2024 Winter

# IT-REPORT

## パーソナルデータの利活用とプライバシー保護
### ～PETs／プライバシーテック～

## Contents




JIPDEC
一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2024 Winter

# Contents

特集

# パーソナルデータの利活用とプライバシー保護　～PETs／プライバシーテック～

## 座談会　PETs／プライバシーテックの可能性 パーソナルデータ利活用の今後の展望

池田・染谷法律事務所　弁護士　今村　敏氏
プライバシーテック協会　事務局長　竹之内　隆夫氏
KDDI株式会社　経営戦略本部　Data＆AIセンター　センター長　木村　塁氏
JIPDEC　電子情報利活用研究部　主幹　恩田　さくら

### はじめに

私たちの暮らしは、すでにさまざまなデータの利活用を前提に成り立っています。パーソナルデータを利活用しサービスを提供する事業者や団体にとって、利用者のプライバシー保護は大変重要なポイントです。

匿名化や仮名化、秘密計算、差分プライバシーなど、個人情報保護・プライバシー保護に関わる技術は日々進化しています。これらの技術はPETs（Privacy-Enhancing Technologies：プライバシー強化技術）やプライバシーテックと呼ばれ、近年OECDや各国政府からガイドライン等が公表されています。また、パーソナルデータに関わるガバナンスやリスクマネジメントなど、プライバシー保護のための組織活動を技術的に支援する取り組みも増えています。

今回は技術の力で課題を解決する側面に焦点を当て、技術・事業・法律の観点から3名の専門家にお集まりいただき、「PETs／プライバシーテックの可能性とパーソナルデータ利活用の今後の展望」として座談会形式でお話を伺いました。

プライバシーテック協会で事務局長を務める竹之内隆夫氏は長年、日本電気株式会社でプライバシー保護技術の研究開発を行い、株式会社デジタルガレージとLINE株式会社（現LINEヤフー株式会社）を経て現在は株式会社Acompanyに在籍し、「プライバシーDX」というプライバシーテックの活用支援や技術の社会実装の活動をされています。KDDI株式会社 経営戦略本部 Data＆AIセンター センター長の木村塁氏は電気通信事業の実務に携わり、最先端のプライバシーテックを応用する現場にいらっしゃいます。池田・染谷法律事務所 弁護士の今村敏氏は総務省総合通信基盤局で政策立案に携わった経験を生かし、パーソナルデータの利活用を伴う事業を実施する企業を支援されています。それぞれの立場から見えるPETsやプライバシーテックの現在地について、座談会を通じて読者の皆さんと共有したいと思います。

### PETs／プライバシーテックの主要な技術

**恩田：**本日はお集まりいただきありがとうございます。はじめに竹之内さんからPETsやプライバシーテックの主要な技術についてご紹介ください。


JIPDEC　恩田　さくら

**竹之内：**データ利活用にあたっては、個人に関する情報も含まれるのでプライバシー保護が不可欠であり、そのための技術として開発が始まったのがプライバシー保護技術です。いろいろな企業がここに研究開発投資を


プライバシーテック協会
竹之内　隆夫氏

行って、発達してきました。主な技術について一つずつ説明したいと思います（図1）。

**①匿名化・仮名化：**個人特定は氏名などを削除しただけでは防げません。属性の組み合わせから特定できる恐れがあるので、それを回避するためにデータを加工する技術です。

**②秘密計算：**データを開示せずに暗号化したまま処理ができる技術です。

**③差分プライバシー：**複数の集計結果の組み合わせから個人が特定される恐れがあるため、あえて集計結果にノイズを入れてその特定を防ぐ技術です。

**④合成データ：**元データをそのまま機械学習に使うのではなく、元データに似せた別のデータを生成し、特徴を維持した別のデータを作る技術です。

**⑤連合学習：**機械学習の分析時に元データを中央に集めるという発想ではなく、それぞれの組織が持っているデータで最初に学習させ、その結果を中央のサーバーに集めて機械学習する技術です。

他にもいろいろありますが、各国が出しているPETsのガイドラインでは大体このような技術が紹介されています。

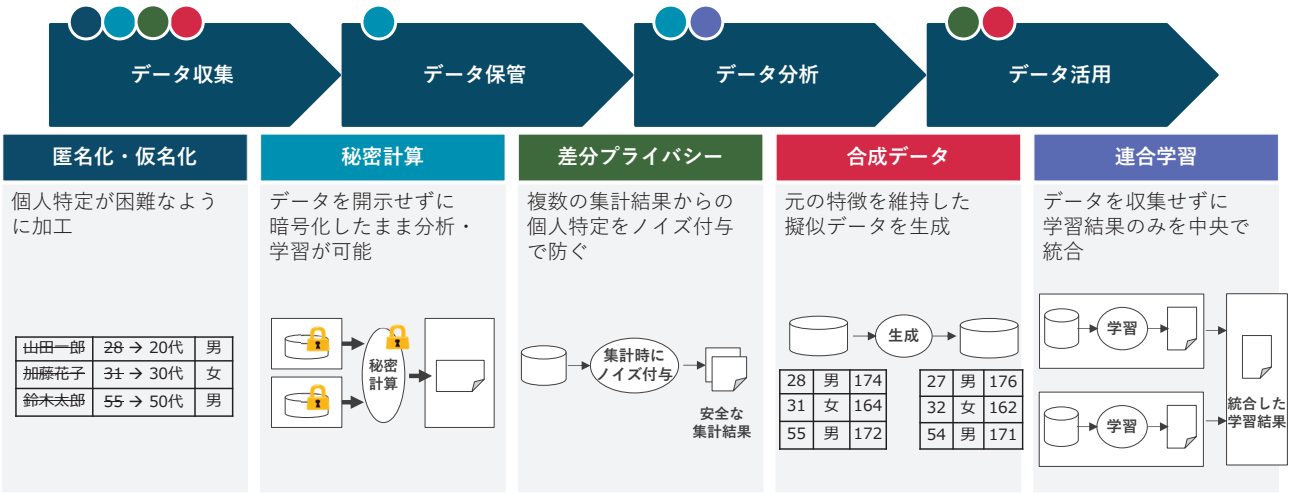


図1. データ処理段階におけるPETs／プライバシーテックの適用例

（出典）プライバシーテック協会資料

TEE：Trusted Execution Environment

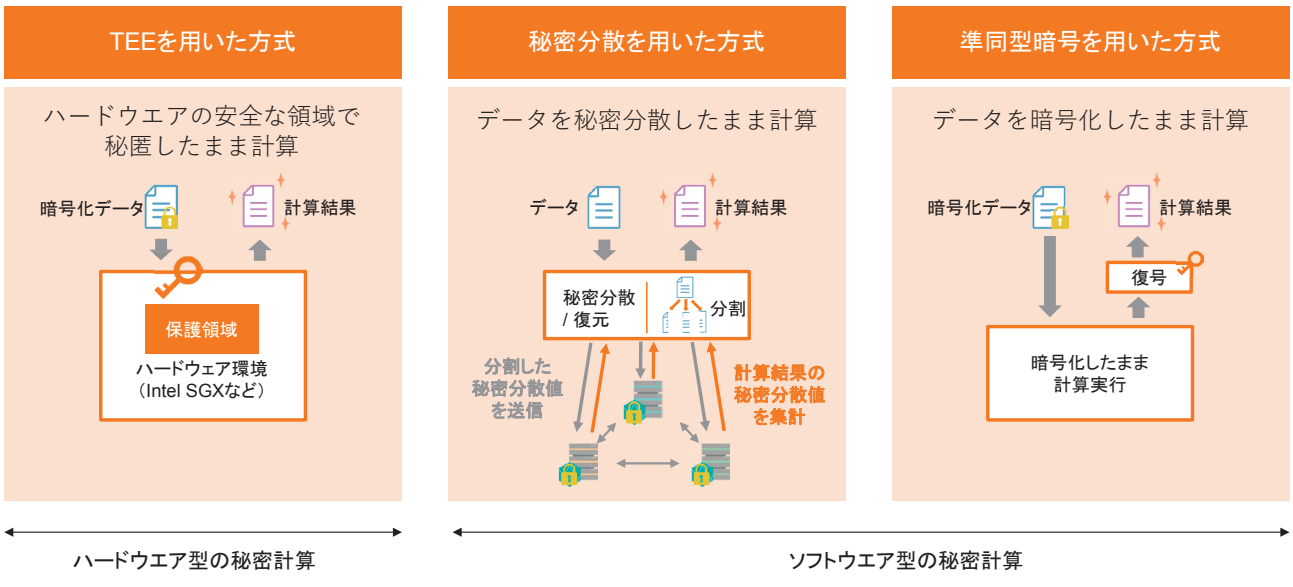


図2. 代表的な三つの秘密計算手法

（出典）プライバシーテック協会資料

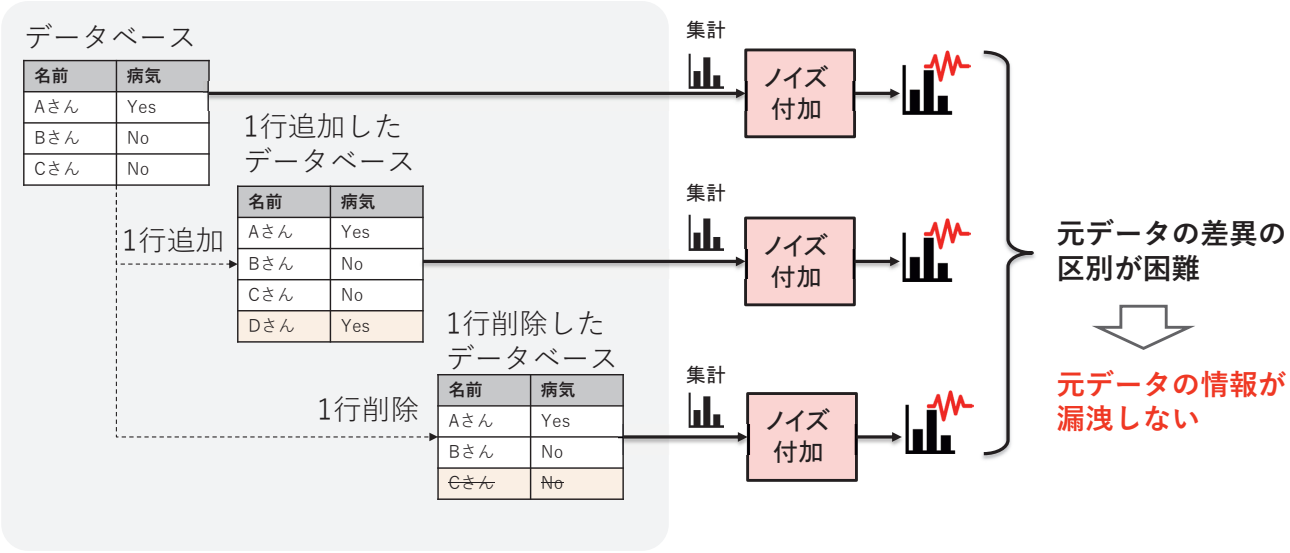


図3.　差分プライバシーとは

（出典）プライバシーテック協会資料

秘密計算は、実は日本独自の用語で、データを秘匿しながら処理できる技術の総称です。通常の暗号技術では処理するためには元データへの復号が必要だったのですが、秘密計算はそういった生データに戻さなくていいところが特長です。秘密計算にもいくつかの方式があります（図2）。

秘密計算は大きく分けるとハードウェア型とソフトウェア型があります。

ハードウェア型はTEE（Trusted Execution Environment）を使った方式で、これはハードウェアのチップの中に鍵があるイメージです。その鍵でデータを保護しながら外から見えない形で処理します。

ソフトウェア型には主に秘密分散を使った方式と準同型暗号を使った方式があります。秘密分散は元のデータを複数の断片に分割し、断片1個1個からは元データが推測できませんが断片を組み合わせると元データに戻せるという技術です。秘密分散した状態は秘匿状態であり、このまま計算できる点が特長です。準同型暗号も暗号化状態のまま計算できる特殊な暗号の技術です。普通の暗号では復号が必要ですが、準同型暗号は暗号化したまま計算ができます。

差分プライバシーも少し難しいので説明したいと思います（図3）。複数の集計結果から個人が特定できてしまうケースがあるのですが、それを防ぐためにデータを追加する技術がこれに当たります。例えば特定疾患の患者が何人かいたとき、最初は10人だったのが、ある日の集計結果として11人に増えたとします。そうすると、その日に増えた人の疾患が分かってしまいます。この推測を防ぐため、集計結果の人数にある程度小さなノイズを入れて差分を作り、漏えいしないようにするのが差分プライバシー技術です。

**恩田：**これらの技術を使った企業としての具体的な取り組みについて、木村さんからご紹介いただければと思います。

**木村：**KDDIでは、中期経営戦略（2022-2025年度）における事業戦略「サテライトグロース戦略」（図4）として、事業を衛星のように立ち上げていく取り組みを推進しています。

KDDI株式会社
木村　塁氏

その中で、事業間でデータのコラボレーションを進めるデータコラボレーション構想（図5）を掲げているところです。

グループ会社間でのデータ連携が基本ではありますが、最近では提携先企業の皆さまとデータクリーンルームを使いながらデータを連携し合い、新たな示唆を得る試みをしています。自社だけでは分からない示唆も得られ、提携先企業のデータを統合することによって新たな価値が生まれます。特にマーケティング分野では成果が顕著です。例えば株式会社AbemaTVとのパートナーシップはユーザーから同意を取得してデータ連携を行った事例ですが、先方には顧客の視聴履歴データがあり、われわれには属性データがあります。データを連携させると「どんな属性にどんなコンテンツが刺さるのか」が分かり、その逆についても統計的に分析ができる。こういった示唆はデータを事業者間でつなげて初めて得られるものです。

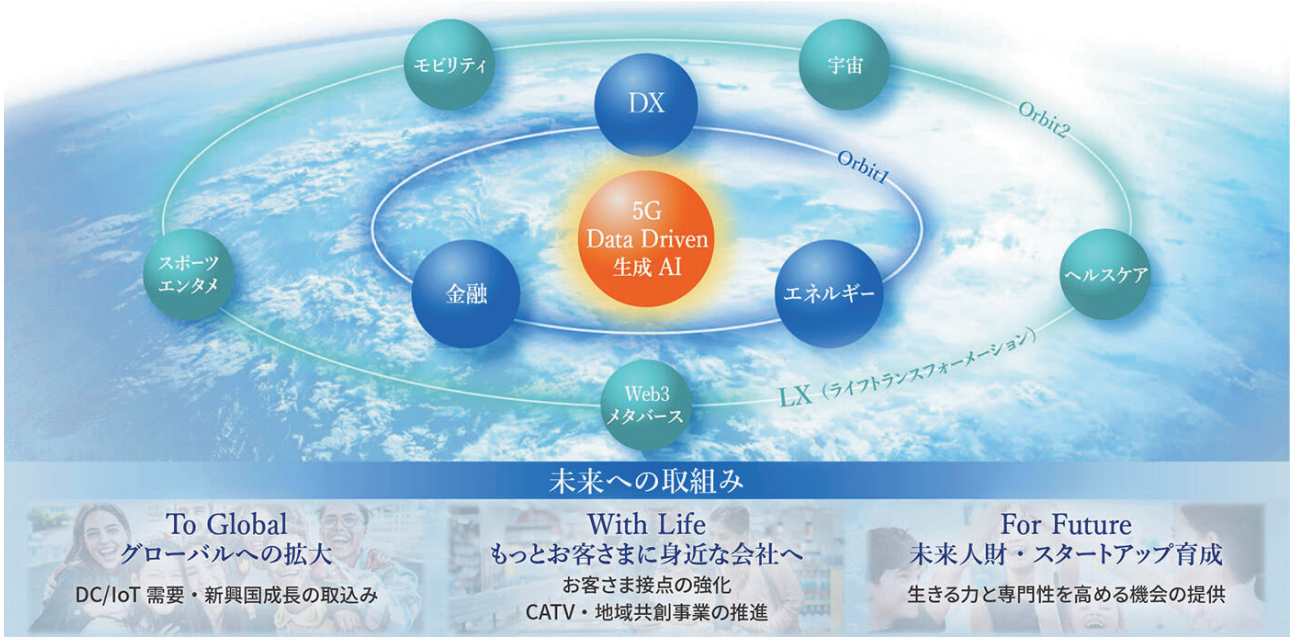


図4. KDDI サテライトグロース戦略

（出典）KDDI株式会社Webサイト

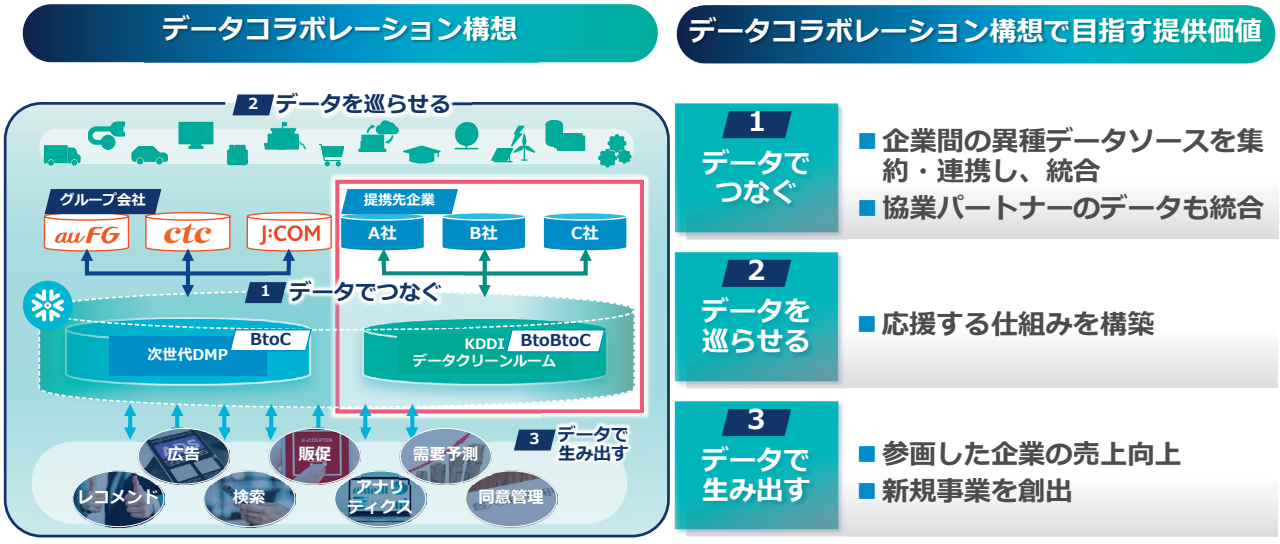


図5. KDDI データコラボレーション構想

（出典）KDDI株式会社資料

連携において重要なのはデータクリーンルーム（図6）です。これまでも二社間のデータ連携は行われてきましたが、旧来の場合だとA社からB社にデータを渡したらB社のデータベースがリッチになる、データが蓄積されるという形で進められていました。しかしデータクリーンルームを使えば、どちらかのデータベースをリッチにすることなく、ルーム内でA社B社のデータを安全に結合させて統計的な示唆を得られます。データの蓄積は顧客像の解像度が高まる可能性も増え、プライバシーのリスクにつながりやすいです。これを防ぎながらデータ分析の結果としての示唆が得られるのがデータクリーンルームの目指すところだと思っています。一般的に、分析官がデータ分析をするためにデータそのものを触り、加工したり結合したりする業務が発生しますが、その業務自体にリスクがあると考えて、なるべく人を関わらせない仕組みを作り、暗号化された状態で計算して統計化したアウトプットだけが得られるように秘密計算を使っています。これはまさにPETsを活用している部分です。

先ほど出てきた連合学習も実用化に向けて準備を進めています。連合学習を使って、複数社が保有するデータから学習結果だけをうまく組み合わせながらモデリングをすることにも取り組んでいます。こういったモデルを作るところをデータクリーンルームと連合学習で進めることによって、特定の個人を識別することなく、プライバシーを守りながらきちんとモデル機械学習活用まで実行できるのが大きなポイントだと思っています。

データクリーンルームはいわばPETsの塊です。お客さまのプライバシーを守り、信頼いただきながら二社のデータを組み合わせて価値を出すために、さまざまな技術を取り入れているところです。

**恩田：**こういったPETsやプライバシーテックの利用に関する法的な側面について、今村先生はどのようにお考えですか。

**今村：**正直に申し上げて、PETsやプライバシーテックを考えたとき「法律はまだ十分対応できていないのかな」というところが共通認識ではないかと思います。法律が現状の後追いになってしまうのは構造的に仕方がな

池田・染谷法律事務所
今村　敏氏

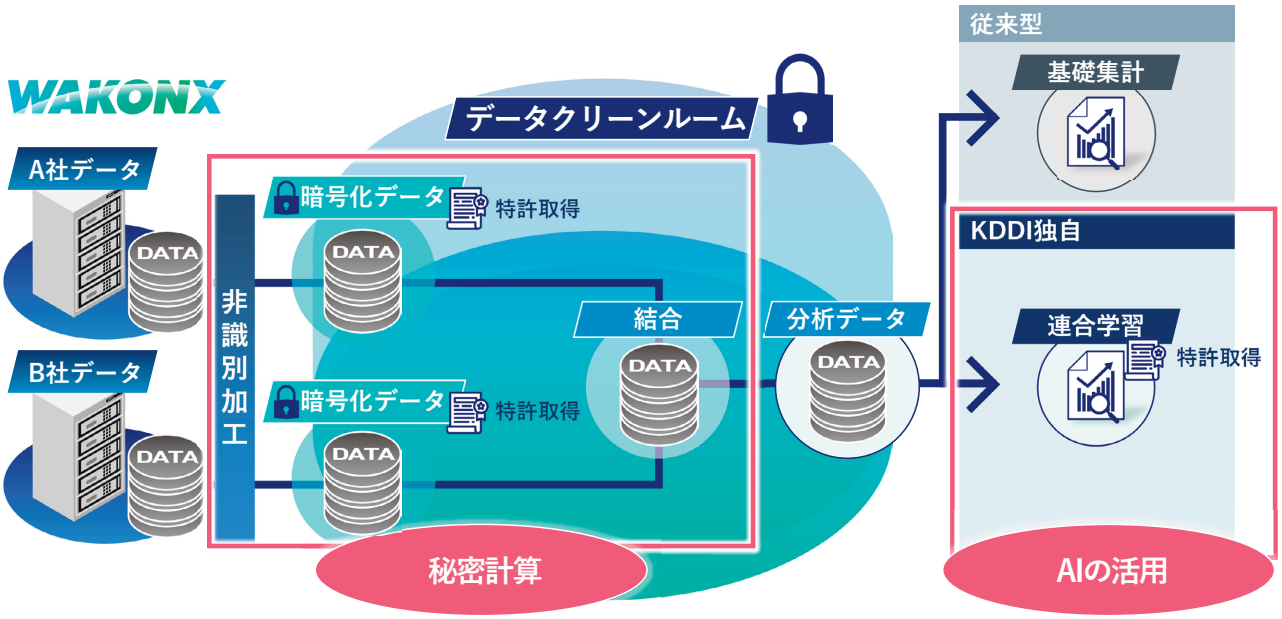


図6.　KDDIのデータクリーンルーム

（出典）KDDI株式会社資料

いことなので、現在のルールの中でまずどう落とし込んでいくのかを考え、不具合が出る部分については改正で対応し、その両輪の中で法律は少しずつバージョンアップしていっているのだと思います。

冒頭、竹之内さんから技術の概要について説明がありましたが、PETsやプライバシーテックに関してはまさに技術の最先端の話ですので法律ではまだまだ未対応な部分が当然存在します。個人情報保護を考える上では、データのライフサイクルで考えましょうというのが基本であり「取得・利用」「保管・管理」「第三者提供」等のそれぞれにおいて、どういうルールとなっているか整理すると分かりやすいです（図7）。PETsやプライバシーテックとの関係でいうと、現行法では整理がほとんどされていないものの、多少は現行のルールに当てはめることができるものもあると考えられています。大きな枠組みとして関係してくるのは個人情報該当性の議論（そもそも個人情報なのか、匿名加工情報なのか、仮名加工情報なのか、統計情報なのか）です。その他は、安全管理措置としてどう位置付けていくのかという議論で取り扱われることが多いという印象です。また、漏えいとの関係で、漏えい報告がいらないという例外的なガイドラインの解釈として「高度な暗号化」というキーワードがありますが、PETsやプライバシーテックの技術がそこに入るかどうかという議論もあります。

このように法律は、最先端の技術にそのままマッチするルールメイクには必ずしもなっていませんが、そのことを個人情報保護法は想定し、より現状に即した法体制構築を目指すべく、いわゆる「3年ごと見直し」を要求します。2024年6月に公表された中間整理案には「プライバシー強化技術（PETs）」というキーワードが入り、文書の最後には、PETsの位置づけについて、ステークホルダーの意見やパブリックコメントの結果を踏まえて引き続き検討す

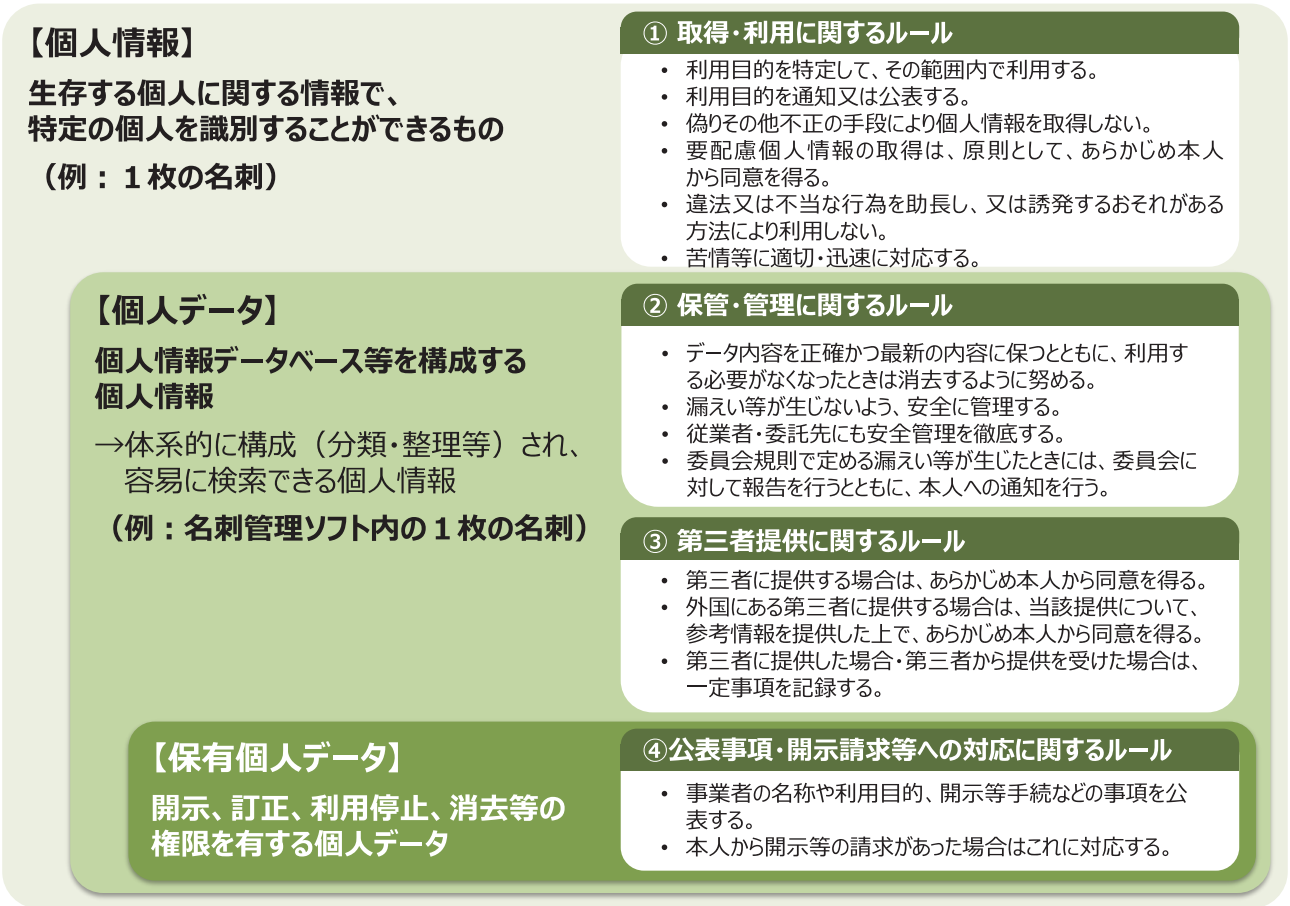


図7. 個人情報保護法の基本 民間部門に適用される規律について

（出典）個人情報保護委員会Webサイト「個人情報保護法の基本」（令和5年9月）（個人情報保護委員会）
（https://www.ppc.go.jp/files/pdf/kihon_202309.pdf）を加工して作成

ると書かれています[1]。PETsやプライバシーテックのステークホルダーが、改正の議論の中でいかにその必要性や重要性を伝えていくかが重要です。中間整理での主な論点である「こどもの個人情報保護」「本人同意を要しないデータ利活用の在り方」という文脈でもPETsやプライバシーテックの技術は有効に使える場合があるのではないかと思いますし、事業者の方々、特に技術側に精通した方が正しくそのことを伝え、法改正等のルールメイクにおいても議論をしていく必要があると思います。

**竹之内：**OECD・アメリカ・イギリスなど各国ではPETsに関するガイドライン化が進められており、PETsの適用推進にも積極的に取り組んでいます。例えば、秘密計算技術は以前から日本企業の技術が国際的にも競争力をもっていると言われているので、日本国内でもPETsやプライバシーテックの議論や検討が進めばいいと考えます。

## ガバナンスやリスクマネジメントの解決策

**恩田：**プライバシー保護のための組織の活動、ガバナンスやリスクマネジメントを補助するようなツールや技術も最近は注目されています。

**竹之内：**プライバシーを保護しながらデータを活用し、よりよいサービスを提供するために企業がまず行うべきこととして、現在企業がどういったデータを収集・利活用しているのかを整理しますが、これがデータマッピングと呼ばれる活動にあたります。データマッピング自体は多くの企業がExcelなどを使って実践していると思いますが、今は管理ツールのように使いやすいアプリが幾つかの企業から提供されています。

さらに、ビジネスの専門家だと法律観点や消費者観点からのリスクが見えてこないということもあり得ます。潜在的なプライバシーリスクを評価するプライバシー影響評価（PIA：Privacy Impact Assessment）という手法もあります。

情報取得時の同意がどこまで取られているかなどを適切に管理・確認するのであれば、Excelより専用の同意管理ツールを使う方が便利な場合もあります。こういった、適切なデータ活用を補助するツールは、日本を含め海外でも提供が進んでいます。

**木村：**われわれの組織でもいわゆるPIAを導入しています。データマッピングや本人同意の確認は各グループ企業で行い、KDDIとしてガバナンスをかけてきちんとチェックするフローで運用中です。また、現場ではチェックの効率性も重要だと思っています。昔ながらのExcel等でのメタデータ管理手法だと、データの利活用システムとの連携が弱くなり、活用時の再チェックが避けられません。このケースは大丈夫なのか、そもそも当該Excelがどこにあるのか、このデータとこのデータを組み合わせたらどうなるのかなど、見直し作業はとても煩雑です。そうすると利活用のスピード感が落ちたり、あまりにも手順が複雑すぎて活用を諦めてしまったりします。

せっかくお客さまから預かったデータを活かせないとなると、提供サービスとしても価値を損なってしまうので、預かったデータは常に利用者に対して最大限の価値を提供できるように準備しなければと考えています。その中でわれわれが注力している活動の一つに、同意管理の仕組み作りがあります。2018年に自社技術で同意管理機能（PPM：Privacy Policy Manager）を構築して自社での運用を開始し、2022年からは他の法人のお客さまへも提供を始めました（図8）。

これまでは、あるデータテーブルを使うにはこの同意文書の内容を見なければいけない、別のデータテーブルを使おうとするとまた別の同意文書の内容を見なければいけないという状況で、手順が煩雑なためデータ利活用の生産性が落ちていました。この障害をなくし、適切な同意項目をお客さま自身で一元管理できるコントローラリビティを提供するのがPPMの主眼です。

どんどんバージョンが上がっていく同意文書は

1　「個人情報保護法 いわゆる3年ごと見直しに係る 検討の中間整理」（個人情報保護委員会、令和6年6月）
https://www.ppc.go.jp/files/pdf/chukanseiri_honbun_r6.pdf

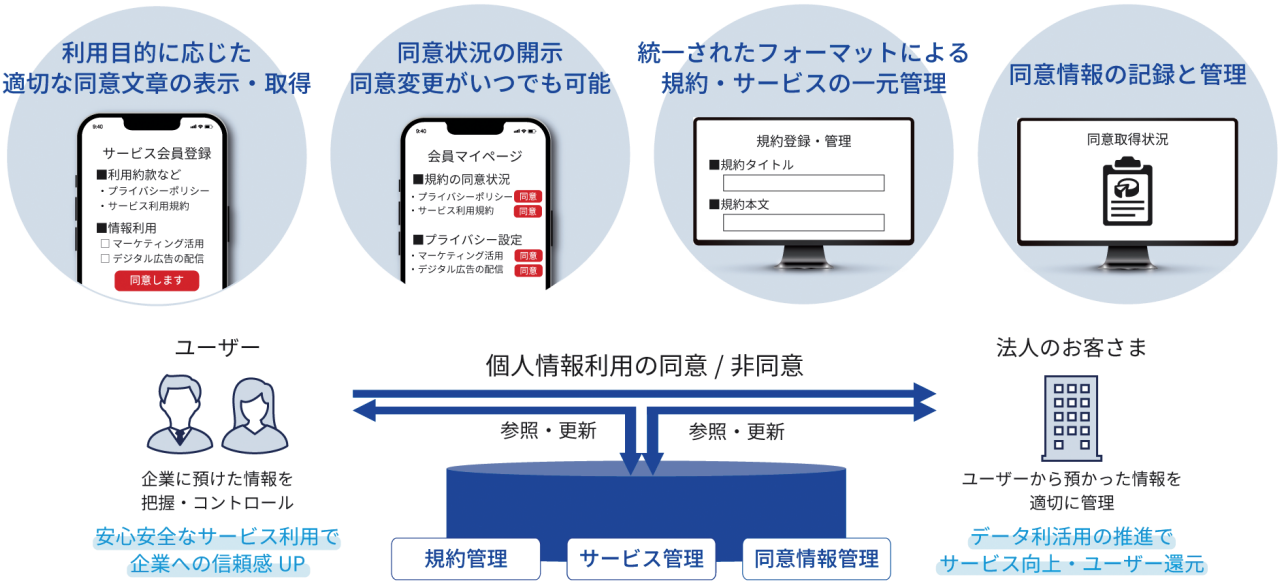


図8. KDDIが提供する同意管理機能（PPM）

（出典）KDDI株式会社資料

Wordで管理していた企業も多かったと思います。ここでPPMを使えば「どのバージョンでどこまでの同意を取れたか」をシステムで管理でき、新たにPIAが必要な部分もチェックしやすくなります。

同意の記録管理を一元化すると、必要なフィルターをかけてデータを利活用する、同意をいただいているお客さまだけデータを利活用するなども容易です。PPMはデータ利活用時の効率性向上と同時に安全性を高めてプライバシー侵害や情報漏えいを防げるのがメリットであり、われわれの社内でも活用しつつ他の法人のお客さまにもぜひこのメリットを享受いただきたいと思って提供しています。

**恩田：**こういったプライバシーガバナンスやリスクマネジメントは民間の自主的な取り組みによるものが多いように思いますが、法的な位置づけはどのようになるでしょうか。

**今村：**日本にはルールとして個人情報保護法がありますが、もう一つ重要な概念としてプライバシー保護があります。個人情報保護法は事業者が守るべき最低限のルールが定められているものであり、利用者のプライバシー保護のためには、事業者のさらなる配慮が求められるという構図になっています。

しかも「守るべきプライバシーの範囲」は一般的に拡大していると言われています（図9）。パーソナルデータに関する技術が進んだ結果、結果として使い方によってはそれを侵す技術にもなり得るからです。そこで事業者による法律範囲外の任意的な取り組みとして重要になってきているのがデータマッピングやPIAであり、これらを全部包含する概念がプライバシーガバナンスだと考えています。

先ほどご説明いただいた同意管理ツールなどはプライバシーガバナンスを技術面から後押しして、企業全体の価値を高めていくものです。さらにピンポイントで個人が「何に同意したのか」を管理できるまでになれば、企業が個人に対する説明責任を尽くすツールになり得ます。社会から、パーソナルデータを利活用するサービスや技術の受容性を高めるという目的においても、PETsやプライバシーテックは効果的にワークすると理解しています。

医療分野などで発展してきたELSI（Ethical, Legal and Social Issues／倫理的・法的・社会的課題）という概念があり、法律面だけでなく、ソーシャルとエシカルの部分から社会との接点を検討することが重要だと示している枠組みがあります（図10）。PETsやプライバシーテックにも重ねて考えることができると思います。大多数の一般消費者からすると、おそらくPETsやプライバシーテックについて、

- 法律の規制はもちろん重要です。しかし、当該対応のみではプライバシーの問題としてリスクとなる場合があります。
- イノベーション（技術革新）と比例してプライバシー保護の観点で考慮すべき範囲（プライバシー問題）が拡大しています（プライバシーは取り扱う情報や技術、取り巻く環境によって変化）。
- プライバシー問題全体を考えられる体制や消費者やステークホルダーへの配慮が必要です。
- プライバシー保護の範囲拡大に伴い法改正により規制範囲も拡大傾向にあります。

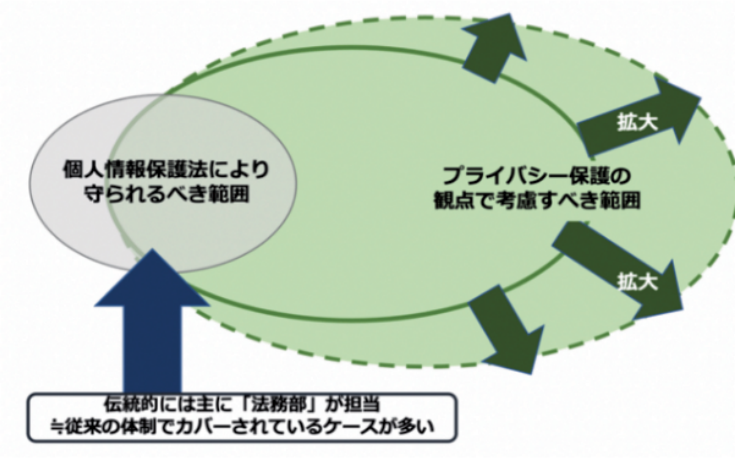


図9.　個人情報保護法とプライバシー保護の適用範囲

（出典）弁護士　今村　敏氏作成資料

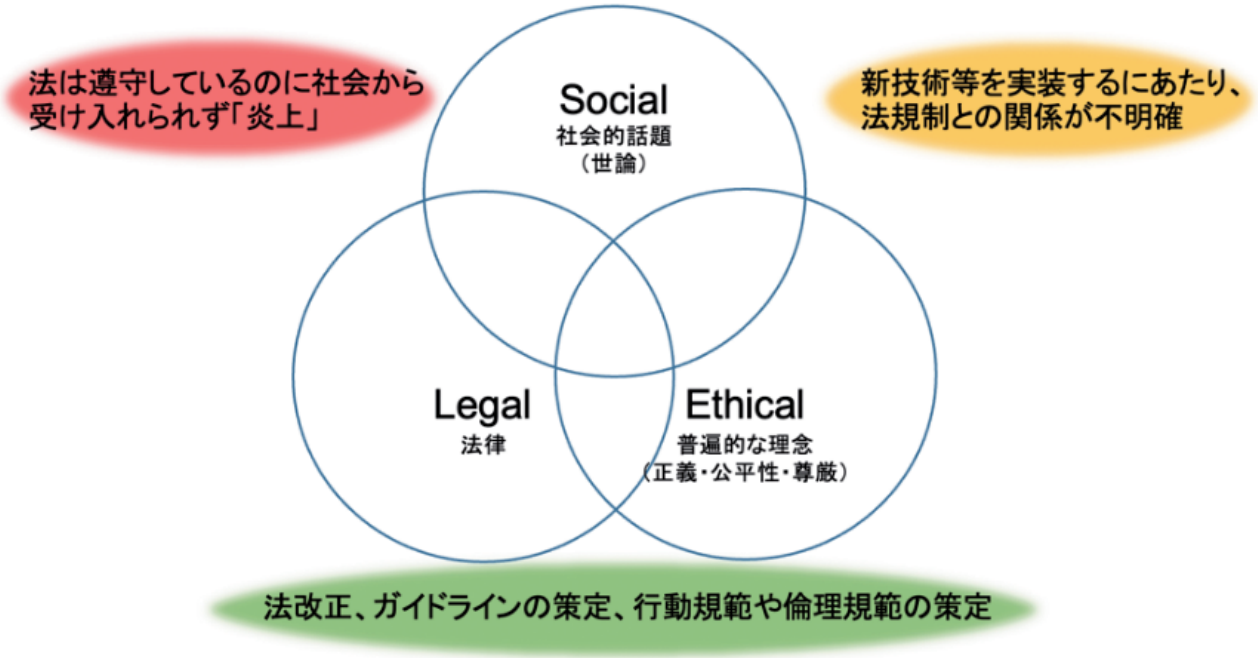


図10.　ELSI（Ethical, Legal and Social Issues／倫理的・法的・社会的課題）

（出典）弁護士　今村　敏作氏成資料

まだよく分からないので不安といった認識なのではないでしょうか。今は、ソーシャルとの関係からPETsやプライバシーテックについて丁寧に説明し、理解を得ていくことが重要なステージなのかなと思います。

また、プライバシー保護の実現には、人材・技術・ガバナンスの3要素が欠かせません（図11）。PETsやプライバシーテックは技術であり、場合によってはガバナンスをさらに高めるものとしてもワークします。人材教育に直接関係するものはまだないかもしれませんが、各従業員のプライバシー意識を高める技術が出てくれば広い意味でPETsやプライバシーテックに当てはまるでしょう。技術がさらに進化して3要素を牽引し、プライバシー保護を実現する未来を期待しています。

**Q　利用者情報保護やプライバシー保護に関して、新しい技術が日々生まれる中で企業はどのように向き合い、何をしていけば良いのか。**

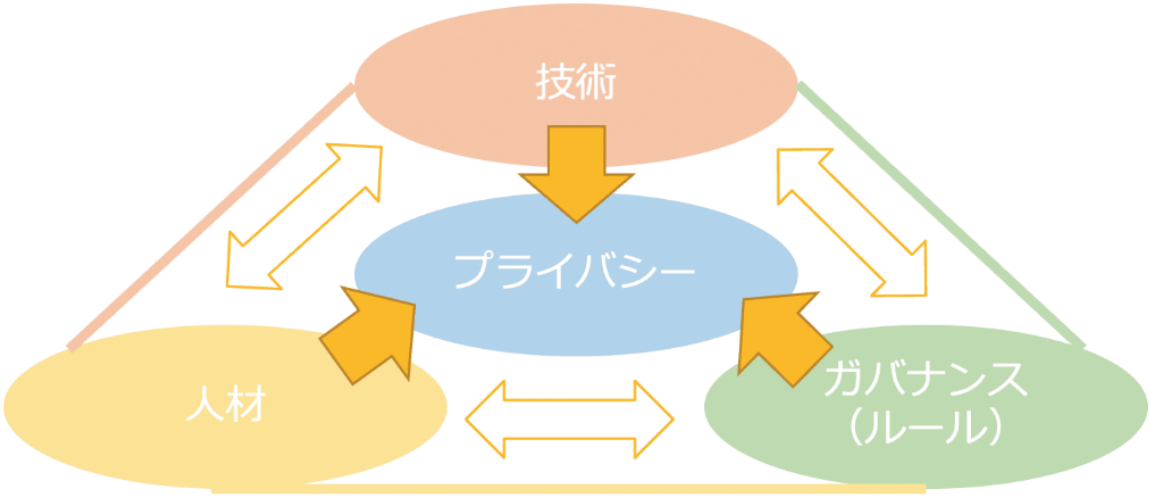


図11．プライバシー保護実現に向けた企業の取り組み（ルール、人材、技術の関係性）

（出典）弁護士　今村　敏氏作成資料

## プライバシー保護の実現にむけて

**恩田：**これまでのPETsやプライバシーテックの議論を踏まえて、今後どのようなことが必要かお聞かせください。

**竹之内：**DX全般で言えることですが、技術者だけが頑張ってもダメで、むしろ技術畑ではない人の方が相当な工数をかけることが重要と考えています。データクリーンルームの活用でも、データを連携したビジネスを考える方が技術より難しい。とはいえ技術を知らないとビジネスの検討も進みません。

より良い結果を得るために、技術を知っている人は新規事業担当者などの専門外の人へ、PETsやプライバシーテックについて分かりやすく説明する努力をもっとすべきだと感じています。どちらも一緒に取り組むという意味で、総力戦だと思います。海外のビッグテックはそれを実現していると感じています。

また、グローバルのトレンドにも注目する必要があります。例えば、先ほど述べた秘密計算方式のうちTEEという技術が近年驚異的に伸びました。昔は秘密計算というと「遅い」という印象がありましたが、今はTEE方式であればAIの処理も高速で可能です。2024年6月にAppleがTEEを使った生成AIの処理を始めると発表して潮流の変化は決定的になりました。この遅れをどう日本が取り戻すかという点に、危機感を感じています。この分野において、ガバナンス・ルール・人材・技術・法律など全部を合わせた総力戦が日本には必要だと思っています。

**今村：**現実にはいろいろなことが起こっていて、「データ分析・解析のためにデータセンターでものすごい計算を行っている」という世界だけではもうなくて、グローバルのテック企業においては、スマートフォンのような端末レイヤーである程度処理し、秘匿化されたデータだけをテック企業が取り扱うような形になっていて、消費者に対してはプライバシー保護に配慮していると上手に説明をしている気がします。

海外では企業がPETsやプライバシーテックを使いながら情報を守っていることを武器にして、それをブランド価値・マーケティング価値として表しています。日本の企業はやはりまだうまくできていない印象です。

クライアントプライバシーを安全に守りつつデータで価値を出していく取り組みについて、きちんと説明する企業が増えていくと消費者の見方も変わり

ます。そうすると消費者もプライバシー情報やセキュリティを守ってくれる企業に対して、データを預けよう、サービスを使おうとなってくると思います。好循環が生まれれば技術的な取り組みも盛り上がり、国際的な競争力も増すと思います。

**竹之内：**今の観点は非常に重要で、一般消費者はプライバシーを守ってくれる企業かどうかを非常に気にしているんですよね。「同じサービスだったら、よりプライバシーを守ってくれるところがいい」と評価しています。[2]

**今村：**そのデータ連携においてやはり同意がベースになりますが、その同意自体をお客さまがきちんと見ているのかというところは課題です。同意してデータをコピーされて自分のデータがどんどん流通してしまうのではなく、PETsやプライバシーテックによって必ずしも同意のみに依存しないデータ連携による価値創出の手法がもう少し広まる方が健全なのかなと、個人として思うところはあります。

**木村：**グローバルではずっと「同意疲れ」というのが言われていて、チェックはしていても何にチェックをしているのか消費者は何も理解していないことがあります。単に同意云々で、事業者側がデータを使うやり方には限界が来ています。そうではない方法で、消費者の理解をどう得ていくのか、その一つの解決策としてPETsやプライバシーテックがあり得ると思います。そこをうまく社会に認めてもらうことが重要だと思います。

**竹之内：**昔はプライバシー保護というと企業からするとコストの感覚で、最低限は守るがそれ以上はやらなくていい、コストをいかに抑えてプライバシーを守るかという視点が強かったかと思います。先ほど今村先生がブランドとおっしゃったとおり、プライバシーを守ることによって利益が上がるという欧米企業の発想を参照しつつ、そういう世界をもっと広げられたらと思っています。

**今村：**社内でデータを使うときも、至るところでPETsやプライバシーテックを使える部分がありそうです。現在はデータを扱える人や場所を限定したり、監視カメラを設置したりと組織的、物理的な対応をすることがありますが、PETsやプライバシーテックを使って安全にデータを活用できるケースが広がってくる可能性があります。そうすると、PETsやプライバシーテックの見方も変わってくるのではないかと思いました。

**木村：**今までは機密性の高いデータについて、セキュリティルームを構築して一部の人しか触れられない管理体制にしていたものが、PETsやプライバシーテックを使うことで分析する人は生データに必ずしも触れずに済むし、より多くの人がそのデータを使って何らかの分析結果を出せるようになるかもしれません。

**竹之内：**物理的な安全管理措置だけではなく、PETsやプライバシーテックに対応したガイドラインや法制度があると変わっていくかなと思っています。一つ例を挙げると、秘密分散は個人情報保護法における「高度な暗号化」にあたらないという判断をされています。技術面から見ると暗号化したまま処理できるなど従来よりも安全とも考えられますが、法的な対応がないことで導入が進まない面もあります。技術の進展に合わせた法制度の適切な改正議論が必要だと思いますし、民間の技術の専門家の知見も必要なので、今後、官民で連携して国内でも検討が進めばと思います。

**木村：**PETsやプライバシーテックについては、技術を選定したときに他の企業や、社会に対して説明して理解していただけるかが重要だと思っていま

2 「プライバシーガバナンスに関する調査結果」（JIPDEC、2022年）
（https://www.meti.go.jp/policy/it_policy/privacy/privacy_governance_research_syosai_gaiyo2022.pdf）
「デジタル社会における消費者意識調査2023」（JIPDEC、2023年）
（https://www.jipdec.or.jp/archives/publications/tjvsos0000001lr5-att/J0005188.pdf）

す。技術的には差分プライバシーの方が、安全性が高く数学的に証明されていたとしても、k-匿名化の方が社会的に説明しやすいからそちらを使わざるを得ないというジレンマもあります。最終的にわれわれとしては、特に法律の壁のあるところは法律上説明できる方を選ぶという形です。技術的にはこちらの方がいいのに、と思いながら選んでいる場合もあるので、そこは変えたいですね。

**今村：**最近ガイドライン等でもやっと「k-匿名化」「ハッシュ化」などの技術ワードが載るようになりました。技術の出口が国内にない状態になってしまうと、能力を持つ人たちが海外に出ていき、自国の技術力低下につながってしまいます。しっかりと技術の出口を作っていくというのは重要になりますね。

**恩田：**皆さん今日は本当に貴重なお話をありがとうございました。

レポート

# データ越境移転の最新動向
## －インドで開催されたワークショップへの参加より－

JIPDEC　認定個人情報保護団体事務局　事務局長　奥原　早苗

2023年8月、インドの個人情報保護法、「デジタル個人データ保護法」（Digital Personal Data Protection Act, 2023：DPDPA）が成立しました。これまで、個人情報の保護に関する包括的な規律を擁した法制度がなかった[1]ため、施行の時期やDPDPAの詳細な規律としてどのような内容が盛り込まれるのか、規則の内容に注目が高まっており、現在、規則の最終決定とDPDPA施行に向けた準備が進められています。

インドは、BRICSおよび、近年目にするようになったグローバルサウスにおいても、その存在感は増す一方で、特にテクノロジー分野では、その成長スピードとスケールメリットを活かした技術革新には目を見張るものがあります。DPDPA成立に伴うニュースリリースや関連するセミナー等が数多く開催されていることからも、日本企業へのインパクトの大きさがうかがえます。

本年9月、インドでNational Association of Software and Services Companies[2]（全国ソフトウェア・サービス企業協会：nasscom）主催でグローバルCBPRシステム[3]に関するワークショップが開催されました。JIPDECも米国政府、個人情報保護委員会（PPC）を通じて招待を受け参加しましたので、本ワークショップで得られた情報をレポートします。

さて、JIPDECは個人データの越境移転に関する国際的な認証制度「CBPRシステム」の日本の審査機関であり、「CBPRシステム」はこれまでAPECの制度として運用されていました。その後、より広範囲での個人データの円滑な越境移転を目的として2022年4月に設立されたグローバルCBPRフォーラムからも審査機関として認定（2024年4月30日）を受けました[4]。

グローバルCBPRフォーラムが開催する年2回のワークショップ[5]のうち、今年1回目が5月に東京で開催され、2回目は11月に台北で開催されます。今回インドで開催されたイベントは、このグローバルCBPRフォーラムが開催するワークショップとは異なり、インド政府とnasscomがDPDPAの成立を踏まえ、よりスムーズなデータの越境移転の可能性を探るべく、CBPRの枠組みを深く理解し、今後どのように進化していけるのかを知ることを目的として開催されたものです。

◆開催概要◆

1. 件名：グローバルCBPRフォーラム テクニカル

1　現行法は、IT法（Information Technology Act, 2000）とIT法の具体的要件を定めたIT規則があります。
2　1988年に設立され、現在会員社数が3,000を超える非営利団体。テクノロジー分野におけるさまざまな取り組み（DeepTech | nasscom）を行っています。加盟企業は、大規模なネットワークを通じた労働力のスキルアップやイノベーションの促進、政府への政策提言に寄与する等の活動を行っており、2025年までに10,000社の加盟を目指しています。
3　当協会がAA（審査機関）を務める国際的な個人データの越境移転の枠組み。
「CBPRシステムとは」（JIPDEC）　https://www.jipdec.or.jp/project/cbpr.html
4　Global CBPR Forum Announces the Establishment of the Global CBPR and Global PRP Systems and Welcomes New Global CAPE Participants（Global CBPR Forum）
https://www.globalcbpr.org/global-cbpr-forum-announces-the-establishment-of-the-global-cbpr-and-global-prp-systems-and-welcomes-new-global-cape-participants/
5　前日には英国大使館でサイドイベントが開催されました。

ワークショップ

2. 日時：2024年9月19日～9月21日
3. 場所：JW Marriot Aero city, New Delhi, India
4. 共催：nasscom、インド データセキュリティ協議会（Data Security Council of India：DSCI）、インド電子情報技術省（Ministry of Electronics and Information Technology：MeitY）、インド外務省（Ministry of External Affairs：MEA）

ワークショップの参加者は、政府機関、規制当局、インドのテクノロジー分野の企業や団体、CBPR認証制度のアカウンタビリティ・エージェント（以下：AA）、CBPR認証取得企業、研究機関等で構成され、活発な議論が展開されました。最終日は、政府機関のみが参加し、今後の展開を話し合うものでしたが、最終日の会合にもご招待を受け、参加しました。また、ランチ、ディナー共にネットワークを目的としてフルカバーされていたため、大変有意義な3日間となりました。

初日は、インド情報技術省による基調講演が行われ、直近にデリーで開催されたCBPRの小規模なワークショップで、CBPRのフレームワークと役割について洞察が深められたこと、国際的なプライバシー法の複雑さと、特に中小企業や振興企業にとってコンプライアンス知識が必要であり、それらがテクノロジーを推進する上で足かせになってはいけないことなどが示されました。

その後の議論では、法域が異なる国や地域の個人情報保護に関する法律がもたらす課題が話し合われ、データ保護の枠組みとしてOECD原則に基づくデータ保護とプライバシーを確保するためのグローバルな枠組みの必要性が話し合われました。

私は初日のセッションで、新たなCBPR認証制度参加国におけるAAの設立について、シンガポール、米国、台湾のパネリストと共に登壇し、認証制度の申請を検討される企業の皆さまに対し、審査機関の成り立ちと申請によるメリット・デメリットを紹介しました。政府系の審査機関は審査料を無料にしたり、中小企業への認証取得に向けたカウンセリングや審査料の援助等を実施しています。しかし、残念ながら日本は米国と同様、非営利ではあるものの民間組織となるため、新しい制度の創成期に認知度を高めるために有効な手段となる審査料の無償化等の思い切った施策を打つことができず難しい側面があります。他方、フェーズが変われば有料化の検討が必要となります。

また、CBPR認証制度の運用において、審査機関と所管官庁との密接な連携も重要な要素として欠かせません。日本は、経済産業省、PPCが両輪でこの制度を推進していくことになりますので、JIPDEC



左からモデレーターCIPL、シンガポールIMDA、日本JIPDEC、台湾III、米国TrustArc

は、日本の審査機関として連携を深め、認証制度の拡大と信頼性の向上に向けて取り組んでいきたいと考えています。

3日目は、前日のワークショップに参加できなかったDPDPAに直接携わっている部門や規則を策定するプロセスに関わっている部門など、さまざまな政府機関関係者が多く参加し、CBPR認証制度と国内法の執行関係をどう整合させるのか、審査機関の設立と連携等について意見が出されました。

もし、インドがアソシエイトとして英国と同様にグローバルCBPRフォーラムに参加した場合、日本のみならず世界的に与える影響は大きいものと考えられます。2023年1月に経済産業省で開催された日米共催のグローバルCBPRワークショップでは、英国がアソシエイトとして参加予定[6]であるという報告を受けて、コモンウェルス[7]の動向について質問が寄せられました。これは、コモンウェルスを構成する56か国のうち、国家元首をチャールズ3世国王陛下としているカナダ、オーストラリア等のCBPR参加国以外の国々がCBPRシステムに参加する可能性を期待されての発言だと思われます。同様に、インドがアソシエイトとして参加する可能性が高まれば、グローバルサウスの国や地域に対するインパクトは計り知れません。

インドがアソシエイトに参加するだけでも、例えばnasscomに加盟する30,000の企業や団体（大手のグローバル企業を含む）がCBPR認証に興味を持つきっかけとなり、個人データの越境移転における通商パスポートとして、グローバルサウスにおけるCBPR認証制度の拡大に、大きな一石を投じることになるのではないでしょうか。当然、世界の注目を集める市場であるインドで事業展開を検討している日本企業も今後広がりを見せることが考えられます。

インドで認証を受けた個社、またはグループ認証[8]として日本法人を含む複数の認証を取得したインドのグローバルテック企業の増加は、CBPR認証が逆輸入される形でその認知度が高まることも可能性としては否めません。現在も、CBPRの認証取得企業数は十分とは言えないものの、Apple、IBM、Mastercard、CISCO、Salesforce等、日本では誰もが知っているであろう名だたる企業が取得しています。それらのグループ会社も含めれば、2,000社を超える企業が認証を取得しており、私達の身近にCBPR認証取得企業が多数存在しているのです（日本の認証企業は4社）。


情報化、グローバル化は今後も加速が予想され、異なる複数の法域間で個人データの移転が行われることは必須であり、現在、国や地域、企業規模を問わず企業が苦慮している膨大な法務コストや労力等に対し、CBPRシステムのような越境移転制度が多くの国や地域、そして事業者の皆さまに活用していただけることを願っています。そのためにも、私たちは現行制度の見直しや申請に伴うハードルを軽減する努力を継続していくことが求められるでしょう。そして、インドで事業を既に展開している、または今後展開を予定している日本企業は、今後リリースが予定されているDPDPA規則の内容に沿って対応の準備が必要となりますので、引き続き動向をウォッチしながら、早めに対策を講じることが肝要です。

6　2023年1月のワークショップ開催時点では、まだ正式に参加が認められていませんでした。その後、2023年7月に英国がアソシエイトとして正式に参加しました。
7　The Commonwealth of Nations：英連邦　56の主権国家からなる自発的な連合体で、27億人の市民が暮らしています。
8　グループ認証は、本稿作成時点で米国とシンガポールのみが実施しており、日本、韓国、台湾では個社単位での認証となりますが、過去に開催されたCBPRの普及セミナーや事業者ヒアリング等では、グループ認証を要望する声も少なくありません。

# あなたのメッセージ、安全に確実に届いていますか？
# ～通信のセキュリティとデータのセキュリティ～

JIPDEC　デジタルトラスト評価センター　副センター長　**米谷　嘉朗**

## はじめに

私たちは日々、スマホやパソコンのアプリを通じてネット上のさまざまなオンラインサービスを利用しています。SNSで近況を知らせたり、フリマアプリで買い物をしたり、生成AIに調べものをしてもらったり、動画や音楽を楽しんだりしていますよね。スマホなどは、ネットがなければただの箱と言っても過言ではないでしょう。

ところで皆さんは、ネットを通じて知人とコミュニケーションをとったり、オンラインサービスを利用している際に相手が本物かどうか、やり取りをしているメッセージが盗み見られたり書き換えられたりしていないか、気にすることはあるでしょうか。おそらく、過去に「本サービスでは通信が暗号化されており安全です」や、「本サービスでは個人情報を適切に取り扱っており安心です」といった表示を見て、安全安心だと理解しているので気にすることはまずないでしょう。もちろん、オンラインサービス提供者も皆さんの安全安心のために最大限の努力をしており、常に疑いの目を向ける必要はありませんが、その仕組みを少しでも知っていれば、ふと不安を感じたときに原因を探る伝手になります。

本レポートでは、オンラインサービス提供者ではなく、皆さんとオンラインサービス提供者の間にあるネットワークや、皆さんが知人やオンラインサービス提供者とやり取りするメッセージが、途中で第三者に盗み見られたり書き換えられたりする可能性は皆無ではないということ、それがどのような場所で起こり得るのかということ、対策としてどのようなことに気を付けたらよいかということを簡単に説明します。

以降、スマホやパソコン上に記録されている情報を「データ」、ネットワークを通じて誰かと交換されるデータを「メッセージ」、安全安心を「セキュリティ」と表現します。また、メッセージを盗み見られないためのセキュリティ技術としては暗号化を、メッセージの作成者を特定し書き換えを見破るためのセキュリティ技術としては電子署名を前提とします。前提からそれる場合は、その都度補足します。

## 通信のセキュリティ

まず、ここでの通信とは、皆さんが使用するアプリとそのアプリがメッセージを交換するオンラインサービスのサーバーを接続する機器とネットワークのことを意味します。Wi-Fiやモバイルはネットワークですし、Wi-Fiルータやセットトップボックスは機器です。アプリとサーバーの間には、運営者が異なる複数のネットワークが相互に接続しており、それぞれのネットワーク内には複数の機器が存在しています。つまり、メッセージを届ける通信は、途中にたくさんのネットワークと機器があって成り立っているのです。

たくさんのネットワークと機器があるので、そこに悪意を持った第三者が存在しない保証はありません。悪意の第三者は、皆さんの個人情報や資産管理情報を盗んだり、知人やオンラインサービス提供者になりすまして偽メッセージを届けたりします。通信では、暗号化によって、アプリとサーバーのみに意味のあるメッセージの交換を可能とします（図1）。

ほとんどのオンラインサービスは、Webを利用しています。Webでは、TLS（トランスポート・レイヤ・セキュリティ）という仕組みを使用することで、通信の暗号化が可能です[1]。現在では、90%以上

1　Web以外の標準的な通信暗号化の仕組みとしてIPsecやSSHなどがありますが、本レポートでは説明の対象外とします。また、Webの通信暗号化の仕組みとしてTLSと並んでQUICが普及し始めていますが、同様の技術であるため、本レポートではTLSにまとめています。
解説「SSL/TLSサーバ証明書とは」（JIPDEC）　https://www.jipdec.or.jp/library/report/ssl_cert.html

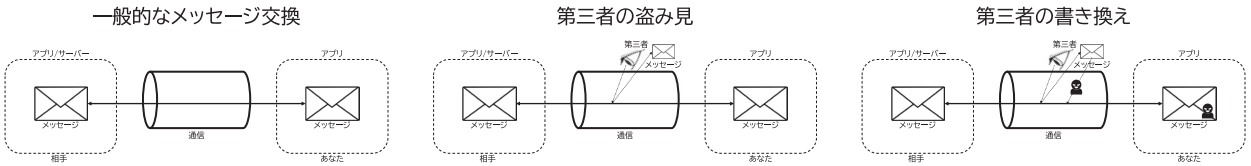


図1.　一般的なメッセージ交換と盗み見・書き換えのイメージ

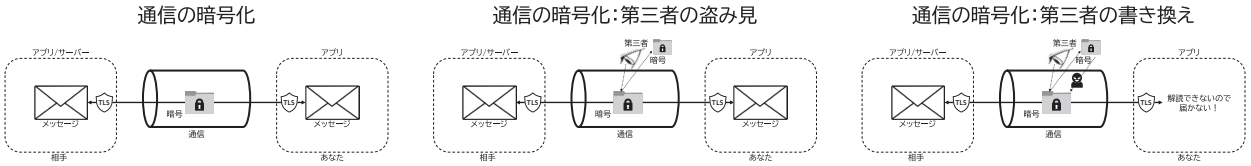


図2.　通信の暗号化と盗み見・書き換えのイメージ

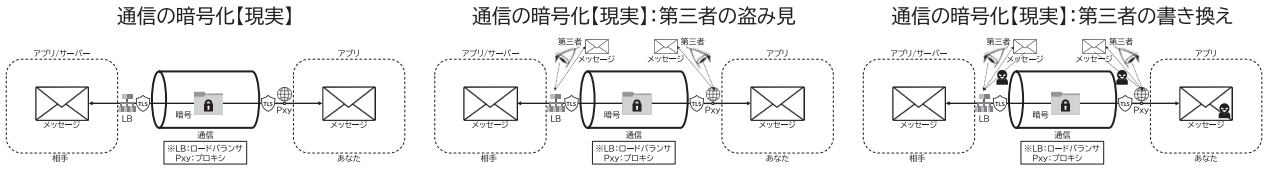


図3.　通信の暗号化と盗み見・書き換えのイメージ【現実】

のWebサイトがTLSを使用していると言われており、TLSを使用していないWebサイトへのアクセスはWebブラウザが警告を出すようになっています。これにより、皆さんは意識する必要もなく悪意の第三者から守られています（図2）。

とはいえ、この世の中に100%確実なことなどありません。前述のとおり、通信には途中に複数の機器が存在しており、中にはTLSの暗号化をいったん終結し、メッセージの内容を確認して通信先を振り替える機能を持ったWebプロキシやロードバランサーが設置されていることがあります。多くの場合、Webプロキシはアプリの近くに、ロードバランサーはサーバーの近くに設置されます。いずれもネットワーク管理者がセキュリティや安定性のために設置するものですが、機器操作が可能な作業員の中に悪意の第三者が紛れ込む（あるいは作業員が事故を起こす）可能性は、残念ながら皆無ではありません。オンラインサービスで機微な事項を含むメッセージを交換する際は、できるだけ事前にTLSのサーバー証明書を確認するようにしてください[2]（図3）。

スノーデン事件（2013年）以降、機器操作者やサーバー操作者によるメッセージの盗み見や書き換えから守るために、アプリとアプリの間でメッセージを暗号化するE2EE（エンドツーエンド暗号化）という仕組みに対応したメッセージングアプリが増えてきています。知人と機微な事柄を含むメッセージを交換する際は、E2EEに対応したメッセージングアプリの活用を検討してください（図4）。

## データのセキュリティ

まず、ここでのデータのセキュリティとは皆さんが通信手段によらずに、自分の作成したデータを第

2　サーバー証明書の確認方法や、確認する際の注意点は、フィッシング対策協議会などのドキュメントを参照してください。
Webサイトのサーバー証明書種類の確認方法（2022/09/06）（フィッシング対策協議会）
https://www.antiphishing.jp/report/wg/certificate_checker_20220906.html

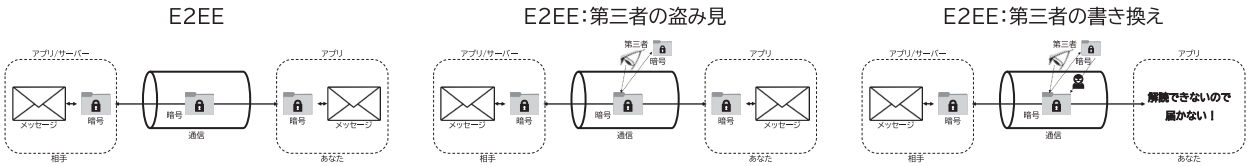


図4. E2EEと盗み見・書き換えのイメージ

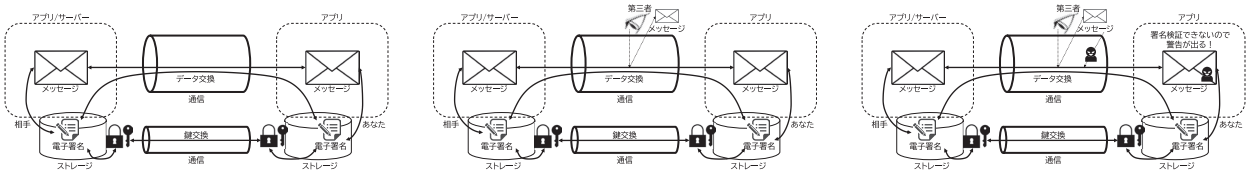


図5. データ署名と盗み見・書き換えのイメージ

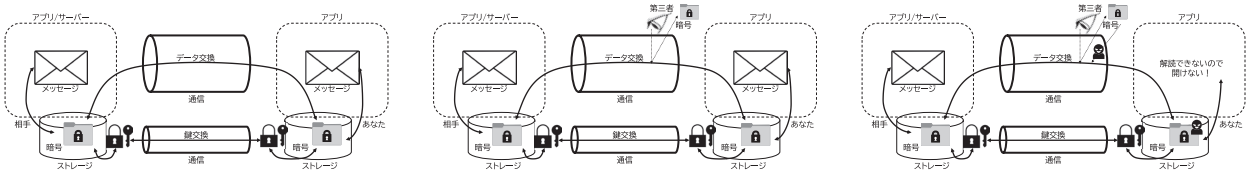


図6. データ暗号化と盗み見・書き換えのイメージ

三者に盗み見られたり書き換えられたりせずに、知人やオンラインサービスと共有できることを意味します。知人には、将来の自分自身も含みます。

フィッシングメールで届けられるWebサイトは、ほぼ100%がTLSを使用していると言われており、そのことから、通信のセキュリティが守られていることと、交換されたメッセージの内容が信頼できることは別の事象であることが分かります。データのセキュリティは、通信のセキュリティだけでは実現できないのです。

データの作成者が皆さんの意図した知人やオンラインサービスであることを確認するためには、データと対になる電子署名[3]を検証する必要があります。検証は複雑で難解な作業ですが、電子署名に電子証明書が使用されていれば、広く普及しているアプリが利用できるため、皆さんの負荷が軽減されます。迷惑メール対策技術であるDKIM・DMARC・BIMIは、電子証明書に相当する情報がドメイン名システム（DNS）で公開された電子署名を使用していますので、メールアプリが自動的に検証し、結果を皆さんに表示してくれます[4]。

電子署名を検証することで、データが書き換えられているかどうかも同時に確認できます。見方を変えると、電子署名があっても検証しなければデータのセキュリティとは無関係です（図5）。

データを盗み見られたり、不特定多数の人に開示されないためには暗号化が必要です。暗号は、自分と共有相手のみが知っている秘密情報（鍵）によって生成されますので、暗号化されたデータが鍵を持たない第三者に渡っても、内容を盗み見られること

3 オンラインサービスによる電子署名には、eシールも含みます。eシールについてはITレポートコラムも参照してください。「eシール」とは～「シール」本来の意味を入り口に～（JIPDEC）
https://www.jipdec.or.jp/library/itreport/2024itreport_spring06.html

4 DKIM・DMARC・BIMIの電子署名は組織に紐づくものであり、データ作成者個人のものではありませんので、メールを送信した組織を特定することはできますが、データ作成者を個人的に特定することはできません。作成者を特定するためには、S/MIMEを併用する必要があります。

はありません。鍵を適切に選ぶことでデータの共有相手を限定することができるのです（図6）。

問題は、どうやって相手と安全安心に鍵を交換するかです。鍵もデータですから、鶏と卵問題です。この問題は、電子署名や暗号化に使用する電子証明書の交換と置き換えることで、皆さんの手間を軽減することができます。電子証明書は、特定少数の認証局と呼ばれる組織の電子証明書（ルート証明書、もしくはルート証明書で署名された中間証明書）で署名されていますので、完全に信頼できる特定少数のルート証明書を持っていれば、連鎖的に検証しながら交換できます[5]。当然ですが、電子証明書の交換は通信なので、通信のセキュリティによって守られる必要があります。他にも、E2EEに対応したメッセージングアプリを使用することで、鍵交換の手間を軽減することが可能です。

## おわりに

通信のセキュリティとデータのセキュリティは別の事象であり、通信のセキュリティだけではデータのセキュリティを得ることができないこと、データのセキュリティを得るために必要な鍵の交換には通信のセキュリティが必要なことを説明しました。どちらか一方だけあればよいというものではありません。双方をバランスよく利用し、あなたのメッセージを安全に確実に、意図する相手に届けてください。

5　通常、ルート証明書は、パソコンやスマホのベンダー、およびWebブラウザベンダーによる厳格な審査に基づいて、OSおよびWebブラウザに事前保持されていますので、皆さんがどこかから手に入れる必要はありません。

コラム

# DXと労働生産性

JIPDEC　電子情報利活用研究部　調査研究グループ　グループリーダ　**松下　尚史**

少子高齢化が進み、生産年齢人口は1997年の8,699万人をピークに2023年には1,303万人減少して7,396万人となっています。また、働き方改革や非正規雇用者比率の上昇なども影響し、雇用者の労働時間も年間1,912時間（1995年度）から1,658時間（2022年度）まで減少しています。このような状況において、企業や自治体はデータやデジタルツールを活用した労働生産性の向上を目的としてDXを推進してきたことから、労働生産性はDXの成果を図る一つの指標として考えることができます。

よく耳にする労働生産性には二つの概念があります。一つは付加価値額（マクロ経済的には名目GDP、企業としては少々語弊がありますが売上総利益）を労働投入量（雇用者数×労働時間）で割り、一人の雇用者が1時間でいくら稼ぐのかを測る数値で、これを付加価値労働生産性と言います。もう一つは、生産量（マクロ経済的には実質GDP、企業としては契約件数・販売台数・生産台数など）を同じく労働投入量で割り、一人の雇用者が1時間でどの程度の生産量を実現できるのかを測る数値で、これを物的労働生産性と言います。「日本の労働生産性は低い」と言われる時は、主に付加価値労働生産性のことを指します。図1を見ていただけると分かりますが、日本の付加価値労働生産性は2000年以降ほぼ横ばいで推移しており、OECD主要7か国の中でも最下位です。ところが、物的労働生産性を見

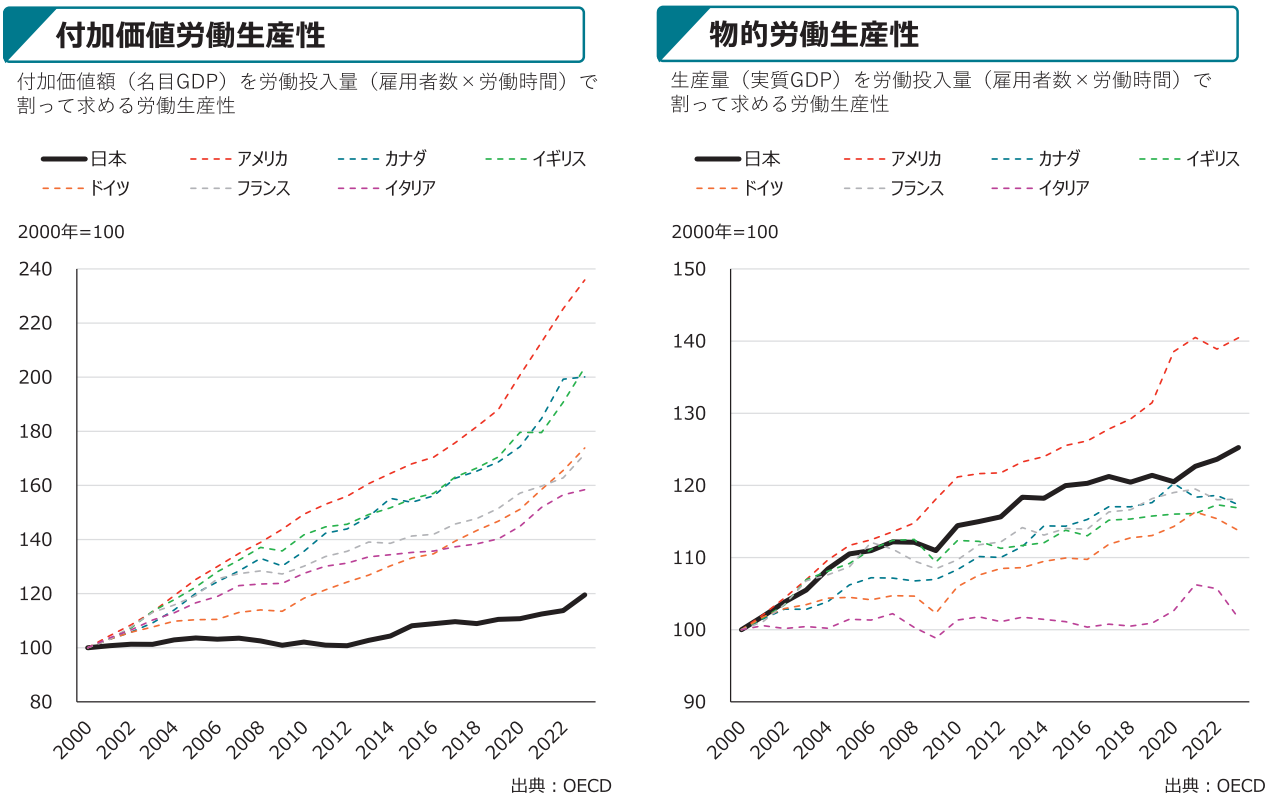


図1．付加価値労働生産性と物的労働生産性の国際比較

てみると、アメリカには負けるもののOECD主要7か国の中で2位になっています。

このような結果につながる要因は何かと、さまざまなDXに関するアンケート調査等を見てみると物的労働生産性のみが上昇した背景が見えてきます。例えば、当協会と株式会社アイ・ティ・アールが企業を対象に実施した「企業IT利活用動向調査2024」の結果では、日本のDXに関する取り組みは業務効率化などの生産量を高める内向きのDXが中心になっています（図2）[1]。つまり、経済産業省の定義[2]では「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること[3]」となっていますが、業務そのものの変革には取り組んでいても、競争上の優位性を確立するところまでは至っていないのではないかと推察されます。また、自治体のDX推進においても、総務省が「自らが担う行政サービスについて、デジタル技術やデータを活用して、住民の利便性を向上させるとともに、デジタル技術やAI等の活用により業務効率化を図り、人的資源を行政サービスの更なる向上に繋げていく[4]」ことが求められると示していることから、職員数が減少していく中において一人ひとりの職員がより多くの業務を捌くという意味で生産量を高める取り組みが中心になっているのではないかと考えられます。このように企業も自治体も生産量を高める物的労働生産性向上の取り組みを中心に行っており、図1の国際比較にもそのような取り組みの結果が表れたのではないかと考えられます。

国際比較の結果が示すように、わが国に足りないのは付加価値労働生産性を向上させることです。DXへの取り組みを通じて競争上の優位性を確立し、付加価値向上を実現するためには、社内的な取り組みから社外に目を向けた取り組みも必要な時期になっているのではないでしょうか。

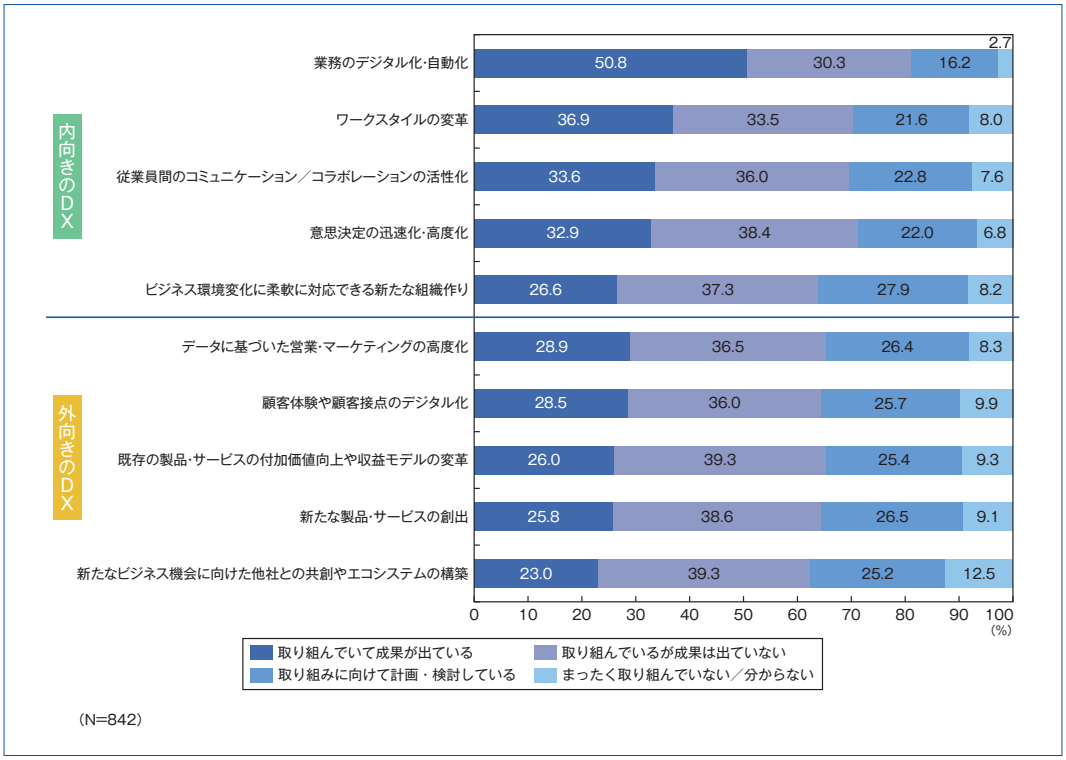


図2.　DXの取り組み内容と成果の状況

（出典）JIPDEC／ITR「企業IT利活用動向調査2024」

1　JIPDEC IT-Report 2024 Spring（JIPDEC）　https://www.jipdec.or.jp/library/itreport/2024itreport_spring.html
2.3　「デジタルガバナンス・コード3.0～DX経営による企業価値向上に向けて～」を策定しました（経済産業省）
　　https://www.meti.go.jp/press/2024/09/20240919001/20240919001.html
4　自治体DXの推進（総務省）　https://www.soumu.go.jp/denshijiti/index_00001.html

# メタバースにおけるアイデンティティ

JIPDEC　電子情報利活用研究部　主査　**石井　美穂**

メタバースは仮想空間において、さまざまな経済活動や体験、そしてコミュニケーションを行うことに加え、ユーザーの自己表現をも可能とするプラットフォームとして、物理的な制約を超えた新たなデジタル世界です。ユーザーは、アバターを用いて、現実空間における自己を仮想空間に投影することも、現実空間とは異なる外見や性別などキャラクターを自由に設定することによって自己を表現することも可能です。メタバースにおいて、ユーザーは現実空間における物理的な制約から解放されるだけではなく、アバターを通じて性別や年齢、身体的な特徴等に縛られない新たな自己像を作り上げることができます。そのため、メタバースは、個人が自己をどう認識し（自己同一性）、社会的にどのように認識されるかを示す多面的な概念であるアイデンティティに関して論点を提示すると共に、大きな示唆を与えてくれます。

メタバースにおけるアイデンティティについて、アバター、その中でも特に「バ美肉（ばびにく）」に着目して整理します。バ美肉とは、バーチャル美少女（セルフ）受肉の略語で、仮想空間上で美少女のアバターを使用し、現実とは異なるキャラクターとして振る舞うことを指します。メタバースにおいて、自由な自己表現が可能であることの象徴であると同時に、バ美肉を通じてアイデンティティに関する課題が浮き彫りになります。

アイデンティティは、個人が自己をどのように認識しているかという「内面的な」側面だけではなく、それが他者や社会にどのように認識されているかといった「社会的な」側面も含めて確立されるものであるとされています。現実空間においては、物理的な制限、例えば、生まれもった容姿や性別、そして社会的な役割を通じて、第三者や社会に認識され確立されます。一方で、メタバースのような仮想空間におけるアイデンティティは、個人が自己をどのように認識しているかを反映させたアバターによって、第三者や社会（メタバースにおけるコミュニティ）に認識されることが可能となります。そして、そのアイデンティティは所属するコミュニティやコンテキストに応じて、使い分けることも可能です。これはつまり、メタバースにおいては「なりたい自分」をユーザー自らがデザインすることで、本来的な自己表現や自己実現が可能となるということを意味します。メタバースのアイデンティティは、個人が物理的・社会的な制約にとらわれずに、自己の認識を反映させてアイデンティティを自由に表現することができるという点で、個人のアイデンティティの確立において望ましいといえるでしょう。同時に、現実空間と仮想空間のアイデンティティの境界という点では新たな課題が生じます。そのため、今後メタバースのような仮想空間における活動が普及することが予想される中で、デジタル・アイデンティティの課題や在り方について、継続的に検討していきたいと思います。

# 個人情報保護法のいわゆる3年ごと見直しについて

JIPDEC　電子情報利活用研究部　主幹　**恩田　さくら**

個人情報の保護に関する法律（個人情報保護法）は、2003年に制定された後、2015年、2020年、2021年と改正が行われてきました。個人情報保護委員会（以下：PPC）は、2023年から、関係団体や有識者からのヒアリングを実施する等、いわゆる3年ごと見直しに係る検討を開始しています。

2024年6月に「個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理」として、PPCの考え方がまとめられました[1]。中間整理において提示された主な論点をいくつかご紹介します。

## 要保護性の高い個人情報の取り扱いについて（生体データ）

現行法では、身体の特徴のいずれかを電子計算機の用に供するために変換した符号のうち、本人を認証することができるようにしたものは、個人識別符号に該当するとして規律がされていますが、生体データであることに着目した特別の規律は定められていません。一方で、諸外国に目を向けると、生体データがセンシティブデータに該当するとし、原則、本人同意の取得を要求する例などが見られます。生体データは、長期にわたり特定の個人を追跡することに利用できる等、個人の権利利益に与える提供が大きいことなどから、実効性のある規律を設けることを検討する必要があるとされています。

## こどもの個人情報等に関する規律の在り方

現行法では、こどもの個人情報の取り扱い等に係る明文の規定は基本的にありません。海外の法制度においては、こどもの個人情報等をセンシティブデータに分類して特別な規律の対象としたり、こどもの個人情報等に特有の規律を設けるなど、こどもの個人情報等に関する規律が存在しています。こどもの脆弱性・敏感性およびこれらに基づく要保護性を考慮するとともに、データの有用性も考慮する必要があるとされています。こどもの権利利益の保護との観点から規律の在り方の検討を深める必要があるとされています。

## 個人の権利救済の手段と在り方

法の規程に違反する個人情報の取り扱いに対する抑止力を強化し、本人に生じた被害の回復の実効性を高めるとの観点から、団体による差止請求制度や被害回復制度の枠組みは有効な選択肢となり得ます。PPCが実施したヒアリングにおいては、その導入について反対もあったため、導入の必要性を含めて多角的な検討を行っていく必要があるとされています。

## 実効性のある監視監督の在り方

国内では、独占禁止法を始め、金融商品取引法、公認会計士法等に課徴金制度が導入されています。これまでの法改正においても課徴金に関する議論がされてきているところではありますが、関係団体からの反対も示されており、導入の必要性を含めて検討する必要があるとされています。

また、漏えい等報告・本人通知に関しては、2022年度から漏えい等報告が義務化されたことなどにより、報告件数が増加傾向にある一方で、これらの義務が事業者の過度な負担になっているとの意見も示され、これを踏まえて、個人の権利利益侵害が発生するリスク等に応じて、漏えい等報告や本人通知の範囲・内容の合理化を検討すべきとされています。また、関係団体からは「おそれ」要件につい

1　論点すべてについては、以下Webページより、中間整理の文書をご参照ください。「個人情報保護法　いわゆる3年ごと見直しについて」（個人情報保護委員会）　https://www.ppc.go.jp/personalinfo/3nengotominaoshi/

ても要望が示されているため、その具体的な当てはめについては現実の事例に応じて精査する必要があるとされています。

## データ利活用に向けた取り組みに対する支援等の在り方

社会にとって有益であり、公益性が高いと考えられる技術やサービスについて、既存の例外規定では対応が困難と考えられるものがあるため、検討が必要であるとされています。

また、民間における自主的取り組みの促進として、プライバシー影響評価（PIA）や個人情報の取り扱いに関する責任者はデータガバナンス体制の構築において主要な要素となるものであり、その取り組みが推進されることが望ましいものの、その義務化については慎重に検討を進める必要があるとされています。

その他、プロファイリング、個人情報等に関する概念の整理、プライバシー強化技術（PETs）等の論点についても、引き続き検討するとされています。

中間整理に対して、2024年6月から7月にかけて実施されたパブリック・コメントでは、各種団体・事業者72者、個人1,659者から、合計2,448件の意見提出がなされました[2]。7月からはPPCにて「個人情報保護法のいわゆる3年ごと見直しに関する検討会」が開催されており、課徴金制度や団体による差し止め請求制度および被害回復制度について検討が進められています[3]。

2 「「個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理」に関する意見募集結果（概要）」（個人情報保護委員会）
https://www.ppc.go.jp/files/pdf/20240905_kentohkai_shiryou-2.pdf
3 「個人情報保護法のいわゆる3年ごと見直しに関する検討会」ページ（個人情報保護委員会）
https://www.ppc.go.jp/personalinfo/kentohkai/

# マイナンバーの利活用と特定個人情報保護評価

JIPDEC　電子情報利活用研究部　主査　**須永　卓也**

## 1. 特定個人情報保護評価とは

JIPDECでは、特定個人情報保護評価に関する支援業務を行っています。「特定個人情報保護評価」とは、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（マイナンバー法）第28条で規定されている[1]もので、行政機関がマイナンバーを取り扱う事務において、その取り扱いに関するリスクを事前に分析し、そのリスクを軽減するための措置を講じているかを確認し、自ら宣言するものです。特定個人情報、つまりマイナンバーに関するもので、諸外国のプライバシー影響評価（Privacy Impact Assessment：PIA）に相当するものであることから、マイナンバーPIAなどとも呼ばれています。

特定個人情報保護評価の根本的な目的・意義として、行政機関におけるマイナンバー取り扱い事務を対象としたものであることから、個人の権利利益の侵害を事前に防止すること、また国民・住民の信頼を確保することとされています[2]。したがって、特定個人情報保護評価においては、権利利益の侵害を未然に防ぐために、事後的な対応ではなく事前防止の観点で自ら実施し、またその取り扱いの内容やリスク対策、措置がどのようなものかを国民・住民に広く開示するとしており、リスク分析・リスク対策といった安全管理措置そのものの適切性だけでなく、マイナンバーの取り扱いそのものが適切かを事前に知らしめることが求められています。

つまり、事務の現場で適切に厳格に取り扱っているというだけではなく、その事務においてマイナンバーを取り扱うことでどういったリスクがあり、そのリスクに対してどのような対策を行っているかをきちんと国民・住民に理解してもらうことが必要となります。

行政機関および関係機関のマイナンバー取り扱いを対象にと言うのは簡単ですが、対象となる機関・システムは膨大なものとなり、すべての取り扱いをもれなく精査することは現実的ではありません[3]。したがって、特定個人情報保護評価に関する規則[4]では、その取り扱いのリスクに応じて実施すべき特定個人情報保護評価の要否や実施内容を定めており、取り扱うマイナンバーの件数、およびマイナンバーを取り扱う者の数、重大事故の発生の有無からしきい値判断を行い、「全項目評価」「重点項目評価」「基礎項目評価」のいずれを実施する必要があるかを定めています。

## 2. マイナンバーの利用促進と指針改正

行政機関における特定個人情報の取り扱いを定める「特定個人情報の適正な取扱いに関するガイドライン」および特定個人情報保護評価の実施事項を定める「特定個人情報保護評価指針」は、社会変化等に対応し定期的に改正が行われています。直近では、2024年5年27日に改正[5]されました。主な改正点としては、マイナンバー紐づけ誤りおよびマイナ総点検の影響により、人的ミス防止対策に関する規定・様式変更と、マイナンバー・マイナンバーカードの利用促進に関するマイナンバー法改正に対応する改正が行われました。

1　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（e－GOV）
https://laws.e-gov.go.jp/law/425AC0000000027/
2　特定個人情報保護評価指針（個人情報保護委員会）　https://www.ppc.go.jp/files/pdf/PIA_shishin.pdf
3　情報保護評価の対象となりうる機関及びそのシステム（内閣官房）
https://www.cas.go.jp/jp/seisaku/jouhouwg/hyoka/dai1/sankou3.pdf
4　特定個人情報保護評価に関する規則（e－GOV）　https://laws.e-gov.go.jp/law/426M60020000001
5　特定個人情報保護評価指針の3年ごとの再検討による主な改正事項（個人情報保護委員会）
https://www.ppc.go.jp/files/pdf/PIA_shishin_minaoshi_point_R060401.pdf

このマイナンバー・マイナンバーカードの利用促進によって、これまで税・社会保険関連等の事務で用いられていたマイナンバーが、国家資格や自動車登録等の事務でも用いられることとなり、特定個人情報保護評価の対象となる事務が一気に増えることになります。[6, 7]

先に述べたように、特定個人情報保護評価は実際に取り扱う前に実施することが求められるものであること、またマイナンバーの利用促進は地方公共団体ごとの取り組みではなく、日本全体での悉皆性のある取り組みであることから、多くの地方公共団体でマイナンバーの取り扱いに関する対応、また特定個人情報保護評価は急務と言える状況にあります。

## 3. 今後の特定個人情報保護評価

マイナンバーの利用促進だけでなく、ガバメントクラウドの導入や自治体情報システムの三層分離構造の見直し等、行政機関におけるマイナンバーの取り扱いや情報セキュリティに関する状況は、技術や社会の変化に応じ大きく変化していくこととなります。また、現状では同様の事務であっても地方公共団体の規模によって評価基準が異なってくることや、多くの事務が対象となる基礎項目評価の意義等について、特定個人情報保護評価制度自体をより実効性のある制度として見直すことも必要となるでしょう。

JIPDECでは、行政機関の特定個人情報保護評価の支援を通じ、より安全、安心な情報化社会を実現していきます。

6　マイナンバー法の改正事項（デジタル庁）　https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/3c34892b-6704-4c74-b1c7-d461c4bccfff/bdba23d0/20221129_meeting_mynumber_outline_01.pdf

7　マイナンバー法等の一部改正法（令和5年法律第48号）について（厚生労働省）
https://www.mhlw.go.jp/content/12401000/001114698.pdf

# 標準化とは

JIPDEC　電子情報利活用研究部　**野町　綺乃**

JIPDECは、1998年にプライバシーマーク制度を創設してから現在に至るまで、プライバシーマークの付与機関および審査機関として活動を行っています。

プライバシーマークを取得するには、事業者は、JIPDECが公開している「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」に則った対応を行い、審査を受ける必要があります。この構築・運用指針は、日本産業規格「JIS Q 15001:2023 個人情報保護マネジメントシステム－要求事項」（JIS Q 15001）に準拠したものとなっています。

このようにJIPDECの事業においてはJISなどの標準が身近なところにあり、標準化は、プライバシーマークを取得された企業の皆さまにも関連する取り組みとなっています。

『標準化（Standardization）』とは、『「もの」や「事柄」の単純化、秩序化、試験・評価方法の統一により、製品やサービスの互換性・品質・性能・安全性の確保、利便性を向上するもの』[1]と定義されているもので、一定の基準を設け、決められた方法で作成、製造することで、日本で作成、製造した「モノ（物）」を海外でも利用でき、販売することができる他、海外で作成、製造された「モノ（物）」を日本でも利用できるようになるため、標準化を行うことは重要な活動となっています。

この標準化によって制定され、取り決められた定義を技術文書として、誰もが閲覧できるようにまとめたものを「規格（Standards）」と呼んでいます。

「規格」は、「国際規格」「地域規格」「国家規格」「団体規格」[2]という四つに分類されており、このうち、日本で共通的により多く閲覧されている規格は、「国際規格」と「国家規格」になります。

「国際規格」は、国際標準化機関で制定される規格を指しており代表的な国際標準化機関としては、ISO（International Organization for Standardization：国際標準化機構）や、IEC（International Electrotechnical Commission：国際電気標準会議）といった機関が国際規格を制定しています。

「国家規格」は、各国の標準化機関で制定される規格を指しており、日本の場合、経済産業省に設置されている審議会である日本産業標準調査会（Japanese Industrial Standards Committee：JISC）で審議されている日本工業規格（JIS）が代表的なものです。

加えて、ISO規格や、IEC規格、JIS規格などは、公的な機関で制定された規格であるため、デジュール規格とも呼ばれています。

このように「規格」は、国際、国内を問わず、さまざまな国や団体、機関などで制定されており、標準化を行うことは、新しい技術、優れた製品やサービスを速やかに普及させるためのツールであり、事業戦略を練るうえで検討するべき事項の一つ[3]となっています。

経済産業省では標準化に関する取り組みとして、企業の皆さまが標準化を事業戦略に活用できるよう、さまざまなサポート[4]が実施されています。標準化を自社の事業戦略に活用することをご検討の方は、経済産業省にお問合せ、相談などをされてみてはいかがでしょうか。

1　標準化って何？（経済産業省）　https://www.meti.go.jp/policy/economy/hyojun-kijun/general.html
2　規格とは（日本規格協会グループ）　https://webdesk.jsa.or.jp/common/W10K0500/index/dev/glossary_3/
3.4　標準化ビジネス戦略検討スキル学習用資料（経済産業省）
https://www.meti.go.jp/policy/economy/hyojun-kijun/katsuyo/business-senryaku/index.html

# 越境データ流通の新時代に向けて
## ―個人データを扱う際の「トータルコンプライアンスコスト」―

JIPDEC　電子情報利活用研究部　客員研究員　**横澤　誠**

「信頼性のある自由なデータ流通」（Data Free Flow with Trust：DFFT[1]）は、近年の外交政策において重要な概念となっています。この「信頼」を基盤にしたデータ流通の考え方は、特に日本やアジア地域の文化に根差した「信頼」の概念に基づいており、西洋の「契約」文化を補完するものとされています。

DFFTは制裁金等のリスクの軽減、データの価値創出（AIやクラウド利用）、国際的な規制の断片化への対応（執行協力と相互運用性）の三つの理由で、企業にとって重要な概念となります。

具体的にDFFT実現の方法については、大まかに二つの方向性があります。①GDPRをモデルにして各国の個人情報保護制度を統一化しようとする方法と、②グローバルCBPR[2]を代表とする自主規制を重視した認証制度の共通化と執行協力の2点です。どちらが絶対優位ということはありません。

ここで重要となるのが、企業目線からの「コスト」評価です。冷静にコストを評価すると、データ保護規制に国際的に対応するために必要な考え方が浮き彫りになってきます。①のGDPRについてはその成立時期から、ベトナムやEUで最大1.7％のGDP損失というマクロ経済評価[3]があります。ミクロな企業側のコスト分解[4]とその試算例では、GDPR遵守にかかる直接・間接費用合計のコンプライアンスコストが非常に大きく、大企業においては初期対応費用として数億円規模になることが指摘されています[5, 6]。

これに対して、②の自主規律やグローバルCBPRを中心としたデータ流通については、実務に基づいた数字を得ることがまだ難しいかもしれません。ただ少なくとも各国・各地域における法制度の調査と予備的な対応措置の理解、漏えい・事象発生時対応方法の予備的定型化、執行機関の明確化と越境執行の確認、データ主体同意の管理方法統一、越境委託先・第三者提供管理の低減、契約案文の一本化と管理の統一化などの各点にかかる直接・間接費用を考えることができるでしょう。今後も分析を進めていくことが必要ですが、コスト分解項目だけを見ても、中規模の企業でも年間数千万円規模の総対応コスト（トータルコンプライアンスコスト）になっている可能性があります。

企業目線では、官民および国際協力に基づき制度設計を改善し、トータルコンプライアンスコストのうちどの部分をどの程度削減することができるのかの議論が必要になると思われます。

その議論を実践と経験に基づいたものとするために、「サンドボックスアプローチ[7]」（規制特区）を設けて実態を明らかにするなどの実践も重要です。グローバルCBPRの認証制度は、その特区の境界を切り分ける条件としての役目を持つこともできそうです。

---

1　Data Free Flow with Trust（デジタル庁）　https://www.digital.go.jp/policies/dfft
2　グローバルCBPRフォーラム（Global CBPR Forum）　https://www.globalcbpr.org/
3　THE COSTS OF DATA LOCALISATION:FRIENDLY FIRE ON ECONOMIC RECOVERY（ECIPE）
https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf
4　Navigating GDPR Compliance Costs（BUSINESSTECHWEEKLY）
https://www.businesstechweekly.com/legal-and-compliance/gdpr-legislation/gdpr-compliance-costs/
5　2017 Veritas GDPR レポート（VERITAS）
https://www.veritas.com/content/dam/Veritas/docs/reports/gdpr-report-jp.pdf
6　Compliance Q&A: How much does GDPR compliance cost?（SPRINTO）
https://sprinto.com/blog/gdpr-compliance-cost/
7　Data Regulatory Sandbox（シンガポール情報通信メディア開発局）
https://www.imda.gov.sg/how-we-can-help/data-innovation/data-regulatory-sandbox

# AIのビジネス利用とマネジメントシステムの活用

JIPDEC　セキュリティマネジメント推進室　室長　**郡司　哲也**

近年、ディープラーニングの技術を活用したさまざまなAIサービスが登場し、それらが一般にも広く利用されるようになったことで、AI技術は私達の生活やビジネスにとって身近なものとなりました。企業はコールセンターの代わりにAIを活用したチャットボットを採用するようになり、写真共有SNSは画像生成AIを用いたさまざまな作品で溢れ、学生はレポート作成にAIをフル活用、といった具合です。一方で、新たなテクノロジーが発明され、それが社会に浸透する際の常として、さまざまな課題も浮き彫りになってきています。特に、生成系AIと呼ばれる技術では、AIが学習し、利用者が望むアウトプットを出力するために入力する情報に「適切ではない情報」が含まれてしまうことで、意図せずして権利侵害を起こしてしまうようなケースも生じています。

また、ロシアによるウクライナ侵攻での情報戦においては、ゼレンスキー大統領が自国民に投降を促す発言をするディープフェイク動画などがニュースになったことも記憶に新しいところです。

このようなさまざまな事象で浮き彫りとなった最も大きな課題は、AIを利用することの是非ではなく、AIを利用する私達が、まだ適切な倫理観やリテラシーを備えていないことかもしれません。要は「使う側の問題」ということです。たとえば、インターネットで何か調べ物をするとします。既に私達は、検索結果の中には真実と思われる情報と真実ではない情報が混在していることを知っていますし、検索結果としてブラウザに表示される画像や動画の中には、著作権侵害の可能性がある内容が含まれていることも知っています。私達は、ある程度の時間をかけて経験し、学習し、道具の使い手としての情報リテラシーを向上させてきたのです。

しかしAIに関しては、予想を上回るスピードで社会に浸透している現実があり、リテラシーの醸成が追いついていない、というのが実情ではないでしょうか。その状況は国際的にも同様に認識されているようで、各国ではAI利用に関する規制が始まっています。欧州では、法規制により安全にAIを活用し、市場の活性化も促進するという目的のもとで、2024年8月に「欧州AI規則」が発効、2030年までに段階的に施行されることになり[1]、日本でも、2024年4月に経済産業省と総務省が「AI事業者ガイドライン」を公表[2]し、メディアでも大きく取り上げられました。ビジネスにおいてAIを活用する際には、これらの規制やガイドラインに対して注視することが大事になるでしょう。

AIをビジネスで活用していく上では、AIを活用する上でのリスク（学習データの品質等）に適切に対応していることを示し、信用を得ることが大事です。そして、それらの事実を取引先やステークホルダーに対してどう示すのかもポイントになります。そのときに有効となるのが、第三者による証明であり、代表的なものが製品の品質管理のリスクに対してQMS認証（ISO 9001に基づく品質マネジメントシステム）、情報保護のリスクに対してISMS認証（ISO/IEC 27001に基づく情報セキュリティマネジメントシステム）のような、リスクマネジメントに関する認証の取得です。

AIを取り扱う上でのリスクに関しても、情報セキュリティマネジメントシステムと同様のアプローチによる適切な管理が有効なのではないかという考え方に基づき、2023年12月にISO/IEC 42001（AI

1　Artificial intelligence act（Council of the EU and the European Council）
https://www.consilium.europa.eu/en/policies/artificial-intelligence/
2　「AI事業者ガイドライン（第1.0版）」を取りまとめました（経済産業省）
https://www.meti.go.jp/press/2024/04/20240419004/20240419004.html

マネジメントシステム：Artificial Intelligence Management System）が発行[3]されました。

ISO/IEC 42001の登場は、AIシステムを提供するベンダーやそれらのAIシステムを活用してAIサービスを提供するサービス提供者には朗報かもしれません。ISO/IEC 42001では、AIシステムの開発者、提供者、利用者等の役割を定義し、それぞれの役割でAIを利用する組織について、AI活用に関するリスクに対応するためのマネジメントシステムを構築するために「しなければならないこと」や「すべきこと」を定義しています。つまり、ISO/IEC 42001に基づくAIマネジメントシステムを構築・運用している組織が認証を取得することで、その組織はAIに関するリスクに適切に対応しているということをアピールすることができ、取引先や消費者も安心してその組織が提供するAIを活用した製品やサービスを利用することができるようになります。

2024年10月現在、日本国内ではISO/IEC 42001認証はごく一部で認知されているにすぎませんが、国際規格に基づくものであることから、ISO/IEC 27001に基づくISMS認証のように、将来的に広く普及する可能性を秘めています。ISO/IEC 42001認証は、急速に社会に浸透しつつあるAI技術について、それを利用する企業や組織に対するベンチマークの一つになり得るでしょう。

なお、JIPDECの関連団体であるISMS-AC（情報マネジメントシステム認定センター）では、ISMS認証をはじめとする情報マネジメントシステム認証を行う認証機関を認定していますが、今後新たな認定制度としてISO/IEC 42001認証を行う認証機関の認定を開始する予定です。認証機関に対する認定は、複数の異なる認証機関が同一の規格のもとで適切な認証活動を行うことを担保する重要な制度です。認定に基づいたISO/IEC 42001認証について、今後の普及に大いに期待しています。

3　AIマネジメントシステムの国際規格が発行されました（経済産業省）
https://www.meti.go.jp/press/2023/01/20240115001/20240115001.html

## 〈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）<br>1989年10月1日に第三章と23条以外の規定が施行<br>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 |
| | 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 |

| 国　内 | 年 | 海　外 | |
|---|---|---|---|
| | 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）<br>（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）<br>（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」成立（5/23）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 | | |
| | 2007 | APEC | ・「越境プライバシールール」策定<br>・「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」および関連法成立（5/24） | 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） | | | |
| 「パーソナルデータの利活用に関する制度改正大綱」公表（6/24） | | | |
| 「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）<br>・「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） |

| 国　内 | 年 | 海　外 | |
|---|---|---|---|
| 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 | 「EU一般データ保護規則（GDPR）」成立（4/27）。2018/5/25施行 |
| 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） | | 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）」成立（11/7）。2017/6/1施行 |
| 「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（EC）、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） | | 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」策定（6/26）。 | 2018 | 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） |
| 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） | | 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） |
| 「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 | | 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 | 米国初、「カリフォルニア州消費者プライバシー法2018年（CCPA）」成立（6/28）。2020/1/1施行 |
| EUとの越境移転に関し、日本の補完的ルール策定を変更。個人情報保護法第24条に基づきEUを指定、ECもGDPR第45条に基づき日本の十分性認定を決定し、相互認証の枠組み発効 | 2019 | タイ | 「個人情報保護法（PDPA）」施行（5/28） |
| 「個人情報の保護に関する法律等の一部を改正する法律」成立（6/5）。2022年4月全面施行 | 2020 | EU-アメリカ | EU司法裁判所、「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）」成立（12月）。2023/1/1施行 |
| 「デジタル社会の形成を図るための関係法律の整備に関する法律」成立（5/11） | 2021 | シンガポール | 「個人情報保護法（2012）」改正法施行（2/1） |
| | | 中国 | ・「データセキュリティ法」成立（6/10）。9/1施行<br>・「個人情報保護法」成立（8/20）。11/1施行 |
| | | EU | EC、「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）」改定案採択（6/4） |

| 国　内 | 年 | 海　外 | |
|---|---|---|---|
| 日本を含む7か国・地域がグローバルCBPR設立宣言に合意（4/21） | 2022 | 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）」成立（9/20）。10/17施行 |
| 「電気通信事業法の一部を改正する法律」成立（6/13）。2023/6/16施行 | | EU | ・「デジタル市場法（DMA）」成立（10/12）。2023/5/2施行<br>・「デジタルサービス法（DSA）」成立（10/27）。2023/2/17施行 |
| 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） | 2023 | イギリス | グローバルCBPRアソシエイト参加（7/6） |
| | | 中国 | 「個人情報域外移転標準契約弁法」成立（2/3）。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） |
| | | ベトナム | 「個人情報保護政令」公布（4/17）。7/1施行 |
| | | 米カリフォルニア州 | CPRA執行規則承認（3/29）。7月執行予定が裁判所命令で2024年3月に延期（6/30） |
| | | 米モンタナ州 | ・「TikTok禁止法」成立（5/17）。2024/1/1施行。その後、連邦地裁が施行を仮差止め（11/30）<br>・「消費者データプライバシー法」成立（5/19）。2024/10/1施行 |
| G7、広島AIプロセスに関するG7首脳声明発出（10/30） | | 米テキサス州 | 「データプライバシーおよびセキュリティ法」成立（6/18）。2024/7/1施行 |
| | | 米オレゴン州 | 消費者データプライバシー法成立（7/18）。2024/7/1施行 |
| | | EU-アメリカ | 「EU-US Data Privacy Framework（DPF）」採択（7/10） |
| | | インド | 「デジタル個人データ保護法」成立（8/11） |
| | | 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」合意（9/21）。10/12発効 |
| | | イギリス | 「オンライン安全法」成立（10/26） |
| 情報流通プラットフォーム対処法（改正プロバイダ―責任制限法）」成立（3/1） | 2024 | 中国 | 「国境を越えたデータフローの促進および規制に関する規定」公表（3/22） |
| METIと総務省、「AI事業者ガイドライン」発行（4/19） | | アメリカ | ・「情報改革およびアメリカの安全保障法（RISAA）」成立（4/20）<br>・「外国の敵対勢力による規制対象アプリケーションからのアメリカ人の保護に関する法律（TikTok禁止法）」成立（4/24） |
| グローバルCBPR稼働（5月） | | 米ニューヨーク州 | 「SAFE for Kids法」、「ニューヨーク児童データ保護法」成立（6/20） |
| 「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律」成立（6/12） | | 米カリフォルニア州 | 2018年制定の消費者プライバシー法（CCPA）を改正。脳神経データを保護する法律「SB-1223」制定（9/28） |
| | | EU | 「欧州人工知能規制法」成立（5/21）。8/1施行 |

## 〈資料２〉情報化に関する動向（2024年4月～2024年9月）

### 【国内／国際連携】

**2024年4月**

- 公正取引委員会、Googleによる旧ヤフーへの検索エンジン検索連動型広告技術の提供制限によりＹ社の広告配信を制限したとして、Ｇ社を独禁法違反で行政処分。
- 東京地裁、KADOKAWA他2社による漫画海賊版サイト「漫画村」掲載17作品を巡る訴訟で運営者に17.4億円の損害賠償命令。7月に知財高裁から運営側への控訴状却下命令で賠償確定。
- 経済産業省（METI）と総務省、AIの開発・提供・利用者が安全安心な活用を促進するための「AI事業者ガイドライン（第1.0版）」策定。

**5月**

- OECD閣僚理事会、ガバナンス強化に向けた各種枠組みの連携を重視した、OECD AI原則の改訂を採択。
- 日・米・欧の捜査当局、世界約120か国・2,500の企業・団体が攻撃を受けた被害規模最大級のハッカー集団LockBitのロシア人首謀者を起訴。脅し取った身代金の総額は5億ドル。
- 個人情報保護委員会（PPC）とMETI、グローバルCBPR稼働に向けたポリシー、ガイドライン等を公表。
- 「情報流通プラットフォーム対処法（改正プロバイダ責任制限法）」成立。誹謗中傷申請を受けたSNS運営事業者に「対応の迅速化」等義務付け。違反すれば最大1億円以下の罰金も。
- 損保大手4社、代理店を通じた不適切な他社契約者情報共有を公表。7月に金融庁が報告徴求命令。8月の報告で漏えい件数約250万件が明らかに。

**6月**

- 「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律」成立。スマホアプリのセキュリティ確保、巨大ITによる独占禁止を義務付け。課徴金は違反分野の売上高の20％。
- PPC、「個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理」公表。
- KADOKAWA、ランサムウェア攻撃によりニコニコ動画はじめ同社運営サイトが利用不能に。また個人情報約25万件が外部流出。その後1,000件弱の情報拡散行為を確認、特損20億円を計上。

**7月**

- Windows、世界的なシステム障害で工場の操業や航空機の運航が停止。約850万台のコンピュータに影響。米Clowdstrike製セキュリティソフトウェアのバグが原因。
- 情報処理サービスのイセトー、ランサムウェア攻撃を受け自治体や企業から委託された住民・顧客情報150万件以上が流出。委託元の自治体や企業が相次いで被害を公表。
- 政府、生成AIの法規制を巡る有識者会議「Ai制度研究会」発足。リスク対応と技術革新の両立を目指す。
- 情報通信研究機構他、世界初、量子コンピュータを利用した屋外多発同時接続実験に成功。

**8月**

- METI、Amazon、Appleに取引改善を求め勧告。手数料の通知不十分や契約説明に日本語なし等。
- 国立情報学研究所、約6.5万件の判例を収録した「日本の判例HTMLデータ」を研究者に無償提供。

**9月**

- AIセーフティ・インスティテュート（AISI）、AIシステムの脆弱性検証ガイドブック「AIセーフティに関するレッドチーミング手法ガイド」策定。
- 日・米等40か国、政府サービス用途のAIシステムの安全・安心・信頼できる開発や利用などに関する共同声明発表。

**【海外】**

**2024年4月**

- Google、2020年に提訴されたシークレットモード使用時の閲覧追跡に対する集団訴訟で和解。G社は数十億件の閲覧データ記録の破棄に合意。
- 米政府、「情報改革およびアメリカの安全保障法（RISAA）」成立。失効した外国情報監視法第702条（FISA）に代わり、監視対象に米国民も追加。2年間の期限付き。
- 欧州委員会（EC）、DSAに基づきTikTokのポイント取得プログラムス「タスク・アンド・リワード・プログラム」の一部停止命令に向けた手続き開始。8月、T社はEUでの該当サービスを完全撤退。
- 米政府、「TikTok規制法」成立。5月にTikTokの運営会社Bytedanceが表現の自由を制限するのは憲法違反と米政府を提訴。
- イタリア政府、医療、仕事、行政、司法、セキュリティ、国家戦略等に係るAIの利用原則を定めた規定成立。AIの犯罪利用については厳罰を科す。
- 米連邦取引委員会（FTC）、利用者の位置情報を同意なしに不法共有、データ仲介事業者が取得可能にしていたとして、AT＆T等通信大手4社に総額1.96億ドルの制裁金。

**5月**

- スペイン銀行大手Santander、ハッキング被害を発表。その後、ハッカーサイドが3,000万件超の顧客情報や2,800万のクレジット情報、スタッフ情報のデータベースアクセス権を200万ドルで販売中とDark Web InformerがXに投稿。
- 欧州評議会、責任あるAI開発によるリスクの特定・軽減や人権尊重を目指す初のAI国際条約採択。日・米・加等もオブザーバーで参加。
- Amazon、Google、Meta等16企業、英韓共催のAIサミットで安全なAI開発を行うための誓約締結。
- 英競争・市場庁、巨大ITを規制する「デジタル市場・競争・消費者法」成立。消費者と企業間での公正な取引の義務付けや偽の口コミ提供など禁止。制裁金は売上高の最大10％。
- 韓国個人情報保護委員会、2023年3月に発生したKakaoユーザー情報6.5万件流出事故で国内過去最高額の151億ウォンの課徴金と780万ウォンの過怠金。K社は処置に反発し、法的措置を検討。
- EU、世界初の包括的なAI規制法「EU AI法」成立。同年8月発効。

**6月**

- 米ニューヨーク州、全米初、18歳未満をソーシャルメディア中毒から守るSAFE for Kids法とニューヨーク児童データ保護法成立。保護者の同意なくアルゴリズムによるコンテンツ配信を禁止し、同意ない収集、使用、共有、販売などを原則禁止。
- 米司法省（DOJ）、Appleのスマホ市場での独禁法訴訟で新たにワシントン州等4州の参画を発表。共同原告団は21に。
- 米連邦最高裁、ミズーリ州他が違憲としたバイデン政権によるSNSの偽・不適切情報削除要請を容認。
- インドネシア政府、ハッカー集団Lockbitからのランサムウェア攻撃で200件以上の政府機関で大規模障害発生。身代金額800万ドルの支払い拒否。

**7月**

- 米保険関連ソフト開発企業IMS、2023年10月に受けたハッカー集団Lockbitのランサムウェア攻撃で600万人以上の個人情報流出を公表。
- ブラジル国家データ保護機関、MetaのユーザーデータのAI学習利用許可を示したプライバシーポリシーの即時停止とデータ処理停止命令。違反金は1日50,000ブラジルレアル。
- 米メッセージサービスのTwillo、2段階認証アプリユーザーの携帯電話番号流出を公表。
- AT＆T、利用するクラウドサービスへのサイバー攻撃により、全携帯電話顧客の通話とテキストメッセージの記録等、約1.1億件流出を公表。
- 米・EU・英、AIがもたらす公正な取引や排他的な手段の防止、既存企業と新規参入企業間の投資や提携の精査に関する原則を含むAI競争問題に関する共同声明発表。
- Meta、許可なくテキサス州民数百万人の個人生体認証データを収集・使用したとして2022年に起こされた訴訟で州と和解。5年間で14億ドルの和解金。

**8月**

- 米司法省とFTC、TikTokとByteDanceを児童オンラインプライバシー保護法およびその実施規則（COPPA）に違反したとしてカリフォルニア州中部地区連邦地方裁判所に提訴。
- 米連邦地方裁判所、Googleが検索および広告市場での独占を維持したとする訴訟で、独禁法違反と判決。
- Meta、個人の生体認証データを違法に取得してテキサス州民数百万人のプライバシーを侵害したとして、テキサス州の訴訟で14億ドルの和解金に合意。州単体では過去最大規模。
- 韓国金融監督院、Kakao Payが中国Alipayに6年余りにわたり顧客の個人信用情報約542億件、累積4,000万人分を同意なく提供していたとする調査結果を公表。
- 米テキサス州、米GMが1,400万台以上の車にデータ収集技術を搭載し、同意なく保険会社等にデータを売却していたとして、ドライバーのプライバシー侵害疑いで提訴。
- 対米外国投資委員会、機密データへの不正アクセスを防止・報告しなかったとしてT-Mobileに6,000万ドル超の罰金。
- オランダデータ保護局、運転手の個人情報移転に関して、米Uberに対し欧州の一般データ保護規則（GDPR）違反で2.9億ユーロの制裁金。

**9月**

- サウジアラビアのサウジデータ・AI庁、個人情報の国外移転に関する規則の改正を発表。
- オランダ当局、米国の顔認識テクノロジー企業Clearview AIに対し、違法なデータベースを構築したとして3,050万ユーロの罰金。
- 米ワシントン連邦地方裁判所、検索エンジンの初期設定で競争を阻害したとしてGoogleに独占禁止法違反判決。
- 欧州司法裁判所、優越的地位乱用でGoogleに制裁金24.2億ユーロを課すECの決定を支持。
- 欧州司法裁判所、アイルランドの税優遇措置を巡りAppleに130億ユーロの追徴を命じるECの決定を支持。
- 欧州一般裁判所、ECによるGoogleへのEU競争法違反の制裁金14.9億ユーロ支払い命令を無効判決。
- 米医薬品流通業者Cencora、サイバー攻撃を仕掛けたハッカーに身代金計7,500万ドルを支払ったことが判明。ハッカーへの支払いとしては過去最大規模。
- 連邦捜査局ら、ルーターやネットワークカメラにマルウェアを感染させた中国のボットネット「Raptor Train」を破壊。
- 欧州刑事警察機構、盗難スマホのロック解除を手助けしたとされる犯罪ネットワーク解体。
- アイルランドデータ保護委員会、Metaに対して数億件のパスワードを暗号化せずにサーバーに保管していたとして9,100万ユーロの制裁金。
- 米カリフォルニア州、2018年制定の「カリフォルニア消費者プライバシー法（CCPA）を改正し、脳神経データも個人情報保護の対象とする法律「SB-1223」を制定。

JIPDEC IT-Report 2024 Winter
2024年12月16日発行（通巻第24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