うデータは本人の健康に関するデータであり、マイナポータルが提供する健診等の情報、電子カルテや処方箋の情報に限定

1　「民間PHR事業者による健診等情報の取扱いに関する基本的指針」2021年４月（2022年4月一部改正）、総務省、厚生労働省、経済産業省
2　https://www.meti.go.jp/press/2022/06/20220620005/20220620005.html（2022年11月時点）
3　https://www.jipdec.or.jp/library/report/20210706.html（2022年11月時点）、1.2ヘルスケアサービスとPHR

されず、本人のライフログ、食事、睡眠等、多様なデータが含まれる。また、PHRサービスは本人の健康維持や疾病予防を支援するサービスであり、PHRサービスの最終的な利用者は本人である。

一方、民間PHRサービスの顧客（サービス対象）には、大きく分けて、本人（BtoC）と、組織（BtoXtoC）がある。本人は民間PHRサービスの直接の利用者であると言える。組織は、本人が所属する組織であり、本人の勤務先や加盟する健康保険組合（BtoBtoC等）、本人が通院している医療機関（BtoMtoC）、本人が住んでいる自治体（BtoGtoC）などが考えられる。

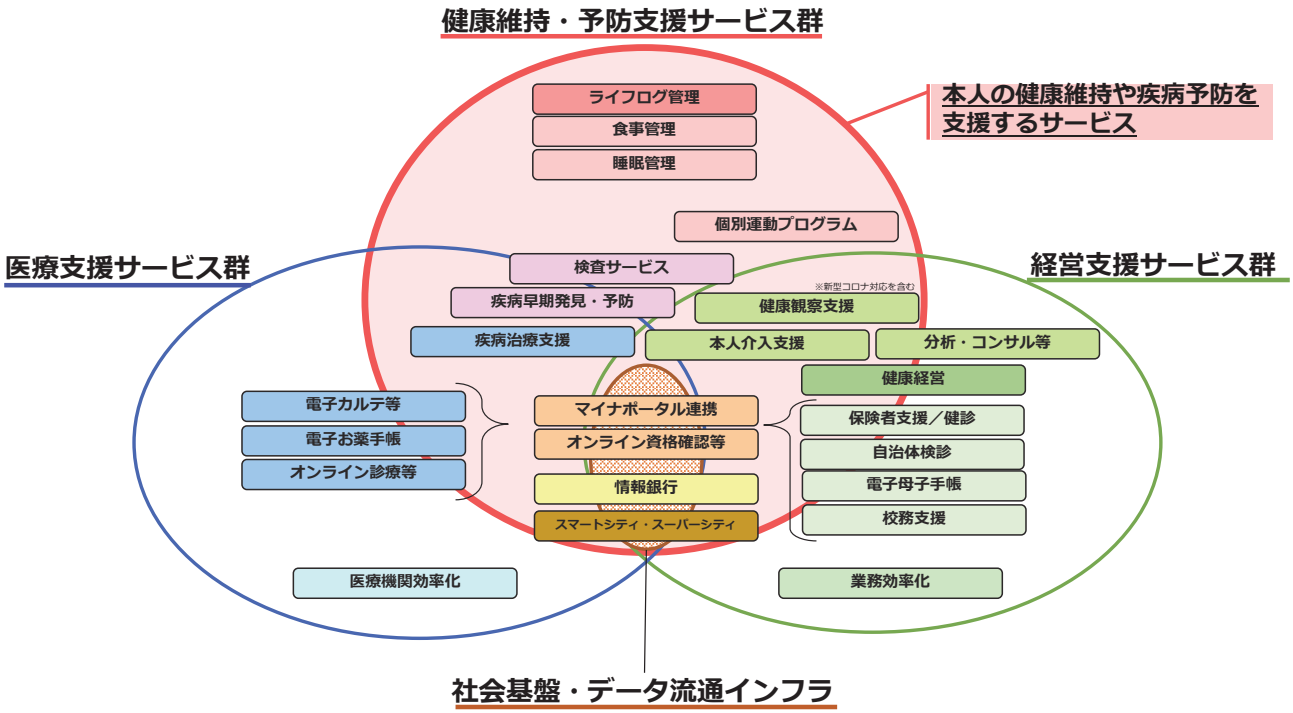
3.2　顧客ニーズとサービス範囲

民間PHRサービスに対する顧客（本人、組織）のニーズは多様である。本人のニーズは、日常生活に支障はないが自身の健康に何らかの関心や不安がある場合から、本人が患者であり治療の支援（自身の治療に関連する情報の管理　等）を求める場合まで幅広い。組織においては、健康経営を通じた生産性の向上、医療費削減など、組織の課題改善に関連するニーズとなる。

民間PHRサービスの範囲と内容は、これらの顧客のニーズに対応するが、組織を顧客とする場合、組織の課題の改善を支援するサービス（経営支援、医療支援）の中に、組織に所属する本人向けのPHRサービスが含まれる場合がある。また、公的なPHRサービスとの連携支援や、民間事業者がインフラを構築しPHRサービスを含むサービス（情報銀行、スマートシティ・スーパーシティ等）を提供する場合もある。このため、民間PHRサービスの在り方の検討にあたっては、特定の形態や方法によらず、何らかの形で本人の健康維持や疾病予防を支援するサービス（健康維持・予防支援サービス）を、広く視野に入れる必要があると考えられる（図表１）。

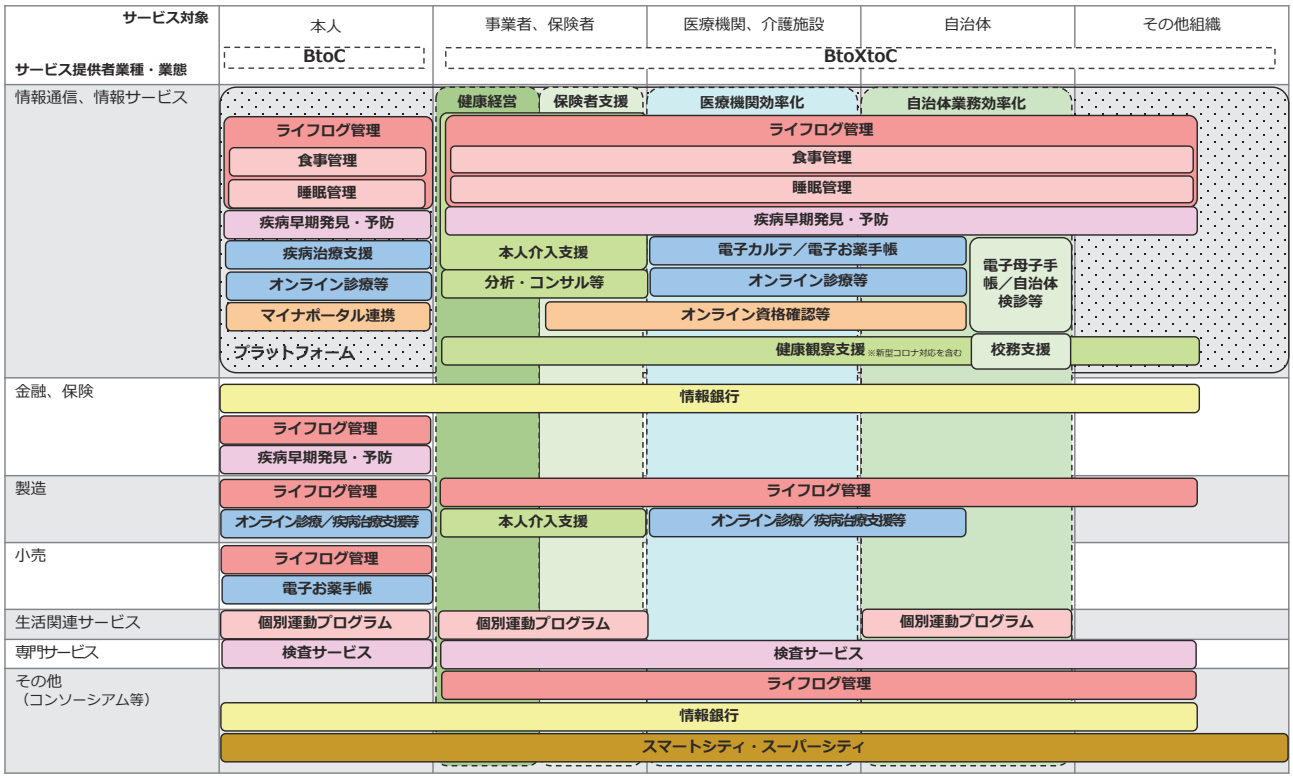
3.3　サービス提供者

民間PHRサービス提供者の業種・業態は、情報通信業、金融・保険業、製造業、小売業、生活関連サービス、娯楽業、専門サービス業等、さまざまである。また、子会社等の設立や複数事業者によるコンソーシアム等によるPHRサービスへの参入も見受けら



健康維持・予防支援サービス群　本人の健康維持の支援（本人のライフログ・食事・睡眠・運動等の管理、検査等による本人の健康状態把握等）
医療支援サービス群　医療機関（薬局を含む）の支援、治療の支援　等
経営支援サービス群　保険者、事業者、自治体等の支援
社会基盤・データ流通インフラ　公的データ基盤（マイナポータル、オンライン資格確認等システム）への連携支援、情報銀行、スマートシティ・スーパーシティ　等

図表１．民間PHRサービスの範囲



※調査日時点のサービス提供状況を参考に作成。

図表２．民間PHRサービスの範囲（業種・顧客別）

れる。さまざまな業種・業態のサービス提供者が、同様の顧客（本人、組織）に対し、同様のサービスを提供している（図表２）。

民間PHRサービス提供者は、必ずしもPHRサービス専業ではなく、PHRサービスの他に、本業の事業を持つ場合も多い。また、PHRサービスを含む事業全体のビジネスモデルや、PHRサービス提供を通じて取得した個人データの利用目的（例：自社商品・サービスに生かす、研究開発向けにデータを提供する　等）に応じてPHRサービスのマネタイズの仕組みも異なると考えられる。

４．PHRサービスに求められる機能

本人の健康維持や疾病予防を支援するサービスを提供するための主要な機能（以下、「主要機能」という。）には、少なくとも、①記録支援、②ダッシュボード、③データ連携・共有、④行動変容支援のための各機能が含まれると考えられる（図表３）。

①の記録支援は、PHRサービスの多くは、本人が自ら測定した数値や、自身の健康や体調に関する所感を記録し、記録した内容に応じてサービスを提供しているため、本人が必要な頻度で確実に記録することができるよう支援する機能である。②のダッシュボードは、収集した複数の本人の健康に関するデータを分析、加工し、数値、表、グラフ等により一覧表示する機能である。③のデータ連携・共有は、デバイス、他のデータベースと連携し、データをインプット／アウトプットする機能である。サービス内容により、医療機関、地域医療連携ネットワーク、マイナポータルとの接続の要否や中長期的に見た相互運用性などを視野に入れる必要がある。④の行動変容支援は、記録支援やダッシュボードを通じて把握した情報を、本人が、自らの健康の維持・予防や改善のために行動しようと思う、または行動を実行するよう働きかけを行う機能である。④行動変容支援には、１）専門家や本人の健康に関する行動を支援する人（家族、友人等）とのデータ共有やコミュニケーション手段の提供による支援、２）本人へのデータ分析結果等のフィードバック、行動変容に伴うインセンティブ付与、健康に関する本人のリテラシー向上の支援など、本人に対する直接の働きかけによる支援がある。

また、主要機能に加えて、PHRサービスの機能に

主要機能	機能例		概要
記録支援	データ取り込み		データ連携等により入力項目を取り込み、記録することにより、本人の入力作業の負荷を軽減する。
	選択式入力		あらかじめ設定された選択肢より選んで入力することにより、本人の入力作業の負荷を軽減する。
	画像認識		スマートフォン等のカメラで撮影した画像（食事、健康診断結果　等）を認識、分析することにより、本人の入力作業の負荷を軽減する。
	お知らせ・アラート		入力作業の行っていない場合の通知等により本人を支援する。
ダッシュボード	本人向けダッシュボード		入力したデータを分析、加工し、数値、表、グラフ等により一覧表示する。
	組織向けダッシュボード		本人（被保険者、従業者等）が入力したデータを分析、加工し、本人が所属する組織に対して、数値、表、グラフ等により一覧表示する。
データ連携・共有	マイナポータルAPI連携		マイナポータルAPI連携により、本人の特定健診情報、薬剤情報、ワクチン接種履歴等を取得する。
	デバイス連携		ウェアラブルデバイスや家庭用測定機により測定した本人のデータを取得する。
	他システムとの連携		他のシステム（EHR、他社提供サービス等）により記録した本人のデータを取得する。
	出力		取得した本人のデータ等を、電子データ、紙媒体などに出力する（本人から医師、在宅医療介護スタッフ間等の共有等）。
行動変容支援	コミュニケーション	専門家とのデータ共有	医師、管理栄養士、トレーナー、AI等に、本人のデータを共有する。
		家族等とのデータ共有	本人の健康に関する行動を支援する人(生活習慣病患者の家族、本人と親しい人等)に、本人のデータを共有する。
		コミュニケーション手段の提供	専門家、家族等、利用者間（同じ症状、病気を持つ本人間）のコミュケーション手段を提供する（面談・個別トレーニング（対面／オンライン）、チャット、掲示板によるやり取り　等）。
	本人への直接の働きかけ	本人へのフィードバック	専門家（AIを含む）へのデータ共有結果を、本人にフィードバックする（罹患リスク分析・リコメンデーション　等）
		インセンティブ付与	健康に関する行動を実行した本人に、行動の内容に応じたインセンティブ（本人へのポイント付与、ポイント数に応じたサービスの提供等）を付与する。
		リテラシー向上	健康に関する本人の理解向上を支援する（健康に関するコンテンツ配信　等）。

図表３．PHRサービスの主要機能と機能例

は、本人確認機能等の個人情報保護および情報セキュリティを満たすための機能は、個人情報を取り扱う他のサービスと同様に必須である。

5．本人に資するPHRサービスの品質評価の在り方

5.1　評価のための基準等

ヘルスケア産業におけるサービス・製品の品質の評価については、経済産業省次世代ヘルスケア産業協議会において、2014年に具体的な議論が行われ、この中間とりまとめ[4]では、フィットネスクラブ等の健康運動サービスにおける品質評価の基準について、“サービスの提供体制の充足度等に関する「インプット評価」”、“消費者の行動変容の促進に関する「アウトプット評価」”、“消費者の健康状態の改善に関する「アウトカム評価」”の３つの評価軸により品質の評価を行うことが適当であることを示している。

民間PHRサービスもこの３つの評価軸で評価することができるが、本人（BtoC）および組織（BtoXtoC）の両方を視野に入れて評価する必要がある。特に、サービス提供者からみた直接の顧客が組織（BtoXtoC）である場合であっても、本人からみたサービスの充足度、本人の行動変容促進および健康状態の改善を視野に入れる必要がある。評価軸ごとに評価の基準と評価項目の例を図表に整理する（図表４）。

5.2　評価スキーム

評価スキームには、セルフチェック（自己宣言）、業界団体認証、第三者認証が考えられ、評価のための基準や項目はそれぞれ異なる。民間PHRサービスの評価においては、これらのスキームに加えて、サービス利用者評価およびサービス対象（組織）評価の在り方を視野に入れる必要がある。このうちサービス利用者評価の在り方はPHRサービスにおいて特に重要であるが、評価の在り方については、たとえば、サービス利用者（本人）のニーズに対する改善の有無を継続的に把握する等の効果測定や本人への意見聴取の在り方を視野に含める必要がある。

また、サービス提供に携わる多様な専門家、サービス提供者が利用するプラットフォーマー、スマートフォンのアプリケーションによるPHRサービスのアプリストア等のステークホルダーを含めた評価

4　「次世代ヘルスケア産業協議会 品質評価 WG 中間報告」2014年６月５日、次世代ヘルスケア産業協議会（経済産業省）、Ⅱ．２．健康運動サービスにおける品質評価の基準

評価の基準		PHRサービスの観点	評価項目(例)
サービス提供状況の評価 （サービスの提供体制の充実度等／インプット評価）	**ア）** 指導・相談に対応する人材の確保・育成	医師、産業医、薬剤師、管理栄養士、トレーナー等の専門家に加えて、専門家の知見を学習したAIによる指導・相談も想定。	• サービス内容 • サービス提供方法 • 表示、UI等のわかりやすさ • 情報セキュリティの状況 • 施設・設備の状況 • 緊急事態対応体制・マニュアル等の整備状況 • 苦情および相談対応体制・マニュアル等の整備状況 • マネジメントシステムの構築・運用状況 • 個人情報保護等、関連法令の遵守状況
	イ） 安全性確保のための対応	データ管理の観点から、本人確認等、情報セキュリティの確保のための基準（ISMSが示す管理策等）は必須。サービス内容や提供方法に応じ基準（医療情報に関するガイドライン、物理的な施設・設備管理等）を参考に検討。	
	ウ） 事故や苦情への対応	本人と組織双方への対応を想定。	
	エ） サービス品質の維持・改善に向けた取組	本人の健康維持や疾病予防を支援するPHRサービスでは、サービスの品質も本人に対するサービスを主に捉えることが重要。	
	オ） コンプライアンス管理	個人情報を含む管理体制の構築の在り方に加えて、関連する法令に留意が必要 。関連する法令は、サービス内容やサービス提供方法に応じて要確認。	
サービス利用中の状況の評価 （行動変容に関する評価／アウトプット評価）	**ア）** 本人のサービス継続利用状況	PHRサービスが持つ基本機能（行動変容支援等）の利用状況及び継続状況の分析等。 顧客が組織である場合も、本人の状況を的確に評価することが重要。このため、組織に関する評価の基準（※）は要否を含めて評価時に検討。	• 本人の基本機能の利用状況および継続状況 • サービス提供者の対応状況 • 本人等のサービスに対する評価
	イ） 本人の満足度		
	ウ） 組織のサービス継続利用状況※		
	エ） 組織の満足度※		
サービス利用結果の評価 （本人の健康状態の改善に関する評価／アウトカム評価）	**ア）** サービス利用者（本人）のニーズに対する変化の有無	幅広い本人のニーズにより改善の有無の評価の在り方に応じて評価の基準を検討。	• 本人のニーズに対する、プラスの方向での変化の有無（効果測定　等） • 組織の課題改善
	イ） 組織のニーズに対する変化の有無	組織の経営課題の改善と関連する事項が評価の基準となり得ることに留意。	

図表４．民間PHRサービスのサービス品質の基準および評価項目の例

の在り方についても検討する必要がある。

６．本人に資する民間PHRサービスの在り方

健康は、本人の問題であると同時に社会の問題である。本人に資するサービスの充実に向けて、まず求められる事項は、ヘルスケア関連産業および医療の環境整備である。環境整備に向けての論点として、①医療機関等の支援とデータ標準化の在り方の検討、②関連する法令等に対するサービス提供者の理解の２点を挙げたい。①は、現在オンライン資格確認等システムの基盤整備が急ピッチで進められているが、シームレスな医療提供に向けては医療機関の電子カルテシステム導入や電子カルテ情報の標準化の促進も求められる。民間PHRサービスにおいても、これらの基盤整備を通じて、新規サービス開拓やサービス内容等の充実が期待される。②は、民間PHRサービスのサービス提供者においては、他のヘルスケアサービスと同様に医療、個人情報保護、消費者保護等に関する法令等への対応が必須であるが、PHRサービスは現状スマートフォンのアプリケーションを通じた提供が多く、これに関連する規制も関連する。PHRサービスのサービス品質の評価のための基準の検討にあたっては、これらの法令遵守を含め、実務レベルでの整理が必要と考えられ、今後の業界団体、関連機関の役割が期待される。

また、これと並行して、ヘルスケア分野における個人情報の取扱いに関する本人の権利の在り方にも目を向ける必要がある。冒頭で述べたEHDS設立の提案理由と目的では、加盟国によるGDPRの不均一な実施と解釈により電子健康データの二次利用が妨げられ、自然人が革新的な治療の恩恵を受けられず、政策立案者が健康危機に対応できない状況にあるとされている。また、提案ではモバイルアプリケーション等に言及し、民間サービスを視野に入れた検討が進められている。日本においては、要配慮個人情報の取得等にあたり本人の同意取得を原則とする一方、次世代医療基盤整備法の整備、改正個人情報保護法における仮名加工情報創設等、医療情報を含む個人情報の保護と利活用促進を両立するよう法整備が進められている。しかしながら、医療情報の二次利用における本人の同意取得の在り方については、未来の研究開発における利用目的の示しづらさや本人が何に同意しているかが理解しづらい等の

課題が指摘され、二次利用固有のルールの在り方が検討されているところである[5]。民間PHRサービスを通じて取得される情報は、医療情報と共に利活用される場面が想定される。国内において医療情報の取扱いに関する議論が進む中、EUのような海外情勢を視野に入れながらも、国内の民間PHRサービスにおけるデータ収集の状況に応じた検討が進むことが期待される。

5 「医療分野における仮名加工情報の保護と利活用に関する検討会　これまでの議論の整理」2022年9月30日、厚生労働省

コラム

本章では、JIPDECの事業テーマである「個人情報保護／プライバシー」「セキュリティ」「デジタルトラスト」「IT動向」に関する最新動向を、当協会職員がご紹介します。

個人情報管理のためのデータマッピング・ツールキット

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　グループリーダ　**松下 尚史**

IT技術の進展に伴い個人情報等の取扱いが増加している中で、事業者が取得する個人情報を適切に管理していく必要性が高まっています。こうした中で、事業者の自主的な取組みの一つとして、データマッピングによる管理手法が注目されています。そこで、個人情報保護委員会は、データマッピング・ツールキット（以下、「本ツールキット」という。）を作成し、多数のデータを保有している等の事業者が、当該データを適切に管理するための自主的な取組みとして、データマッピングを開始する際の一助となることを目的に、本ツールキットを公開しました[1]。本ツールキットは、本編、データマッピング表の項目例、外国にある第三者への個人データ提供に係るチェックリスト、外国において個人データを取り扱う場合のチェックリストの４つの資料から構成されています。

データマッピングによって、事業者全体としてどのようなデータを取り扱っているのかを把握し、①個人情報保護法（以下、「法」という。）を含む当該データに適用される法令の遵守状況の確認、② 当該データの取扱状況等に起因するリスクに応じた必要な対応の実施等を行うことができる、とされています。なお、個人データについてデータマッピングする場合には、法第23条の定める個人データの安全管理措置の一つの手法となる（ガイドライン（通則編）10－３（３））とされています。具体的には、データマッピングは、個人データの項目、責任者・取扱部署等をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可能とするものであり、安全管理措置の一つである、組織的安全管理措置の「個人データの取扱状況を確認する手段の整備」の一つの手法とされています。

プライバシー影響評価（PIA：Privacy Impact Assessment）や個人情報保護マネジメントシステム（PMS：Personal information protection Management Systems）における個人情報管理台帳の整備においても活用できるのではないかと考えられます。

1　https://www.ppc.go.jp/personalinfo/independent_effort/

海外のプライバシー動向に係る日本への影響

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　主査　**石井 美穂**

EUでは、大手プラットフォーム企業の社会的・経済的影響に対応するため、「デジタルサービス法（DSA：Digital Services Act）」と「デジタル市場法（DMA：Digital Markets Act）」が、2022年７月５日に、EU議会で賛成多数で採択されました。DSAとDMAは、その制裁金の大きさにとどまらず、規制が広範囲に及び、かつ強力であることから、とりわけ、米IT大手プラットフォーム企業に大きな影響を与えます。具体的には、DSAによって、特定の種類の広告をプラットフォーム上に掲載することが禁止され、子ども向けのターゲット広告や、ユーザーの民族性や性的指向に合わせたターゲット広告が排除されることになります。また、DMAによって、プラットフォーム企業はメッセージングアプリの相互運用を可能にするよう求められる可能性があります。

DSA・DMAの日本への影響について、DSAに関しては、プラットフォーム企業に対して日本のユーザーや権利者等が直接的に履行の義務を求める場面が発生する可能性は低いですが、日本における法規制の議論において有益な参考材料となりえます。他方、DMAに関しては、日本企業のEUにおける取引環境に影響を与える可能性があるため、日本の政策動向等にも直接的な影響を与える可能性があります。

米国では、2022年７月20日、米国初の包括的な個人情報保護のための法律となるデータプライバシー保護法（ADPPA：American Data Privacy and Protection Act）の法案が、米下院のエネルギー・商業委員会で可決されました。人権としての個人情報保護の意識が高いEUに比べ、これまで米国では、自国企業のイノベーション阻害要因となりかねない個人情報保護法策定には消極的でした。しかし、近年はメガプラットフォーマーの経済的影響力に加え、民主主義に与える影響が懸念されることから、ADPPAも個人の権利に配慮した法案となっています。たとえば、個人情報の取得や利用に関して、企業の個人に対する「duty of loyalty（忠実義務）」、受益者のため忠実に信託事務を処理する義務を課す点が特徴としてあげられます。これは、GDPRや日本の個人情報保護法における、個人への通知と同意に基づく義務を超えて、はるかに厳しい制限を課すものです。

ADPPAは、適用スコープが広い上に、強力なエンフォースメントによりその実効性が担保されていることから、日本企業への影響は少なくありません。また、個人への通知と同意に基づく個人情報の取得の限界を超えた制度設計という点においても、政策的に重要な論点が含まれます。

ISMS認証基準（ISO/IEC 27001）の改訂

一般財団法人日本情報経済社会推進協会　セキュリティマネジメント推進室　室長　**成田 康正**

ISMS適合性評価制度における認証基準のISO/IEC 27001が2022年10月25日に改訂されました。

JIPDECは、経済産業省の協力を得ながら2002年度からISMS適合性評価制度を開始し、ISMS（情報セキュリティマネジメントシステム）の普及に取り組んできており、ISO/IEC JTC 1/SC 27における国際標準化活動に積極的に貢献してきました。現在、国内認証機関に対する認定業務は、関連法人である一般社団法人情報マネジメントシステム認定センター（ISMS-AC）に移管しており、ISMS-AC認定下の被認証組織数は増加し続けています（2022年11月現在、約7,100件）。

ISO/IEC 27001は、企業などの組織がISMSを構築・運用するための際に適合すべき事項が定められています。今回の改訂では、ISO/IEC 27001の附属書Aにある情報セキュリティの対策集（情報セキュリティ管理策）を更新しました。附属書Aの管理策は情報セキュリティ対策実施のためのガイダンス規格であるISO/IEC 27002と整合がとられていますが、ISO/IEC 27002が2022年2月に改訂されたため、附属書Aが更新されました。管理策は、最新の動向を考慮して再構成され、追加・統合されて、15分類の構成から4分類（組織的、人的、物理的、技術的）に簡素化されました（管理策数は114から93になりました）。追加された管理策としては、たとえば、「データマスキング（匿名化／仮名化）」「監視活動」等、情報に着目した管理策や積極的な監視・情報収集のための管理策等があります。さらに、管理策の位置づけや効果を理解するための情報として、各管理策に「属性」（attribute）が設けられました。なお、ISO/IEC 27001:2022本文は最新のISOマネジメントシステム共通要素[1]を反映するために若干更新されましたが、大きな変更はなくISO/IEC 27001:2013から高い連続性を維持しています。

ISMS-ACでは、ISMS適合性評価制度の認定機関の立場として、ISMS認証機関が適切にISMSの認証審査を実施できる体制・能力をもっているかを審査し、認定しています。

認証登録証等で認証機関のマーク（図の左）と認定シンボル（図の右）とが2つ並んでいることは、その認証機関が国際規格に従った適切な審査を実施していることを、認定機関であるISMS-ACが保証していることを示します。

認証機関マーク（左）と認定シンボル（右）が並んだ表示例

なお、ISMS認証の移行計画はISMS-ACから発表されており、認証の移行期間として3年間が設定されています。JIPDECおよびISMS-ACでは、認証取得組織が適切にISO/IEC 27001:2022へ認証の移行ができるよう、さまざまな面で情報発信していく予定です。

https://isms.jp/topics/news/20221025.html

一般社団法人情報マネジメントシステム認定センター（ISMS-AC）：https://isms.jp

1　ISO/IEC Directives, Part 1, Annex SL（normative）Harmonized approach for management system standards：マネジメントシステム規格（MSS）の共通要素（共通箇条、共通テキスト、用語等）を定めた附属書

デジタルトラストと電子証明書の役割

一般財団法人日本情報経済社会推進協会　デジタルトラスト評価センター　主査　**成田 ミキ**

デジタルトラストとは、デジタル社会において、情報の担い手の人や法人等が本物であることや、その情報が改ざんされていないことを保証することを言います。その実現のためには電子証明書等を提供するトラストサービスが不可欠です。

最近ではテレビCMでも電子証明書という言葉が聞かれるようになりましたが、マイナンバーカードには、この電子証明書が格納されています。

マイナンバーカードを使用し、住民票の写しをコンビニエンスストアで取得したり、各自治体の行政手続きをオンライン上で行うことができます。その際に使用されるのが、マイナンバーカードのICチップに格納された、以下の２種類の電子証明書です。

・署名用電子証明書
・利用者証明用電子証明書

署名用電子証明書には、利用者の氏名、住所、生年月日、性別が記載され、確定申告等で使用されます。マイナンバーカードの署名用電子証明書を用いて、電子的に作成された申告書に対し電子署名を行うことで、居住地に住む本人がたしかに申請していることを示すことができます。

一方、利用者証明用電子証明書には上記の４つの個人情報は含まれず、コンピュータでのみ判読可能な文字列によって構成された情報と、有効期限等が記載されています。端末にマイナンバーカードをかざすことで、個人情報の提出が不要な場面での本人確認（コンビニエンスストアでの住民票の写しの自動交付等）を可能にしています。

マイナンバーカードに格納された電子証明書以外にも、日本には電子署名法に係る認定制度に基づく民間のトラストサービス（認証局）があります。2021年には、スマートフォンを活用したサービス（my電子証明書）が認定され、地方公共団体情報システム機構（J-LIS）の公的個人認証サービスを利用してスムーズな本人確認を行い、公的個人認証サービスよりも自由度がある電子証明書を、スマートフォンで利用できるようになりました。

JIPDECは、この国による認定制度における指定調査機関として実地調査を行うと共に、電子証明書の発行や電子契約サービスが一定の安全基準を満たしていることを評価するJIPDECトラステッド・サービス登録事業を運営しています。デジタル社会において、トラストサービスは大きな役割を持っています。JIPDECは多くの皆さんが、安心、安全にトラストサービスを利用できるよう、デジタルトラストを支える裏方として活動してまいります。

準天頂衛星システムの今後

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　グループリーダ　**松下 尚史**

Society5.0の実現を目指すわが国において、宇宙システムは、地上システムと連携し、ビッグデータの重要な構成要素となる３次元測位データや地上のさまざまな状態を捉えるリモートセンシングデータを提供する上で、非常に重要な位置を占めています。また、災害大国と呼ばれるわが国では、地上の状況に左右されずに機能が継続するなど、広域な観測や通信が可能な宇宙システムのポテンシャルは高いと言えます。そうした中、自動走行等の実現や、地理空間情報が高度に活用される社会基盤の確立に向けて、高精度な位置情報を活用した宇宙利活用ビジネスの進展が期待されています。このような分野において高精度な衛星測位サービスを提供しているものが、準天頂衛星システム（QZSS: Quasi-Zenith Satellite System、愛称：みちびき）です。

みちびきは、現在４機体制で運用されており、衛星測位サービス、測位補強サービス（SLAS／CLAS）、メッセージサービス（災害・危機管理通報サービス／Q-ANPI）を提供しています。さらに、みちびきは、2023年度を目途に単独で位置情報の取得が可能になる７機体制の構築を、2024年度を目途に信号認証機能の正式運用開始を目指しています。

信号認証機能は、測位信号のなりすまし（スプーフィング）を防ぐことを目的に、測位信号に含まれる航法メッセージが本物であることを「電子署名」技術により証明するものです。信号認証機能が整備されることで、取得できる位置および時刻情報[1]の“信頼性”が高まるため、さまざまなユースケースでの活用が見込まれています。

1　みちびきなどの一般的な測位衛星は巨大な原子時計を搭載して航行しており、その時刻情報を信号として配信しています。

〈資料１〉国内外の主な個人情報保護関連の年表

国　内	年	海　外	
	1970	ドイツ	ヘッセン州において世界初の「データ保護法」採択
徳島県徳島市「電子計算組織運営審議会条例」施行（6/28）	1973		
	1974	アメリカ	「プライバシー法」制定
「電子計算機処理データ保護管理準則」策定	1976		
	1977	ドイツ	「データ処理における個人データの濫用防止に関する法律（連邦データ保護法）」制定（１月）（2009年に改正）
	1978	フランス	「データ処理・データファイル及び個人の自由に関する法律」制定
		カナダ	「カナダ人権法」制定
	1979	コミッショナー	「プライバシー・コミッショナー会議」開始
	1980	欧州評議会	閣僚委員会が「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」採択（9/17）
		OECD	「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」採択（9/23）
	1981	欧州評議会	「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」発布（1/28）
	1982	カナダ	「連邦プライバシー法」制定
	1983	ドイツ	ドイツの憲法にはデータに関連したプライバシーの権利が含まれていないが、連邦憲法裁判所が個人の「情報を自己決定する権利」を公式に認める
福岡県春日市にて「個人情報保護条例」可決（7/4）。10/1施行	1984	アメリカ	「ケーブル通信政策法」制定
		イギリス	「データ保護法」制定（1998年に改正）
	1985	欧州評議会	「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」発効（10/1）
JIPDEC、民間事業者を対象とした「個人情報保護に関する調査研究」に着手	1986	アメリカ	「電子通信プライバシー法」制定
「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律案」閣議決定	1988	アメリカ	「コンピュータ・マッチング及びプライバシー保護法」制定
JIPDEC、「民間部門における個人情報保護のためのガイドライン」策定（５月）			
「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」公布（12/16）（「行政機関の保有する個人情報の保護に関する法律」で全部改正） 1989年10月１日に第三章と23条以外の規定が施行 1990年10月１日に全面施行			「ビデオプライバシー保護法」制定

国　内	年	海　外	
	1994	韓国	「公共機関における個人情報保護に関する法律」制定
		フランス	フランス憲法では明示的にはプライバシーの権利は保護されていないが、憲法裁判院がプライバシーの権利は憲法に内在的に含まれていると裁定
	1995	香港	「個人データ（プライバシー）法」制定
		台湾	「1995年コンピュータ処理に係る個人情報の保護に関する法律」制定
		EU	「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州会議及び理事会の指令」公示（10/24） （加盟国に３年以内の個人情報保護法制の整備を求める）
	1996	アメリカ	「電気通信法」制定
通商産業省、「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」公表（3/4）	1997		
JIPDEC、プライバシーマーク制度開始（4/1） （1997年の「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」に基づく）	1998	アメリカ	「児童オンラインプライバシー保護法」成立（10/21）
		EU	「EUデータ保護指令」施行（10/24）
			スウェーデンで、アメリカン航空に対してスウェーデン国内で収集した搭乗者の個人情報を米国内の予約センターに移転することを禁じる（11月）
		イギリス	「人権法」採択（11月）
「JIS Q 15001個人情報保護に関するコンプライアンス・プログラムの要求事項」制定（3/20）	1999		
	2000	カナダ	「個人情報保護及び電子文書法」制定
		EU-アメリカ	EU・米国間における「セーフハーバー協定」締結（７月）
	2001	アメリカ	「米国愛国者法」制定（10/26）。2015年６月失効
「個人情報保護法」公布・一部施行（5/30）	2003		
	2004	APEC	「APECプライバシーフレームワーク」採択（10/29）
「個人情報保護法」全面施行（4/1）	2005		
「JIS Q 15001：2006」改正（５月）	2006		
	2007	APEC	「越境プライバシールール」策定 「パスファインダープロジェクト」の試験的な取組み開始
	2012	EU	「EUデータ保護規則案」提出
		アメリカ	「消費者プライバシー権利章典」が掲載された行政白書にオバマ大統領が署名（2/23）
「行政手続における特定の個人を識別するための番号の利用等に関する法律」および関連法公布（5/31）	2013	OECD	「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」改正（7/11）

国　内	年	海　外	
特定個人情報保護委員会発足（1/1）	2014		
APEC越境プライバシールール（CBPR）システムに参加（４月）			
「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」成立（9/3）	2015	アメリカ	・「米国自由法」成立（6/2） ・「サイバーセキュリティ情報共有法」にオバマ大統領が署名（12/18）
		EU-アメリカ	欧州で「セーフハーバー協定」無効判決（10月）
特定個人情報保護委員会が改組し、個人情報保護委員会発足（1/1）	2016	EU	欧州本会議「一般データ保護規則（GDPR）」を正式可決（4/14）
APEC-CBPRシステムの認証団体として、JIPDECがアカウンタビリティ・エージェント（AA）に認定（１月）			
個人情報保護委員会、アジア太平洋プライバシー機関フォーラム（APPA）の正式メンバーに就任（６月）		EU-アメリカ	EU・米国間における「プライバシーシールド」がEU諸国で承認（7/12）。８月から米商務省への参加申請受付開始
「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律の施行に伴う関係政令の整備及び経過措置に関する政令」および「個人情報の保護に関する法律施行規則」制定（10月）			
「カメラ画像利活用ガイドブックver. 1.0」公表（1/31）	2017	EU	欧州委員会、電気通信分野のプライバシー保護を目的とする「e-プライバシー規則案」公表（1月）
「改正個人情報保護法」全面施行（5/30）		中国	「中華人民共和国サイバーセキュリティ法（インターネット安全法）」施行（6/1）
「JIS Q 15001：2017」改正（12/20）		ドイツ	GDPR施行に向け「連邦データ保護法」全面改正（6/30）
情報銀行に求められる「情報信託機能の認定に係る指針ver. 1.0」公表（6/26）	2018	EU	「EU一般データ保護規則（GDPR）」施行（5/25）
日-EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意確認、および個人データの越境移転に言及した共同声明発出（7/17）		ベトナム	「サイバーセキュリティ法」公布。国内でのデータ保存と事務所設置を義務化（6/12）。2019/1/1施行
「個人情報の保護に関する法律に係るＥＵ域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」策定（９月）。2019/1/23施行		フランス	「個人情報保護に関する法律」成立（5/14）
		EU-アメリカ	欧州議会、「プライバシーシールド」がEUの求める保護水準に達していないとして、米国当局に対応を要求（7/5）。米商務省は「準拠している」と声明（8/30）
		ベルギー	「個人データの処理に関する保護法」制定（7/30）
		イタリア	「改正個人データ保護法典」施行（9/19）
		米カリフォルニア州	「カリフォルニア州消費者プライバシー法2018年（CCPA）」発効（9/23）。2020/1/1施行
		EU	欧州委員会、日本の個人情報保護に対する十分性認定の採択手続きに着手（９月）
	2019	タイ	「個人情報保護法」施行（5/28）

国　内	年	海　外	
「個人情報の保護に関する法律等の一部を改正する法律」」公布（6/12）。2022年４月全面施行	2020	EU-アメリカ	EU司法裁、「プライバシーシールド」無効判決（7/16）
「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ver1.0」策定（8/28）		米カリフォルニア州	「CCPA」改正提議が住民投票で可決。より厳しい「カリフォルニア州プライバシー権利法（CPRA）」承認（７月）。2023年施行予定
		EU	欧州委員会、プライバシーシールドの無効判決を受け、標準契約条項（SCC）改定案発表（11/12）
	2021	シンガポール	個人情報保護法（2012）改正法施行（２月）
		米バージニア州	米国で２番目の「消費者データ保護法」制定（３月）
		中国	・「データセキュリティ法」成立（6/10）。9/1施行 ・「個人情報保護法」成立（8/20）。11/１施行
電気通信事業法改正（6/17公布）	2022	EU	・デジタル市場法（DMA）暫定合意（３月）。11/1発効 ・EU理事会がデジタルサービス法案（DSA）を正式採択（７月）。10月最終承認
		EU-アメリカ	2020年に無効判決を受けたプライバシーシールドに代わる「Trans-Atlantic Data Privacy Framework」原則的に合意（３月）
		アメリカ	連邦レベルのデータプライバシー法（ADPPA）が下院委員会で可決（7/20）
		中国	「データ海外越境安全評価弁法」施行（９月）
		インドネシア	初の「個人情報保護法」制定（９月）

〈資料２〉情報化に関する動向（2022年４月～2022年９月）

国　内	海　外
2022年４月	
・公正取引委員会、経済分析専門部署「経済分析室」設置。IT企業の取引慣行、規制で競争が働いていない分野の調査、取引慣行の改善や規制見直しへ。 ・富士通と帝国データバンク、日本版ｅシール社会実装に向けた実証実験開始。JIPDECはトラストサービスの適合性評価機関として参加。 ・日米ほかAPEC CBPR参加エコノミー７カ国、CBPRシステム拡大に向け、グローバルCBPRフォーラム設立宣言に合意。広範囲な個人データの円滑な越境移転、各国相互運用の促進を目指す。 ・東京大学、世界最高性能で真贋判定できるディープフェイク検出AI開発。 ・情報通信研究機構（NICT）、AI分野の研究開発を自ら行う研究開発法人として初のISO/IEC27001認証取得。	・米国務省、サイバー空間上の国家安全保障問題やデジタル政策を担うサイバー空間・デジタル政策局（CDP）発足。 ・ベトナム政府、消費者権利保護法改正案公表。 ・欧州連合（EU）、デジタルサービス法案（DSA）合意。巨大IT企業に違法コンテンツ対応義務付け。 ・カリフォルニア州地裁、Zoom爆撃被害ユーザーによる集団訴訟で、Zoomの8,500万ドル支払い和解合意を最終承認。 ・イーロン・マスク氏、Twitter買収を宣言。その後買収契約解除の可能性の提示やTwitter側の提訴等を経て、10月買収成立。

国　内	海　外
2022年５月	
・PayPayカード、システム不具合のリカバリー手順ミスで顧客の過去の情報を誤登録、29万人に影響。	・Ｇ７デジタル相会合、信頼性のある自由なデータ流通（DFFT）推進についての付属書、デジタルインフラのサイバー・レジリエンスに関する共同宣言等採択。 ・米コネチカット州、個人のデータプライバシーとオンライン監視に関する法案成立。包括的なプライバシー法成立は全米で５州目。 ・英ICO、SNSから200億人超の顔画像データを無断で収集、DB化していた顔認証技術企業Clearview AI社に755.2万ポンドの罰金と、英国居住者のデータ削除命令。 ・米連邦取引委員会（FTC）と司法省、Twitterによる追跡広告へのユーザーアカウント不正利用はFTC命令違反とする訴訟で、1.5億ドルの制裁金支払いで和解。 ・米最高裁、SNS企業によるユーザーアカウント停止や検閲を禁止するテキサス州法HB20（2021年９月成立）を一時差止め。

国　内	海　外
2022年６月	
・NICT、世界初、光格子時計をもとに、標準時の生成に成功。 ・政府、ネット利用者保護規制を盛り込んだ改正電気通信事業法成立。 ・公正取引委員会、巨大IT企業の独占禁止法違反審査にあたり、初期段階から社名、概要公表へ。 ・東京地裁、文化シャッター社のシステム開発中断に係る訴訟問題で、日本IBMに19.8億円の損害賠償命令。 ・尼崎市、データ移管作業の委託先社員が全市民46万人の個人情報を記録したUSBメモリ紛失。後日、USBが見つかり、情報流出の事実は確認されず。 ・最高裁、Twitter社に逮捕歴投稿に対する初の削除命令。東京高裁では削除認めず。	・米連邦捜査局、2,400万人の個人情報売買の闇市場「SSNDOB」のドメイン差押え、閉鎖。 ・Google、100兆桁の円周率計算成功で世界記録達成。 ・米下院商業委員長他、米国データプライバシー法案草案公表。対象事業者に対する透明性に関する義務の必須化等。 ・Microsoft、Internet Explorer（IE）のサポート終了。サービス提供から27年。 ・欧州委員会（EC）、偽情報に関する行動規範について、巨大IT企業33社と流通防止対策強化で合意。 ・仏競争委員会、Googleが検索結果で得たニュースの間接的な収入推計をコンテンツ発行人に支払うことで合意。Googleは罰金５億ユーロ支払いへ。 ・Microsoft等33企業、メタバースの標準化団体「Metaverse Standards Forum」設立。 ・ECと各国消費者保護当局、TikTokがEU域内消費者保護強化に同意したと発表。欧州消費者機構の警告がきっかけ。 ・中国政府、2008年施行の独占禁止法改正案を可決。ネット大手の規制強化を目的に、届け出義務違反厳罰化等。 ・ブロックチェーン新興企業Harmony、ハッキングで約１億ドルの盗難被害。 ・英国政府、2025年に向けてアイデア、人材、投資に焦点を当てたデジタル戦略発表。 ・中国政府、個人情報の海外移転制限規制案でパブコメ実施。

国　内	海　外
2022年７月	
・KDDI、メンテナンスの手順誤りで３日間にわたり大規模通信障害発生。計3,655万人に補償金総計73億円、１人当たり200円を請求額から減算。総務省が重大事故として８月に行政指導。 ・ｅラーニング提供サービスのリスクモンスター、自社サーバ内の個人情報25万件が検索可能に。数千件のダウンロード履歴あり。 ・Google他海外巨大IT企業、日本国内で初の登記。国内代表者の明確化により、国内トラブル処理迅速化へ。 ・クレディセゾン、国内初、クレジット申請にマイナカードで本人確認可能に。	・Google、複数の州による中絶禁止法施行を受け、プライバシー性の高い健康関連施設訪問履歴をロケーション履歴から自動削除すると公表。 ・欧州議会、デジタルサービス法案（DSA）とデジタル市場法案（DMA）可決。 ・中国警察機関、１年以上にわたり10億人の個人情報を記録したデータベースがアクセス可能に。 ・米国立標準技術研究所、IBM等開発の暗号「CRYSTALS-KYBER」を標準技術に採用。 ・中国政府、「データ海外越境安全評価弁法」公布、９月１日施行。海外への100万人以上の個人データ持出し時の審査義務付け。 ・バイデン大統領、中絶の権利に関する「ロー対ウェイド」判決を連邦裁が覆した判断を受け、中絶と患者のプライバシーに関する大統領令に署名。国民の医療へのアクセス、患者の安全、患者情報のプライバシー保護を明示。 ・米債券回収会社PFC、サイバー攻撃被害で2月に190万人超の医療記録等個人データ流出していたと発表。 ・モスクワ裁判所、YouTubeでウクライナ侵攻等に関し違法な情報を提供し続けたとして、Googleに210.7億ルーブルの罰金判決。 ・中国、利用客の顔認証情報や個人情報を違法に収集していたとして、滴滴に10億ドルの罰金。 ・米連邦議会下院、連邦初のデータプライバシー・保護法（ADPPA）案可決。 ・欧州理事会、DMAを最終承認。 ・ロシア連邦独占禁止局、YouTubeの独占的地位乱用で、Googleに20億ルーブルの罰金。 ・米上院「CHIPS法」可決。国内の半導体製造企業に対し、５年で527億ドルの資金提供へ。 ・Facebook、米国内でのニュース発行元との契約終了。

国　内	海　外
2022年８月	
・政府、2021年施行の「デジタルプラットフォーム取引透明化法」に巨大IT企業のネット広告規制を盛り込んだ政令施行。 ・NTTドコモ、送信ドメイン認証「DKIM」「DMARC」導入。 ・NTT西日本、伝送装置故障によるインターネット通信障害で最大263万回線に影響。	・中国政府、改正独占禁止法施行でAlibaba等プラットフォーマー規制強化。 ・Twitter、ゼロディ脆弱性悪用で約540万のアカウント情報流出を発表。 ・Google、位置情報機能オフ設定のユーザーの情報収集に関する世界規模の訴訟。オーストラリアでは6,000万豪ドルの罰金。 ・上海市、新型コロナウイルス対策アプリへのサイバー攻撃で4,850万人の情報流出報道。 ・Meta、Facebookの位置情報無断追跡訴訟で3,750万ドルの和解金支払いで合意。 ・Meta、Cambridge Analytica事件のFacebookユーザーによる訴訟で和解合意。 ・FTC、中絶クリニック、礼拝所への訪問者の位置情報を大量販売したとして、トラッキングツール販売業者Kochavaを提訴。 ・カリフォルニア州議会、18歳未満のオンライン保護提供を目的とする「カリフォルニア年齢適正デザイン規範法」可決。

国　内	海　外
2022年９月	
・政府、e-Gov等４省庁23サイトとeLTAXが一時閲覧不能に。親ロシア派ハッカー集団KILLNETが犯行声明。 ・政府、新型コロナウイルス接触確認アプリ「COCOA」機能停止方針発表。 ・内閣府、約9.5万人分の医療情報を通知なく収集したとして、NTTデータ他に再発防止策の提出命令。	・アイルランドデータ保護委員会、GDPR違反でInstagramに４億500万ユーロの罰金。10代も作成可能なビジネスアカウントの個人データ公開設定を問題視。Instagramは異議申立て。 ・米政府、巨大IT企業規制強化に向け６原則「競争促進」「プライバシー保護」「子どもの保護」「巨大ITへの特別な法的保護解除」「透明性向上」「アルゴリズムによる差別禁止」を発表。 ・EU第一審裁判所、ECが欧州独禁法違反でGoogleに43.4億ユーロの制裁金支払いを命じた（2018年）ことを支持。制裁金は41.2億ユーロに減額。 ・暗号資産取引大手Wintermute Trading、ハッキング被害で1.6億万ドル相当のデジタル資産盗難。 ・インドネシア政府、初の個人情報保護法制定。 ・豪通信大手Optus、サイバー攻撃による顧客情報流出で最大980万人に影響の可能性。

JIPDEC IT-Report 2022 Winter
2022年12月16日発行（通巻第20号）
発行所　一般財団法人日本情報経済社会推進協会
〒106-0032 東京都港区六本木1-9-9
六本木ファーストビル12階
TEL：03-5860-7555
制　作　株式会社ウィザップ
禁・無断転載