IT-Report
2020 Winter

特集

ビジネス変革とプライバシー保護の両立
―プライバシーガバナンス構築に向けて

IT-REPORT

2020
Winter

Contents

JIPDEC
一般財団法人日本情報経済社会推進協会

今年度第２号となる「JIPDEC IT-Report 2020 Winter」は、「ビジネス変革とプライバシー保護の両立－プライバシーガバナンス構築に向けて」と題し、特集を組みました。

デジタル技術の活用により、国境を越えた社会の急激な変化に対応するため、経済産業省は「イノベーションの促進」と「社会的価値の実現」の両立に向け、新たなガバナンスモデルの必要性と在り方を検討し、「GOVERNANCE INNOVATION：Society5.0の実現に向けた法とアーキテクチャのリ・デザイン」報告書を2020年７月にとりまとめました。この中で、国内の法規制を基に組織・企業の行動規範を統制する従来のガバナンスから、世の中の変化に対応できる、国境を越えた柔軟なガバナンスが今後求められる、と提言しています。

政府が推進するデジタル・トランスフォーメーション（DX）に関連して、データとデジタル技術を活用した新規ビジネスへの参入や業務変革を進める企業が増えてきています。特にパーソナルデータを活用したビジネスについては、消費者への不利益や不当な扱い、炎上などのトラブル発生から、企業の信頼失墜、経営にまで影響する可能性も考えられることから、データ主体である消費者のプライバシーに対する十分な配慮が必要とされます。このため、パーソナルデータを取り扱う企業を対象に、経済産業省・総務省はプライバシー保護に関わるガバナンスの指針として、2020年８月28日に「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」を公表しました。

今号では、プライバシー保護のためのガバナンスをどう考えるか、ガイドブック策定の背景、ガバナンス・イノベーションとの関係等を有識者の方に座談会形式で伺いました。

また、2018年のGDPR施行以降のEU域内外への影響、各国の個人情報保護法施行など、海外の個人情報保護施策やデータプライバシー規制等について、最新動向を有識者の方に解説していただきました。

資料編では個人情報保護関連の年表と2020年４月から９月の情報化動向を掲載しています。

本誌をビジネスでデータを利活用される事業者はもとより、個人の皆様にも参考としていただければ幸いです。

2020年12月

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2020 Winter

Contents

特集

ビジネス変革とプライバシー保護の両立 ―プライバシーガバナンス構築に向けて

I 座談会　プライバシーガバナンス構築の勧め ―プライバシーガバナンスガイドブック作成の背景について

国立情報学研究所　教授　**佐藤 一郎**
東京大学大学院法学政治学研究科　教授　**宍戸 常寿**
司会：JIPDEC電子情報利活用研究部グループリーダー　**岡田 光輝**

岡田　今日は、今年８月に経済産業省と総務省が公表した「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ver1.0[1]」をとりまとめた「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　佐藤先生と、同じく検討会に委員として参加された東京大学　宍戸先生に、ガイドブックの話だけでなく、これからのデータ活用時代における企業のプライバシーへの対応について、幅広くご意見を伺いたいと思います。佐藤先生、宍戸先生、よろしくお願いします。

■なぜ今、「プライバシーガバナンスガイドブック」か

岡田　まず、プライバシーガバナンスガイドブックを策定するに至った背景について、どのようにお考えですか？なぜこのタイミングでガイドブックが策定されたのでしょう？

佐藤　データ利活用が企業経営を含めビジネスの源泉となってきている現在、企業としては、プライバシーに関わる情報を含めて多様なデータを徹底的に使いたいと考えることになります。

しかし、現実には個人情報の利用には規制もあり、さらに個人情報にならなくても、プライバシーに関わるデータをきちんと考えていかないといろいろなトラブルが起きてしまいます。

いま企業にとっては社会や個人からの信頼性が重要になっていますが、その信頼性はプライバシーに関わるようなデータの取扱い方によって左右されます。経済産業省、総務省は企業の方々に真剣にプライバシーについて考えてもらう時期だとお考えになって、このガイドブックに取り組まれたと考えています。

宍戸　また、データ利活用の前提となる技術・サービスが著しく高度に進化し、企業活動もグローバル化する中で、副次的に取得したデータが思わぬ価値を持ったり、逆に日本で問題ないとされていたサービスを海外展開した途端にデータの取得・活用面で大きな問題を引き起こしてしまう等、データを巡る企業の環境が大きく急速に変化しています。

これまでも、企業は海外に事業展開する際

1　https://www.meti.go.jp/press/2020/08/20200828012/20200828012.html

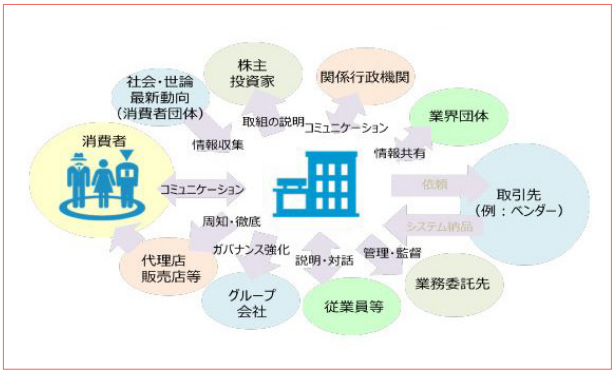
には、従業者の労働環境や雇用について、その土地土地の文化や宗教、習慣等を考慮していたと思いますが、今後はデータの取扱いやプライバシーに関しても同様のことが求められます。ただ、日本企業はまだ、「使うべきところは使い、守るべきところは守る」と前向きに取り組むための十分な体制、新たな企業文化を醸成できていないので、その状況に対するメッセージとして、このガイドブックは検討されたと理解しています。

佐藤　日本企業は、法律に外形的な対応をしがちですが、今後は社会規範や文化といった法律以外の部分が重要になってくるということだと思います。

個人情報やプライバシーの先には「人」がいますから、「人」がどう思っているかというところは考えないといけません。なお、プライバシーは、個人情報よりも外延が曖昧です。堀部先生[2]が「プライバシーの法制化は難しい」とおっしゃっていたと思いますが、そうだとすると、なおのこと企業の取組みとして対応することが必要不可欠になるのでしょう。

もう１点、今回のガイドブックではコーポレートガバナンスに焦点を当てています。本来は技術屋なのに、日本にコーポレートガバナンスという概念が入ってきた頃、つまり20年程前にガバナンス策定作業に参加したことがあります。その当時はガバナンスとは、経営に関わる不正を排除することがメインでした。しかし、その後、世界的に見るとコーポレートガバナンスの考え方や対象範囲は、株主との関係や多様なステークホルダーとの関係、さらに現在ではSDGsへの対応等と非常に広範になってきています。日本もそうした変化への対応が必要となり、このガイドブックもその流れの一つとして位置づけられます。

岡田　プライバシーの法制化は難しいというお話がありましたが、それはなぜなのでしょうか？



図Ⅰ-1．ステークホルダーとのコミュニケーション

（出典：経済産業省ウェブサイト
https://www.meti.go.jp/press/2020/08/20200828012/20200828012-2.pdf ）

宍戸　古典的には、プライバシーは「私生活の平穏」と捉えられていましたが、情報技術が進化すれば考え方も変わります。

19世紀の終わり頃は、空間的に人のプライバシーを捉え、その空間への侵入、たとえば家の中での姿を盗撮され、公開されることが問題とされていました。

その後、情報技術が発達すると、本来は人の内面まではわからないはずの氏名やID等にさまざまな情報を紐づけて収集・分析され、その個人の生き方までが丸裸の状態で晒されるような状況が生じるようになり、プラ

2　初代個人情報保護委員会　委員長

イバシーを「自己情報のコントロール」として捉えなおす必要性が1980年代以降広く認識され、OECD 8 原則等につながっていくわけです。

OECD 8 原則

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 8 つの原則。

1）**「目的明確化の原則」**（収集目的を明確にし、データ利用は収集目的に合致するべき）
2）**「利用制限の原則」**（データ主体の同意がある場合、法律の規定による場合以外は、目的以外に利用してはならない）
3）**「収集制限の原則」**（適法・公正な手段により、かつ、情報主体に通知又は同意を得て収集されるべき）
4）**「データ内容の原則」**（利用目的に沿ったもので、かつ、正確、完全、最新であるべき）
5）**「安全保護の原則」**（合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき）
6）**「公開の原則」**（データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき）
7）**「個人参加の原則」**（自己に関するデータの所在及び内容を確認させ、又は異議申立てを保証するべき）
8）**「責任の原則」**（管理者は諸原則実施の責任を有する）

こういった流れを踏まえて考えると、そもそもプライバシーとは複合的・複層的で、最終的には個人の私生活や自立して生きていくための手段的な権利としての位置づけを持っているものなので、その本丸である個人、あるいは個人に対する脅威との関係によって、プライバシーの概念は変わります。ここが、法制化が難しいとされる要因の 1 つだと思います。

しかし、同時に、手段としてのプライバシーをあまりにも広範に強く捉えすぎてしまうと、有用であるはずの個々人のコミュニケーションや企業のビジネス活動、政府の公益的な活動にあらかじめ制約がかかり、支障が出てしまう。これも法制化の難しさの一面です。

そこで、まずは個人情報を識別できるものは広く個人情報として捉え、同時にその個人情報の利用目的を特定し、その範囲内で利用する。あるいは企業の個人データの持ち方・使い方の状況に応じて本人関与のあり方を予め手続き的に法律で定めるというのが、データ保護法や日本の個人情報保護法の考え方です。

ただしこれは、プライバシーの観点で見ると、一面では過小であり、他面では過剰です。どんなに有益な活用でも本人同意が必須なのか、あるいは本人の同意さえあればどのような使い方でも許されるのか。この過小・過剰な部分が炎上を起こし、企業の健全なデータ利活用を委縮させたり、外形的な判断に走らせてしまったりする等、より問題を複雑化させています。

したがって、個人情報保護はあくまでも最低限のルールとして遵守しつつ、特にデータ活用によって企業利益を上げたり、有益なサービス提供、公益的活動を行おうと考える企業・組織は、自らの信頼・価値を高めるための前向きな取組みとして、プライバシーに配慮することが求められていると思います。

岡田　たしかに、個人情報保護法は遵守していても炎上リスクが気になり、なかなか新たなデータ活用に踏み出せないと悩まれている企業の方のお話は多く聞きます。そういった企業の方へのメッセージとして、今回のガイドブックを読んでいただくと良さそうですね。

佐藤　このガイドブックは、書かれていることを守ればプライバシーが守れるというものではなく、ガイドブックを契機にして、企業が自社ビジネスの中でどのようなプライバシー情報を守る必要があるのかを考えてもらうためのものです。

ガイドブックでは非常にシンプルに、その第一歩を踏み出すために「プライバシーガバナンスに係る姿勢の明文化」「責任者を決める」「プライバシー保護のためのリソースを割く」という点を挙げています。

個人情報は、国が定めたルールを遵守して保護する、という側面がありますが、プライバシーを保護するためには各人・各社が自ら考えなければなりません。

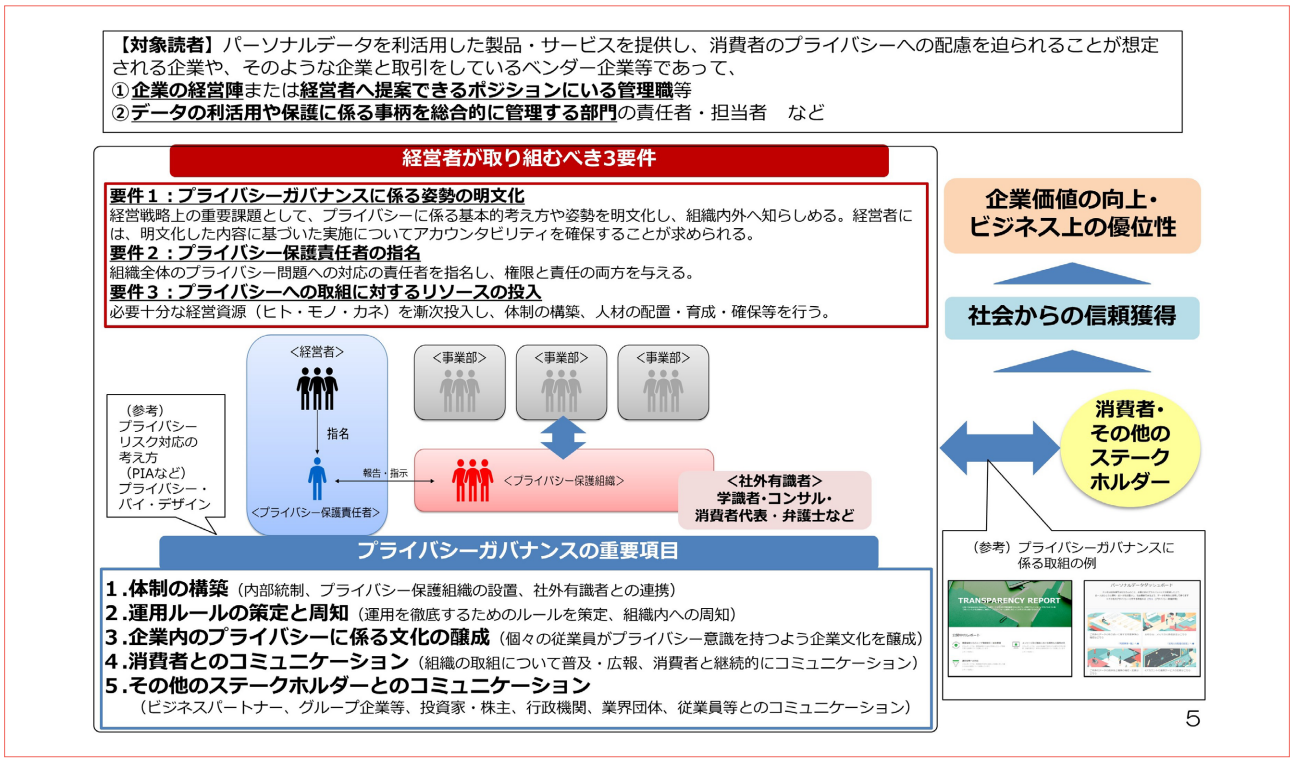
宍戸　佐藤先生のおっしゃるとおり、プライバシーはそれぞれの企業で考えなければならない問題で、その際には「他の誰かの考え方を持ってくる」のではなく、自社の事業環境や顧客の関係等と考えあわせる必要があります。ただし、そのためには当然ながら「考えるための体力」が必要です。

このガイドブックは、その体力・体制を備えておくことが日々刻々と変わるプライバシー問題に対応するために必要だ、ということを伝えていると理解しています。

自分たちで考えることによって、「なぜ自分たちがこのような使い方をしようとしているのか」「そのためには何に気を付けているのか」を説明できるようになったり、説明が求められそうな部分に事前に対応することも可能となっていきます。

岡田　コーポレートガバナンスを内部統制寄りで考えてしまうと、どうしても外的なルールを持ち込んでそれを遵守する、となりがちですが、プライバシーに関しては、企業の置かれている環境や持っている情報によって大きく対応は変わるので、自ら考えることが重要だということがガイドブックの大きなメッセージだということですね。

佐藤　ガイドブック公表後、ガイドブックを紹介



図Ⅰ-2．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.1.0の概要

（出典：経済産業省ウェブサイト https://www.meti.go.jp/press/2020/08/20200828012/20200828012-2.pdf ）

する機会をいろいろいただいています。また検討会メンバーの方々も講演会やメディア等、さまざまなルートで情報発信してくださっているので、今後さらに企業で参照していただけるのではないかと思っています。

宍戸　今、産学官すべてがデータ活用を進める必要がある中で、特に公的部門や研究機関、官民をまたいだデータ流通プラットフォーム構築を検討する場などでこのガイドブックが参照されています。そういった点からも、時代の要請に応えたものであり、さらに多くの企業で参照してもらうべきものだと思います。

■プライバシー対応は品質向上のための経営課題

岡田　一方で、企業の中でもこの問題を担当されている方は必要性を痛感されているものの、どうやって企業内にこういった捉え方を浸透させていけばよいかという悩みをお聞きすることがあります。この壁を乗り越える方法はあるのでしょうか？

佐藤　これまでは、どうしてもプライバシー対応は炎上対策等のように後ろ向きになりがちでしたが、本来は信頼を得るための前向きな活動です。そのマインドチェンジが必要だと考えています。

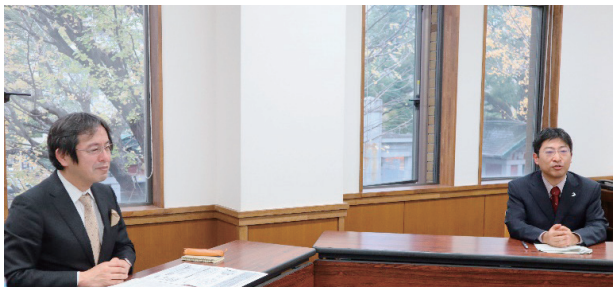
私自身も技術者としてデータを利活用する機会が多いのですが、長期的にわたって個人に関する質の高いデータを得るためには、個人から信頼を得ることが不可欠です。信頼されなければプライバシーに関わるデータは入手できません。その信頼を得るにはプライバシーへの配慮が必須になる、という点を経営層に理解してもらうことが第一歩になるのだと思います。特にAIの利用においては質の高い学習データが大量に必要です。企業の差別化を考えると、他社が持ち得ないデータ、その中でもプライバシーに関わるデータを入手し、AIに利用できるかが鍵になります。そうしたデータを得るためにもプライバシーに配慮して、個人から信頼されることが重要です。

宍戸　企業の経営層の方々で、自社商品・サービスの市場動向を考えていない方はいないと思います。さらにもう一歩踏み込んで企業の責任や企業の持続的発展を考えていれば、当然、金融や雇用の情勢も真剣にご覧になっています。これと同じようにデータも経営リソースの一つとなっているので、CFOを置くようにCIO、CPOを置く必要があるということです。

岡田　つまり、プライバシーに適切に対応するということは、自社製品・サービスの品質向上であり、経営問題だということを、ガイドブックははっきり打ち出しているということですね。

佐藤　さらに、現在、企業はSDGsのように社会・環境への貢献をコーポレートガバナンスに取り込んでいますが、その背景には、投資家やステークホルダーが企業を評価する際に重要視しているということが挙げられます。今後、プライバシーに関しても同様な動き、つまり適切にプライバシーを保護していないと投資も取引にも影響することを前提として、プライバシーに向き合ってもらいたいと思います。

宍戸　憲法の視点から言えば、SDGs等の要請はこれまで近代社会から築きあげてきた基本的人権を現代社会においても保障するための要請であり、企業についていえば「企業の社会的責任」や「ビジネスと人権に関する指導原則」で言われるように、企業には公共的役割・地位が伴い、その中で人権への配慮を課すという流れは今後さらに強まると思います。その中心にはプライバシーやデータの問題があるということを意識する必要があります。



■企業でプライバシーを考える際のポイント

岡田　佐藤先生も宍戸先生も、実際に企業が設置している有識者検討会に参加されて企業の生の声も聞かれていると思います。その中で、「ここがポイントだな」と思われる点はありますか？

佐藤　私が座長となっている企業のプライバシー検討会は、今回のガイドブックの実践的なことにも取り組んでもらっていて、第三者委員会的に数カ月に１回開催されています。そこでの経験から言うと、企業の中の人が見る視点と、外の人が見る視点は大きく異なっています。

検討会では、いわゆる個人情報に関するプライバシーポリシーよりさらにメタな、プライバシーに対する企業姿勢の明文化にも取り組んでいますが、プライバシーに関しては「相手がどう感じるか」という部分が重要になるので、外部の目を入れた検討が本当に重要だと感じています。

岡田　やはり自社だけでなく、お客様の目、ガイドブックではステークホルダーという言い方をしていますが、いろいろな視点を入れることが大切だということですね。

宍戸　私がデータ利用に関する原則の策定等に参加している企業は共通して、消費者との向き合い方を考えたり、「何がやっても良くて、何がダメなのか」を探る際に、外部有識者や消費者代表の方と議論することにとてもメリットを感じているという印象を受けます。

また、広範多岐にサービス展開していくと、企業としての全体を把握することが難しくなる場合も見られます。そういったときに事業部ごとの縦割りの視点だけでなく、外部の目で横串的に眺めたり、社会全般の動向等と照らし合わせることで、自社の全体を整理し直し、より明確に自社の方針を統一・修正することができるという面もあります。

岡田　ガイドブックでは、縦割りになりがちな組織内の情報収集・発信のハブとなるプライバシー保護組織設置の必要性も書かれていましたね。

佐藤　たとえば、これまでプライバシーには無縁と考えていたメーカー企業でも、製品販売からサービス提供へと業態が変化して、これまで接点のなかった個人の多様なデータを取り扱うようになったり、思わぬ製品がプライバシー情報を集めてしまったりといったことが起きています。さらに、相違な情報を組み合わせた結果、プライバシーに関わるケースもあり、従前のように事業部単位で管理・対応することは不可能なので、企業としての対応が必要です。そう考えると企業横断的にプライバシーを考える専門部署はきわめて重要になってきます。

宍戸　佐藤先生がご指摘のとおり、不測の形で利用者のプライバシー情報を持ってしまう可能性がある中では、全体を横断的に見る組織があった方が良いと思います。

また、今後開発する製品やサービスは、設計段階から部署横断でさまざまな視点を入れ、プライバシーバイデザインで検討していくことが重要になると思います。

さらに、ガイドブックでは企業全体としての価値向上とプライバシーの問題を取り上げています。消費者から見れば、一つのサービスで問題が発生しても「〇〇社が問題を起こした」となり、場合によってはグループ企業全体が

ダメージを受けることにもなりかねません。

岡田　今までは「同意を取っているから法律的にはクリア」と考えていた企業も少なくないと思われますが、お話を聞いていて、利用する方々に利用の目的や方法、取扱いを説明して、きちんと理解していただくことが重要だと改めて感じました。

実際にガイドブックに書かれているような内容に取り組まれている企業もすでにあると思いますが、お二人から見て「これは良い」と思われた取組みはありますか？

宍戸　難しいのは、きちんと説明しようとすればするほどどうしても説明が細かくなってしまうということです。企業法務的に考えれば「書いてあること」が重要ではあるのですが、対消費者で考えれば「自分たちが何をして、何をしないのか」を明確にわかりやすく示すことが必要です。このため、漫画や動画で伝えたり、ユーザが自分自身のデータの状況を確認できるような仕組みを用意しているケース等は参考になると思います。

佐藤　ガイドブックでは、メタなポリシーを策定することを推奨しています。まずは大きく企業としての姿勢を理解してもらえるものを示し、必要があればさらに詳細なポリシーも参照できるような二段構えの発想が求められていると思います。

■ガバナンス・イノベーションとの関係

岡田　少し話は変わりますが、ガイドブック公表の１カ月ほど前に、宍戸先生が副座長を務められた「Society5.0における新たなガバナンスモデル検討会」の報告書「GOVERNANCE INNOVATION Society5.0の実現に向けた法とアーキテクチャのリ・デザイン」が公表されました。その中では、世の中の変化に合わせて法の在り方も変化させる必要がある、といったかなり上位概念的な内容が提示されていましたが、一方で今回のガイドブックとの間には距離があるように感じました。

宍戸　ガバナンス・イノベーションに関する報告書は、広範な規制改革のシナリオとして若手の研究者・実務家の方々の自由闊達な議論から生まれたものです。

報告書のポイントの一つは、デジタル化が進む中で現在の法規制の在り方は限界を迎えているため、ゴールベースの規制に変えていくべきだという点です。

報告書では、法規制がしばしば行為規制になっているため、「この行為さえ行えば（行わなければ）良い」となり、人権や公益の実現といった本来の目的達成が阻害されてしまう状況が見られるので、まずは抽象的なゴールを設定し、企業が自らゴールを具体化してそこに向かってより良い行動を取るよう、インセンティブや制裁金等を組み合わせて、よりイノベーティブな力を引き出す規制への見直しを求めていますが、これはガイドブックにも通ずる精神です。

佐藤　ガイドブックで求めている「プライバシーに対する姿勢の明文化」は、ある意味でゴールベースの一つの取組みと言えると思います。

■改めて、プライバシーとは何なのか

岡田　ここまでお聞きして、改めての質問なのですが、お二人はプライバシーをどのようなものと捉えていらっしゃいますか？企業の方とお話をしていて、プライバシーの定義を聞かれることは多いのですが。

佐藤　プライバシーの外延を定義しようとする時点で、プライバシーを理解していないとしか言えないように思います。プライバシーは人によっても、また同じ人でもコンテキスト、たとえば会社にいるときと家では異なりま

す。企業が取得するデータやその利用を鑑みながら、何がプライバシーとなり、個人の権利利益の侵害となるかを考えて、対策を考えることが重要です。

宍戸　プライバシーが、現代においてデータ保護を求める権利というEU基本的憲章８条に書かれているような側面を持つことは間違いないとは思います。そしてそれが、個人の主観的な権利を超えて、プライバシーコミッショナーのような客観的な組織や企業の内部的な仕組み・手続き等、全体的重層的な取組みによって担保されるという点が、プライバシーの実現に関して大きなポイントだと思います。

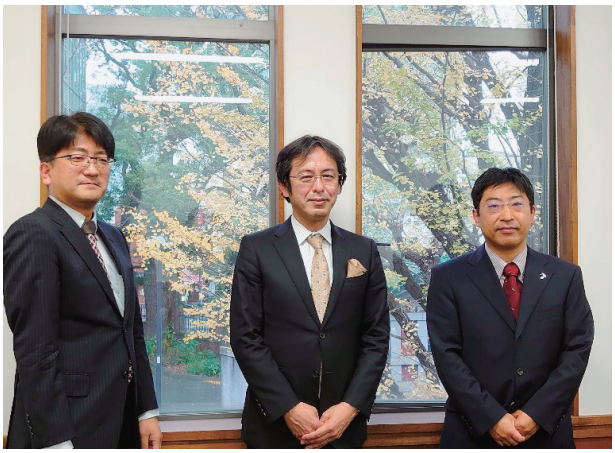
他方、佐藤先生がおっしゃるようにプライバシーの本丸を定義することは非常に難しいのですが、私はプライバシーは１人のものとして捉えるのではなく、人間と人間の関係として捉えた方が良いように考えています。企業と消費者、家族、友人の間に生まれる関係は浅い一時的なものであったり、深く継続的なものであったりとそれぞれです。そして深く継続的な関係の中ではお互いにコミットし合うような絆も成り立たせるし、同時にそこからプライバシーも生まれてきます。だからこそ、それを壊してはいけない。企業で言えば、企業が消費者やステークホルダーとより良い関係を築こうと考えるのであれば、それは同時にプライバシーについても考えるということなのだと思います。

■企業へのメッセージ

岡田　最後に、企業の中でプライバシーガバナンスに取り組んでいこうとされている方々にメッセージをお願いします。

佐藤　繰り返しになってしまいますが、プライバシー問題はどうしても後ろ向きの対応になりがちで、コストとして捉えられがちですが、ぜひマインドチェンジして、今後は、企業が信頼を得るための前向きな投資であり、サービス・商品の品質を上げるものだと捉えて取り組んでいただきたいと思います。プライバシーガバナンスガイドブックに関しては、まずは数多くの企業がプライバシー保護に取り組めるように、多様な企業が対応できるガイドブックになるように考慮しました。まずはガイドブックをお読みいただき，自社にとって保護すべきプライバシーをお考えいただき、その対応をしていただければ幸いです。

宍戸　企業で働く人は、同時に消費者でもあります。他社の提供するサービスを利用する際に、自分はどのように扱ってもらいたいか、どのような状況だと絆が結ばれ、どのような場合に絆が破壊されるかを考えていただき、それを反転させて自社の取組みに活かしていく必要があります。そういった点で、このガイドブックを企業人として読むだけでなく、ぜひ消費者の立場でも読んでみてもらいたいと思います。



岡田　今日は貴重なお話を伺い、とても勉強になりました。ありがとうございました。

参考資料
JIPDECセミナー講演レポート
「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について」

Ⅱ 欧米を中心とした新しいデータ保護にまつわる動き

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

2018年５月30日のGDPR（EU一般データ保護規則）施行から約２年半が経過し、個人データ保護を取り巻く環境も徐々に変化しつつある。特に国を越えたデータ移転に関しては、これまで議論されてきていた欧州米国間でのプライバシーシールドが無効になるなど、今後国を越えたデータビジネスへの影響もより広がっていくと考えられる。

Ⅱ-1．欧州のデータ保護関連動向

1．GDPR下での判例とその傾向

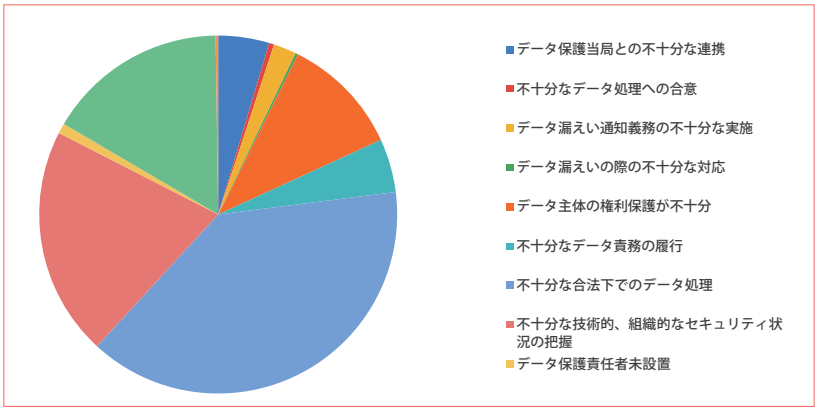
GDPRが施行されて以降、2020年11月８日（レポート執筆時）までの約２年半の期間で435件の制裁金事例が発表されている。制裁理由を順に見ていくと最も多かったのが、不十分な合法下でのデータ処理（169件）、次いで不十分な技術的、組織的なセキュリティ状況の把握（90件）、データ保護下でのデータ処理規則コンプライアンス違反（71件）となっている。上位３つの理由が全体の75％を占める結果となり、組織内でのデータ処理やコンプライアンス違反が数多く制裁理由として挙げられている（複数の制裁理由を指摘されている事例については、その中でも制裁理由として取り上げられている上位理由とした）。

制裁金事例が多い点については、企業内での個人データを取り扱う機会が増えたことも一つの理由と考えられるが、それ以外に組織内で個人データに関する共通認識がうまく浸透できていない点も考えられる。消費者保護の観点からは、事前に十分なデータ保護の対応を実施することに加えて、消費者からの問合せや個人データ漏えいが起きた際の適切な通知および対応などが早急に求められる。

GDPRに関しては、GAFAを始めとした大手テクノロジー企業に注目がいくことが多いが、実際は中小企業や非テクノロジー系の企業など、これまで個人データを十分に取り扱っていなかった企業が急速なデジタル化対応を進めていく中で、十分に内部体制が整備されていないことによって問題になるケースも少なくない。そういった意味では、昨今DXと呼ばれるようなデジタル化を推奨するだけでなく、内部での個人データ保護、および個人データ処理に関しては組織ガバナンスとして適切に対策を講じる必要がある。

2．GDPR下で執行の問題

制裁金に関してはこれまでの制裁金に関する発表を参考に紹介してきたが、一方でGDPR下のデータ保護法の下での執行に大きな課題が生じてきている。執行における問題点として、執行に係る制度設



図Ⅱ-１．GDPR Trackerよりインシデント別分類（2020/11/８時点）

計が挙げられる。欧州域内の複数国に跨りデータ利用を行う事業者に対してはワンストップショップと呼ばれる制度を導入し、代表監督当局（Supervisory Authority）と呼ばれる1カ国（大抵は本社がある国）の監督当局から承認を得ることによって、その他の国からは承認を得る必要がなくなる制度を採用している。これは、複数国に跨ってデータビジネスを実施する際の手続きを緩和するために導入が決定した制度で、域内のデータ流通の意味合いでも有効に機能すると考えられていた。しかし、実際は管理当局と他国のデータ保護監督当局（Data Protection Authority）が執行の意思決定を行うための情報提供での連携が必要になるなど、執行までの手続き上多くの問題が発生しており、想定以上に執行まで時間がかかっている。

ワンストップショップの適用と異なる決定が発表された例としてはGoogleがフランスのデータ保護監督当局によって透明性のある情報提供を行う義務に違反したとして制裁を課せられたケースがある。このケースでは最終的にGoogleの欧州統括拠点があるアイルランドデータ保護監督当局ではなく、フランスのCNIL（データ保護監督当局）が管轄権限を有する、とフランス国家評議会（Conseil d'etat）によって発表されている。Googleはアイルランドデータ保護監督当局が執行を実施していると主張していたが、データを活用してビジネスを展開する地域によって判断されるべきという判断になったケースである。

他方で、Facebookのケースではベルギーデータ監督当局との間でデータ保護に関する調査で意見交換を行った上で、どの国が代表監督当局として調査を実施するか検討に入るなど、ケースによって判断が異なり、現時点で明確な解は見つかっていない状態である。

テクノロジー企業の本社が集積するアイルランドでは、2019年10月に160万ユーロを追加で予算調達し、人員の増加を実施すると発表しており、調査体制を強化していく考えである。これにより、各国のデータ保護監督当局との連携をスムーズに行いテクノロジー大手企業への対応も強化していく方針で進めている。

3．市民団体を通じた訴訟問題

GDPRの執行に関する問題に対して、市民団体や弁護士事務所による集団訴訟も徐々に始まっている。英国とオランダでは、セールスフォースとオラクルが展開するリアルタイムビディング（広告のオークション入札）に対して、十分にユーザ同意を取得しない状態でデータ処理を実施しているとして集団訴訟が起きている。このケースではThe Privacy Collectiveと呼ばれる非営利組織が中心となり、アムステルダムの地方裁判所に申立てを行っている。提供するサードパーティCookieや広告に関するテクノロジーの解釈を争点として訴えを起こしているBureau Brandeisと呼ばれる法律事務所が訴訟を担当しており、同様にロンドンの高等裁判所ではCadwalader法律事務所が担当し訴訟を行っている。こういった集団訴訟が起こり始めている背景には、各国のデータ保護監督当局がアドテクノロジー（リアルタイムビディングを含む）に対して、適切に制裁を加えることができていないという背景がある。

英国ICO（情報コミッショナーオフィス）は2020年始めに複数のプライバシー関係者よりアドテクノロジーのデータ保護違反に関して指摘を受け、調査を開始しているにも関わらず、一定の成果を上げられていない点が指摘されている。特にデータ保護評価（DPIA）に関しては、制度として未成熟な部分が多く、データ保護監督当局も精査を行うにあたり、相当の労力が必要とされている。そのため、市民団体やプライバシー専門家からはデータ保護監督当局のリソース不足や不備などが指摘され、監督当局を通さずに集団訴訟を行うケースが生まれていると考えられる。

別のケースでは、英国のUberがADLU（アプリドライバー宅配便組合）によって採用するアルゴリズム問題を指摘されている。オランダの裁判所で行われて争点になった問題は、採用したアルゴリズムを通じて機械がドライバーに対して利用停止を促す仕組みを実装していた点が指摘されている。GDPR第22条では、「プロファイリングを含む個人に対する自動化された意思決定」という項目で、データ管理

者がデータ主体（この場合はドライバー）の権利を安全に守るために機械処理に加えて人の介入が必要なケースも定めており、Uber側でのデータ処理が適切に行われていないのではないかということがこのケースの争点になっている。背景として、ドライバーがサービス提供において不正を実施していないと主張したにも関わらず、その主張を十分に検討せず、ドライバーが不正な行為を働いたとしてシステム上で自動利用停止処理を行ったことが発端となった。Uber側は内部スタッフによって利用停止処理かどうかを精査した上で決定したと表明しているが、Uberが明記する不正に対する解釈があまりにも広義であるために、説明責任の要求をドライバーは求めている。

紹介した2つのケースは共に新しいテクノロジーを組織内部で実装し処理した事例になるため、データ保護監督当局だけでは調査および判断が難しいケースである。監督当局のリソース問題に加えて、緊急性を要する場合などは監督当局を通さずに弁護士事務所や市民団体、組合等の第三者機関を通じた訴訟などが今後も増えていくと考えられる。

4．EU-USプライバシーシールドの無効化

2000年にEUから米国にデータ移転する枠組みとして欧州委員会と米国間で合意されたセーフハーバー協定が2015年10月6日に無効（Schrems I事件）とされて以降、協定にかわる新たなフレームワークを認めるよう議論が行われ、その結果、新たな枠組み「プライバシーシールド」が2016年8月1日から開始された。しかし、2020年6月16日欧州司法裁判所（ECJ）よって「欧州が要求するデータ保護レベルに米国国内法が条件を満たしていない」と判決が下され、プライバシーシールドは無効となり、このフレームワーク利用を検討中、および、すでに利用していた米国の5,000社以上の企業が影響を受けることになった。以後は標準契約条項（SCC）を利用し、個別のケースで欧州が定める要求に十分対応できているかを精査した上で、データ移転が可能かどうかの判断を行うことになる。

条項に関しては各国のデータ保護監督当局によって精査粒度が異なることに加えて、個別企業によってはデータ移転が認められないケースがある。実際、Facebookは欧州と米国の間でのデータ移転について、欧州本社を管轄するアイルランド裁判所により、9月14日に一時的に停止するよう要求されている。

欧州と米国間では特に民間企業に対して政府による介入が合法か違法か、が問われており、欧州側は米国の既存法の下で十分にデータ保護が実現できないとして今回のフレームワークの停止に踏み切っている。米国の既存法として問題視されているのが外国情報監視法（FISA）第702条である。米国下院での可決により、国家安全保障局（NSA）が令状なしでインターネットを監視できる外国情報監視法の延長を2018年1月から6年間認められることになった。民主党および共和党の一部の議員からは反対の声が上げられたが、法によってNSAがプライバシーへの介入が可能になる期間が延長され、欧州側では米国の外国情報監視法に対する懸念からプライバシーシールドの停止に踏み切ったとされる。

フレームワーク停止問題はすでにプライバシーシールドを利用してデータ移転を実施している企業が存在していたため、対応の修正が求められる点と、中小事業者にとっては個別対応コストが重くのしかかるという点が挙げられる。

前者に関しては、Amazon社が2020年11月にドイツの欧州社会データ保護組織（EuGD）からミュンヘン裁判所に訴訟を起こされている。プライバシーシールド無効が発表されてから2カ月以上が経った段階で移行が進んでいないという理由で、消費者保護の観点から訴訟に踏み切った。

プライバシーシールドの無効化は、主に各国の政府による介入が合法的に行われるかどうかが一つの争点になっており、現在十分性認定が行われている国に関しても再度見直し等が入る可能性はある。

プライバシーシールドの無効化に伴い、欧州の一部の国ではデータ保護監督当局によって米国のクラウドシステム以外を利用するように推奨する動きが出始めている。CNILはマイクロソフトのAzure、AmazonのAWS、GoogleのCloudサービス以外を利用する推奨通知を実施している。健康データ等センシティブなデータに関しては国レベルのシステム利用

を推奨し始めている。外国情報監視法による米国企業への影響は欧州域内のビジネスにも及びつつある。

SCCに関しては2020年12月10日までコンサルティング期間が準備されており、コンサルティング後の2021年の早い段階から改訂版が発表される予定である。改訂版ではこれまで明記されていなかった点が明記されることに加えて、越境データ移転に関して事前の審査がより明確に求められるようになる。

改訂版は既存のSCCよりも広範囲に確認事項が要求される予定で、特に越境データ移転に関してはデータを輸出する国とデータを輸入する国（たとえば、欧州のフランスから米国へデータを移転する場合）、のデータ保護レベルが輸出国のデータ保護レベルに十分に準拠しているかの査定が要求される。

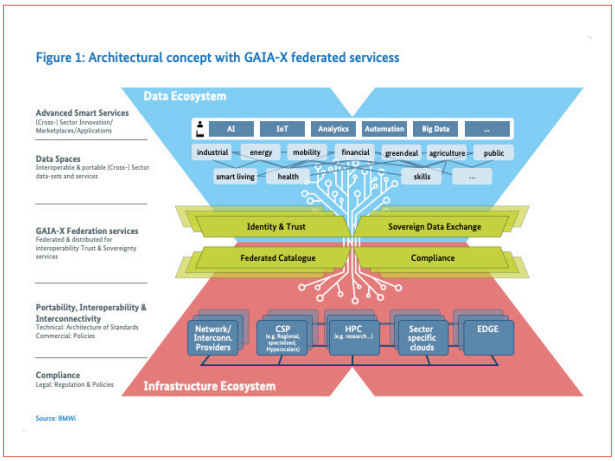
既存のSCCではデータ管理者、データ処理者に関するデータの処理に限定されていたため、それ以外の項目に関しては個別に複雑な項目を処理する必要があり、非常に非効率であった。改訂版に関しては、データ処理者間、およびデータ処理者とデータ管理者間に関しても明記される予定で、複雑なGDPRのデータ保護に幅広く対応できるように項目を広げる検討が進んでいる。

個人データのセキュリティ強度に関してはより厳格に求められる予定で、特にデータ輸出者が拠点を置く国のデータ保護レベルに関しては、政府からのデータアクセスが法的に認められるか否かが争点になる。そのため、十分な技術評価と厳格な管理が必要になる。

改訂版のSCCが有効になるまでは、既存のSCCを活用することが求められる。改定後はデータ輸出者とデータ輸入者間での見直しが必要になる。

5．欧州統一のクラウドシステムの開発

欧州ではデータ保護規則以外にもさまざまな個人データにまつわるプロジェクトをスタートさせており、欧州間で統一したクラウドシステムの開発も進めている。GAIA-Xは代表的なプロジェクトの一つである。2019年にドイツ、フランス政府の取組みとしてスタートしたプロジェクトは、財団本部をベルギーに持ち、合計で22の組織と団体（フランス11、ドイツ11）で構成されている。



図Ⅱ-２．GAIA-Xのコンセプトの図　GAIA-X資料より

GDPRや欧州サイバーセキュリティ法の下で透明性と相互互換性を担保した欧州独自のデータ共通インフラとして実装が進んでいる。

プロジェクトの背景としては、中国、米国によるクラウドマーケットの寡占化への対抗と域内の個人データへのセキュリティ懸念から独自のシステム構築に踏み切った形で、域内でのパートナー連携を今後は拡大させていく予定で、データ主権を個人に提供したクラウドシステムの設計を目指している。

6．欧州域内でのデジタルサービス提供者への新たな規制

欧州では2000年７月に電子商取引指令と呼ばれるオンラインサービスにおける指令を定めており、オンラインサービス事業者に対して透明性のある情報の提供、電子契約と中間事業者の法的責任の制限や商業的なコミュニケーションの必要性を求めている。指令は欧州域内のデジタル単一市場での電子商取引に対して、消費者との公正な取引を実現するための基準としての役割を担っている。

現在、電子商取引指令に関して新しく法制化の動きが始まっており、デジタルサービス法（Digital Service Act）と呼ばれる取引指令を規制化する議論が進んでいる。これはデジタルサービスを利用する消費者に対して、プラットフォーム企業が適切な

ユーザコンテンツ運営に対して法的責任を持つものである。これによりデジタルサービスを展開するプラットフォーマー企業はオンラインサービス上で提供されるコンテンツに対し、アルゴリズムやシステム等の透明性を担保するなど、一部責任を課せられることになるが、サーバを通じて違法なコンテンツが流通した際のプラットフォーマーの責任は免除される可能性がある。これは、取引指令から引き継がれる可能性が高い免除内容の一つで、現在責任の所在に関して議論が行われている。

プラットフォーマーに対しては相互に互換性のある仕組みを検討し、データ共有が実現できるように取り組むように働きかけを行っている。実際に、大手EC取引事業社（Amazon、Alibaba、eBay、楽天等を始めとしたオンライン商取引事業者）、ソーシャルメディア等サービス事業社（Facebook等）と欧州委員会ディディエ・レンデルス議員は面会を行い、コロナ禍でプラットフォームを利用する不正取引事業社の取締りに関して協力するように訴えかけている。特にコロナ禍では、インターネットプラットフォームを介して商品を購入する機会が増えたことにより、不正な取引や詐欺取引が横行していることから、消費者保護に向けた協力を進めていきたいという意向を欧州委員会では示している。

7．デジタル広告のフレームワークに関する動き

ネット広告業界団体のIAB 欧州（Interactive Advertising Bureau）はIAB Tech Labと協力し、2019年８月21日にTCF v2.0（透明性と同意のフレームワーク）を発表し、広告主や媒体を運営する企業、アド（広告）テクノロジーベンダーらが規制への準拠を支援する枠組みを公開している。このフレームワークに沿ってCMP（同意取得・管理プラットフォーム）等の実装が行われており、アドテクノロジーベンダーの間で幅広く普及が期待されていた。

GDPRや想定されていたeプライバシー法（2017年より検討が進んでいたが、現時点では業界団体からの反対等もあり、2021年の制定も見送る方針）対策としてフレームワークを標準的に活用する機運が高まっていた。しかし、10月にベルギーデータ保護監督当局より、IAB欧州が提供するTCFに関して、GDPRが定める法的な要求を満たしていない、RTB（リアルタイムビディング）のような広告オークションの仕組みは高速で個人データの取引が行われるため、法で定めるデータセキュリティ要求に見合っていない、という見解が調査を通じて発表された。

これに対してIAB欧州側はブログを通じて指摘を受けた点に対する返答と、引き続きデータ保護監督当局とは意見交換を行っていくと発表した。加えて、今回のベルギー当局からの調査に関しては第一回のレビューでフレームワーク運営すべてに影響することはないと発表している。今後は、ベルギーデータ保護当局以外とも定期的に情報交換およびフレームワーク自体の改善も発表していくと考えられるため、アドテクノロジー分野のビジネスはフレームワーク動向に注目が必要だと考える。

TCF以外にも各国の個人データ保護法の下で明確に個人データに関する定義を定めていない地域もあるため、アドテクノロジービジネスに関しては、各国のデータ保護制度の変化に敏感に対応していくことが必要になる。

8．日本に関連した今後の影響

（1）GDPR対策の動き

GDPRを前提にしたガイドラインが数多く発表されているが、事業者としてはガイドラインの読込みを前提知識として準備が必要になると考えられる。国内ではテクノロジー大手企業を中心に多額な賠償金の判例が取り上げられることが多いが、中小規模の企業を対象にした判例も数多く公開されているので、所属する業種に合わせてどういったインシデントが起きる可能性があるか、事前に確認した上で対策を実施する必要がある。

データの越境移転に関しては、2021年のBrexit後の欧州と英国間でのデータ移転に関する議論が大きなテーマになると考えられる。これまで英国と日本でデータ移転を実施していた企業も見直しが入る可能性があるので、今後の動向およびアップデートに注目する必要がある。

（2）フレームワークの妥当性に関する動き

デジタル広告を始めとしてこれまで数多くのフレームワークを業界団体が開発してきているが、ここにきてフレームワークと法の整合性に関する議論が行われている。代表的なデジタル広告のフレームワーク（TCF）に関しては、ベルギーデータ保護監督当局より前述のとおり指摘されており、今回の調査以外にも、法との整合性に関する議論を実施していく中でフレームワーク自体が修正される可能性がある。そのため、現在利用しているGDPR対策ソリューションが十分にGDPRの要求を満たしているか、見直しも迫られる可能性も出てくるため、今後の判決や動向のアップデート、およびデータ保護インパクト評価（DPIA）を行う必要があると考える。

Ⅱ-2．米国のプライバシー関連動向

1．CCPAの施行とプライバシー判例動向

2020年1月より施行されたCCPA（カリフォルニア州消費者プライバシー法）は施行当初、子供のプライバシー等を中心に精査を行うと発表されており、7月1日には最終的な修正案が司法長官によって承認された。修正案の中にはいくつか個人データの取扱いに関してポイントとなる点が見られる。

一つがAB713（匿名化された健康情報に関する法案）によるCCPAの適用除外である。これは、HIPPA（医療情報のポータビリティおよびアカウンタビリティ法）の要件に従い、匿名化された情報に関してCCPAの適用条件が除外されるというもの。これまではHIPPAとCCPA双方で匿名化に関する条件が異なっていたため、双方の法律が適用されることで医療関連のデータ処理が複雑になることが問題とされていた。今回はその修正が加えられた形となった。加えてAB1281（従業員情報および企業間取引における個人データに関する法律の適用猶予を2022年1月1日まで延長する法案）が9月に承認されたことである。なお、11月3日に実施された住民投票によってカリフォルニアプライバシー権利法（CPRA）が承認されたため、適用除外は2023年1月まで延長された。

2．2020年にCCPAの下で起きた訴訟

2020年1月に施行されて以来、CCPAの下で23件の訴訟が確認されている（IAPP調べ、2020年10月19日まで）。代表的な訴訟は2月3日に提訴されたセールスフォースおよび子供服販売のハンナ・アンダーソンに対する集団訴訟の問題である。この訴訟ではセールスフォースのソリューションから流出した個人データに関して、暗号化された個人データが不正アクセスを受けた場合にCCPA違反となるかどうかが争点になっている。

Zoomに対する集団訴訟問題は、利用者に対して明確な同意なくFacebookを含む第三者に対して個人データを公開していた問題が問われている。この問題は、ZoomがSDK（ソフトウェアデベロップメントキット）と呼ばれるFacebookが提供していたソフトウェア開発キットを導入することで、開発キットを通じてFacebookに同意なく個人データが渡っていたにも関わらず、プライバシーポリシー等で十分に説明を実施していなかった点が争点になっている。

これ以外にもソーシャルメディアサービスを中心として訴訟が起こっており、今後、カリフォルニアを中心にデータビジネスを展開する際には事前に対策を確認しておく必要がある。

3．カリフォルニア州プライバシー権法の可決と今後

大統領選が行われた11月3日にカリフォルニアでは複数の住民投票が同じタイミングで実施された（最終的に賛成9,233,900票、反対7,203,295票で可決）。CPRAはCCPAの提案にも関わったプライバシー保護団体の「カリフォルニアンズ・フォー・コンシューマ・プライバシー（Californians for Consumer Privacy）」によって推進され、これまでCCPA下で争点になっていたデータの第三者提供の解釈を“Selling（販売）”ではなく、“Share（共有）”と解釈して規制を回避しようとする企業に対し、よりプライバシーが保護される仕組みを設計する狙いから始まっている。CPRAは2023年1月以降で施行

される予定で、それまではCCPAの下でプライバシー規制が行われる。CPRAの施行によって変化していくポイントとしては、以下の点が考えられる。

・ビジネス目的での個人データ共有の制限
・正確な位置情報、人種、医療情報等のセンシティブな個人データにあたる情報の利用制限
・必要以上の個人データ保持の禁止
・16歳以下の個人データに対する罰則の強化
・カリフォルニア州プライバシー保護庁の設置
・消費者のプライベート権利の拡大
・オプトアウトリンクへの新たな責務の作成

これ以外にCCPAでは“Sell”という解釈だけでなく、“Sharing”という文言が追加され、新しく金銭的な見返りに関わらず、第三者間でビジネス上価値のある行為を行っている場合（“cross-context behavioral advertising（クロスコンテキスト行動ターゲティング広告）”）に適応されることになる。

消費者は“Sell”、“Sharing”が行われたデータをオプトアウト請求できるというのがCCPAに追加される新しい考え方である。これ以外にも一部消費者に対して権利を認めるなど、CCPAと比較してプライバシー保護を強化した形の法案として検討されていく予定である。

4．米国連邦プライバシー法の制定と議論

連邦プライバシー法に関する政策は民主、共和両党からすでに提出されており、選挙後に一部動きがあると考えられる。民主党上院議員により2019年11月に消費者オンラインプライバシー権法（COPRA）が提出されている。背景にはオンラインを通じたサービス利用が拡大したことに加え、消費者のプライバシー権を守るだけでなく、消費者の同意なくデータ利用を進める事業者に対する懸念と姿勢を変えていく必要性から法案の提出に至っている。

一方の共和党上院議員により消費者データ保護法（CDPA）、米国消費者データプライバシー法（USCDPA）が提出され、米国国民が消費者として事業者に対し責任を追及できる権利を認めるものとして議論が進められている。

CDPAに関しては両党でも合意されており、今後上院での議論が進められていくと考えられるが、一方で事業者に対して猶予を与えるような解釈にならないか、健康データとは一体何か、など明確になっていない点も多く、今後の議論を通じて具体化していくと考えられる。

連邦法で争点になっているのがプリエンプション（州の法規に対する連邦法規の優先）に関する問題で、消費者が居住する州によってプライバシー保護に対するレベルが異なることを現時点では懸念しており、消費者保護の一貫性を前提にした上で議論が進められていくのではないかとBROOKINGS等の現地メディアが予測している。

連邦法の議論に関しては、USCDPAを修正する形で2020年９月に紹介されたSAFE DATA法（データアクセス、透明性、アカウンタビリティにおける米国のフレームワークを制定した法律）、民主党上院議員、無所属の上院議員が提出した米国生態情報プライバシー法（同意なく生態情報を取得し、取引を行うことは違法であり、顔認識や機械学習等のテクノロジーを活用する際に検討が必要）なども検討されており、連邦プライバシー法の動向は引き続き注目が必要な分野である。

大統領選後はこれまで提出されてきた連邦プライバシー法に関して一部議論が進む可能性があるので、米国で展開する事業者はそれぞれの分野で確認が必要になると考えられる。特にコロナ禍での医療データおよび子供のデータ等は連邦取引委員会（FTC）から警告を受けるケース（TikTokの訴訟等）も増えてきているので、対策が必要になると考えられる。

5．顔認識技術に対する動き

顔認識技術に関してはIBMやマイクロソフト等、これまでに開発を主導してきた企業が一部開発を中止するなど、転換期に差し掛かっている。背景として、技術的な問題に加え、社会全体で顔認識技術に対する姿勢が変化してきているため、社会全体で実装を積極的に進めていく動きに変化が起きている。

米国のオレゴン州ポートランドでは2021年１月よ

りポートランド警察での顔認識技術の利用、および公園や建物等の公共施設（公の学校は除く）での技術の採用を禁止する投票を可決した。ブラック・ライヴズ・マター騒動以降、カリフォルニア州のサンフランシスコ、オークランド、マサチューセッツ州のサマービルの地下鉄でも顔認識技術の利用を禁止する動きが出てきている。

2008年に各州に先駆けて生体認証に関連した法律の制定を行ったイリノイ州では、2015年11月20日にFacebookの顔認証によるタグ付けでのクラスアクション訴訟を一時却下したものの、2020年１月29日にFacebook側から訴訟に対して和解金として600億円を支払う合意を発表している。

アメリカ合衆国税関・国境警備局では生体認証を活用した出入国プログラム（CBP）を実施していたが、政府アカウンタビリティ局（GAO）によって実施された監査で技術的、および運用における問題が発覚し（利用者からのデータ提供要求への不十分な対応、顔認識がどの時点で実施されているかサイト上などで不十分な説明等）、NEC等のパートナー企業に対してもプライバシーを前提にしたコンプライアンス要求に従うように通知された。

GAOによる指摘の中には、CBP全体で十分にプログラムのポリシー設計がなされていなかったこと、技術提供を行うパートナーの監査を十分に実施していなかったことなどが指摘され、同時に技術自体のバイアス等が指摘された。

公共施設に関してはニューヨーク州で2022年までに一時的に学校内での顔認識技術利用を禁止すると発表された。背景にはニューヨーク自由人権協会から2019年にニューヨーク州教育部門が顔認識技術をLockport City Schoolsで採用した件に関して訴訟を起こしていたことが発端となり、学生のデータ保護の権利を毀損しているとして、学生の親から要望を受けていたものである。

このように公の施設や場所での顔認識技術に関する風当たりは徐々に強くなり始めており、技術的な正確性だけでなく、導入にあたってのリスクを十分に検討しておく必要がある。

6．市民および第三者機関によるプライバシーモニタリング組織の動き

法律によるプライバシー規制に加えて、非営利組織や人権団体などを通じた訴訟、およびクラスアクションのケースが徐々に際立ってきている。アメリカ自由人権協会（ACLU）、ACLUイリノイを含めた複数の非営利、人権団体は顔認識技術を提供するClearviewAIに対して訴訟を行い、顔認識技術の危険性に警鐘を鳴らしている。

イリノイの裁判所に持ち込まれたケースでは、イリノイ州の生体認証情報プライバシー権法（BIPA）の下でソーシャルメディア上の個人データをスクレーピングし、個人の同意なくプロファイリングを実施していることを問題としている。ClearviewAIは訴訟を受けて民間企業とのデータ販売の契約（イリノイ州内）を停止し、ライセンスを提供する政府機関のみの契約に変更した。これによってBIPAによる訴訟の免除を訴えているが、それに対して人権団体等からはClearviewAIから原告に対しての説明がないことに加えて、第三者へのデータ提供契約による被害に対しての法的な責任の議論がなされていないことなどを継続して訴えている。

ACLUなどの人権団体以外でもアプリから取得される個人データ権利侵害が発生していないか指摘、警告する第三者組織が誕生している。Future of Privacy Forumよりスピンアウトした国際デジタルアカウンタビリティカウンシル（IDAC）は代表的な非営利組織の一つで、AppleやGoogleが展開するアプリストアを通じてダウンロードできるアプリの調査を実施し、個人データの権利侵害が考えられる際は警告や公表などを実施している。SDK等開発環境をより快適にする仕組みが徐々に普及する一方で、こういった仕組みを通じて違法にデータを取得する（厳密にはプライバシーポリシー上で定義された以上のデータを取得、およびSDK等を提供する第三者へ同意なく転送される）ケースも増えてきており、違法なケースを未然に防ぐために第三者組織が組成され、調査にあたっている。

組織内には弁護士を始めとした法の専門家に加えて、テクノロジーに長けたエンジニアなど複数の

バックグランドを持つ専門家が参加し調査にあたっている。このような動きは各国で非営利組織を中心に立ち上がっており、各国の非営利組織間の連携が今後は進んでいくと考えられる。

10月に発表されたTechcrunchの記事ではIDACが対応したケースが紹介されている。Googleのデータポリシーに違反していた3つのゲームアプリ（Princess Salon、Number Coloring、Cats & Cosplay）がストア上から削除されており、Unity、Umeng（アリババグループのアプリプロモーションプラットフォーム）、Appodeal（モバイル収益化プラットフォーム）のSDKsを活用してアンドロイドID、アンドロイド広告IDを取得していたことが原因となった。特に子供が利用するゲームコンテンツなどはプライバシーポリシーを含めた同意を十分に検討する必要（親の同意含め）があり、ストアなどのプラットフォームのプライバシーポリシーとの整合性（Inconsistency）が求められる。

7．日本に関連した今後の影響

（1）連邦法に関する議論

米国ではオバマ政権以来、連邦法を前提としたプライバシー法に関する議論を積極的に進めてきた。テクノロジーの広がりに伴い、消費者保護の視点から対策が必要になっていることに加えて、越境データ移転に関してはプライバシーシールドが無効とされた判決による影響によって、国内法（消費者プライバシーよりは政府による監視の文脈）の見直しが迫られている。仮に連邦法の議論が進めば、現在の州法とのプリエンプション（州の法規に対する連邦法規の優先）に関する問題が事業者視点では重要になると考えられる。これまでは各州での対策が求められていたが、連邦法でプライバシー法が制定された場合は州法規制との関連性を確認しておく必要がある。また、取り扱うデータによっては（医療データや子供のデータ等）、これまでの法規制とどのように関連してくるのかを理解しておく必要がある。

（2）州法に関する議論

前述のとおり、カリフォルニア州では11月3日の住民投票を通過したためCCPAを改定し、CPRAを2023年施行する事が決定した。これにより住民がセンシティブ情報（位置情報、生態情報等をSPIと定義）の販売制限を要求することが可能になったことに加えて、16歳以下のユーザに対するオプトイン等の要求、カリフォルニアプライバシー保護当局の設置など、これまで以上にプライバシー強化の方向に進んでいくことになる。CCPAのように一律でオプトアウトができるような仕組みとは異なり、マニュアルでサイトごとのオプトアウトが要求されている点も今回新たに加わったポイントになる。

ACLUやEEF（電子フロンティア財団）はCPRAに対して反対の立場を主張しており、事業者側でプライバシーに厳格なユーザに対して公正なサービス提供を実施しなくなる可能性に言及している。（データ取得を拒む際にディスカウントや特定サービスへのアクセスを制限する）。以上の動きからCPRAに関しては2023年施行と少し期間が開くものの、特に広告モデルを始めとしたデータ共有型のビジネスへの影響はより強くなっていくと考えられるため、サードパーティCookieに加えて、日本企業を含めた提供先のデータ保護の内部デューデリジェンス等は、より厳しく求められると考えられる。

（3）越境のデータ移転に関して

越境データ移転に関しては直接米国からの影響を受けるというよりは、日本企業が米国企業のサービス（クラウド等）の導入を実施している場合、欧州に居住する個人のデータを米国のサービスを介して取り扱う際に問題になる可能性がある。越境データの取扱いに関しては、EDPB（欧州データ保護委員会）が発表したガイドラインで、追加の精査（Supplementary Measurement）が求められるとされており、移転元（Exporter）と移転先（Importer）がそれぞれ国を越えてデータ移転が行われる際に、移転先の国が十分にデータ保護レベルに達しているかを事前に精査する必要が出てくる。米国は欧州基準で十分にデータ保護が実施されていないため、日本企業にデータ移転が行われた際、米国サーバ上に個人データが保管されるケースなどで問題になる可能性はある。

越境移転に関しては欧州と米国の企業の間でもプライバシーシールドの無効により、数多くの中小規模事業者が損害を被ることになっている。プライバシーシールドの代替としてSCCを国ごとに確認して、導入を実施していく必要があり、今後日本と欧州の十分性の議論によっては検討が必要になる可能性も考えられる。

（4）その他の動き

大手プラットフォーマーに関しては軒並みプライバシーを重視した動きへと戦略の転換を始めている。AppleはiOS14でよりプライバシーを強化する方向性を発表している。特にアプリ等の開発者およびこれまでAppleが広告で使用していたIDFA（広告識別子）を活用してビジネスを展開していた事業者にとっては、大きく事業戦略の見直しが必要になるだろう。デジタルマーケティング活動においてプロモーションでプラットフォームを選定する際には、AndroidとiOS双方を規約レベルで見比べた上で自社に合わせたプロモーションの選定を行う必要が出てくる。

Ⅱ-3. アジア圏のプライバシー関連動向

最近ではシンガポールでの個人情報保護法（PDPA）に関する動きがいくつか発生している。Data Protection Excellence（DPEX）センターは2016年以降、4年続けて罰則に関するレポートを公表している。2016年には23件、2017年には18件、2018年には23件、そして2019年8月までには26件まで増加している。2020年に発生した例を紹介すると、自動車配車アプリのGrabが2019年8月に個人情報保護委員会（PDPC）へ展開するモバイルアプリの脆弱性を報告し、その後追加調査でGrabHitchのドライバー21,541人の個人データへ非承認アクセスが可能になっていたことが判明した。この件でPDPCより罰金として7,325ドルと120日以内にプライバシーポリシーに見直し要求を求められた。このケースでは始めの報告よりAPIのアップデートを実施していたが、十分にデータ保護対策が実施されていなかった点が問題になっている。

Ⅱ-4. 全体の総括

GDPR施行から2年以上経ち、数多くの判例が各国のデータ保護監督当局によって公表されてきている。国内では一部罰則が大きな事例として取り上げられることが多いが（当初の制裁金よりは減額されるケースも出てきている）、多くは消費者保護の観点から組織内でのデータ管理のミスやアクセス制御に関する問題、同意取得やデータの目的外利用など、組織内の初歩的なミスが指摘されることが多い。

これは企業としてデータ利用を進めていきたいという思惑がありつつも、十分に組織体制が作れていないことの現れであり、国内で取り上げられる大手テクノロジー企業への制裁と比較して、実際は中小規模の非テクノロジー企業が対象になることが多い。大手企業の場合は潤沢に資産があるため、人材や技術への投資が可能であるが、人材や資金に限界がある中小企業にとっては非常に悩ましい問題でもある。そのため、海外ではチェックポイント等を通じて事前にリスクになりそうなポイントを把握するなど、資金的に難しい場合にも対応できる方法の模索が進んでいる。

今後、GDPRだけでなくカリフォルニアで可決したCPRAに加え、ブラジル、中国など世界的に個人データの取扱いに関しては見直しが始まっているため、国内の個人データ保護に関してもある程度各国との整合性を取らざるを得ないのではないかと考える。そういった中で、特に中小規模の事業者は、できる限り必要ないデータを取得せず、かつ目的に沿った形でのみデータ利用を検討することが必要になってくるのではないか。個人データの問題は国内法だけでなく、データ移転の問題から海外動向も理解した上で、データ活用を検討する必要があり、今後はよりその流れが加速していくものと考えられる。

〈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「電子計算機処理に係る個人情報の保護に関する条例」施行 コンピュータ処理された個人情報の適正な管理が目的（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個人情報保護マネジメントシステムー要求事項」制定（３/20）	1999		
	2000	カナダ	「個人情報保護及び電子文書法」制定
		EU-アメリカ	EU・米国間における「セーフハーバー協定」締結（７月）
	2001	アメリカ	「米国愛国者法」制定（10/26）。2015年６月失効
「個人情報保護法」公布・一部施行（５/30）	2003		
	2004	APEC	「APECプライバシーフレームワーク」採択（10/29）
「個人情報保護法」全面施行（４/１）	2005		
「JIS Q 15001：2006」改正（５月）	2006		
	2007	APEC	「越境プライバシールール」策定 「パスファインダープロジェクト」の試験的な取組み開始
	2012	EU	「EUデータ保護規則案」提出
		アメリカ	「消費者プライバシー権利章典」が掲載された行政白書にオバマ大統領が署名（２/23）
「行政手続における特定の個人を識別するための番号の利用等に関する法律」および関連法公布（５/31）	2013	OECD	「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」改正（７/11）

国　内	年	海　外	
特定個人情報保護委員会発足（1/1）	2014		
APEC越境プライバシールール（CBPR）システムに参加（4月）			
「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」成立（9/3）	2015	アメリカ	・「米国自由法」成立（6/2） ・「サイバーセキュリティ情報共有法」にオバマ大統領が署名（12/18）
		EU-アメリカ	欧州で「セーフハーバー協定」無効判決（10月）
特定個人情報保護委員会が改組し、個人情報保護委員会発足（1/1）	2016	EU	欧州本会議「一般データ保護規則（GDPR）」を正式可決（4/14）
APEC-CBPRシステムの認証団体として、JIPDECがアカウンタビリティ・エージェント（AA）に認定（1月）			
個人情報保護委員会、アジア太平洋プライバシー機関フォーラム（APPA）の正式メンバーに就任（6月）			
「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）		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
「改正個人情報保護法」全面施行（5/30）	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）
		中国	「中華人民共和国サイバーセキュリティ法（インターネット安全法）」施行（6/1）
「JIS Q 15001：2017」改正（12/20）		ドイツ	GDPR施行に向け「連邦データ保護法」全面改正（6/30）
情報銀行に求められる「情報信託機能の認定に係る指針ver.1.0」公表（6/26）。 2019年10月にver2.0公表	2018	EU	「EU一般データ保護規則（GDPR）」施行（5/25）
日-EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意確認、および個人データの越境移転に言及した共同声明発出（7/17）		ベトナム	「サイバーセキュリティ法」公布。国内でのデータ保存と事務所設置を義務化（6/12）。 2019年1月1日施行
「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年1月23日施行		フランス	「個人情報保護に関する法律」成立（5/14）
		EU-米国	欧州議会、「プライバシーシールド」がEUの求める保護水準に達していないとして、米国当局に対応を要求（7/5） 米商務省は「準拠している」と声明（8/30）
		ベルギー	「個人データの処理に関する保護法」制定（7/30）
		イタリア	「改正個人データ保護法典」施行（9/19）
		米国	「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年1月1日施行
		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）

国　内	年	海　外	
	2019	タイ	「個人情報保護法（PDPA）」施行（5/28） 2020年5月完全施行がコロナの影響で1年延期
「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）	2020	EU-米国	EU司法裁、「プライバシーシールド」無効判決（7/16）
「DX時代における企業のプライバシーガバナンスガイドブックver1.0」策定（8/28）		米国	「CCPA」改正提議が住民投票で可決。より厳しい「カリフォルニア州プライバシー権利法（CPRA）」承認（7月）
		EU	欧州委員会、プライバシーシールの無効判決を受け、標準契約条項（SCC）改定案発表（11/12）

〈資料2〉情報化に関する動向（2020年４月～2020年９月）

国　内	海　外
2020年４月	
・航空、空港、鉄道、物流事業者、計66社参加の「交通ISAC（アイザック）」発足。サイバーセキュリティの情報共有・分析を図る。 ・LINE、COVID-19対策調査で約2,450万人から回答。オンライン調査上桁違いの回答数。 ・政府、COVID-19対策に向け、官民合同のデータ活用会議「テックチーム」設置。IT大手企業に利用者データ提供を求める。 ・政府、COVID-19緊急事態宣言。 ・教育機関SaaSのClassi、不正アクセスで約122万ユーザのIDが閲覧可能に。 ・NTTデータ経営研究所調査、情報銀行利用に関し、消費者の７割が位置情報の提供に否定的。 ・任天堂、なりすましによりID約16万件への不正ログインの可能性。６月には新たに14万件の被害判明。 ・トレンドマイクロ調査、COVID-19を悪用したサイバー攻撃被害が増加。３カ月で6,500件超。	・欧州アプリ開発団体PEPP-PT、GDPR準拠の新型コロナウイルス感染症（COVID-19）追跡アプリのコード公開。 ・マリオットホテル、約520万人の個人情報漏えいの可能性を発表。2018年の3.9億件の不正アクセス事件から２年も経たず。 ・中国政府、国際電気通信連合（ITU）に新たなインターネットプロトコルを提案。米国等は中国国営プロバイダによる市民のインターネット利用統制を懸念。 ・台湾やインド政府、Zoomの公務利用禁止。セキュリティを問題視。 ・仏競争当局、Googleにニュース記事使用料支払いについてメディアとの協議命令。 ・仮想通貨取引所Uniswapと貸付プラットフォームLendf.Me、サイバー攻撃で2,500万ドル相当の仮想通貨盗難被害。 ・COVID-19給付金詐欺、世界各国で多発。ドイツでは数千万ドルの被害。 ・豪政府、COVID-19感染者追跡アプリが公開半日で110万DL。

国　内	海　外
2020年５月	
・IPA、DX促進の一環で、デジタル技術を取り入れたビジネス変革に取り組む優良企業の認定開始。 ・総務省他調査、脆弱なIoT機器、マルウェア感染したIoT機器利用者への注意喚起、2019年度は延べ2,249件。 ・政府、緊急事態解除宣言。 ・「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」成立。巨大IT企業の公正な取引遂行が狙い。 ・「スーパーシティ法」成立。AI、ビッグデータ活用の最先端都市の実現を目指す。 ・NTTドコモ、厚労省のCOVID-19クラスター対策に、モバイル空間人口統計データ提供で協力。	・欧州データ保護会議（EDPB）、個人データ使用時のオンラインでの同意に関する規約のため、最新の指針発表。 ・米商務省、華為と関連企業に対する米国内外製品の輸出管理を強化。許可ない再輸出を禁止。 ・世界的知的所有権機関、電子書籍の真正性証明のタイムスタンプサービス開始。 ・タイ通信最大手AIS、80億件以上のインターネット利用記録流出。 ・豪研究チーム、超高速データ転送システムで世界新記録。１秒でHD映画1,000本転送可能。 ・Twitter、トランプ大統領の投稿に初の真偽確認警告。これを受け大統領はSNS企業規制の大統領令に署名。

国　内	海　外
2020年 6 月	
・改正個人情報保護法成立。個人の権利保護、事故時の国への報告と本人への通知責務、仮名加工情報の創設、第三者提供時の同意確認義務、外国事業者への罰則適用などを規制。 ・改正著作権法成立。違法にアップロードされた漫画、映像を違法と知りつつダウンロードする行為も対象に。 ・東京地方裁判所、神奈川県のHDD転売事件で懲役 2 年の有罪判決。 ・NTT東・西日本、ハローページ発行を2021年10月から順次終了へ。 ・厚生労働省、COVID-19 接触確認アプリ「COCOA」公開。公開 8 時間で85万件、24時間で179万件DL。 ・スパコン「富岳」、計算速度で 8 年半ぶりの世界一位獲得。	・Google、プライベートモード設定ブラウザの閲覧記録の不正収集はプライバシー侵害に当たるとして、賠償額50億ドルを求める集団訴訟に。 ・IBM、顔認識技術開発事業から撤退。 ・Amazon、警察で自社の顔認識技術使用を 1 年停止に。 ・Google、差別的なターゲティング広告表示を禁じ、違法差別をなくす取組みに着手。 ・Microsoft（MS）、2019年の警察への顔認識技術販売拒否について見解を再表明。人権法による規制なくして技術の使用認めず。 ・セキュリティ企業Awake Security報告、Google Chrome向け拡張機能で170万人超の個人情報が大量窃取。 ・Oracle、世界各国のユーザデータ数十億件流出。セキュリティが脆弱なサーバにパスワード設定なしで保管。 ・ドイツ連邦裁判所、Facebookに対し独カルテル庁のデータ収集制限に従うよう判決。F社は不服申立て裁判を開始。

国　内	海　外
2020年 7 月	
・政府、「規制改革実施計画」で、電子署名のない電子証明書の法的効力を認める見解。行政手続きでの脱ハンコによるデジタル化にも言及。 ・JPCERT/CC他、マルウェアEmotetの被害拡大を注意喚起。2019年10月の感染拡大後、一時鎮静化するも再拡大の恐れ。 ・個人情報保護委員会、破産者情報掲載サイトに対し、本人同意取得や利用目的提示なしは保護法違反として、運営停止命令。 ・フィッシング対策協議会調査、フィッシング詐欺メールの報告が2020年上期で6.6万件。大手サイトになりすましたメールやSMSを不特定多数に送り偽サイトに誘導する手口多し。	・顔認証技術提供のClearview AI、カナダ全法的機関が契約打切り。ネット上の顔写真30億枚の無断収集行為を問題視。 ・Apple、アイルランドの税優遇を違法とするEUからの130億ユーロの追徴課税命令に対する不服申立て裁判で勝訴。 ・MS、Google、Amazon、生体認証データの無断使用はイリノイ州生体認証情報私権法違反として州民が提訴。 ・欧州司法裁判所、「プライバシーシールド」無効判決。データ移転に関し、米国国内法による監視行為がEU法上の保護と同等レベルと認められないと判断。 ・豪競争・消費者委員会、Googleがユーザに明確な同意説明を行わずにユーザデータを収集しているとして提訴。 ・豪政府、FacebookとGoogleにメディア記事使用料の支払いを義務づけ。支払い強制は豪政府が初。

国　内	海　外
2020年 8 月	
・国勢調査100周年。COVID-19、プライバシー意識の変化等への対応として、インターネット回答 5 割を目標に。 ・NECや富士通他、「デジタルトラスト協議会」設立。電子認証の法制度への提言や電子認証サービス共通化の検討に着手。 ・内閣サイバーセキュリティセンター調査、国内38社を含む世界900社のVPNの暗証番号流出の可能性。ロシアのハッカー関与。 ・経済産業省と総務省、「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ver1.0」策定。経営者が行うべき 3 要件、プライバシーガバナンス構築上取り組むべき事項をとりまとめ。 ・日・英政府、政府による個人・企業のデータ収集制限で大筋合意。11月に日英通商協定締結。	・Twitter、米連邦取引委員会（FTC）から個人情報不正利用を指摘され、最大 2 億5,000万ドルの罰金の可能性。 ・英内務省、人種差別的との批判を受けアルゴリズム利用のビザ申請審査を中止。 ・TikTok、Andoroid端末で個別の識別番号収集。Googleの利用者追跡制限規則に違反。 ・英控訴裁判所、南ウェールズ警察の顔認識システム利用は人権侵害で違法と判決。利用場所や照合対象者に対する運用ルールが不十分。 ・Qualcomm、FTCによる反トラスト法違反訴訟で、連邦高等裁判所が連邦地方裁判所の違反判決を破棄し、逆転勝利。 ・OracleとSalesforce、サードパーティCookieによるデータ収集がGDPR違反にあたるとして、英・蘭で集団訴訟に。 ・米連邦地方裁判所、Facebookの生体認証データの同意なし収集に関する2015年の集団訴訟に対し、和解合意を仮承諾。和解金6.5億ドル。 ・米司法省、Uber元CSOを起訴。2016年に発生した5,700万人のデータ漏えいを 1 年間隠ぺい。 ・無料素材サイトFreepik、サイバー攻撃で830万ユーザの情報流出。

国　内	海　外
2020年 9 月	
・NTTドコモ、電子決済サービス「ドコモ口座」経由で複数の提携銀行の預貯金不正引出し発覚。本人確認の仕組み不十分。最終被害総額は約2,850万円。 ・ゆうちょ銀行、キャッシュレス決済サービスの不正引出し被害。連携企業 7 社で計2,150万円の被害。 ・SBI証券、顧客の証券口座への不正ログインで約9,800万円が偽口座に送金。 ・PayPay、ゆうちょ銀行、イオン銀行、愛知銀行で不正引出し被害。被害総額は約265万円。 ・LINE、パスワード攻撃で約7.4万件アカウントのログイン情報特定。	・WordPress、35万以上のサイトにリモートでコードが実行できる脆弱性発覚。 ・米連邦控訴裁判所、国家安全保障局が大規模な米国民の通話記録を電話事業者から収集した活動は米国自由法および憲法違法と判断。 ・シカゴ連邦地方裁判所、Googleが位置情報で特定地域にいるすべての人を割り出し警察に提供する「ジオフェンス令状」は違憲と判決。 ・仮想通貨取引所KuCoin、大規模ハッキング攻撃で1.5億ドル相当の流出被害。11月に大半の資金回収を発表。

JIPDEC IT-Report 2020 Winter
2020年12月21日発行（通巻第16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　　FAX：03-5573-0561
制　作　株式会社ウィザップ