

2023 WINTER

# IT-REPORT

特 集

## 企業における プライバシーガバナンス

### Contents

【特集】 企業におけるプライバシーガバナンス 座談会 今考えるプライバシーガバナンス ～生成AIをはじめデータの高度な利用が進む中で～ 国立情報学研究所 教授 佐藤 一郎氏 PwC Japan有限責任監査法人 システム・プロセス・アシュアランス パートナー 平岩 久人氏 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 主幹 恩田 さくら	01 01
【JIPDECレポート】 DFFT促進の現況と課題 元一般財団法人日本情報経済社会推進協会 上河辺 康子 グローバル化する個人情報の越境移転ツール 一般財団法人日本情報経済社会推進協会 認定個人情報保護団体事務局 事務局長 奥原 早苗 メタバースと個人情報やプライバシーについて 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 野町 綺乃	09 09 13 19
AIガバナンスに係る国内外の動き 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 主幹 恩田 さくら	22
プライバシーマーク25周年 記念表彰式 【記念講演レポート】 JIPDECプライバシーマーク制度創設25周年を迎えて ～更なる発展を目指して～ 一橋大学名誉教授、元JIPDECプライバシーマーク制度委員会委員長、 元個人情報保護委員会委員長 堀部 政男氏	24 26 26
【コラム】 JIS Q 15001の改正について 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 主幹 恩田 さくら	31 31
英国政府のサイバーセキュリティ戦略 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 主任研究員 大熊 三恵子 ドメイン名のご利用は計画的に 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 主幹 高倉 万記子 デジタルトラストとトラストサービスの信頼性評価 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 副センター長 萩原 隆	32 33 33 34
〈資料編〉 国内外の主な個人情報保護関連の年表 情報化に関する動向 (2023年4月～2023年9月)	35 39

ChatGPTの登場から早1年。生成AIの進化によって、私たちの生活、ビジネスは大きな変革期を迎えています。

早々にAI利用に関するガイドラインや声明を発表する企業や大学も相次ぎ、技術の進歩に合わせていかに社内の体制構築を行うかは、今後、とても重要な経営テーマになると感じています。

つい1年前にはなかったものが自分たちの仕事を大きく変える。このような変革がこの後もどんどん起こっていくとすれば、状況を素早く把握して、理解した上で必要か不要か、必要であればどのような体制、ルールで活用していけばいいのかを変化を恐れず柔軟に受け入れる姿勢が必要だと思います。

IT-Report 2023 Winterでは、生成AIなど技術の進歩に伴いますます配慮が必要になっているパーソナルデータと、さらにはデータの利活用が高度

化するに当たり、より効果的かつ安全に取り扱うためのヒントとして、「プライバシーガバナンス」の観点から高度化するデータの利活用に対してどう向き合うかについて特集を組みました。

また、データ流通の国際的な取組みとして、「グローバルCBPR」や「DFFT」に関する調査レポートのほか、今年4月に25周年を迎えたプライバシーマークの表彰式の模様等も収録しています。

本誌掲載の内容は、JIPDECのWebサイトでも公開中です。資料の引用・転載等をご希望の方はぜひお問い合わせください。皆さまの日々の業務対応、改善の一助になれば幸いです。

2023年12月

一般財団法人日本情報経済社会推進協会

## Contents

<b>【特集】 企業におけるプライバシーガバナンス</b> .....	01
座談会 今考えるプライバシーガバナンス ～生成AIをはじめデータの高度な利用が進む中で～ ...	01
国立情報学研究所 教授 佐藤 一郎氏 PwC Japan有限責任監査法人 システム・プロセス・アシュアランス パートナー 平岩 久人氏 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 主幹 恩田 さくら	
<b>【JIPDECレポート】</b> .....	09
DFFT促進の現況と課題 .....	09
元 一般財団法人日本情報経済社会推進協会 上河辺 康子 グローバル化する個人情報の越境移転ツール .....	13
一般財団法人日本情報経済社会推進協会 認定個人情報保護団体事務局 事務局長 奥原 早苗	
メタバースと個人情報やプライバシーについて .....	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 野町 綺乃 AIガバナンスに係る国内外の動き .....	22
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 主幹 恩田 さくら	
プライバシーマーク25周年 記念表彰式 .....	24
<b>【記念講演レポート】</b> .....	26
JIPDECプライバシーマーク制度創設25周年を迎えて ～更なる発展を目指して～ .....	26
一橋大学名誉教授、元JIPDECプライバシーマーク制度委員会委員長、元個人情報保護委員会委員長 堀部 政男氏	
<b>【コラム】</b> .....	31
JIS Q 15001の改正について .....	31
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 主幹 恩田 さくら	
英国政府のサイバーセキュリティ戦略 .....	32
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 主任研究員 大熊 三恵子	
ドメイン名のご利用は計画的に .....	33
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 主幹 高倉 万記子	
デジタルトラストとトラストサービスの信頼性評価 .....	34
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 副センター長 萩原 隆	
<b>【資料編】 国内外の主な個人情報保護関連の年表</b> .....	35
情報化に関する動向（2023年4月～2023年9月） .....	39

特集

# 企業におけるプライバシーガバナンス

## 座談会 今考えるプライバシーガバナンス ～生成AIをはじめデータの高度な利用が進む中で～

国立情報学研究所 教授 佐藤 一郎氏

PwC Japan有限責任監査法人 システム・プロセス・アシュアランス パートナー 平岩 久人氏

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 主幹 恩田 さくら

### はじめに

デジタル化の加速を背景に、パーソナルデータの利活用におけるプライバシーへの配慮はますます重要になってきています。経済産業省、総務省は、「企業のプライバシーガバナンスモデル検討会」での議論を通じて、企業が社会から信頼を獲得するためのプライバシーガバナンスの構築に向けて取り組むべきことを取りまとめた「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」（以下、ガイドブック）を2020年8月に発表し、その後も2023年4月に公表されたガイドブックver1.3に至るまで、改訂を重ねてきました。

企業のプライバシーガバナンスとは、プライバシー問題の適切なリスク管理と信頼の確保による企業価値向上に向けて、経営者が積極的にプライバシー問題への取組みにコミットし、組織全体でプライバシー問題に取り組むための体制を構築し、それを機能させることをいいます。ガイドブックでは、プライバシーガバナンスの構築のために、経営者が取り組むべき3要件及びプライバシーガバナンスの重要項目（5項目）が整理されています（図1参照）。

2021年7月に公表されたガイドブックver1.1や2022年2月に公表されたガイドブックver1.2では、具体的な事例の充実が図られました。そして、2023年4月に公表されたガイドブックver1.3では、

**【対象読者】** パーソナルデータを利活用した製品・サービスを提供し、消費者のプライバシーへの配慮を迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等であって、  
①**企業の経営陣または経営者へ提案できるポジションにいる管理職等**  
②**データの利活用や保護に係る事柄を総合的に管理する部門の責任者・担当者** など

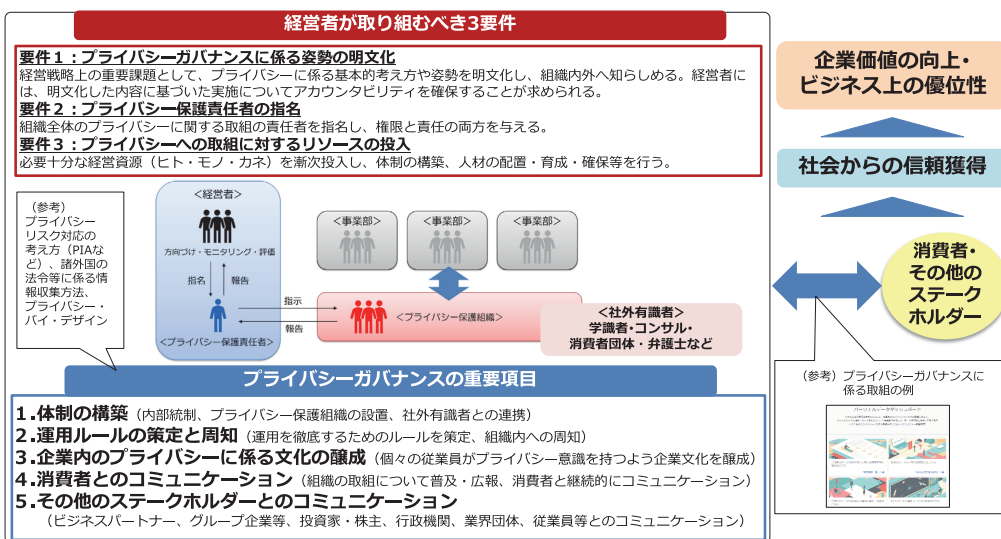


図1. DX時代における企業のプライバシーガバナンスガイドブックver1.3の概要

（出典）「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ver1.3概要」

ガイドブックの理解をさらに深めていただくことができるよう、ガイドブックに記載される概念整理が進められ、プライバシーガバナンスについてのフレームワークによる整理等が追加されました。またあわせて、海外への発信を見据えたガイドブックver1.3英訳版や、実務において参照できる具体的な情報を充実してほしいとのニーズを踏まえて、ガイドブックの要件、重要項目別に整理した、実践例集「企業のプライバシーガバナンスに関する実践例の整理」（以下、実践例の整理）が公表されました。

ガイドブックや実践例の整理の内容の詳細については、ぜひ本文や概要資料を参照ください<sup>1</sup>。

2020年8月のガイドブックver1.0リリース後、3年が経過しました。今回は、ガイドブックを取りまとめた「企業のプライバシーガバナンスモデル検討会」座長 国立情報学研究所 佐藤一郎氏と、検討会に委員として参加されたPwC Japan有限責任監査法人 平岩久人氏に、今、改めてガイドブックをどのように捉えていらっしゃるか、企業の皆さまが自社の有するプライバシーリスクや組織構造の特性に応じてプライバシーガバナンスを実践される際のポイントやヒント、生成AIをはじめ高度なデータ利活用が進む現状を踏まえ、今後のプライバシーガバナンスをどう考えられるかについて、対談形式でお話を伺いました。

## 今考える、プライバシーガバナンスガイドブックの意義

**恩田：**2020年8月のガイドブックver1.0リリースから3年が経過しました。いま、ガイドブックをどのように捉えられているかから、お話を聞かせてください。

**佐藤：**この3年の間に、多様な業界の特にトップ企業を中心に、ガイドブックに沿った、プライバシー

ガバナンス体制を構築していただけたと思います。私も他の検討会の委員も、ここまで皆様にご賛同いただいたことを、素直に喜んでいるところです。まずはお礼を申し上げたいと思います。啓発活動を続けていただいた、経済産業省、総務省、検討会の委員の方々、JIPDECにも、検討会の座長として深く感謝申し上げます。

**平岩：**この3年間、多くの企業の方とお話する中で実感しているのは、技術やサービスの進展に伴い、様々なデータの利活用のアイデアは生まれてきていても、このような使い方を本当にして良いのだろうかという不安がつきまとっている、ということです。そのような

時に、このガイドブックを参照してもらいたいです。実際、多くの企業がガイドブックを参考に、ガバナンスの構築を進めていただいていると思います。2023年4月に「実践例の整理」として、多くの事例を取りまとめることができたのは、とても意義のあることだったと思います。

**佐藤：**検討会の議論でも何度か話題に上がりましたが、日本では、個人情報、法律に基づく情報の類型であり、比較的明確です。では、個人情報保護法



国立情報学研究所 教授  
佐藤 一郎氏



PwC Japan有限責任監査法人  
平岩 久人氏



JIPDEC 恩田 さくら

1 経済産業省「DX時代における企業のプライバシーガバナンスモデルガイドブックver1.3（令和5年4月25日改訂）」  
[https://www.meti.go.jp/policy/it\\_policy/privacy/privacy.html#book](https://www.meti.go.jp/policy/it_policy/privacy/privacy.html#book)  
総務省「「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ver1.3」を策定しました（令和5年4月25日）」  
[https://www.soumu.go.jp/menu\\_kyotsuu/important/kinkyu02\\_000513.html](https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000513.html)

ですが、その前身となったOECDのプライバシー8原則<sup>2</sup>を考えると、個人情報とプライバシーに関することの重なりが大きいという点を利用して、個人情報保護を通じて間接的にプライバシーを保護するということが、個人情報保護法の考え方なのか、とも思います。プライバシーの保護として考慮すべき範囲と、個人情報保護法により守られる範囲は重なっていますが、一方で、両者の範囲は同じではない（図2参照）ということは、ガイドブックを理解する上で、重要な点だと思っています。近年、ビッグデータ、IoT、AIなどが進化することによって、個人情報ではなくても、プライバシー保護の観点からは配慮しなければならない、利用の仕方によっては、個人の権利利益の侵害になるような情報の範囲が広がっています。そのため、個人情報保護法を守れば、プライバシーが守れるということではなくなってきていて、プライバシーを保護することと、そのプライバシーの保護のためのガバナンスが、より重要になってきていると思います。

**平岩：**個人情報の保護とプライバシーに関する情報の保護については、プライバシーに関する情報の利用の仕方が進化していて、今まで想像すらできなかったような使い方ができてしまい、分析や推論を経てプライバシーを侵害しうるような状況がありま

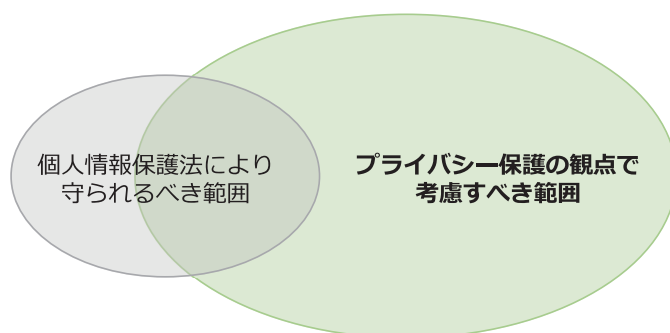
す。この点について、今後、法令対応は当然として、ガバナンスという形でどのように配慮、保護を実践していくのかというところが、今、多くの企業の方が悩まれている点だと思います。

**佐藤：**プライバシーの保護に関して権利利益の侵害ということになれば、当然民事的な訴訟にはなりますが、個人情報保護法で保護できる範囲は限定的です。プライバシー保護の観点から配慮すべき情報の範囲が広がっていることを考えると、どのような情報を、どのように利用すれば、適切な保護をした上での活用となるのか、企業自身が考える必要があります。このガイドブックは、それを考えていただくための基本的な枠組みを提供しています。ガイドブックは、繰り返しバージョンアップを行い、その時その時点で必要な情報や事例を追加する等していますが、骨格はあまり変わっていません。

## プライバシーガバナンスへの主体的な取組みと企業文化の醸成

**恩田：**ガイドブック策定や改訂の検討の中で、他に強調されたい点や、印象的であった点について、さらにお話を伺います。

プライバシーの保護の観点で考慮すべき範囲は、消費者保護とプライバシー保護の重要性に基づいて、個人情報保護法上で守られるべき範囲に限定されず、取り扱い情報や技術、取り巻く環境によって変化することから、特段の配慮が必要となる。



【例】

- 個人が意図しないところで、私的空間の個人の姿態を撮影・公表する
- 個人が意図しないところで、長期に広範囲にわたる個人の追跡を行う
- カメラでの撮影によって個人に不安や居心地が悪い感情を与える
- データが勝手に個人に結びつけられてしまい、個人にとって害のある情報も収集されるのではないかの疑念が生じる
- 目的外利用されてしまい、自分の情報が意図に反して利用されてしまうのではないかの恐怖と不安が生まれる
- 第三者への提供により、二次利用によって更なるプライバシー問題が引き起こされるのではないかという不安がうまれる

など…

図2. プライバシー保護の観点で考慮すべき範囲（イメージ）

（出典）「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ver1.3」

2 OECDが1980年9月に採択した「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」に記述されている以下8つの原則。「目的明確化の原則」、「利用制限の原則」、「収集制限の原則」、「データ内容の原則」、「安全保護の原則」、「公開の原則」、「個人参加の原則」、「責任の原則」が定められている。

**佐藤：**このガイドブックは、企業の自主的な取組みを促す枠組みです。検討会で議論になった内容で、「北風と太陽」という話があります。企業にプライバシーガバナンスに取り組んでいただく際に、「プライバシー侵害が起きると社会的にも怒られますよ、だから対策をしてください」という「北風」的な、ネガティブインセンティブにより説明するという考え方と、「企業がプライバシーを適切に保護することによって、消費者の信頼が得られ、結果的に収益の改善につながります」という、いわゆる「太陽」路線、ポジティブインセンティブにより説明するという考え方があると思います。どちらも成立すると思いますが、私の個人的な見解としては、企業に自主的に対応いただくとなると、やはりポジティブインセンティブ、「太陽」路線を強調せざるを得ないところがあると考えています。皆さんにご理解いただきたいのは、プライバシーの対応は、嫌々するというものではなく、それによってお客様の信頼が上がり、自社の売上げが伸びるという観点からすれば、むしろ企業の商品やサービスの品質改善と同じものなのだと思います。その観点でプライバシーへの対応をしていただくことが、重要だと思っています。

**平岩：**プライバシーという、時間の経過やコンテキストに応じて可変的であるものに対して、企業がどう向き合っていくかを考えたときに、「静的で固定的な組織やプロセスを構築し、一般的・典型的なリスクと対策が整備されてさえいれば十分にプライバシーへの対応ができる」ということではない、という点を、常に意識していました。具体的には、例えばプライバシー保護体制を検討するときに、「適切な形を提示してほしい」という気持ちはとてもよくわかるのですが、やはりこれまで培ってきた企業の特徴や組織構造、風土や文化に即した形で考えていただく必要がある、と強調してきたつもりです。可変的なものに対して静的に対応するのではなく、その時々技術の進化や、社会的な受容性の変化に対応できるような柔軟な組織や対応の在り方はどういうものか、という問題意識のもとで、そう申し上げてきました。

大事になってくるのは、組織に根付いた企業風土や文化であると最近つくづく思います。担当役員を指名し、組織を作ってプライバシー保護活動を始めるのももちろん大切であり必要です。他方、プライバシーに関する情報の利活用を伴う新しいビジネスを企画する、あるいはプライバシーに関する情報を実際に取り扱う際には、その情報の背後にいるお客様、生活者を、リアルに想像して、プライバシー保護という取組みを行っていただけるかどうか、非常に重要なポイントなのだと思います。こういったプライバシー保護に関する企業風土や文化は、社内規程を定めるだけで実現できるものではありませんし、プライバシー保護のための社内組織があるだけでも十分ではなく、一人ひとりが意識し続けざるを得ない。これから、データの利活用が高度化し、ますます難しい判断や対応を迫られることが多くなってくると思いますが、先ほどの佐藤先生のお話の、ポジティブインセンティブの基礎になりうるのは、企業のプライバシー保護に関する風土や文化なのではないかと思っています。

### 自社の特性にあわせたプライバシーガバナンスの実践に向けて

**恩田：**自社の有するプライバシーリスクや組織構造の特性にあわせた実践が強調されたところですが、実際にプライバシーガバナンスに取り組もうという企業においては、もう少し踏み込んだアドバイスやヒントをいただけたらありがたいという面もあるのではないかと思います。本年4月にガイドブック ver.1.3にあわせて「実践例の整理」を公表していますが、これは実際に事業者の方から、実務で参照できる具体的な情報（プラクティス）を充実して欲しいという声を受けて整理されたものでした。

**佐藤：**確かに、急にプライバシーガバナンス、プライバシー保護をしてくださいと言っても、なかなかそういった経験がない企業からすると「どうやったらいいのか」と思うところです。ガイドブック中でも、「実践例の整理」でも、いろいろな企業の事例をご紹介しているので、それを見ていただくことは

有益だと思えます。ただ、平岩さんからも指摘があったように、プライバシー保護は企業のカルチャーに大きく依存しています。もう少し具体的なお話をすると、同じ情報でも、利活用する企業の業種によって、プライバシー的な懸念が起きる場合もあれば、起きない場合もあります。例えば、「人が在宅しているかどうか」という情報は、警備会社が持ってもプライバシー的に問題とは言われないうかもしれない（もちろん、言われる場合もあるかもしれませんが、気にしない人もいます）。でも、それを家電メーカーが持っていたとしたら、プライバシーの観点からすると、変でしょう、という話になるかもしれない。このように、同じ情報であっても、利活用する企業の業種によって、消費者の捉え方は違って来るし、また、同じ業種の中においてもどういうビジネスでその情報を利用するかによって、「ここまでは利用できる」という範囲は違って来るところがあります。したがって、事例を参考にさせていただくことは大切ですが、結局は、企業自身が考えなくては行けない。実際にプライバシーを守るのは、組織だけでなく、従業員一人ひとりなので、一人ひとりがその企業でどういうプライバシーを守っていくのかという共通の認識を、きちんと作るということが大切だと思えます。こういった取組みには、なかなか「銀の弾丸」はないと思えますが、ただ一方で、プライバシーの保護は、企業によっては自社の利益やビジネスと相反するところがあっ

て、プライバシーを侵害してもいいので売上げを上げたいという誘惑に駆られることがあるかもしれません。それを避けるために、我々はちゃんとガバナンスを作ってくださいと申しているのと、企業の考え方と、消費者やそのほか多くの方々の考え方は違って来る可能性があるの、消費者団体を含めた第三者の意見を聞いて、取り入れて、どういう情報をプライバシーとして守るべきなのか、またはその中でどのように利用すればプライバシーの問題が起きずに済むのかということ、よく理解して進めていただくことが大切だと思えます。

**平岩：**ガイドブックver.1.3への改訂に当たって、概念整理を行い、フレームワークのイメージを具体的にすることができました（図3参照）。フレームワーク自体は非常に抽象度の高いものなのですが、それでもこのようなフレームワークがあれば、フレームワーク中のいくつかの機能は、自社の中で、既に確立した、あるいは類似した機能や組織、プロセスなどがあり、それらを活用してプライバシーガバナンス構築を検討する契機として役に立つのではないかと考えたからです。プライバシーガバナンス構築に当たり、どこから手を付けたらいいかわからないということがもしあれば、このフレームワークを自社のプライバシー保護活動に当てはめてみて、自社の取組みで既に実現できているところや、逆に足りないところはどこか、不足する点を実現するにはいつ

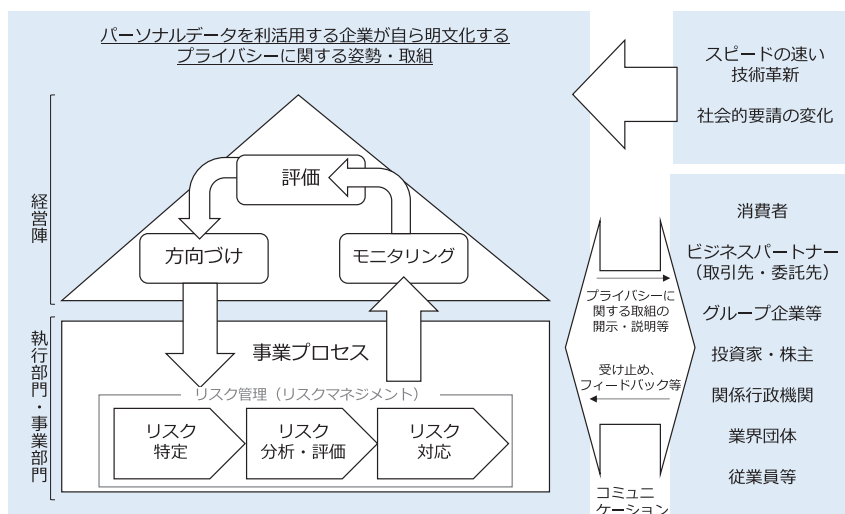


図3. プライバシーガバナンスのフレームワーク (イメージ)

(出典) 「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ver.1.3」

までに何が必要か、そういった議論からはじめていただくのも、一つの進め方だと思います。

また、実際に取り扱うプライバシーに関する情報のリスクを検討するときには、第三者、外部の目線を入れ続けることができる体制・組織にすることが重要です。有識者の先生方からご意見を伺うことも一案ですし、プライバシーに関して問題になった事案を含む社会の動向や実際のお客様の声なども含めて、プライバシーに関する多様な考え方、感じ方、受止め方というものを、リスク管理のインプットとして確保できるような仕組みにしてもらえると良いのではないかと思います。

## 進む高度なデータ利活用とプライバシーガバナンス

**恩田：**次に、プライバシーガバナンスをめぐる今後の動きについて、お話を伺います。目下、生成AIの利活用が急激に進んでおり、各社がガバナンスを効かせつつどう生成AIを活用していくか、悩まれている状況もあると思います。

**佐藤：**生成AIに関しては、ChatGPTが出てきたのが2022年11月30日で、比較的新しい話題です。生成AIについては、いろいろなリスクがある中に、プライバシーに関するリスクもありますが、必ずしもしっかりとした手当てがまだできていない、という状況だと思っています。実際、生成AIに関するプライバシーにかかわる問題はいくつかありますが、主なものは以下の4つと認識しています。

- ①プライバシーに関する情報が生成AIの学習対象、学習データに含まれてしまうという問題
- ②利用者が生成AIを利用するときに入力（プロンプト）に誰かのプライバシー情報を入れてしまうという問題

③生成AIの出力に個人のプライバシーに関する情報が出てくるという問題

④AIの生成物にプライバシーの情報が含まれているとして、それが正しくなかった場合の問題

4つとも、個人情報保護法だけで守れるかというと、そうではなさそうです。

①は、学習モデルと特定の個人との対応関係が排斥されている場合には、学習モデルは個人情報ではないとされています<sup>3</sup>、そもそも統計データについては利用目的の特定が不要とされています。このことから、個人情報ではない学習モデルについて、利用目的規制との関係でどのような解釈をすることが不明瞭との指摘もあります。②は、入力（プロンプト）が利用目的の範囲内であることを十分に確認するよう注意喚起されていますが（入力に対する応答結果の出力以外の目的で取り扱われる場合（生成AIを提供する事業者の側で学習データとして利用されることが予定されている場合）には、個人情報保護法の規定（利用者が入力した情報が個人データであれば第三者提供に当たるため本人同意が必要となる等の規定等）に違反することとなる可能性がある等<sup>4</sup>）、やはりそもそもプロンプトとしてプライバシーに関する情報を入力するのは、学習モデルに反映されていなくても生成AIの事業者のログには残るので、プライバシーの観点では配慮がいるのではないかと思います。③は、個人情報保護法では、出力を規律するのは、個人データの第三者提供に係るものであり、体系化されていない状態の個人情報やプライバシー情報については規律が十分にできない可能性があります。④に関しては、個人情報保護法の場合、開示請求をすることができるのは保有個人データ（個人データであって、事業者が修正や訂正ができる場合）となるため、やはりこの条件に当てはまらなければ、開示請求への対応が法的には求めきれない可能性があります。個人情報保護法で十分

3 「個人情報の保護に関する法律についてのガイドライン」に関するQA1-8

（[https://www.ppc.go.jp/all\\_faq\\_index/faq1-q1-8/](https://www.ppc.go.jp/all_faq_index/faq1-q1-8/)）

4 「生成AIサービスの利用に関する注意喚起等について」

（個人情報保護委員会、2023年6月 [https://www.ppc.go.jp/news/careful\\_information/230602\\_AI\\_utilize\\_alert/](https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/)）

リーフレット「生成AIサービスの利用に関する注意喚起」

（個人情報保護委員会、[https://www.ppc.go.jp/files/pdf/generativeAI\\_notice\\_leaflet2023.pdf](https://www.ppc.go.jp/files/pdf/generativeAI_notice_leaflet2023.pdf)）



に保護しきれないと思われるところは、現状は、企業が、個人情報に限らずプライバシーに関しても配慮いただきながら、自主的に保護していただかなければならない状況なのではないか、と思います。

**平岩：**生成AIを利用していきたいと考えている企業が多くある一方で、今ご指摘のあったようなリスクや懸念事項も、多く挙げられています。まずは自社で規定やルールを整備したいというご相談をいただくことが多いです。生成AIのユーザー側においては、個人情報やプライバシーに関する情報は入力しない、生成AIを利用して出力されたものは人がチェックするということが多いようですが、現状は、企業がそれぞれ自主防衛的、保守的に対応せざるを得ない状況ではないかと思います。

**恩田：**ありがとうございます。他方、データ流通や連携の基盤の整備が進むなど、複数社の中でデータを流通・連携させて、新たな価値を生んでいく取り組みも進んでいます。プライバシーガバナンスとの関連で、将来像や、今後検討が必要となること等があれば、お聞かせください。

**佐藤：**1社ではなく複数社におけるプライバシーガバナンスは、なかなか難しい問題です。コーポレートガバナンスは、基本的には個社単位の考え方なので、まずは個社でガバナンスを作っていただくことが先で、その上で、複数社間で、何らかのプライバシーに関するルールや、考え方を作っていくということかと思います。

データの流通の観点では、日本ではDFFT（Data Free Flow with Trust：信頼性のある自由なデータ流通）といった考え方も非常に強いですが、なかなか進んでいないところもあります。それは、一つはデータの取得経緯が見えないと分析が難しいことです。例えば、スーパーの購買履歴であれば、スーパーがある商品を安売りしていた時のデータなのかどうかで、分析が全く違ってくるというように、データの取得経緯がわからないと、分析はできないという点が挙げられます。さらに、プライバシーや法的な問題がでてきたときには、そのデータが、適

切な同意なり手順に則って取得されたものなのかどうか、わからないと、使えないわけです。こういったことに対して、プライバシーガバナンスをしっかりと構築していただくことによって、他社のデータでも取得経緯、同意及びそのときの説明内容がある程度見えてくることで、データの利用が広がる可能性はあると思います。

**平岩：**佐藤先生の仰るように、まずは各社で個々にガバナンスを構築してもらうことが大前提であると思います。その上で初めて、データ流通させたとき、あるいは共通のデータ流通の基盤を複数社で利用するようなとき、責任分界点はどこで、どの企業が何をやるべきなのかという話ができるのだろうと思います。利活用の仕方のモデルやアーキテクチャにも依存しますが、各社の責任範囲として行うべき領域がある一方で、共通的な基盤として、どこの会社がやってもいいが、どこもあまりやりたがらないような領域も、おそらく出てくるのではないのでしょうか。この点、公的な機関か業界団体等が担うのかわかりませんが、いずれにせよ各個社のガバナンスでは拾いきれないところを誰がどのようにサポートできるかが、データ流通が進展するかどうかの一つの鍵ではないかと思います。

**佐藤：**複数社のアライアンスに入りさえすればよいと考える企業が出てくると思うので、複数社でデータを利活用するような将来においても、各社が責任をもって個社のガバナンスをするという線は、押さえておいた方がいいと思います。

**平岩：**確かに、そのようなケースも考えられますので、各社が責任をもって個社のガバナンスをすべきであることは、前提として確認しておきたいですね。

## 企業の皆さまへのメッセージ

**恩田：**それでは最後に企業の皆さまへのメッセージをお願いします。

**佐藤：**はじめの方で申し上げた通り、プライバシー

の観点で配慮すべき範囲と、個人情報保護法により守られる範囲は、同じではないということを認識していただきたいです。プライバシーに関しては、利用の仕方や企業の業種であったり企業の特性によって、プライバシーの侵害が起きる場合があったり、起きない場合もあって、企業自身が考えていかなければいけないところです。それを考えるための枠組みや、実現するための方法論、考え方が、ガイドブックにまとめてあるのでぜひ参考にさせていただきたいと思います。企業自身で考えて、そこで働いている一人ひとりがその考え方を共有することが、大切だということを再度強調したいと思います。

2点目としては、ややアカデミックな観点ですが、現状、プライバシーについて、主に2つの考え方があると思っています。一つは、憲法13条に基づく、いわゆる「自己コントロール権」説、もう一つは、「適正な取扱いを受ける権利」説です。自己コントロール権は、自己に関する情報の開示範囲や利用について自分自身で決められるという考え方です。同意するか否かが重要となってきます。一方、適正な取扱いを受ける権利は、同意やオプトアウトは、自己の情報が適正に扱われる手段にすぎないので、適正に扱われることを担保できさえすればいいのではないか、という考え方です。ガイドブックは、一見、後者として読めてしまうかもしれませんが、例えば、企業が個人に対して同意を求めたり、オプトアウトを提供することによってプライバシーの侵害を未然に防ぐという、前者となる自己コントロール的なやり方を積極的に使っていくことを否定していません。なお、現状は、後者、つまり「適正な取扱いを受ける権利」説の場合、適正な取扱いはなにかというところは不明確なところもあり、また、同意やオプトアウトをさぼってもよいという理由付けに利

用されてしまう恐れもあるところには注意が必要だと感じています。

**恩田：**ガイドブックでは、第5章でDANIEL J. SOLOVEの「A Taxonomy of Privacy」を参照して「プライバシー問題の例」が掲載されています。プライバシー問題を提起する特定の諸活動に焦点を当て、類型論として整理されたものと理解しています。プライバシーの捉え方には様々な考え方、アプローチがありますが、ガイドブック記載の内容が、企業の皆様の検討のお役に立てばと思います。

**平岩：**プライバシーガバナンスは、プライバシーという可変的なものを対象としなければならない以上、社内規程や組織、プロセスを一回作って終わり、というものではないということを、改めて強調しておきたいと思います。これからプライバシーガバナンスの構築に取り組みられようとする企業の皆さんには、このガイドブックが、基本的なところから解きほぐして、本質的なところをすべてカバーしていると思いますので、まずご一読いただければと思います。その上で、具体的にどうしたらいいかわからないときには、「実践例の整理」を見ていただければと思います。そこで試行錯誤をしながら、取り組み続けることが何よりも大事だと思います。その先にあるのは、プライバシーを保護する企業風土や文化だと思いますので、そこに向けて、地道な取組みかもしれませんが、懲りずにやり続けていただくことが一番重要なことだと思います。

**恩田：**今日は貴重なお話を伺わせていただき、ありがとうございました。

## DFFT促進の現況と課題

元 一般財団法人日本情報経済社会推進協会 上河辺 康子

### はじめに

信頼性のある自由なデータ流通（Data Free Flow with Trust、以下、DFFT）は、日本が国際社会に向けて提唱したデータ利活用の在り方を示す概念であり、提唱後は国際的な議論の論点として定着してきた。また、気候変動、COVID-19のパンデミック、ウクライナ情勢、生成AI利用拡大等を通じて、データ越境移転の必要性及びその国際的な規制の在り方に関わるDFFTは、ますますその重要性を増していると考えられる。今回は、DFFTに関する国際的な議論の経緯をふまえ、DFFT推進に向けた取組みの進捗と課題を検討したい。

### 1. 日本によるDFFTの提唱

DFFTは、2019年1月の世界経済フォーラム年次総会（ダボス会議）における安倍総理大臣（当時）の演説において言及された<sup>1</sup>。その意味は、「デジタル時代の新たなIT政策大綱」（2019年6月7日、高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議）において、“プライバシーやセキュリティ・知的財産権に関する信頼を確保しながら、国際的に自由なデータ流通の促進を目指すというコンセプト”<sup>2</sup>と説明された。

さらに、同年6月のG20大阪サミット（議長国：日本）の成果文書であるG20大阪首脳宣言にDFFTが盛り込まれ、DFFTは各国が共有するところと

なった。G20大阪首脳宣言では、DFFTはデジタル経済の機会を活かすものとされ、“データ、情報、アイデア及び知識の越境流通は、生産性の向上、イノベーションの増大及びより良い持続的開発をもたらす一方で、プライバシー、データ保護、知的財産権及びセキュリティに関する課題を提起する”<sup>3</sup>とし、国内的及び国際的な法的枠組みの双方が尊重されることの必要性や、異なる枠組みの相互運用性に言及された。

### 2. DFFTのための協力体制の構築

DFFTは、日本による提唱後、国際的なデータ流通のあるべき姿として、G20、G7の国際会議の場において議題に挙げられてきた。G20は、2020年以降も首脳宣言等でDFFTに言及してきた。2023年は、インドがG20の議長国を務め、G20デジタル経済大臣会合の成果文書及びG20ニューデリー首脳宣言では、デジタル公共インフラの相互運用の観点からDFFTを実現することの重要性に言及された<sup>4</sup>。

G7では、DFFT具体化に向けた協力体制の構築が進められてきた。2019年8月のG7ピアリッツサミット（議長国：フランス）の成果文書「開かれた自由で安全なデジタル化による変革のためのピアリッツ戦略」では、DFFTはデジタル化による変革の機会を活かすものとされ、G20大阪首脳宣言と同様、国内及び国際的な法的枠組みの双方が尊重されることの必要性や、異なる枠組みの相互運用性に言及され

1 安倍総理大臣演説「希望が生まれ出す経済」の新しい時代に向かって（政府仮訳）  
[https://www.mofa.go.jp/mofaj/ecm/ec/page4\\_004675.html](https://www.mofa.go.jp/mofaj/ecm/ec/page4_004675.html)

2 デジタル時代の新たなIT政策大綱 41項

3 G20大阪首脳宣言 11項

4 G20デジタル経済大臣会合 成果文書・議長総括 9項（2023年8月）、G20ニューデリー首脳宣言 55項（2023年9月）

た<sup>5</sup>。2021年6月のG7コーンウォールサミット（議長国：英国）の首脳コミュニケを通じて「信頼性のある自由なデータ流通に関する協力のためのG7ロードマップ」が承認された<sup>6</sup>。このロードマップは、同年4月のG7デジタル・技術大臣会合での成果物<sup>7</sup>であり、2021年Q2からQ4の簡略なロードマップと協力の主要分野を示した。このロードマップに基づき、各国の規制協力のためデータ保護・プライバシー保護機関（以下、DPA）による会合として「G7データ保護・プライバシー機関ラウンドテーブル」（以下、DPAラウンドテーブル）が、2021年9月に、G7議長国である英DPAを議長に開催された。会合の結果、翌年のG7議長国であるドイツのDPAが再びDPAラウンドテーブルを開催することが合意された<sup>8</sup>。2022年6月のG7エルマウサミット（議長国：ドイツ）の首脳コミュニケにおいても、同年5月開催のデジタル大臣会合の成果である「信頼性のある自由なデータ流通の促進のためのG7アクションプラン」<sup>9</sup>が承認され<sup>10</sup>、同年9月にドイツDPAを議長に第2回目のDPAラウンドテーブルが開催され、翌年のG7議長国である日本の個人情報保護委員会が次回DPAラウンドテーブルを開催することとされた<sup>11</sup>。

2022年から2023年にかけて顕在化した生成AIの利用拡大は、デジタル分野におけるエポックメイキングであり、G7における議論にも大きな影響を与え、2023年5月のG7広島サミットの議論を通じて広島AIプロセスの発出に至ったが、G7におけるDFFT具体化に向けた議論も維持された。G7広島サミットの首脳コミュニケでは、2023年4月のG7デジタル・技術大臣会合の成果である「DFFT具体化のためのG7ビジョン及びそのプライオリティに関

する附属書」<sup>12</sup>及びDFFT具体化に向けたパートナーシップのためのアレンジメント（IAP：the Institutional Arrangement for Partnership）の設立<sup>13</sup>が承認された<sup>14</sup>。IAPは、ステークホルダーと関連するデータ保護当局を含め、様々なバックグラウンドを持つデータガバナンスに関する専門家からなるコミュニティを結集することとされ<sup>15</sup>、何らかのコミュニティの設立が想定されている可能性がある。日本は、G7広島サミット後、北欧諸国とDFFT及びIAPに関する意見交換を行い、賛同を得たとしている<sup>16</sup>。また、2023年6月に開催された第3回DPAラウンドテーブルのG7 DPAコミュニケ及びG7 DPA行動計画では、柱の第一にDFFTを挙げ、IAPを支持する方向性を示すとともに、次のG7議長国であるイタリアのDPAが次回DPAラウンドテーブルを開催予定とされ、G7のDPAラウンドテーブルも継続する見込みである。

### 3. DFFTの論点

2021年から2023年のG7デジタル大臣会合におけるDFFTの主たる論点は、①データローカライゼーション、②規制協力、③ガバメントアクセス、④データ共有である。

DFFTは、国境を越えてデータを移転しかつ保護することにより、経済成長とイノベーションを促進する立場である。このため、国境を越えたデータ流通に影響を与える可能性があるデータローカライゼーションへの対応（論点①）、国境を越えたデータ流通に向けた国内の規制アプローチの違いへの対応（論点②）、政府による民主主義的な価値と法の支配に基づく個人データへのアクセス（論点③）に

5 開かれた自由で安全なデジタル化による変革のためのピアリッツ戦略 6項

6 G7カービスベイ首脳コミュニケ 34項

7 2021年G7デジタル・技術大臣会合 大臣宣言 附属書2

8 2021年G7データ保護・プライバシー機関ラウンドテーブル コミュニケ 将来に向けて第1段落

9 2022年G7デジタル大臣会合 大臣宣言 附属書1

10 2022年G7首脳コミュニケ デジタル化第7段落

11 2022年G7データ保護・プライバシー機関ラウンドテーブル コミュニケ 44項

12 2023年G7デジタル・技術大臣会合 閣僚宣言 附属書1

13 2023年G7デジタル・技術大臣会合 閣僚宣言 13項

14 G7広島首脳コミュニケ 39項

15 2023年G7デジタル・技術大臣会合 閣僚宣言 附属書1 2項

16 <https://www.digital.go.jp/news/2ed46224-c0cc-4a1b-be3d-8e25ed7d974a/>

2021年 <sup>1</sup>	2022年 <sup>2</sup>	2023年 <sup>3</sup>
データローカライゼーション ※貿易大臣会合との整合性を考慮	DFFTのための証拠基盤の強化 ※データローカライゼーションを含む デジタル貿易の文脈におけるDFFTの促進	データローカライゼーション
規制協力 ※G7データ保護機関等による会合開催を含む	規制協力の継続	規制協力
ガバメントアクセス	将来の相互運用性促進のための共通性の構築 ※標準契約条項等の分析、ガバメントアクセスを含む	信頼された政府のデータへのアクセス
優先分野のためのデータ共有 優先分野：医療分野等	国際データスペースの展望に関する知識の共有	データ共有 優先分野：ヘルスケア、グリーン/環境、モビリティ

表1. G7デジタル大臣会合におけるDFFTの論点

- 1 G7「信頼に基づくデータの自由な流れに関する協力のためのG7ロードマップ」を参考に作成
- 2 G7「信頼性のある自由なデータ流通の促進のためのG7アクションプラン」を参考に作成
- 3 G7「DFFT具体化のためのG7ビジョン及びそのプライオリティに関する附属書」を参考に作成

取り組むとともに、国際的な共通課題に関するデータ共有を促進しようとしている（論点④）。

論点①については、DFFTは、日本による提案当初より、デジタル貿易の拡大を想定していた。このため、デジタル大臣会合におけるDFFTの議論においても、貿易分野を考慮していると考えられる。実際に、日本とEUは、2022年10月より日・EU経済連携協定に「データの自由な流通」に関する規定を含めることに関する正式交渉を開始した<sup>17</sup>。

論点④データ共有は、COVID-19のパンデミックを通じて、実現の必要性がより明確になったと考えられる。2022年は国際データスペースに言及されたが、この背景には欧州が進めた独自のデータインフラ構築（GAIA-X）があると考えられる。2023年は、データ共有の優先分野としてヘルスケア、グリーン/環境、モビリティを挙げている。この分野において、日本は、電子文書の発行元を証明するトラストサービスであるeシールについて、日本とEUのeIDAS規則に基づくeシール等の国際相互認証に向けた検討を開始している<sup>18</sup>。

#### 4. DFFTにおけるDPAの役割

DFFTは、日本による提案後、G7を中心に協力体制が構築され、具体化に向けた検討が進められてきた。特に、前述の論点のうち、①データローカライゼーション、②規制協力、③ガバメントアクセスについては、G7各国のDPAの協力体制のもとに対応が進められてきたと考えられる。

論点②規制協力については、DPAラウンドテーブルの開催などの協力体制も規制協力の一部であり、また、G7のDPAは、規制協力に向けて、生成AI等の先端技術、プライバシー強化技術（PETs）の検討、OECD等の国際機関との連携に取り組んでいる。

G7のDPAは、2023年のDPAラウンドテーブルを通じて、DFFTの促進に向けて次の事項に取り組んでいる。

##### (1) データ移転ツール

データ移転ツールの相互運用性の促進に向けて、CBPRなどの認証システムやモデル契約状況等の比較分析を行い、2024年にかけても継続するとしている。このようなデータ移転ツールの相互運用性の

17 <https://www.mofa.go.jp/mofaj/files/000415752.pdf>

18 [https://www.soumu.go.jp/menu\\_news/s-news/01cyber01\\_02000001\\_00173.html](https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00173.html)

促進は、論点①データローカライゼーションの対策につながると考えられる。

## (2) ガバメントアクセス

論点③ガバメントアクセスについて、G7のDPAは、「OECDの民間が保有するデータへの政府のアクセスに関する宣言」（2022年12月）を支持した。宣言は、ガバメントアクセスが、各国の法的枠組みにより規制されることや、正当な目的のために実施されること等の原則を示している。

## 5. DFFT促進に向けた課題

DFFT促進に向けた論点の背景には、デジタル経済においても法の支配と民主的価値、人権尊重を重視し、かつ気候変動やパンデミック等のグローバルな課題に対応しようとするG7の姿勢があると考えられる。しかし、DFFT促進に向けては、G7を超えて、諸外国や国際機関の協力が必要であり、具体的な協力体制の拡大は、DFFT促進に向けた課題と考えられる。マルチステークホルダーによるIAP設立は今後の協力体制整備に向けた布石と捉えることもできる。日本は、2023年3月に「自由で開かれたインド太平洋（FOIP）」のための新たなプラン」の取組み例としてDFFT推進のための途上国の法整備・基盤整備等支援を挙げ<sup>19</sup>、2023年9月の日ASEAN包括的連結性イニシアティブにおいても、ASEANへのインフラ整備支援を通じたDFFT推進を掲げている<sup>20</sup>。

アジア太平洋を含むインド太平洋地域との協力関係の構築の在り方は、従来より課題として認識され

てきた。アジア太平洋地域の国と地域の経済協力の枠組みであるAPECが2017年に採択した「APECインターネット・デジタル経済に関するロードマップ（AIDER）」<sup>21</sup>や、2022年5月に米国主導で立ち上げられたインド太平洋14カ国の経済枠組みであるIPEFは、日本が提唱するDFFTと同等の方向性を含むと考えられる。2023年のAPEC（議長国：米国）においても、APEC首脳宣言において、個人情報保護やデジタル貿易等の分野においてAIDERの加速化を推奨する<sup>22</sup>ことが引き続き示され、また、同じタイミングで米国で開催されたIPEF首脳会合では、主要な4つの柱のうち、デジタル貿易を含む貿易分野<sup>23</sup>を除く3分野での成果が示される形<sup>24</sup>となり、データ流通分野のインド太平洋地域との協力関係の構築は途上にあるといえる。

## おわりに

DFFTは、2019年に日本が提唱し、G7、G20を中心に共有され、2023年G7サミットでは、G7に留まらないマルチステークホルダーによるIAPを設立する方向性が示された。この間、デジタル分野においては生成AIの利用拡大を通じた、プライバシー、偽情報、知的財産権の在り方などがグローバルな課題となったが、DFFTは、生成AIを含むデジタル分野の課題検討の基盤となる概念と考えられる。G7のDPAの取組み等を通じたDFFT推進が、今後どのように世界に展開されるのか、引き続き動向を注視したい。

19 <https://www.mofa.go.jp/mofaj/files/100477405.pdf>

20 <https://www.mofa.go.jp/mofaj/files/100548765.pdf>

21 AIDER 8項 [http://mddb.apec.org/Documents/2017/SOM/CSOM/17\\_csom\\_006.pdf](http://mddb.apec.org/Documents/2017/SOM/CSOM/17_csom_006.pdf)

22 2023年APEC首脳宣言「ゴールデンゲート宣言」全ての人々にとって強靱で持続可能な未来を創造 13項

23 IPEF Pillar1 (Trade)

[https://ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text%20\(Trade%20Pillar\)\\_FOR%20PUBLIC%20RELEASE%20\(1\).pdf](https://ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text%20(Trade%20Pillar)_FOR%20PUBLIC%20RELEASE%20(1).pdf)

24 <https://www.mofa.go.jp/mofaj/files/100582858.pdf>

# グローバル化する個人情報の越境移転ツール

一般財団法人日本情報経済社会推進協会 認定個人情報保護団体事務局 事務局長 奥原 早苗

## 1. はじめに

2023年6月に「第3回G7データ保護・プライバシー機関ラウンドテーブル会合」が個人情報保護委員会（以下、PPC）によって開催された。このラウンドテーブルは、個人データの保護を図りつつ、利活用を進めるDFFT（Data Free Flow with Trust）（以下、DFFT）の推進に向けて、G7各国のデータ保護・プライバシー機関の委員長級による議論が行われるものである。DFFT、生成AIを始めとする先端技術及び執行協力の3つの柱<sup>1</sup>に基づいた議論が行われ、データ保護・プライバシーに関するグローバルな共通課題の解決に向けた具体的な方策などが合意された<sup>2</sup>。この方策の内容を示した「G7 DPAコミュニケ」（以下、コミュニケ）では、第1の柱-DFFTにおいて、本稿で取り上げる越境移転ツールについて触れており、越境移転ツールの選択肢を創出することの必要性と、それらを開発することについて、更なる提唱・促進・助言することを目指すとしている。

現在、EUとの間でデータを越境移転する場合は、GDPRに則した対応となるが、数十・数百の国と取引があるグローバルな活動を行っている企業等は、越境移転に莫大なコストや時間、労力等が必要となり、大企業には良いがとりわけ中小企業にとっては経済合理性と相反する状況となっている。世界各国の異なる法域で、データ保護・プライバシーの要件や法制度等を遵守する上で、今後越境移転ツールの新たな開発は重要な役割を果たすことに違いない。

また、コミュニケを具体的に推進するために策定された「G7 DPA行動計画」（以下、行動計画）の「移

転ツール」の項では、「安全かつ信頼性のある移転ツールに関する知識を、とりわけ、グローバル越境プライバシールール（以下、グローバルCBPR）及びEU認証の要件の比較や、既存のモデル契約条項の比較を通じて、共有する。本作業は、異なる認証メカニズムその他の移転ツール間の相互運用性及び収斂の水準を評価し、共通点、考えられる相違点及び更なる改善のための領域をマッピングする。」ことが行動計画の一つとして示された。これまでわが国では、PPCのガイドラインに記載のある<sup>3</sup>APECのCBPRシステムが越境移転ツールとして知られているが、多様な選択肢があるとは言えない中、グローバルCBPRは、コミュニケにあった越境移転ツールの有力な選択肢候補として期待できるものである。具体的には、安全かつ信頼性のある移転ツールに関する知識を共有するために、グローバルCBPR及びEU認証の要件比較や、既存のモデル契約条項の比較等が行われる<sup>4</sup>が、これらが行動計画に明示的に盛り込まれたこと、この新しい越境移転ツールが国際的な枠組みで継続的に議論・推進されること等の意義は大きい。

## 2. APEC CBPRシステム（APEC Cross Border Privacy Rules System）

前項で触れたグローバルCBPRは、3. で後述することとし、グローバルCBPRのベースとなったAPEC CBPRシステム（以下、APEC CBPR）について、主要なポイントを示したい。

### 1) APEC CBPR とは

APECのWebサイトでは、「データプライバシー

1 2022年のラウンドテーブル会合でPPCが提案したもの。

2 PPCの当該Webサイトでは、「G7 DPAコミュニケ」「生成AIに関する声明」「行動計画」の原文と仮訳が掲載されている。

3 外国にある第三者に個人データを提供する場合は本人の同意が必要となるが、PPCが定める基準に適合する体制を整備している者に対して個人データを提供する場合は、本人の同意を得ることなく外国にある第三者へ個人データの提供が可能となる他、詳細は、「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」を参照。

4 認証メカニズムその他の越境移転ツール間の相互運用性等を評価し、改善のための領域をマッピングする。

の協力に対するAPECの革新的なアプローチが、個人データを保護し、貿易を促進して消費者と企業に利益をもたらす方法であり、政府が支援するデータプライバシー認証である。』<sup>5</sup>と説明されており、認証を取得する企業には、APECプライバシーフレームワークへの適合が求められ、適合しているかどうかは説明責任代理人（アカウントビリティ・エージェント（以下、AA）<sup>6</sup>と呼ばれる各国の認証審査機関によって、APEC CBPRのプログラム要件に準拠していると評価される必要があり、各国法によって執行可能でなければならない。

APEC CBPRに関する枠組みに参加する国・地域（以下、エコノミー<sup>7</sup>）の状況を取りまとめたものは図表1の通りで、APECプライバシーフレームワークは21すべてのエコノミーが参加しているが、越境執行協力協定（以下、CPEA）に参加するエコノミーは11にとどまる。そのうち、9エコノミーがAPEC CBPRに参加を表明し、AAを擁するエコノミーにおいてのみ認証を受けることができる。

APEC (アジア太平洋経済協力) の取組み		JIPDEC
■ APECプライバシーフレームワーク (2004年10月採択)	21エコノミー	
<ul style="list-style-type: none"> <li>オーストラリア、ブルネイ、カナダ、チリ、中国、香港、インドネシア、日本、韓国、マレーシア、メキシコ、ニュージーランド、パプアニューギニア、ペルー、フィリピン、ロシア、シンガポール、台湾、タイ、米、ベトナム</li> </ul>		
■ CPEA (越境執行協力協定)	2009年11月	11エコノミー
<ul style="list-style-type: none"> <li>エコノミー内での情報の取得と管理について、国内の法規や指針を対象に参加国で対応</li> <li>米国、日本、韓国、シンガポール、カナダ、メキシコ、豪州、台湾、フィリピン、ニュージーランド、香港</li> </ul>		
■ CBPR (越境プライバシールールシステム)	2011年11月	9エコノミー
<ul style="list-style-type: none"> <li>運用するための仕組みとしてのCBPRシステム (APEC越境プライバシールールシステム、APEC Cross Border Privacy Rules System)</li> <li>米国、日本、韓国、シンガポール、カナダ、台湾、フィリピン、豪州、メキシコ</li> </ul>		
		
■ AA (アカウントビリティ・エージェント)	5エコノミー	(2021年12月時点)
米国、日本、韓国、シンガポール、台湾		

図表1. APEC (アジア太平洋経済協力) の取組み

2023年10月時点で、AAの認定があるのは米国・シンガポール・韓国・台湾・日本の5エコノミーとなっており、それぞれのAAが認証するCBPRの認証企業数は71社（図表2参照）で、グループ認証<sup>8</sup>を含めると1,800社を超える。

国名	AA名	AA認定	CBPR認証取得事業者数	PRP認証取得事業者数
米国	TrustArc	2013年	37	29
米国	Schellman	2019年	1	9
米国	NCC Group	2020年	4	4
米国	HiTrust	2020年	-	-
米国	BBB National Programs	2019年	6	4
シンガポール	IMDA	2019年	11	5
韓国	KISA	2019年	8	-
台湾	III	2021年	-	-
日本	JIPDEC	2016年	4	-
合計			71社	51社

<http://cbprs.org/compliance-directory/cbpr-system/> <http://cbprs.org/compliance-directory/prp/>

図表2. APEC CBPR 各国AA別CBPR、PRP認証事業者数 (2023年10月末時点)

## 2) 日本の参加

わが国は2014年からこの制度に参加しており、わが国初のAAとしてJIPDECが2016年1月に認定を受け、2016年12月に初めてAPEC CBPRの認証付与を行った。2023年10月末時点で、APEC CBPRの認証を取得している事業者は4社である（図表3）。

会社名等	主な事業内容	初回認証日	認証番号
1 インタセクト・コミュニケーションズ株式会社	インバウンド事業等	2016年12月	JP01-00001-07
2 株式会社Paidy	後払い決済サービスの提供等	2018年12月	JP01-00003-05
3 株式会社インターネットイニシアティブ	IT運用支援等	2022年9月	JP01-00005-02
4 PayPay株式会社	電子決済サービスの開発・提供等	2022年12月	JP01-00006-01

図表3. APEC CBPR認証取得事業者 (JIPDEC)

## 3) CBPR 認証と PRP 認証

図表2に示すCBPR認証とPRP認証の違いは、個人情報取得や利用の管理者（コントローラー）か処理者（プロセッサー）かによるものである。米国やシンガポールでは、当該国に所在する親会社がコントローラーとなるため、グループ会社は法人として当該国に登録されていても処理者となり、CBPRの認証を申請することができない。また、SaaS等のサービスを展開する事業者は、処理者としてPRPの認証を受けている。現在、わが国では日本の個人情報保護法上、管理者と処理者の区分がなく、“個

5 「APEC CBPRs」 <https://cbprs.org/> APEC CBPRの概要の他、認証された企業情報を公開している。

6 当該国の政府機関、APEC JOP監視パネル並びに全APECエコノミーの同意を得て認証される。

7 主権国家として承認されていない地域も参加しているため、参加国・地域を表す場合は「エコノミー」と称される。

8 AAの認定がある5エコノミーのうち、米国とシンガポールのみが実施している。



人情報取扱事業者”となるため、日本国内で法人登記がなされている場合、親会社やグループ会社を問わず、個社単位でCBPRの認証取得を行うことはできるが、PRPの認証を行うことはできない。ただし、わが国では処理者としてのサービスを提供するグローバル企業も少なくない。今後、事業者のニーズが高まれば、PRP認証に向けて個人情報保護法上の新たなメリットが創出される可能性も否定できない。

### 3. グローバルCBPR

1. 項で、世界的な枠組みで推進されることとなった越境移転ツールの創出や開発に向けて、グローバルCBPRとEU認証の要件の比較が具体的な行動の一つに挙げられていることを確認した。また、現在わが国が参加し、JIPDECがAAとなっている個人情報の越境移転ツールとして、APEC CBPRを2. 項で紹介した。本項では、APEC CBPRをベースとして策定され、今後注目が集まるであろうグローバルCBPRについて概観する。

#### 1) グローバル CBPR フォーラム

グローバルCBPRを運営するグローバルCBPRフォーラム<sup>9</sup>は、APEC CBPRに参加している現在の経済圏であるカナダ、日本、韓国、フィリピン、シンガポール、チャイニーズタイペイ及び米国によって2022年4月21日に設立された。わが国は、経済産業省とPPCが設立当日同時に、「我が国を含むAPEC CBPR参加エコノミーの連名で、より広範囲での個人データの円滑な越境移転や各国における規律の相互運用性を促進させる等の目的で、CBPRの拡大に向けた宣言をすることに合意しました。」という内容を公表した<sup>10</sup>。グローバルCBPRフォーラムのサイトでは、各種資料が公開され、認証制度の開始に向けた準備が進められている。2023年10月16日にはAPEC CBPRのCPEAに当たるCAPE (The Global Cooperation Arrangement for Privacy Enforcement) が公開された。ここでは宣言内容のみを掲載する。

#### 2) 設立宣言

宣言された内容は以下の通り。

1. 相互運用性を促進し、データ保護及びプライバシーに関する様々な規制アプローチを橋渡しするために、グローバルCBPRフォーラムを設立する。
2. グローバルCBPRフォーラムの目的は、
  - a. APEC CBPRシステム及び処理者向けプライバシー認証 (PRP) システムをベースとした、国際的な認証システムを設立すること
  - b. グローバルCBPRシステム及びPRPシステムを通じて、データの自由な流通と効果的なデータ保護及びプライバシーを支えること
  - c. グローバルCBPRシステム及びPRPシステムに関する事案について情報交換及び連携のためのフォーラムを提供すること
  - d. ベストプラクティスに沿ったグローバルCBPRやPRPプログラム要件を確保するためにメンバーのデータ保護及びプライバシーの水準を定期的にレビューすること
  - e. 他のデータ保護及びプライバシー枠組みとの相互運用性を促進すること

〈活動の範囲〉

3. グローバルCBPRフォーラムは、
  - a. データ保護と自由なデータ流通を促進するためにグローバルCBPRシステム及びPRPシステムの認証取得を世界的に促進する
  - b. データ保護及びプライバシーと相互運用性に関するベストプラクティスを広める
  - c. 他のデータ保護及びプライバシー枠組みとの相互運用性を追求する

〈運用〉

4. 連携は、以下に基づく。
  - a. すべてのメンバーの意見を公平に尊重した、相互利益主義及び開かれた対話と合意形成へのコミットメント
  - b. メンバーや関係機関が実施する調査、分析、政策に基づくメンバー間のコンサルテーション

<sup>9</sup> <https://www.globalcbpr.org/>

<sup>10</sup> 「経済産業省」Webサイト <https://www.meti.go.jp/press/2022/04/20220421001/20220421001.html>  
「PPC」Webサイト [https://www.ppc.go.jp/files/pdf/220421\\_houdou.pdf](https://www.ppc.go.jp/files/pdf/220421_houdou.pdf)

ン及び意見交換

c. 適切な活動における活発なマルチステークホルダーによる積極的な参画

〈参加〉

5. 基本的にグローバルCBPRフォーラムは、本宣言文に謳われる組織の目的と原則を承諾する以下の領域に開かれることを意図している。

6. 将来の組織への参加に関する決定は、全メンバーの合意に基づいてなされるものとする。

7. メンバーではない者は、全メンバーによって決定される条件に基づいて、会合に参加することができる。

〈組織〉

8. グローバルCBPRフォーラムの会合は少なくとも1年に2回開催され、本宣言文の範囲内の活動の方針や性質を決定する。会合は対面あるいはオンラインで開催される。

9. 全メンバーの決定に基づいて、追加の会合を開催することができる。

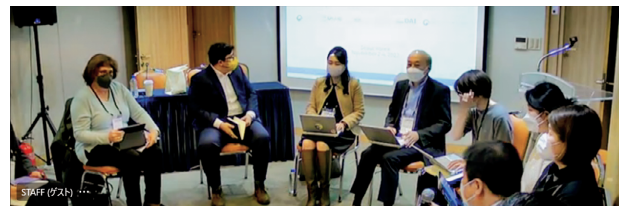
わが国も〈組織〉8.で規定するグローバルCBPRフォーラムの会合に参加し、JIPDECも日本のAPEC CBPRのAAとして参加し、新しい枠組みの開始に備えて準備中である。2022年4月に宣言されてから、直近の2023年10月25日～27日に米国サンディエゴで開催されたものまで、4回の会合が年に2回開催されている。参加者は毎回100名程度で（第1回～第3回はオンライン参加も含む）、3日間に亘り開催される。

- ・第1回：2022.4 米国 ホノルル  
「The Global Cooperation on Data Privacy & CBPR System: The Path Forward Workshop」
- ・第2回：2022.11 韓国 ソウル  
「Global CBPR Forum: Realizing Our Shared Vision」
- ・第3回：2023.4 英国 ロンドン  
「The Global CBPR Forum At One Year: Challenges and Opportunities」
- ・第4回：2023.10 米国 サンディエゴ  
「Global CBPR Forum: CBPR2.0」

## 第2回会合：2022.11 韓国 ソウル



出所：米国商務省Shannon Coe氏 SNSサイトより（集合写真）



### 3日目AA連携にて

出所：グローバルCBPRフォーラム提供（中央 JIPDEC奥原）

## 第3回会合：2023.4 英国 ロンドン



出所：グローバルCBPRフォーラム提供（集合写真）

2023年4月13日に、グローバルCBPRフォーラムは「Global CBPR Framework」及びフォーラムの「Terms of Reference」を公開し、関心のある世界の国・地域の参加を歓迎するリリースを行った。第3回会合開催の前夜、2023年4月17日に英国外務省で行われたイブニングレセプションで、英国政府関



### 初日セッション1：CBPR・PRPの機会と課題

出所：JIPDEC職員撮影（左端 JIPDEC奥原）

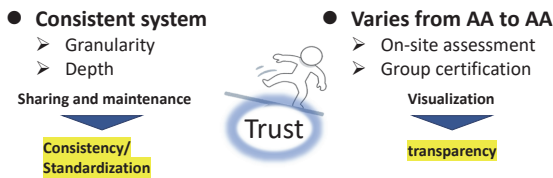
係者より準会員としてグローバルCBPRフォーラムに参加の意向である旨が宣言された。

第3回会合が開催されたロンドンでは、AAの立場から米国AAのTrustArc ノエル・ルーク氏（左から2人目）と共にCBPRへの参加を検討する事業者に向けたパネルに参加し、JIPDECはAPEC CBPR上の課題を「本来目指すべき認証制度とは？」を問題意識として講演を行った（資料1）。

1)-1 Method of Assessment



Do we understand how AAs in each country review against the CBPR program requirements and can we raise issue appropriately?



(資料1)

各国の審査機関における審査内容の粒度や審査員の要件の差異等に対し、一貫性と透明性の確保が制度の信頼性向上に重要であるという主旨で、BCRとの比較検証や審査の標準化、審査員の資格要件等の導入による一貫性確保を提案した。また、現地審査やグループ認証等、AAにより導入状況が異なるものは、可視化による透明性の担保が有効であること、年2回の会合間に定期的なミーティングを導入すること等を提案し、第4回会合までの間に進捗状況他の共有がなされた。

第4回：2023.10 米国 サンディエゴ

このパネルは、初日のセッションで政府関係者・規制当局向けに「政府と規制当局にとってのCBPRとPRP制度の利点と機会」をテーマに開催され、米国商務省のサラ氏をモデレーターとして、各国規制当局からシンガポール、フィリピン、英国の政府機関関係者が登壇し、AAの代表として日本からJIPDECがパネルに参加した。CBPRは消費者苦情の対応を審査機関、政府機関が共に対応窓口となっている消費者保護に手厚いユニークな制度であること、規制当局と審査機関との良好な協力体制が、CBPR制度



出所：グローバルCBPRフォーラム（集合写真）



出所：グローバルCBPRフォーラム（GCBPR総会議長 米国商務省 Shannon Coe氏）

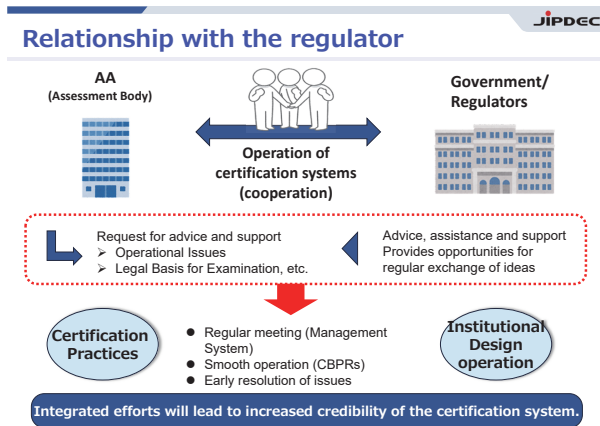


出所：グローバルCBPRフォーラム（演台 JIPDEC 奥原）

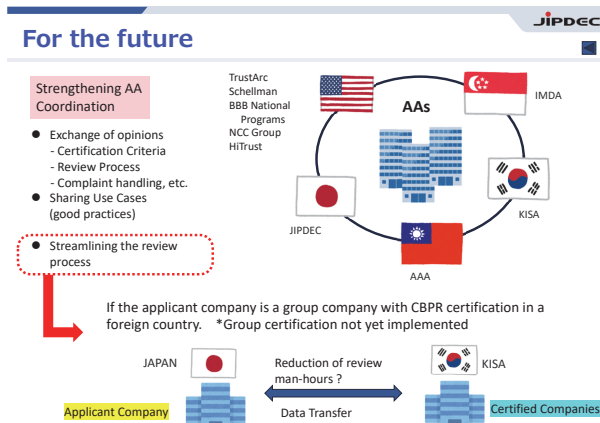
の円滑な運用につながることで、その結果認証制度に対する社会や事業者からの信頼性向上につながる等を説明した（資料2）。例えば、わが国の場合は、定期的な意見交換や認証制度の運用における実務上の課題や法解釈等について、規制当局より助言・サポートを得て認証を付与する事業者への正確かつ納得感のある丁寧な説明を行っている。

なお、今後に向けては、事業者からみたグローバルCBPRの認証取得におけるメリットの創出について触れている。現在、APEC CBPRでグループ認証を行っているのは、米国とシンガポールの審査機関のみであり、わが国では法的な執行の仕組みがないため、実施していないが、事業者からのニーズは少なくない。特に、処理者（プロセッサー）としての業務を実施する企業からは、PRP認証が実施されることを期待しているという声が聞かれる。グループ認証やPRP認証の導入検討以外に、グループ認証を

導入しておらず、個社単位で審査を行っている日本と韓国を例に挙げれば、もしデータの移転先がCBPR認証を取得している場合、認証を取得していない企業と比較し、審査工数の軽減等が実施できないか、審査の効率化を検討する余地もあるのではないかということを提起した（資料3）。



(資料2)



(資料3)

#### 4. おわりに

本稿では、今後注目が高まるであろう個人情報の越境移転ツールについて、グローバルCBPRを中心とした内容を取り上げた。現在、APEC CBPRに参加するエコノミーのうち、自国の個人情報の保護に関する法律に紐づくメリットがあるのは日本とシンガポールのみであり、国際会議の場では事業者が認証制度を取得する動機付けとして有益である事例としてたびたび取り上げられる。しかし、現状は果た

してそれほど有効に機能しているだろうか。グローバルCBPRの会合では、政府機関関係者及び参加企業共に、APEC CBPRの拡大が限定的なのは認証制度の知名度が低いことが原因の一つとして挙げており、わが国でもAPEC CBPRの認知度は決して高いとは言えない。

越境移転ツールを利用しなくてもデータの越境移転は可能だが、企業の個人情報の取扱いに対して第三者の視点を導入することは、例えばグローバルCBPRフォーラムの会合でも、企業の説明責任を果たすと共にデューデリジェンスとしても機能することやグローバルな規模で企業の信頼の証になること、とりわけ中小企業にとっては規制コストの削減につながる等をメリットとして挙げる声が、規制当局及び参加企業を問わず共通して聞かれた。また、AAの存在は事業者間の情報の取扱いに係る紛争を軽減する意味で政府をサポートする役割もあると述べていたAAもあった。

日本政府が参加を表明したグローバルCBPRは、個人情報保護法上でもAPEC CBPRと同様のメリットが受けられると想定され、対象とする国・地域も制限を設けていないことから今後も英国のみならず、APEC域外の幅広い国・地域の参加が期待される。繰り返しとなるが、冒頭で触れた第3回G7データ保護・プライバシー機関ラウンドテーブル会合で、DFFTを推進するための具体的な議論の中にグローバルCBPRが取り上げられたため、本格的にグローバルCBPRの制度運用が開始されれば、企業にとって越境移転ツールの選択肢が広がる第一歩となる。政府が支援する越境移転の認証制度として、JIPDECは日本のAAとして政府機関と協力しながらこれまで以上に普及啓発活動を推進する。その結果、企業が個人情報の越境移転を行う上で、APEC CBPRやグローバルCBPR等の認証を取得することが企業の信頼の証となることや、異なる法域への対応コストの削減につながる一助になれば幸いである。

# メタバースと個人情報やプライバシーについて

一般財団法人日本情報経済社会推進協会 電子情報活用研究部 野町 綺乃

## 1. はじめに

2007年のセカンドライフが登場した際に、メタバースというワードが一定数検索され、2021年秋ごろ、Facebook社が社名をMeta社に変更するということから、以前よりGoogle Trendsでの検索数が急上昇し、話題となった。

「メタバース」とは、ギリシャ語で“超越した”、“より高次の”という意味を持つ「メタ (meta)」と“世界”、“宇宙”を意味する「ユニバース (Universe)」を組み合わせて作られた言葉で、1992年に発表されたニール・スティーヴンズのSF小説『スノウ・クラッシュ』の作品内で、「インターネット上の仮想空間 (情報によって構築されたサイバー空間)」として扱われたものがメタバースの始まりと考えられている<sup>1</sup>。

メタバースについては明確に定義されていないが、一般的には、「VRなどを利用し、没入感がある仮想空間において、ユーザーが物理的な制約を受けることなく、現実世界に近い体験、すなわち、アバターなどのアイデンティティを起点として、他のユーザーとコミュニケーション、コンテンツ制作、売買などの経済活動ができるもの<sup>2</sup>」を指すと考えられている。

近年、社会全般において、個人情報やプライバ

シーへの関心が高まっていることから、今回は、メタバースにおける個人情報やプライバシーに関する問題として、アバターやメタバース上で収集される情報 (行動履歴) の取扱いについて取り上げる。

## 2. アバターについて

メタバースにおける「アバター」の取扱いについて考えていく。

個人情報保護法における「個人情報」とは、生存する「個人に関する情報」であって、「当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの (他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。)」又は「個人識別符号が含まれるもの」<sup>3</sup>と定められている。

メタバースにおける「アバター」とは、「ゲームやネット上で動かすキャラクター<sup>4</sup>」である場合だけでなく、「自己の分身として、顔のパーツ (例：目、鼻、髪型、肌色) や身体の形状、あるいは服装のデザインなど、極めて詳細に設定・調整されたもの<sup>5</sup>」である場合もある。

アバターを自己の分身として、「個人」を忠実に再現する場合や「個人」を忠実に再現していない場合でも、他の情報と容易に照合することができ、そ

1 國光宏尚, 2022年, 『メタバースとWeb3』, 東京: 株式会社エムディエヌコーポレーション、成原慧, 2022年, 「特集論文 メタバースのアーキテクチャと法—世界創造のプラットフォームとそのガバナンス—」『Nexcom Vol.52 2022 Winter』、AMTメタバース法務研究会, 2022, 「(第1回総論—メタバースと法)」, 『NBL』, No.1223、三宅陽一郎, 2022年6月, 「[メタバースがやってきた] 2. メタバースの成立と未来—新しい時間と空間の獲得へ向けて—」『情報処理』, Vol.63 No.7他

2 西村あさひ法律事務所, 「メタバースにおける法律と論点 (上)」, 2022年4月15日, P.1  
<https://www.nishimura.com/ja/knowledge/newsletters/20220415-34251>

3 個人情報保護委員会, 「個人情報の保護に関する法律についてのガイドライン (通則編)」, 2016年11月 (2022年9月一部改正), P.5  
[https://www.ppc.go.jp/personalinfo/legal/guidelines\\_tsusoku/](https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/)

4 一般社団法人日本デジタル空間経済連盟, 「デジタル空間の経済発展に向けた報告書」, 2022年11月16日, P.39  
[https://jdsef.or.jp/assets/document/achievement/report\\_20221116.pdf](https://jdsef.or.jp/assets/document/achievement/report_20221116.pdf)

5 上野達弘, 2022, 「メタバースをめぐる知的財産法上の課題」, 『Nextcom』, Vol.52, P.11

の情報を参照して、特定の個人を識別することができるものを含む場合<sup>6</sup>には、個人情報に該当し、個人情報保護法を遵守することが必要となる。

他方で、アバターが「個人」を忠実に再現しておらず、他の情報と容易に照合することができず、特定の個人を識別することができない場合には、「個人情報」には該当しないと考えられる<sup>7</sup>。ただし「個人情報」には該当しない場合であっても、ユーザー本人のプライバシーへの配慮の観点から、個人情報を取り扱う場合と同程度の保護措置を講ずることが望ましい<sup>8</sup>と考えられる。

### 3. メタバース上で収集される情報（行動履歴）について

「メタバース上で収集される情報（行動履歴）」の取扱いについて考えていく。

メタバースでは、メタバース内に一度入ってしまうと、利用者の行動に関するデータが収集・記録できる。

ユーザーがアイトラック・フェイストラック・フルトラックなどを利用している場合には、人の視線・表情・体の動作などの動きのデータを収集することもできる<sup>9</sup>。

メタバース上では、既存のインターネットサービスよりも、より多くのパーソナルデータを収集することが可能である<sup>10</sup>と考えられているため、プライバシー侵害のリスクの程度も大きくなる<sup>11</sup>と考えられる。

また、プラットフォームは利用者の行動に関す

るデータを活用することにより、ユーザーに対するパーソナライズされたサービス提供や提案、ビッグデータとして利活用することなどが想定される。

ユーザーのIDや登録情報に、メタバース空間上でのアバターやその行動などに関する記録が紐づけられている場合など、特定の個人を識別することができる場合には、行動履歴なども含めて個人情報に該当するため、個人情報保護法を遵守することが求められる。

他方で、ユーザーのIDと登録情報、メタバース空間上でのアバターやその行動などに関する記録が紐づけられていない場合（行動履歴単体）など、個人情報に該当しないデータを収集する場合でもプライバシー配慮の観点から、ユーザーが、「データを勝手に取得・蓄積し、利用されている」と感じてしまわないよう、利用目的の特定、本人への通知・公表、同意の取得などを丁寧に行う必要があると考えられる。

メタバースを通じて取得し、利活用する情報をプラットフォーム自らが制限し、当該情報の取扱いについてはその管理方針や管理方法についてのプロセスを公表する等して、透明性を確保することが望ましい<sup>12</sup>と考えられている。

さらに、透明性確保に加えて、ユーザー自身がメタバースを通じてプラットフォームに取得される情報の対象や利活用の方法をコントロールできるような仕組みを導入することも望ましい<sup>13</sup>と考えられている。

今後、メタバース内で様々な活動が行われていき、メタバース内で生活する人々も増えていくこと

6 他の情報と容易に照合することができ、その情報を参照して、特定の個人を識別することができるものを含む場合というのは、メタバースのサービス上、ユーザー登録をする際に、氏名や住所などの個人情報を登録し、利用者IDやパスワードの付与を受けることとされている場合に、当該利用者IDその他の登録情報と、メタバース空間上でのアバターやその行動などに関する記録との紐づけが容易に可能であるということを指している。

7 なお、この場合に、個人情報保護法上の「個人関連情報」に該当する可能性があり、その場合に、「個人関連情報」の取扱いに関する規律が及ぶ可能性があることには注意が必要である。

8 PWC, 「企業のためのメタバースビジネスインサイト 法の観点から見るメタバース 個人情報の取り扱い編」2023年5月9日 <https://www.pwc.com/jp/ja/knowledge/column/metaverse/vol31.html>

9 西村あさひ法律事務所, 「メタバースにおける法律と論点（下）」, 2022年5月9日, P.5 <https://www.nishimura.com/ja/knowledge/newsletters/20220509-80296>

10 西村あさひ法律事務所, 「メタバースにおける法律と論点（下）」, 2022年5月9日, P.5

11 西村あさひ法律事務所, 「メタバースにおける法律と論点（下）」, 2022年5月9日, P.5

12 バーチャルシティコンソーシアム「バーチャルシティガイドライン Ver2.0.0」, 2023年7月20日, P.37 <https://shibuya5g.org/research/docs/guideline.pdf>

13 バーチャルシティコンソーシアム「バーチャルシティガイドライン Ver2.0.0」, 2023年7月20日, P.37 <https://shibuya5g.org/research/docs/guideline.pdf>

から、既存のインターネットサービス以上に、データや情報などのプライバシーの保護は重要である<sup>14</sup>と考えられている。

#### 4. おわりに

---

今回は、メタバースにおける個人情報やプライバシーに関する問題について取り上げたが、メタバー

スはゲームに限らず、SNSといったコミュニケーションツールや、エンターテインメント、オフィス、学校・教育、医療、観光など様々な分野で活用されつつある。

そのため、メタバースを利用する分野ごとやコンテンツごとにも、個別の状況を踏まえて、具体的な検討を行い、プライバシー侵害が起こらないように、丁寧に進める必要があると考える。

---

14 バーチャルシティコンソーシアム「バーチャルシティガイドライン Ver2.0.0」, 2023年7月20日, P.37

## AIガバナンスに係る国内外の動き

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 主幹 恩田 さくら

2022年11月、米国のOpenAI社が、ChatGPTの提供を開始した。GoogleやMicrosoftをはじめとする米国の大手IT企業も大規模言語モデル（LLM）の開発・提供を進めている。生成AIの利用者は急増しており、文章、画像、音声、音楽、動画、プログラムコード等を生成する生成AIが多くの人に広く利用されることで、生活やビジネスにおけるイノベーションの期待が高まっている一方で、偽情報、プライバシー、著作権、公平性等の課題も、改めて認識されている<sup>1</sup>。

AIをめぐる政策的な議論は2015年頃から始まったといわれ、2016年のG7情報通信大臣会合（高松）にて日本からAIの開発原則の議論を提案し、2019年5月にOECDで合意されたAI原則が公開され、同年6月のG20首脳会合で、AI原則を首脳宣言の付属文書として、G20AI原則が合意された<sup>2</sup>。このように当時AI原則については概ねコンセンサスが形成されつつあり、AI原則を社会に実装するための具体的な制度や規律の策定についての議論に移行してきていたが、2022年の生成AIの登場により、各国においても、G7等の国際協調の場においても、AIガバナンスの議論が加速している。

2023年4月のG7デジタル・技術大臣会合（高崎）では、G7メンバーの間で異なる場合のある、AIガバナンスの枠組み間の相互運用性の重要性が確認され、5月に開催されたG7広島サミット首脳宣言においては、包摂的なAIガバナンス及び相互運用性に関

する国際的な議論を進めることとなり、広島AIプロセスが創設された。同年10月には、広島AIプロセスに関し、まずは、開発者を対象とした行動規範と指針について、G7首脳声明が発出された<sup>3</sup>。AIの利用者や事業者向けのルールは、別途2023年中にまとめられる予定である。

各国のレベルで、AIに関する具体的な制度や規律の策定も進んでいる<sup>4</sup>。欧州においては、AI法案について、2023年6月に欧州議会が修正案を採択し、今後早期の法の公布と施行を目指し調整を行う方向とされている。リスクベースアプローチで、許容できないリスクをもつAIシステム（個人の意思決定を歪ませるAI、公的機関によるソーシャルスコアリング、法執行を目的とした公にアクセスできる場所でのリアルタイム遠隔生体識別システムの利用等）は原則禁止、ハイリスクなAIとされるものには、データベース登録、適合性評価等、厳格な要件が課せられる。米国においては、2023年7月に、AI開発で先行する米国企業7社（OpenAI、Google、Microsoft、Meta等）がAIの安全な開発のための自主的な取組みを約束したこと、9月にはさらに8社（Amazon、Adobe等）が新たにそれに参加することを米国政府が発表した。10月30日には、バイデン大統領が、AIに関して、新たな安全性評価、公平性と公民権に関するガイダンス、AIが労働市場に与える影響に関する調査を義務付ける大統領令を発表した<sup>5</sup>。英国は、2023年11月1日～2日に、世界28カ国がAIの安

- 1 「AIに関する暫定的な論点整理」（AI戦略会議、2023年5月、[https://www8.cao.go.jp/cstp/ai/ronten\\_honbun.pdf](https://www8.cao.go.jp/cstp/ai/ronten_honbun.pdf)）、  
「AIの責任ある展開に向けて 広島AIプロセスへの政策提言」（東京大学未来ビジョン研究センター 技術ガバナンス研究ユニット、2023年9月、<https://ifi.u-tokyo.ac.jp/news/16642/>）
- 2 「我が国のAIガバナンスの在り方 ver.1.1」  
（経済産業省、2021年3月、[https://www.meti.go.jp/shingikai/mono\\_info\\_service/ai\\_shakai\\_jisso/pdf/20210709\\_1.pdf](https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_1.pdf)）
- 3 「広島AIプロセスに関するG7首脳声明」（2023年10月、[https://www.mofa.go.jp/mofaj/ecm/ec/page5\\_000483.html](https://www.mofa.go.jp/mofaj/ecm/ec/page5_000483.html)）
- 4 詳細は以下のレポートも参照いただきたい。  
「AIに関する国際的なルールメイキングと生成AIのインパクト（1）欧米における議論の動向」（JIPDEC、2023年9月、<https://www.jipdec.or.jp/library/report/20230925.html>）  
「AIに関する国際的なルールメイキングと生成AIのインパクト（2）広島AIプロセス及び国際動向」（JIPDEC、2023年10月、<https://www.jipdec.or.jp/library/report/20231012.html>）
- 5 「バイデン米政権、AIの安全性に関する新基準などの大統領令公表」（JETRO、2023年11月、<https://www.jetro.go.jp/biznews/2023/11/495833ae70119dbf.html>）



全性を議論する国際会議「AI安全サミット」を英国で開催し、報道によれば、AIの安全性を政府の研究機関で事前検証することなどが議論されたという。このように、AIガバナンスをめぐる各国の取り組みや議論は、日々更新されている状況である。

日本においては、2019年に「AI利活用ガイドライン」<sup>6</sup>「人間中心のAI社会原則」<sup>7</sup>、2021年に「AI原則実践のためのガバナンス・ガイドライン」(2022年に改訂)<sup>8</sup>等が制定されてきた。2023年、政府はAI戦略会議を設置し5月に初会合を開催し、6月に「AIに関する暫定的な論点整理」<sup>9</sup>を公表するとともに、各省庁のガイドラインの統合に向けた作業を進めることとされ、9月には同会議にて「新AI事業者ガイドライン スケルトン(案)」が示された<sup>10</sup>。原稿執筆点(2023年11月)では、政府で検討が進められているところであり、公表が待たれる。

個人情報保護の観点では、2023年6月には、個人情報保護委員会が、「生成AIサービスの利用に関する注意喚起等」を発出した<sup>11</sup>。生成AIに個人情報を含むプロンプトを入力する場合には、特定された利

用目的を達成するために必要な範囲かを十分確認することや、特に、入力する情報が、生成AIサービスの提供者において、AIの学習データとして利用されることが予定されている場合には、あらかじめ本人同意を得ることなく個人データを含むプロンプトを入力してしまうと、個人情報保護法の規定に違反することとなる可能性があることが注意喚起されている。

今回は生成AIに係る制度・規律の議論の状況を中心に記載したが、制度・規律の議論・検討状況や関係省庁からの注意喚起等の情報と併せて、実務においては生成AIやLLM自体の技術革新、提供されるサービス自体のアップデートの状況等も注視していくこととなる。業界団体、関連する協議会、商工会議所などから、生成AIの利活用を進める際のポイントや注意事項等、実務で参照できる内容が公表されているものもある。こういった成果物を活用することや、場合によっては団体活動への参画なども、利活用を進める企業にとって有益であると考えられる<sup>12</sup>。

- 
- 6 「AI利活用ガイドライン～AI利活用のためのプラクティカルリファレンス～」(AIネットワーク社会推進会議、2019年8月、[https://www.soumu.go.jp/menu\\_news/s-news/01iicp01\\_02000081.html](https://www.soumu.go.jp/menu_news/s-news/01iicp01_02000081.html))
- 7 「人間中心のAI社会原則」(統合イノベーション戦略推進会議、2019年3月、<https://www8.cao.go.jp/cstp/aigensoku.pdf>)
- 8 「AI原則実践のためのガバナンス・ガイドライン ver.1.1」(経済産業省、2022年1月、[https://www.meti.go.jp/shingikai/mono\\_info\\_service/ai\\_shakai\\_jisso/20220128\\_report.html](https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20220128_report.html))
- 9 「AIに関する暫定的な論点整理」(AI戦略会議、2023年5月、[https://www8.cao.go.jp/cstp/ai/ronten\\_honbun.pdf](https://www8.cao.go.jp/cstp/ai/ronten_honbun.pdf))
- 10 AI戦略会議 第5回 議事次第・配布資料(2023年9月、[https://www8.cao.go.jp/cstp/ai/ai\\_senryaku/5kai/5kai.html](https://www8.cao.go.jp/cstp/ai/ai_senryaku/5kai/5kai.html))
- 11 「生成AIサービスの利用に関する注意喚起等について」(個人情報保護委員会、2023年6月、[https://www.ppc.go.jp/news/careful\\_information/230602\\_AI\\_utilize\\_alert/](https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/))リーフレット「生成AIサービスの利用に関する注意喚起」(個人情報保護委員会、[https://www.ppc.go.jp/files/pdf/generativeAI\\_notice\\_leaflet2023.pdf](https://www.ppc.go.jp/files/pdf/generativeAI_notice_leaflet2023.pdf))
- 12 日本ディープラーニング協会からは、生成AIの活用を考える組織の円滑な導入のために利用ガイドラインのひな形が公表されている(<https://www.jdla.org/document/#ai-guideline>)。2023年10月には、AIガバナンスをめぐるマルチステークホルダーでの議論の必要性を受けて、有志企業で構成されるAIガバナンス協会が設立された(<https://www.ai-governance.jp/>)。また、東京商工会議所からは「中小企業のための『生成AI』活用入門ガイド」が公表されており、2023年10月31日には第2版が公表されている(<https://www.tokyo-cci.or.jp/page.jsp?id=1201389>)。

## プライバシーマーク25周年 記念表彰式



プライバシーマーク制度は、2023年4月に制度創設25周年を迎えました。25周年という節目に、これまでの制度運営にご尽力いただいた関係者の皆さまをお迎えして開催した記念表彰式の模様をご紹介します。



表彰式の様子：品川プリンスホテル

表彰式では、プライバシーマーク付与事業者、指定審査機関から約100名の来賓の皆さまにご臨席いただきました。

冒頭、会長 杉山より、「プライバシーマーク制度が25周年を迎えることができたのも、ひとえに事業者、審査・研修機関、審査員の皆さまのご尽力によるものです。制度発足当初はまだ認知



JIPDEC会長 杉山 秀二

度が低かったものの、初期に付与された事業者の皆さまの個人情報保護に対する高いご見識とご協力が心強く、また当協会の原動力となっております。今後のプライバシーマーク制度の姿を見据えるための貴重なこの機会に、忌憚なきご意見を賜り、30周年、50周年が迎えらるよう尽力してまいります」と挨拶をしました。

続いて、記念講演としてプライバシーマーク制度

創設に当たり多大なるご尽力をいただき、1998年から2014年1月に特定個人情報保護委員会委員長に就任されるまでプライバシーマーク制度委員会委員長を務めていただいた堀部政男氏に「JIPDECプライバシーマーク創設25周年を迎えて、さらなる発展を目指して」と題しご講演いただきました。なお、講演の様子は記念講演レポートとしてとりまとめ、本誌で紹介しています。

その後、これまでの制度運営にご尽力いただいた関係者の皆さまへの感謝の意を表し、杉山よりプライバシーマーク付与事業者、指定審査機関、指定研修機関、審査員の各代表の方に記念品を贈呈しました。2社のプライバシーマーク付与事業者の方をはじめ、ご登壇の皆さまには、日頃のご苦労や工夫、今後の課題などのご挨拶を賜り、また、プライバシーマーク制度への心強い激励のメッセージをいただきました。表彰式後にご参加の皆さま方との懇親会にて、日頃のご尽力に感謝をお伝えするとともに、今後のプライバシーマーク制度へのご支援ならびにご協力をお願いし、閉会しました。

### プライバシーマーク付与事業者



NOCアウトソーシング＆  
コンサルティング株式会社  
代表取締役社長  
澤登 哲也様



株式会社日本総合研究所  
執行役員 法務部長  
大谷 和子様

## プライバシーマーク制度創設25周年記念表彰対象者一覧

- ・ プライバシーマーク制度創設年度である1998年4月1日から1999年3月31日までに付与適格決定を受け、2023年6月30日現在、付与継続中の事業者様

	事業者名	プライバシーマーク 登録番号	登記上の本店所在地
1	株式会社アイネス	11820026 (13)	神奈川県
2	株式会社インテージ	12390001 (13)	東京都
3	株式会社HDC	11820034 (12)	北海道
4	AGS株式会社	11820038 (12)	埼玉県
5	株式会社SRA	11820033 (12)	東京都
6	SCSK株式会社	11820015 (13)	東京都
7	NOCアウトソーシング&コンサルティング株式会社	10820002 (13)	東京都
8	NCS&A株式会社	11820030 (13)	大阪府
9	株式会社エネコム	11820037 (13)	広島県
10	株式会社エフコム	11820024 (13)	福島県
11	株式会社オーネット	10740002 (13)	東京都
12	株式会社学情	10820003 (13)	東京都
13	キーウェアソリューションズ株式会社	11820063 (12)	東京都
14	株式会社さくらケーシーエス	11820011 (13)	兵庫県
15	株式会社シーイーシー	11820032 (12)	神奈川県
16	株式会社シーエーシー	11820025 (12)	東京都
17	株式会社ジーシーシー	11820009 (13)	群馬県
18	JFEシステムズ株式会社	11820008 (13)	東京都
19	株式会社JOE	11820005 (13)	東京都
20	株式会社ジャステック	11820012 (13)	東京都
21	情報技術開発株式会社	11820031 (13)	東京都
22	株式会社中電シーティーアイ	11820036 (12)	愛知県
23	株式会社ZWEI	10740003 (12)	東京都
24	TIS株式会社	11820020 (13)	東京都
25	TISシステムサービス株式会社	11820021 (13)	東京都
26	株式会社ディーエムエス	10860001 (13)	東京都
27	株式会社テプコシステムズ	11820027 (13)	東京都
28	東芝情報システム株式会社	11820014 (13)	神奈川県
29	日鉄ソリューションズ株式会社	11820028 (12)	東京都
30	株式会社日本総研情報サービス	11820004 (13)	東京都
31	株式会社日本総合研究所	11820002 (12)	東京都
32	株式会社日立インフォメーションエンジニアリング	10820009 (13)	神奈川県
33	株式会社日立ソリューションズ	11820016 (13)	東京都
34	株式会社日比谷コンピュータシステム	11820013 (13)	東京都
35	株式会社マーケティングセンター	12390002 (13)	東京都
36	みずほリサーチ&テクノロジーズ株式会社	11820010 (13)	東京都
37	三菱総研DCS株式会社	11820035 (12)	東京都
38	明治安田オフィスパートナーズ株式会社	10820006 (13)	東京都
39	株式会社ラポールエム・アール・エス	12390004 (13)	東京都
40	株式会社リクルートスタッフィング	10860002 (13)	東京都
41	株式会社両毛システムズ	11820018 (13)	群馬県

五十音順：41社（2023年9月25日時点の表記による）

- ・ プライバシーマーク指定機関：指定審査機関（19機関）／指定研修機関（3機関）
- ・ プライバシーマーク審査員（2023年3月31日時点の契約審査員）

# 記念講演 レポート

## JIPDECプライバシーマーク制度創設25周年を迎えて ～更なる発展を目指して～

一橋大学名誉教授、元JIPDECプライバシーマーク制度委員会委員長、元個人情報保護委員会委員長 **堀部 政男氏**

本レポートは、2023年9月15日に開催されたプライバシーマーク制度創設25周年記念表彰式で行われた、堀部政男氏による記念講演の内容をまとめたものです。



### プライバシー・個人情報保護論議の歴史的展開

私は「歴史を知らずして現代は語れない」と述べていますが、「プライバシー・個人情報保護論議の世界的展開」について第1期から第8期まで時期区分しています。

- 第1期 プライバシー権の歴史的展開期（19世紀末以降）
- 第2期 歴史的展開期・データ保護法議論期（1960年代）
- 第3期 データ保護法制定萌芽期（1970年代）
- 第4期 国際機関基準確立・データ保護法制定発展期（1980年代）
- 第5期 国際機関基準確立・データ保護法展開期（1990年代）
- 第6期 データ保護法制定拡大期（2000年代）
- 第7期 現行制度の再検討議論期（2010年代）
- 第8期 プライバシー・個人情報保護制度のグローバル展開期（2020年代）

### はじめに

1998年にプライバシーマークが創設され、今年、25周年ということで大変おめでたく存じます。

これからお話していきますように、国際的にもこのプライバシーマーク制度は大きな関心を呼んでいます。今やJIPDECといえばプライバシーマーク、プライバシーマークといえばJIPDECであると、関連付けられているように、プライバシーマークは、日本国内はもとより世界的にも知られるようになっています。

### 第1～3期「プライバシー権の歴史的展開期～データ保護法制定萌芽期」

1970年代あたりからは10年ごとに区切ることができますが、最初の第1期「**プライバシー権の歴史的展開期**」は19世紀末に遡ります。

1890年にHarvard Law Reviewという法律雑誌に掲載されたSamuel D. Warrenと Louis D. BrandeisのThe Right to Privacyという論文で、プライバシーが法的権利として論じられました。日本でプライバシーマークが創設されたのは1998年ですから、世

界で最初に「プライバシーを法的なものとしてきちんと保護していこう」という提案がなされてから、108年後にプライバシーマークは始まったことになります。

第3期になりますと、データ保護法制定の議論が行われるようになります。

JIPDECでどういう議論がなされてきたかについては、第4期「国際機関基準確立・データ保護法制定発展期」以降で見たいと思います。

#### 第4期「国際機関基準確立・データ保護法制定発展期」

OECD（経済協力開発機構）のプライバシー・ガイドラインは1980年9月23日に採択されましたが、それを受けて日本ではいろいろ検討が始まりました。OECDの勧告を受け、当時の行政管理庁、現在は総務省の一部になっていますが、そこで「プライバシー保護研究会」ができ、1982年には立法化を提唱しました。私は、当時、構成員の中では最年少者でした。

しかし日本ではなかなか民間部門を対象とする法律制定まで至りませんでした。2003年になって法律ができるわけですが、その間「民間できちんとプライバシー・個人情報を保護していこう」ということになり、JIPDECでは1986年1月に「民間部門におけるプライバシー保護調査研究委員会」が立ち上がりました。私はその委員長を仰せつかり、いろいろ検討をして翌年には報告書をまとめました。その後、1987年度には「これを一つのガイドラインにして民間部門できちんと守るようにしよう」ということでガイドラインの策定に当たり、5月にJIPDECでガイドラインをまとめました。

JIPDECと密接に連絡をとりながら検討していたのが通商産業省でした。財団法人であるJIPDECが作ったガイドラインをきちんと守ってもらうためには「通商産業省としてガイドラインを出したい」ということで今度は同省で検討が始まりました。

当時の通産省機械情報産業局長の諮問機関として「個人情報保護部会」が設置され、私はその部会長

を務めました。その間、1988年12月には「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」が制定されており、この法律の制定にも携わりました。1989年4月に「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ついて」という報告書をまとめ、指針を示しました。このような経緯で、1980年代は行政機関について国の法律ができ、通産省とJIPDECで民間向けのガイドラインを作りました。

#### 第5期「国際機関基準確立・データ保護法制定展開期」

次に1990年代を第5期「国際機関基準確立・データ保護法制定展開期」として見てみます。自治体レベルでは、これまでも市町村では1975年から、電子計算機処理関係の条例が制定されるようになり、その中で個人情報を保護するという規定が設けられてきました。都道府県では、神奈川県で本格的に検討を始めたのが1980年代中頃です。同県は、1990年3月に「神奈川県個人情報保護条例」を制定し、PDマーク（下図）を導入しました。中央のPはパーソナル（個人）、周囲のDはデータ（情報）を表し、DがPを囲み個人情報を保護することを表現しています。ちなみに東京都も1990年12月に「東京都個人情報の保護に関する条例」を制定しましたが、神奈川県・東京都両方とも関わったのは私だけです。



図. 神奈川県「PDマーク」（2014年に制度廃止）

1980年代にJIPDECでガイドラインを議論したときはOECDの理事会勧告にある「プライバシー8原則」を参考にしましたが、1990年代になると欧州委員会（European Commission）が新たな動きを示してきます。

この1990年には、欧州委員会がData Protection Directive（データ保護指令）の提案をします。当

時の通産省幹部が欧州委員会と貿易問題などで話をしている際に、「日本の個人情報保護はどうなっているか」と聞かれました。1989年のガイドラインを英訳したもので説明すると「ガイドラインに違反したらどうなるのか、sanction（制裁）があるのか」などと問われ、「ない」と答えると「それではeffective（効果的）ではない」と言われたということです。

このようなこともあり、1995年に通産省で「プライバシー問題検討ワーキンググループ」ができ、私はその座長を務めました。そこではEUの「データ保護指令」をも念頭に置きながら1989年のガイドラインの改正を検討しました。

EUの「データ保護指令」は1995年10月24日に採択され、3年後に施行されました。その間、通産省ではワーキンググループでいろいろ議論を行い、1997年3月4日には同省が改正ガイドラインとして「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」を官報告示しました。改正後のガイドラインはかなり詳しいものになっています。

そこでは、認証制度は議論になりませんでした。神奈川県で創設されたPDマークの審査なども経験していましたので、民間が個人情報を保護していく上でインセンティブになるようなものとして、私が提案したのが神奈川県のPDマークのようなものでした。

1990年に神奈川県で取り入れ、今JIPDECの指定機関で行っている審査ほど厳密なものではなかったものの、私も実際に審査を行っていました。1997年までそういう経験を持っていたため神奈川県の事例を話したところ、当時の通産省幹部の方が「それは重要なものですね」と興味を示してくれました。「JIPDECで検討してみてほしい」という要請を受けました。

1997年7月からはJIPDECの「個人情報保護に係る環境整備検討委員会」で委員長として、マーク制度の検討を始めました。神奈川県のような自治体とは違い、JIPDECでの取組みは全国規模になるため、規程類もいくつも策定しました。通産省の改正ガイ

ドラインを基に「プライバシーマーク制度」を作り、発足したのが1998年4月1日です。

その後、通産省工業技術院関係者から「通産省のガイドラインで運用すると通産省所管の団体や事業者に限定されるのではないか」「これを日本工業規格（現：産業規格）として、もっと広く、いろいろな業種でこのマークを取り入れてもらうようにしてはどうか」とアドバイスをいただき、JISとして提案していくことになりました。

原案はJIPDECで作成し、日本規格協会でJIS原案を審議する「個人情報保護規格審議委員会」が立ち上がり、私が委員長を務めました。ここで1999年3月に日本工業規格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」をまとめました。「プライバシーマーク制度」は1998年4月に発足し、そのときは通産省のガイドラインを基にしていたのですが、1999年4月からはJIS Q 15001に基づく運用を開始しました。

この年には、政府の「高度情報通信社会推進本部」（本部長・小淵恵三内閣総理大臣）において「個人情報保護検討部会」が立ち上がり、私はその座長を務めることになりました。7月に第1回会合を開き、この年の12月までには報告をまとめるように要請され、大忙しでした。

## 第6期「データ保護法制定拡大期」

21世紀に入ると、世界的に個人情報保護法がますます多くの国で制定されるようになりました。2000年代の第6期「データ保護法制定拡大期」です。

当時の経済界の方々などと話してみると、厳しい法律は困ると言います。ならば「日本には基本法という体系があるので、それでルールを作っていくのはどうだろうか」と話し基本法で進めることになりました。

当時の検討部会では様々な分野の方が入り、「基本法を作るのはなかなか難しいだろう」ということもあり、全閣僚で構成されている「高度情報通信社会推進本部」へ説明に行き、新たな委員会を作っていたきたいと提案しました。

青木幹雄官房長官に検討していただくことにな

り、新たに「個人情報保護法制化専門委員会」が2000年に設けられることになりました。委員長は、前最高裁判事の園部逸夫さんで、今日お見えの高芝利仁先生と藤原静雄先生はその委員を務めました。私は検討部会座長の立場で、名簿には「以上のほか、堀部政男検討部会座長が常時出席するものとする」ということで参加しました。

2001年には国会に法案が提出されましたが、なかなか通らずようやく2003年に成立しました。

先ほど述べた1988年の「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」も全部改正されましたので、その他の関係法律も含め個人情報保護関係5法というような言い方をしますが、2003年5月23日に成立、5月30日に公布され、2005年4月1日に全面施行されました。

2003年から2005年までは施行準備期に入りますが、その間にプライバシーマークの申請が急増しました。

### プライバシーマーク付与事業者数の推移

「プライバシーマーク付与事業者数」の推移を見ますと、最初は58件ほどで、2004年度は1,294件とずいぶん増えています。これは「個人情報保護法」が2005年4月1日に施行されるということで、民間で「プライバシーマーク制度」への関心が高まっていったことがよくわかります。その後、2005年度3,656件、2006年度7,347件と、倍々といってもいいぐらいに付与事業者数が増えていきました。

2022年度の終わりで17,480件と、発足後は順調に増えています。これも指定機関・事業者の方々のおかげと感謝しております。

### 国外への情報発信

JIPDECでは英語での資料も作っており、私も国際的にずいぶん発信してきました。最も早くは1999年の香港での国際会議でRecent National Privacy Standards Initiatives : Japanというタイトルで報告しました。

ボードに神奈川県「PDマーク」とJIPDECの

「プライバシーマーク」を描いて「日本ではこういうマークも取り入れてJIS Q 15001で保護措置を講じるようになった」とスピーチしたところ、規格とマークを一体化させたことに関心が集まりました。主催者だったカナダ規格協会からは「日本が中心になってISO化を進めてほしい」という声も上がりましたが、日本でそれを引き受けるだけの余力がなかったので、引き受けないままになりました。

その後も海外への発信はかなり行いました。例えば、2002年3月25日、ニュージーランドのオークランドで開催の「第3回プライバシー・データ保護アジア太平洋フォーラム」で、2003年2月13日、タイのチェンライで開かれた「APECプライバシー・ワークショップ」でもプライバシーマークを紹介しています。

また、国際会議の参加者や外国のデータ保護関係者などからよく質問され、説明してきています。

後になりますが、2020年にWolters Kluwer社が発行したジャーナルGlobal Privacy Law Review, vol.1, issue3では日本が特集され、プライバシーマークについても触れられています。そのうちのひとつが、ブリュッセルの弁護士であるTanguy Van Overstraeten氏による論稿です。次のように書いています。

私が2006年に初めて堀部教授にお会いしたときには、日本ではすでに1998年4月から始まった「プライバシーマーク」と呼ばれる認証制度が導入されていた。簡単に言うと、プライバシーマーク制度の目的は、事業者の個人情報処理が、特定の基準に基づいて安全かつ適切な方法で行われることを証明することにある。この制度はJIPDECが主導し、一定の要件を満たす企業は「プライバシーマークロゴ」を使用することができるようになっている。

最近、こういうこともありました。現在の世界プライバシー会議（Global Privacy Assembly, GPA）の2021年の主催国はメキシコでした。そのデータ保護機関であるINAI（National Institute for Transparency, Access to Information and Personal Data Protection）から、「データ保護の人間中心のアプローチ」

(Human-centric approach) について、500語以内で原稿を書いてほしいという依頼を受けました。INAIは、依頼論稿や2021年の国際会議（オンライン中心）の報告・記録などをMemory Bookと題する書籍にまとめて、2022年10月にトルコのイスタンブールで開かれたGPAで一定数を配布しました。それを読んだイギリスのStewart Dresner氏から、同氏が発行するPrivacy Laws & Businessにも書くように要請されました。Dresner氏は、プライバシーマークについていくつか質問したいということで、それへの回答も含めて原稿をまとめてみてほしいと言ってきました。それに答えて書いたものが、Privacy Laws & Businessの2022年12月号に掲載されました。

それを見た、Journal of Data Protection and Privacyという雑誌（イギリスのHenry Stewart Publicationsという出版社発行）の編集委員会の委員長から、プライバシーマークについてやや詳しい原稿を頼まれました（ただし、査読ありとのことでした）。JIPDECの英文の資料も紹介しながら原稿を書きました。査読も通り、同誌の第6巻第1号（2023年秋発行）に載りました。14頁にわたる拙稿は、その制度創設の歴史から現状までを記述した、これまでのところ最も詳しい情報を英文で提供しているものであると言えます。

このように、国際的発信もしてきています。

## 国内での紹介

プライバシーマークについては、日本でも様々な

形で紹介されています。NHKが2005年4月に全国ニュースでプライバシーマーク制度の審査風景を取材、放送するなどメディアからの注目も集めています。

ここでは、審査員が厳正な審査を行う過程を事細かに伝え、個人情報保護法をきっかけに取得企業が急増している現状を伝えていました。番組では「個人情報の適切な管理次第では取引ができない事態も招きかねず、企業にとって生き残りをかけた取引はこれからも続く」と締め括られ、実際の審査が適切に行われていることがよくわかる内容となっていました。

## 更なる発展を目指して

述べたいことは尽きませんが、JIPDECの事業計画書で明らかにしている展望を紹介します。「2023年度事業計画書」は、次のような項目を挙げて、具体的に説明しています。

- (1) 制度運用の基盤強化（デジタル化）
- (2) 普及促進活動の充実
- (3) 時代の変化に対応した事故の評価と対応
- (4) 審査の迅速化

更なる発展のためには、これらが具体化されることが必須であり、そうすることを望んでいます。

指定審査機関には、これからもぜひ厳格に審査をしていただき、付与事業者の数を増やしていただくことを期待しています。



## コラム

## JIS Q 15001の改正について

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 主幹 恩田 さくら

「JIS Q 15001 個人情報保護マネジメントシステム—要求事項」は、事業者が大量の個人情報を扱い、個人情報の適切な利用及び保護が極めて重要となるなか、各事業者におけるマネジメントシステムによる個人情報保護の取組みを促進し、高度情報通信社会の健全な発展及び消費者保護を目的として、1999年に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として制定されました。この規格の制定後、情報技術の発展に伴い、個人情報の保護の必要性が一層高まるとともに、個人情報保護法が2003年に制定され、2007年4月からの全面施行を迎え、規格を取り巻く環境が大きく変化したことを受け、2006年に個人情報保護法に基づく個人情報保護ルール及びマネジメントシステムをあわせもった規格へ改訂されました。その後複数回の改訂を経て、2023年9月20日に、JIS Q 15001:2023が発行されました<sup>1</sup>。

2023年版規格は、令和2年改正個人情報保護法（2020年6月12日公布、2020年12月12日一部施行、2022年4月1日全面施行）及び令和3年改正個人情報保護法（2021年5月19日公布）が公布され、これらの改正法に整合する規格とするため、改正が行われています。なお、令和2年改正個人情報保護法では、仮名加工情報、個人関連情報などが新しく定義されるとともに、保有個人データにかかる規律が

変更されており、それらへの対応がなされています。

また、組織のマネジメントシステム規定は、2017年版規格では、ISO/IEC専門業務用指針 第1部 統合版ISO補足指針の付属書SLを参考に、原則として規格の本体に規定されることとされつつ、それ以前の版の要求事項の基本的な考えを変更しないこととしたため、2017年版規格の付属書Aには、マネジメントシステム規定と、個人情報保護法に対応する規定の両方が含まれていました。そのため、2017年版規格本体のマネジメントシステム規定と、付属書Aに含まれるマネジメントシステム規定との対応がわかりにくい状況があり、今回の改正においては、2017年版規格の付属書Aのうち、マネジメントシステム規定は、規格の本体に規定を設けることとし、2023年版規格の付属書Aは、改正個人情報保護法の内容に対応する規定として整理されました。

これまで、この規格の適用範囲は、個人情報取扱事業者を単位とすることが想定されてきました。一方で、組織の形態は、必ずしも事業者単位ではなく、カンパニー制などのように事業者の一部または複数の事業者を対象とするマネジメントシステムの運用も想定されるところ、規格利用者が、事業者単位に限定されず、組織の形態に応じた個人情報保護マネジメントシステムに適用可能な規格とするための改正も、併せて行われています。

1 「JIS Q 15001 個人情報保護マネジメントシステム—要求事項」（一般財団法人日本規格協会、2023年9月）を参照。

# 英国政府のサイバーセキュリティ戦略

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 主任研究員 大熊 三恵子

2023年10月24日、英国下院の科学・イノベーション及び技術委員会<sup>1</sup>は、英国の重要国家インフラ（Critical National Infrastructure：CNI）のサイバーレジリエンスの調査のため、コメント募集を開始しました。英国は、ITUの“Global Cyber Security Index”で世界第2位（2021年版）<sup>2</sup>、ハーバードベルファーセンターの“Cyber Power Index”では第4位（2022年）と高いサイバーセキュリティ能力を誇る一方で、米国、ウクライナに次いで世界第3位のサイバー攻撃の標的国であり<sup>3</sup>、2023年8月には、数千万人分の有権者情報がサイバー攻撃によって漏えいしていた事実が1年以上検出されなかったというインシデントが報道されています。ここでは、今回のコメント募集の対象の一つとなっている『政府サイバーセキュリティ戦略2022-2030』（2022年1月25日発表。以下、本戦略）<sup>4</sup>について概説します。

本戦略の目標は、2025年までに政府の重要な機能をサイバー攻撃に対して大幅に強化し、遅くとも2030年までに、公共部門全体にわたるすべての政府組織が既知の脆弱性（known vulnerabilities）と攻撃手法に対して回復力を持つようにすることです。この目標を達成するために、政府は、①政府機関がサイバーセキュリティリスクを管理するための適切な構造、メカニズム、ツール、サポートを確保すること、②サイバーセキュリティに関するデータ、専門知識、能力を政府全体で共有し、一丸と

なって防衛すること、の2つを戦略的柱に据えています。

これらの戦略的柱を支えるために、変革案の一つとして盛り込まれたものが、サイバーアセスメントフレームワーク（Cyber Assessment Framework：CAF）の採用です。CAFは、①セキュリティリスクの管理、②サイバー攻撃に対する防御、③サイバーセキュリティ事象の検知、④サイバーセキュリティインシデントの影響の最小化という4つの目的、「ガバナンス」「リスクマネジメント」「資産管理」等を含む14の原則、「リスクマネジメントプロセス」「保証」「資産管理」「アイデンティティ及びアクセス管理」を含む、39の成果による段階的な構成となっています。このCAFの採用によって、政府は英国の重要なサービスを運営する他の組織と整合のとれた比較可能な方法でサイバーレジリエンスを評価することが可能です。CAFは、政府省庁の一貫したサイバーセキュリティ保証を提供するための枠組みとして使用されますが、各省庁は、サイバーセキュリティリスクの管理を最も適切に行うことができると考える枠組みを引き続き使用することができるとしています。特に、CAFと整合がとれているサイバーセキュリティフレームワークとして、米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワークやISO/IEC 27001が挙げられています。

1 Science, Innovation and Technology committee

2 <https://www.itu.int/pub/D-STR-GCI.01-2021>

3 英国議会 Cyber resilience of the UK's critical national infrastructure - Committees - UK Parliament <https://committees.parliament.uk/work/7934/cyber-resilience-of-the-uks-critical-national-infrastructure/>

4 Government Cyber Security Strategy 2022-2030：Government Cyber Security Strategy: 2022 to 2030 - GOV.UK ([www.gov.uk](http://www.gov.uk)) <https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030>

## ドメイン名のご利用は計画的に

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 主幹 高倉 万記子

Webサイトを運営したり、メールを送信したりするのに必要なドメイン名ですが、2023年10月1日現在、日本の企業が登録できるco.jpドメイン名は47万件以上、企業以外の日本の法人組織が登録できるor.jpは4万件以上が登録されています<sup>1</sup>。

国内の企業数は1999年に485万社、2009年に421万社、2016年に359万社<sup>2</sup>でしたが、co.jpドメイン名は1999年に9万件、2009年に33万件、2016年に39万件<sup>3</sup>となっており、企業数に対するドメイン名登録数は1.9%、7.8%、10.9%と、増加の一途をたどっています。実際にはco.jpドメイン名以外の汎用JPドメイン名や、.COMなど、いろいろなドメイン名が利用できるため、ドメイン名を登録している企業ははるかに多いと推測されます。

ドメイン名は安いものだと年額数百円で登録でき、オンラインで簡単に登録申請ができます。ドメイン名の登録数に制限はないため、組織の活動のデジタル化が進むにつれ、コーポレートサイト用のドメイン名に加え、ブランド用、キャンペーン用にと、手軽に登録が進んでいます。

一方で、キャンペーンが終了したり、ブランドの取扱いを終了したりした場合、そのドメイン名が不要になったということで、登録を更新せずに廃止す

ることがあります。

その廃止されたドメインがどうなるかという点、携帯電話の番号のように、一定期間経過後再利用（再登録）できるようになっているため、オークションサイトで販売されたりします。

元々、知名度の高い企業や公的なサイトは、多くの人に周知され、ブックマークにも追加されており、検索サイトの検索結果でも最初の方にヒットもします。このようにアクセス回数が望めるわけですから、価値が高いわけです。

このため第三者が登録し、そのドメイン名でウェブサイト構築することがたびたびあるのですが、中には悪意ある者が登録して、前の登録者と同じように見えるウェブサイト構築する、なりすましサイトが作られセキュリティ上の脅威となることがあります。

このようなことがあるため、オークションにかけられていたことに後から気づいて買い戻した企業もあります。

第三者に登録されないようにするためにも、一度登録したドメイン名は手放さないこと、そもそも後で不要となり手放すかどうかを吟味してからドメイン名を登録することをお勧めしています。

1 JPRS「JPドメイン名の登録数」より

2 中小企業庁：2020年版「中小企業白書」第1部第3章第1節 企業数の変化と開廃業の動向 (meti.go.jp)

3 JPRS「JPドメインの登録推移」より

## デジタルトラストとトラストサービスの信頼性評価

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 副センター長 萩原 隆

インターネットやクラウドサービスの普及により、デジタルデータのやり取りが日常的に行われています。しかし、デジタルデータはなりすましや改ざんなどのリスクを伴うため、これらのリスクを防止するための対策が施されていることを示すことができるデジタルトラストの確保が不可欠となっています。

デジタルトラストの確保には、認証局により発行された電子証明書を使った電子署名や、eシールの機能であるデータの改ざん防止などが有効です。近年、リモート署名などの利用者の利用しやすさを高める技術も普及しつつあります。リモート署名とは、物理的に離れた場所からでも電子署名やeシールを行うことができる技術です。リモート署名は、署名者の利便性を向上させる一方で、署名者の秘密鍵を第三者（トラストサービス提供者）が保管することになるため、署名の信頼性を証明できることが重要です。

トラストサービスは、その信頼性が一般にはわかりにくいという課題があります。この課題を解決するために、JIPDECは、認証局、リモート署名などのトラストサービスの運用、技術及び設備を審査し、その結果を公開する「JIPDECトラステッド・サービス登録（JTS登録）」を実施しています<sup>1</sup>。

JTS登録は、トラストサービスの信頼性を公平性・中立性の観点から評価する事業です。電子契約サービス等を提供する事業者は、JTS登録を通じて、利用者に安心して利用いただけるサービスであることを対外的にアピールすることができます。

JIPDECは、これまで登録のための要件の概要のみ公開していましたが、JTS登録の透明性をより高めるために、2023年7月にJTS登録基準（認証局）をWebサイトで公開しました<sup>2</sup>。この基準は、電子署名やeシール用電子証明書を発行する認証局の運用、技術及び設備に関する要件を定めた基準です。今後も他の基準を公開していく予定です。eシールは、電子文書等の発行元の組織等を示す目的で行われる措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組みです（総務省「eシールに係る指針」<sup>3</sup>より）。

なお、総務省は、「eシールに係る検討会」を開催しており、JIPDECも構成員として参加しています。本検討会においては、eシールの定義として、「措置」と捉えるか「データ」として捉えるかが論点の一つとなっています。

JIPDECは、認証局、リモート署名等のトラストサービスの評価を通して、デジタル社会の実現に貢献してまいります。

1 JIPDECトラステッド・サービス登録（JTS登録） <https://www.jipdec.or.jp/project/jtsr.html>

2 JIPDEC トラステッド・サービス登録（認証局）登録基準 [https://www.jipdec.or.jp/project/jtsr/isp5410000000aee-att/JTS\\_CA\\_TOROKU\\_KIJUN.pdf](https://www.jipdec.or.jp/project/jtsr/isp5410000000aee-att/JTS_CA_TOROKU_KIJUN.pdf)

3 総務省「eシールに係る指針（令和3年6月25日）」 [https://www.soumu.go.jp/main\\_content/000756907.pdf](https://www.soumu.go.jp/main_content/000756907.pdf)

## 〈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）

国内	年	海外	
「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」及び関連法公布（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）
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がアカウントビリティ・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」及び「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）
「カメラ画像利活用ガイドブックver.2.0」公表（3/30）	2018	EU	「EU一般データ保護規則（GDPR）」施行（5/25）
		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
		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）
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）。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、及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
「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		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（PDPA）」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-米国	EU司法裁判所、「プライバシーシールド」無効判決（7/16）
		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）成立（12月）。2023/1/1施行
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）	
「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）	2021	シンガポール	「個人情報保護法（2012）」改正法施行（2/1）
「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ver1.1」策定（7/19）		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（3/2）
		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
日本を含む7カ国・地域がグローバルCBPRフォーラム設立宣言に合意（4/21）	2022	EU-アメリカ	2020年に無効判決を受けた「Privacy Shield」に代わる「Trans-Atlantic Data Privacy Framework」原則的に合意（3/25）
「電気通信事業法」改正（6/17）。2023/6/16施行		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）。2022年中の成立なし
「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ver1.2」策定（2/22）		中国	「データ越境安全評価弁法」公布（7/7）。9/1施行
		インドネシア	初の「個人データ保護法（PDPL）」制定・施行（10/17）
「カメラ画像利活用ガイドブックver3.0」策定（3/30）		EU	・「デジタル市場法（DMA）」公布（10/12）。11/1発効 ・「デジタルサービス法（DSA）」公布（10/27）。11/16発効
「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ver1.3」策定（4/25）	2023	英国	グローバルCBPRフォーラムへの参加表明（4/17）
G7データ保護・プライバシー期間ラウンドテーブル、生成AIに関する共同声明採択（6/21）		中国	「個人情報域外移転標準契約弁法」公布（2/24）。6/1施行
		米ユタ州	18歳未満のソーシャルメディア使用を制限する規制法「SB152」「HB311」成立（3/23）
「JIS Q 15001：2023」改正（9/20）		ベトナム	「個人情報保護政令」公布（4/17）。7/1施行
		米モンタナ州	「TikTok禁止法」成立（5/17）。2024/1/1施行
G7、広島AIプロセスに関するG7首脳声明発出（10/30）		米カリフォルニア州	CPRA執行規則発効（3/29）。7月執行予定が裁判所命令で2024年3月に延期（6/30）
		EU-アメリカ	「EU-US Data Privacy Framework（DPF）」始動（7/10）
		インド	「デジタル個人データ保護法」成立（8/11）
G7、広島AIプロセスに関するG7首脳声明発出（10/30）		スイス	「改正連邦データ保護法」と関連条例施行（9/1）
	イギリス-アメリカ	データ移転のための十分性認定「データブリッジ」発効（10/12）	



## 〈資料2〉情報化に関する動向（2023年4月～2023年9月）

### 【国内／国際連携】

2023年4月
<ul style="list-style-type: none"> <li>・日立ソリューションズ、システム開発頓挫の訴訟でZ会に11億円の賠償金支払い。抗争5年で結審。</li> <li>・経済産業省・総務省「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Ver1.3」策定。概念の整理、実践事例集を収録。</li> <li>・G7、生成AI活用のための5原則設立合意へ。G7群馬高崎デジタル・技術大臣会合では、越境データ移転推進等6つのテーマを盛り込んだ「G7デジタル・技術閣僚宣言」採択。</li> </ul>
5月
<ul style="list-style-type: none"> <li>・政府、生成AIの利活用・開発・規制について検討する「AI戦略会議」設置。</li> <li>・神戸市議会、生成AIの利用ルールを追加する条例改正。自治体のAI利用規制は初。</li> <li>・厚生労働省、サイバー攻撃で約10万件の迷惑メール送信の踏み台に。</li> <li>・トヨタ自動車、クラウド誤設定で、約10年にわたり約215万人分の車の位置情報が閲覧可能であったことと、26万人分の顧客情報漏えいの可能性を公表。7月に総務省が行政指導。</li> <li>・富士通、コンビニ交付用証明書発行システムの度重なる証明書誤交付で、システム再点検。個人情報漏えいに関し、9月にPPCが行政指導。</li> </ul>
6月
<ul style="list-style-type: none"> <li>・改正マイナンバー法成立。2024年秋に健康保険証を廃止し、「マイナ保険証」に一本化。</li> <li>・個人情報保護委員会（PPC）、利用者の同意方法に問題ありとして、OpenAIに注意喚起。生成AI事業者への行政指導は初。</li> <li>・尼崎市、46万人の住民情報入りUSBメモリ紛失は業務委託契約不履行として、委託先BIPROGYが損害賠償金2,950万円支払い。</li> <li>・改正電気通信事業法施行。電気通信事業者に対するCookie情報の利用規制強化。</li> <li>・G7データ保護・プライバシー機関ラウンドテーブル会合、生成AIに関する声明。生成AI開発段階からプライバシーに配慮して設計するよう訴え。</li> </ul>
7月
<ul style="list-style-type: none"> <li>・名古屋港、ランサムウェア攻撃によるシステム障害で、3日間コンテナ搬入・搬出不能に。</li> <li>・NTTドコモ、3月に発覚した元派遣社員の顧客情報不正持出しによる件数は約596万件と発表。</li> </ul>
8月
<ul style="list-style-type: none"> <li>・サイバートラスト、JIPDECトラステッド・サービス（JTS）登録取得の認証局発行のeシール用証明書を提供開始。</li> <li>・総務省、eシールの認定制度創設に向けた有識者会議設置。</li> <li>・ヤフー、利用者に十分な周知なく、約756万のユニークブラウザ分の検索クエリを韓国企業に試験的に提供。総務省が行政指導。</li> </ul>
9月
<ul style="list-style-type: none"> <li>・警視庁、前勤務先保有の名刺情報を転職先同業他社に不正提供したとして、転職者を個人情報保護法違反の疑いで逮捕。保護法違反逮捕者は初。</li> <li>・PPC、別人のマイナンバーを公金受取口座に紐づけた誤登録問題で、安全管理面を問題視し、デジタル庁に行政指導。</li> </ul>

## 【海外】

### 2023年4月

- ・米ユタ州、18歳未満のソーシャルメディア使用を制限する2つの規制法（SB152とHB311）成立。閲覧時間制限や利用時の親の同意、メディア依存時の提供企業への罰金など盛り込み。
- ・韓国公正取引委員会、モバイルゲーム市場地位の独占でGoogleに421億ウォンの支払い命令。G社は異議表明。
- ・Twitter社、Eron Musk氏が経営するX社に統合され、SNS「Twitter」消滅してXへ。投稿呼称はtweetからPostに。
- ・ベトナム政府、個人情報保護政令公布。個人情報の処理に当たっては情報主体からの同意を義務付け。本人からの回答がなければ同意と認めず。
- ・米ミシガン州他8州、2023年1月の司法省によるGoogleのデジタル広告市場に対する反トラスト法訴訟に参加。
- ・英政府、グローバルCBPRフォーラム参加意向表明。APEC参加国以外の参加は初。
- ・米最高裁判所、生成AIによる発明特許出願認めぬ判決。人間による発明のみが特許発行対象に。
- ・米連邦取引委員会（FTC）他3機関、AIを含む新しい自動化システムに影響されない機会均等を守るための監視強化を共同宣言。
- ・欧州委員会（EC）、デジタルサービス法（DSA）の適用対象に19のSNSサービス指定。本年8月までにDSA規定準拠対応へ。
- ・イタリア政府、3月31日にChatGPTを一時禁止措置するも、OpenAIが個人データ取扱いの改善策を導入し、約1カ月後に禁止解除。

### 5月

- ・FTC、Metaが子どもから収集した情報の収益化を禁ずる包括的規制案公表。Metaは連邦地裁に差止要請。
- ・米モンタナ州、全米初、一般ユーザーのTikTok利用、運営会社によるアプリ提供を禁止する「TikTok禁止法」成立。2024年1月1日施行。ByteDanceは、事業活動禁止は言論の自由に反すると州を提訴。
- ・Google、位置情報追跡に関する慣行が消費者に誤解を与えるとする問題で、米ワシントン州に3,990万ドルの和解金。位置情報追跡の透明性記載へ。
- ・アイルランドデータ保護委員会（IE DPA）、Facebookユーザーデータを米国に移転したとして、GDPR違反でMetaに12億ユーロの制裁金。M社は控訴を発表。
- ・FTC、Alexaが子どもの音声データを不正に保持していたとして、児童オンラインプライバシー法（COPPA）違反でAmazonに2,500万ドルの罰金。その他ドアホン事業でユーザー情報を不適切に利用したとして、580万ドル支払いで合意。

### 6月

- ・中国インターネット情報弁公室、「個人情報域外移転標準契約弁法」施行。個人情報取扱者や受取事業者の義務、標準契約の必須条件を規制。
- ・Microsoft、FTCからXboxを利用する子どもの情報を親の同意なしに不正収集するのはCOPPA違反と指摘を受け、2,000万ドル支払い。
- ・英-米政府、データプライバシーを安全に保持しつつ、自由なデータ移転を行うための「データブリッジ」創設に向け原則合意。10月発効。
- ・米ルイジアナ州、親の同意なしに子どものSNSアカウント作成を禁止する法案可決。2024年8月施行予定。
- ・欧州議会、生成AIを含むAIを包括的に規制する「EU AI Act」可決。リスクレベルを4段階に分類して使用規制。
- ・FTC、消費者の同意なく不当な方法で有料会員登録を誘導、多額な会費を徴収したとして、Amazonを提訴。A社は簡単・明確に登録・解約可能と反論。
- ・米カリフォルニア州、州消費者プライバシー法（CCPA）を改正する州法「カリフォルニアプライバシー権法（CPRA）」の最終規則を7月1日付で執行予定も、上級裁判所が2024年3月に執行延期の判断。

## 7月

- Meta、コミュニケーションアプリ「Threds」公開。公開5日でユーザー数1億人超。
- EU-米政府、「EU-US Data Privacy Framework (DPF)」実施に向け、米国側手続き完了。次いで欧州委員会 (EC) が充分性に関する決定を採択し、始動。
- 仏経済・財務省、ネット検索結果で適切な情報提供を怠ったとして、Google欧州法人に200万ユーロの制裁金。
- EC、国境を越える案件の処理迅速化を目指すため、各国データ保護機関間の協力の合理化を図る規則を発表。
- 中国政府、国家の発展、安全を重視した生成型AIサービスに関する「生成型人工知能サービス管理暫定弁法」公布。
- 欧州司法裁判所、Metaの独占地位による同意なし情報収集に対する独カルテル庁の利用者データ収集制限命令への不服申立てを覆し、M社へのプライバシー侵害の調査、対応権限を許可。
- 経済協力開発機構 (OECD)、グローバル企業のデジタル課税、法人税の引下げルールを改める多国間条約の大枠とりまとめ。
- Googleユーザー、G社の生成AI開発への個人データの無断使用、著作権侵害で集団訴訟。AI機能強化にデータ利用可能とするG社のプライバシーポリシー改定にも言及。
- FTC、OpenAIが消費者保護の取組みで個人情報の不正取得、風評被害を招くような慣行に従事していないか調査開始。
- Google、豪Touchstream Technologiesからの特許侵害訴訟で、米テキサス州連邦地方裁判所が3.4億ドルの損害賠償命令。
- Google、Microsoft、Anthropic、OpenAI、業界団体「Frontier Model Forum」設立。AIの安全性研究の推進等取組み。

## 8月

- ノルウェーデータ保護局、行動ターゲティング広告がプライバシー侵害に当たるとして、Metaに1日100万ノルウェー・クローネの制裁金と広告表示の一時停止命令。
- インド政府、インド国内の個人情報のデジタル処理を規制する「デジタル個人データ保護法」成立。データ受託者はデータの正確性の維持、安全保管、目的達成後のデータ削除を義務付け。
- 米イリノイ州、子どものインフルエンサーを保護する全米初の法律成立。収益の一部受取り、コンテンツ削除が可能に。

## 9月

- スイス連邦法務省、改正連邦データ保護法 (DSG) と関連条例施行。データ処理の透明性向上、個人データ管理を強化。
- EC、デジタル市場法 (DMA) の適用対象企業公表。Apple、Microsoft、Meta、Alphabet、Amazon、ByteDanceの6社、22サービスを規制。2024年2月の全面適用に向けた対応必須。
- 中国国家インターネット情報弁公室、学術情報大手「知網」に、必要以上の個人情報の収集、同意なし収集など「インターネット安全法」「個人情報保護法」「行政処罰法」違反で5,000万元の罰金。
- Google、司法省が2020年に提訴した反トラスト法違反訴訟の公判開始。検索サービス市場独占維持のために年100億ドルをスマホメーカーに支払い。
- IE DPA、TikTokの子どもの個人データ取扱い不備でByteDanceに3.4億ユーロの制裁金。
- Google、同意なく位置情報履歴を追跡、データを使用したとする米カリフォルニア州と個人による団体訴訟で、計1.5億ドルの和解金支払い。
- EC、CPUの市場独占的地位乱用によるEU競争法違反でIntelに3.6億ユーロの制裁金。2009年に10.6億ユーロの制裁金が決定した際は、EU司法裁判所が決定取消し。
- FTCと17州政府、Amazonのネット通販事業が独占的で競合他社のビジネス機会損失、消費者に損害を与えたとして、反トラスト法違反で提訴。



JIPDEC IT-Report 2023 Winter

2023年12月22日発行（通巻第22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