IT-REPORT

IT-REPORT 2021 Winter

特集 プライバシー保護規制とデータの利活用

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 2021 Winter」は、「プライバシー保護規制とデータの利活用」と題し、特集を組みました。

わが国では、2021年４月１日に改正個人情報保護法が全面施行され、個人の権利利益が保護されるようになるとともに、事業者に対する個人情報保護責任がより厳しくなります。その一方で、企業のデータ活用を促進するため仮名加工情報制度も新設されるなど、今後のデータ社会における新たなビジネス展開に向けた環境整備が進んでいます。

また、海外では、2020年12月に欧州データ戦略の一環として、データの利用可能性を促進することを目的としたデータガバナンス規則案やデジタルプラットフォーム規則案などが発表されています。米国では、2018年に先進してプライバシー法を施行したカリフォルニア州において、消費者の権利拡大をうたったカリフォルニア プライバシー権利法（CPRA）が2020年11月に成立し、その後、他州においても法制化が進んできています。また、中国でも2017年６月に施行されたサイバーセキュリティ法を筆頭に、今年６月にはデータの越境移転を管理するデータセキュリティ法や、ユーザ情報の収集への法的制限を課す個人情報保護法が成立するなど、世界的にプライバシー保護規制の動きが活発化しています。

そこで、今号では、欧米、中国、OECDのプライバシー保護規制に関する最新動向、国内における位置情報活用事例とデータ利活用にあたっての消費者目線での問題点について、当協会職員がレポートします。

資料編では個人情報保護関連の年表と2021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。

2021年12月
一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2021 Winter

Contents

特集

プライバシー保護規制とデータの利活用

I はじめに

一般財団法人日本情報経済社会推進協会　常務理事　**坂下 哲也**

1957年10月４日、ソ連が人類初の人工衛星「スプートニク１号」の打上げに成功した。重さ83.6kg、直径58cmとバレーボール程の球体が軌道を一周したことが世界を変えていく。当時、冷戦期だったアメリカは核爆弾を搭載した爆撃機に対処するSAGE（半自動式防空管制組織：Semi-Automatic Ground Environment）が完成した矢先だった。重さ275トン、真空管55,000本を使うコンピュータAN/FSQ-7を駆使し、カナダ北極圏とアメリカ全土に設置されたレーダーを使って、ソ連の戦略爆撃機がアメリカに飛来した際に８時間程度かかる時間を利用して対処する仕組みだった。しかし、人工衛星の速度の場合、96分でアメリカに飛来することになる。

核爆発による電子パルス等により地上の通信網などが破壊されるリスクに対処するため、アメリカは1958年ナリンダー・S・カパニー（インド）が試作した光ファイバーに投資し、1965年に実用化した。同時にランドコーポレーションが交換局のないネットワークを考案し、1969年に初の通信が行われた。インターネットが産声を上げた瞬間である。

インターネット技術が商用化されたのは、1992年11月にAT&T Jensが商用ISPサービスを開始、日本では翌1993年11月にIIJがインターネット商用サービスを開始したのが最初である。そして、現在では、一人最低１台のスマートデバイスを用い、24時間高速通信を使い、インターネットの利便性を享受し続けている。

インターネットが日本に導入された当時、自由な空間として期待されていた。それが変化するのが2010年である。この年、アメリカは米国サイバー軍（CYBERCOM）を発足した。そして、2010年６月、VirusBlokAda社（ベラルーシ）により報告され、米国がイランの核施設処理をサイバー兵器によって攻撃したことが明らかになった。2012年６月１日付のニューヨーク・タイムズは、このサイバー兵器（ワーム）は米国国家安全保障局（NSA）とイスラエル軍の情報機関である8200部隊がイラン攻撃用に作ったと報じている。そして、2013年、スノーデン文書が米国国家安全保障局を中心とする情報機関が独・仏・日本などの友好国に対して、サイバー空間を使い情報収集活動を行っていることを告発した。それまで、民主的で自由でグローバルな空間であった情報空間は、実は自らの影響力をサイバー空間において躊躇なく行使する場なのではないかという疑問が世界を覆った。

情報空間に国境はない。サイバー空間は物理的・地理的制約が少なく、行動の単位としての国家や政府の有効性は減少してしまう。そのため、プラットフォーマーという存在も生み出した。その中で、各国は制度をもってその執行力を行使すべく切磋琢磨している。

日本では、Society5.0というビジョンを掲げている。現実空間を情報空間へフルコピーし、情報空間から現実空間を制御し、複雑系の壁を乗り越えようとする営みである。情報空間上には、現実空間の私たち個人も投射される。その投射された個人のデータについて、どのように規律すべきなのか。2016年、EUがGDPR（一般データ保護規則）を制定した。現実空間でも、情報空間でも個人の人権を守るため、個人データ保護を目的とした個人データの処理と移転に関する法律を定めた。

この動きを皮切りに、データを国から出さないようにする制度（データローカライゼーション）など

の動きや、APEC諸国でも個人情報保護制度を整備する動きが顕著になった。このような制度は、経済活動に影響を及ぼす。APECでは域内の個人データの移転に関する関所手形のような認証制度CBPR（Cross Border Privacy Rules／APEC越境プライバシールールシステム）が運用されている。（現在、日本国内では２社が認証を受けている。）

DFFT（データフリーフロー・ウィズ・トラスト）という政策ベクトルが志向される一方で、TPP11協定（環太平洋パートナーシップに関する包括的及び先進的な協定）、日米クラウド協定（2019年に署名された日米貿易協定）、およびRCEP（Regional Comprehensive Economic Partnership／東アジア地域包括的経済連携）では、サーバの相手国内設置義務を要しないものとなっている。

情報空間を一つの世界として扱う中で、産業界はどのようにガバナンスを効かせ、また個人はどのように自身のプライバシーを守っていくことが求められるのか。当協会の『IT-Report 2021 Winter』では、以上のような問題意識の下で、これまで電子情報利活用研究部が調査してきた各国の制度を解説し、アイデンティティの在り方などについて考察している。

情報空間では“これが正しい”ということを証明する術が必要である。また、アメリカなどで広がりつつあるiPaaS（Integration Platform as a Service）はデータの質に課金するモデルだという。情報空間において、現実空間にある『信頼』（トラスト）が体現しつつあり、その中で本レポートの各論考は産業界の参考になるものと考えている。今後の企業活動の中で活用いただきたい。

Ⅱ 各国のプライバシー保護施策

Ⅱ-1 欧米のプライバシー関連法規制

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　主任研究員　**大熊 三恵子**

1．EUの動き

1.1　データガバナンス規則案

2020年11月25日、欧州委員会は、「データに関する2020年欧州戦略」で発表された一連の施策の最初のものとなる「データガバナンス規則案（データガバナンス法：Data Governance Act)」を発表した。これは、公的機関が保有する、他者の権利の対象となっているデータ（知的財産権、商業上の秘密の観点から保護されたデータ、個人情報などが含まれる）の再利用を推進し、データ仲介者への信頼を高め、EU全域でのデータ共有メカニズムを強化することで、データの利用可能性を高めることを目的としており、こうしたデータを対象としていない2019年のオープンデータ指令（Open data and the re-use of public sector information）を補完するものである。

特に、エネルギー、モビリティ、健康などの戦略的分野において、EU全体で共通かつ相互運用可能なデータスペースを構築し、パーソナライズ医療の改善、新しいモビリティ、欧州グリーンディールへの貢献などを通じて、市民に利益をもたらすことを目的としている。

データガバナンス法の主な規定は、図表Ⅱ-1のとおりである。

商業上の秘密、知的財産、個人データ保護など、既存の保護の対象となっている、公共部門のデータを再利用するための条件。
さまざまなタイプの仲介サービスを提供する企業として定義される、特定のデータ共有サービスの提供者に対する義務。
データ利他主義の概念を導入し、EUで認められたデータ利他主義組織を登録。
欧州委員会が議長を務める新しい正式な専門家グループであるEuropean Data Innovation Board（欧州データ革新会議）の設立。

図表Ⅱ-1．データガバナンス法の主な規定

データガバナンス法の対象となる「データ」は「行為、事実または情報のデジタル表現、およびそのような行為、事実または情報の編集物（音声、映像またはオーディオビジュアルの記録の形を含む)」と定義されており、これは、GDPRで定義されている個人データをも含む広い定義である。したがって、GDPRとデータガバナンス法が今後同時に適用される可能性があり、同法の説明文や規定が、特にGDPRの適用を「妨げるものではない」ことを何度か示しているのはそのためである。

データガバナンス法の第２章では、公共機関が保有する特定のデータの再利用を認める場合に、公共機関が従うべき一連の義務と制限が規定されている。公共機関とは、「国、地域・地方自治体、公法上の機関、１つ又は複数の公法上の機関、１つ又は複数の公法上の機関によって形成された団体」と定義されている。また、この法律は、公共機関がデータを再利用できるようにする義務を生じさせるものでも、GDPRや他の適用法に基づく既存の法的義務を免除するものでもないが、データを再利用できるようにすることを決めた公共機関に対しては、一定

第１章	一般条項
第２章	第三者が権利（商業上の秘密、統計上の秘密、知的財産権、個人データの保護）を有する機密性の高い公的機関保有データの二次利用を可能とするための枠組み （オープンデータ指令の補完、EU域外移転は、原則としてEUと本質的に同等な知的財産保護制度を有すると認められた国のみに認める）
第３章	「データ共有サービスプロバイダー」に関する信頼性を向上させるための、規律的枠組みの創設（他事業との分離、公正・透明性、安全性、事業継続性、データ提供者の利益保護、海外事業者の場合はEU域内代理人指名　等）
第４章	企業・個人による公益のための自発的なデータ提供（報酬を伴わないデータ提供、データ利他主義）に基づくサービスの規律的枠組みの創設と、「欧州データ利他主義同意フォーム」の採択
第５章	担当当局と手続き規定
第６章	担当当局により構成されるEuropean Data Innovation Board（欧州データ革新会議）の創設
第７章	欧州委員会と実装行為
第８章	経過措置と最終規定

図表Ⅱ-２．データガバナンス法の章立て

の例外を除き、排他的な取決めをすることを禁止している。

第３章では、「データ共有サービスプロバイダー」と呼ばれるデータ仲介者の運営に関する新しいルールについて、第４章では、データ利他主義という概念について規定している。

データ利他主義とは、科学的研究や公共サービスの向上などの公益のために、個人や企業が報酬なしで自発的にデータを再利用できるようにする状況を表しており、データ利他主義を促進する組織の登録と監視体制の確立を提案している。

データ利他主義組織は、所轄官庁に登録するための一定の条件（非営利であること、他の活動から切り離された法的に独立した構造で運営されていることなど）を満たす必要があり、データ主体および法人のデータに関する権利と利益を保護するための透明性義務およびその他の要件が課せられる。

1.2　デジタルサービス法とデジタル市場法

2020年12月15日、欧州委員会はデジタルサービス法（Digital Services Act: DSA）とデジタル市場法（Digital Markets Act: DMA）と題する新たなデジタルプラットフォーム規則案を欧州議会とEU理事会に提出した。両規則案の核心は、オンラインプラットフォーム、特に商品やサービス／情報のプロバイダーと消費者を結びつける仲介的なプラットフォームを規制する点にある。

DSAは、2000年のe-Commerce指令を更新するもので、特に、近年のオンライン上での違法・有害コンテンツ、商品やサービスの拡散に対処し、オンライン市場を利用する消費者や中小企業に対して、より高い透明性と保護を提供することを目的としている。DSAは、サービス提供者の設立地にかかわらず、EU域内の受領者にサービスを提供するすべての仲介業者に適用され、EUの消費者の10％以上（4,500万人以上）が利用する仲介業者には追加の要件が課せられる。

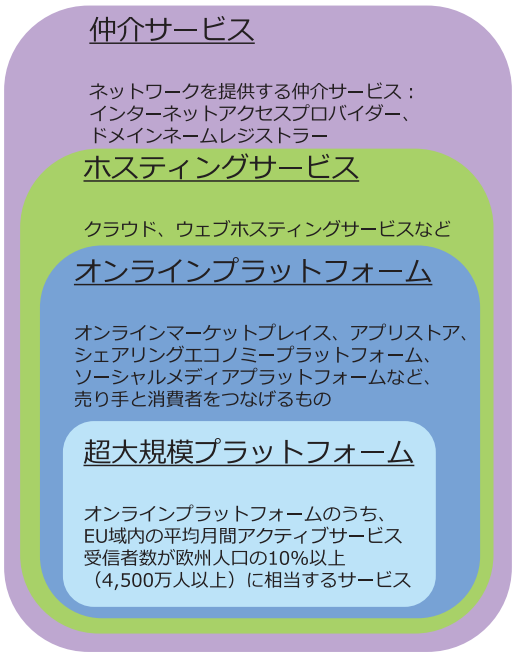
一方、DMAの対象となるのは、月間アクティブユーザー数が4,500万人以上のプラットフォーマー、いわゆる「ゲートキーパー」のみで、主にデジタル経済における競争に関係し、大手ハイテク企業が市場を支配して新規参入を阻むような行為を防止することを目的としている。

	DMA	DSA
包括的な目的	新しいプラットフォームが市場に参入しやすくすることで、競争を可能にする。	透明性、ユーザーの安全性、およびプラットフォームのアカウンタビリティを実現する。
対象	ゲートキーパー（図表Ⅱ-７参照）	仲介サービスプロバイダー、オンラインプラットフォーム。 ※月間アクティブユーザー数が4,500万人以上の「超大規模」オンラインプラットフォームに関する特別ルールあり。
箇条の種類	競争を阻害しないために、ゲートキーパーが必ずしなければならないことと、してはならないことを定める。	責任規定、透明性報告義務、デューデリジェンス義務。
施行方法	EUレベルで、通信ネットワーク・コンテンツ・技術総局を通じて施行される。	主に各国の規制当局を通じて施行される。独立した諮問機関として新たに提案されたEBDS（European Board for Digital Services）の支援を受ける。
制裁措置	ゲートキーパーが規則に従わない場合、欧州委員会は直前の会計年度における全世界の総売上高の「４％以上20％以下」の制裁金を課すことができる。	最大で全世界の売上高の６％の罰金、極端な場合にはプラットフォームへのアクセス制限。

図表Ⅱ-３．両規則案の目的および対象事業者等

1.3　デジタルサービス法（DSA）について

DSAは、オンライン仲介サービスプロバイダー、つまりソーシャルメディアやマーケットプレイスなどのオンラインプラットフォーマーに対し、オンライン上の透明性とアカウンタビリティを実現するために、明確な義務を課すものである。広告、アルゴリズムプロセスの透明性を向上し、違法コンテンツに対する通知義務、明確なデューデリジェンス義務を定めることで、EU全体でのオンライン上の安全性を向上させ、ユーザーの基本的権利の保護を向上しようとするものである。



図表Ⅱ-４．デジタルサービス法（DSA）におけるオンライン仲介サービス分類

DSAは、オンライン仲介サービスをサービスの種別と規模に応じて分類しており（図表II-４）、課せられる義務はプラットフォーマーごとに異なる（図表II-５）。特に、影響力が大きい超大規模プラットフォーマーに対しては、より一層の透明性とアカウンタビリティが求められている。

	仲介サービス	ホスティングサービス	オンラインプラットフォーム	超大規模プラットフォーム
透明性の高い報告	●	●	●	●
基本的権利を考慮したサービス条件の要求	●	●	●	●
命令に基づく各国当局との協力	●	●	●	●
連絡先および必要に応じて法定代理人	●	●	●	●
ユーザーへの通知と行動、情報提供の義務		●	●	●
苦情、救済メカニズムと裁判外紛争解決			●	●
信頼された旗手（Trusted flagger）			●	●
濫用的通知に対する措置および異議申立て			●	●
サードパーティサプライヤーの資格審査（KYBC）			●	●
オンライン広告のユーザー視点での透明性			●	●
犯罪行為の報告			●	●
リスクマネジメント義務とコンプライアンスオフィサー				●
外部によるリスク監査と公的なアカウンタビリティ				●
リスク管理義務とコンプライアンスオフィサー				●
当局や研究者とのデータ共有				●
行動規範				●
危機対応のための協力				●

図表Ⅱ-５．仲介サービスプロバイダーに対する義務

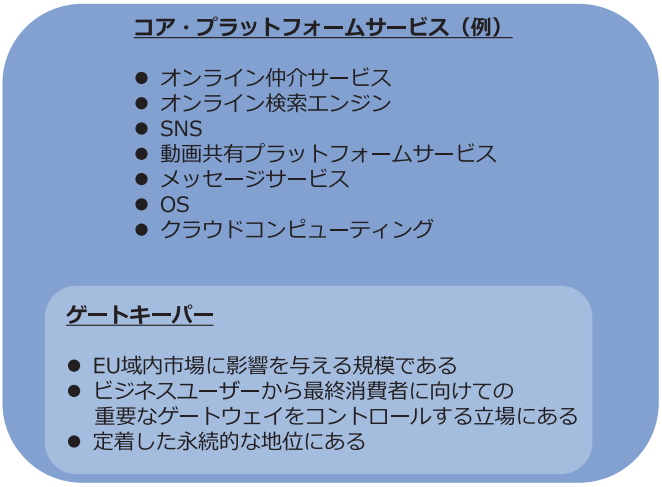
1.4　デジタル市場法（DMA）について

2019年５月に公表されたイギリス人のインターネット利用状況の調査によると、オンライン利用時間のうち40％をわずか２社（GoogleとFacebook）が所有するサイトで費やしており、GoogleとFacebookを毎月利用していると回答した割合は96％と87％に上るという[1]。

また、近年の巨大プラットフォーマーの市場にお

1　https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803576/CMA_past_digital_mergers_GOV.UK_version.pdf

ける優位性は、デジタルの黎明期とは比較にならない。これまで、欧米の政策立案者はデジタル市場の寡占化をそれほど憂慮していなかった。市場を巡る競争、つまり外部からの市場参入によって競争が促進されると考えていたのである[2]。ところが、FacebookはMySpaceを凌駕し、GoogleはAltaVistaを追い抜き、AltaVistaの優位性が１年（Myspaceは３年）であったのに対し、GoogleやFacebookの優位性はもう10年が経過している[3]。こうした巨大プラットフォーマーによるオンライン市場の支配的状況を背景に、DMAは、市場参入を阻害する行為を禁止することを目的としている。



図表Ⅱ-６．DMAにおけるおコア・プラットフォームサービス（例）

DMAは、企業が大規模なオンラインプラットフォーマー、すなわち「ゲートキーパー」に該当すると認定する際の基準を、図表Ⅱ-７のとおり定めており、１）EU域内市場に影響を与える規模である、２）ビジネスユーザーから最終消費者に向けた重要なゲートウェイをコントロールする立場にある、３）定着した永続的な地位にある、という３つの基準をすべて満たした場合には、該当しないことを示す証拠を当該企業が提出しない限り、ゲートキーパーであると判断される。また、これらの閾値をすべて満たしていない場合でも、欧州委員会による市場調査の中で、具体的な状況を評価してその企業をゲートキーパーとして認定する可能性もある。

「ゲートキーパー」は、２つ以上のユーザーグループをつなぐ結節点として機能する。ゲートキーパーがプラットフォームの片側のユーザー（たとえばバイヤー）に大きなシェアをもたらすと、特定の市場や顧客へのルートとして当該企業を使わざるを得ない。プラットフォームの反対側にいるユーザー（たとえば売り手）も、ゲートキーパーのインフラを使わざるを得なくなってしまう。DMAは、「高い参入障壁」と「ゲートキーパーによる反競争的行為」という２つの問題に対処し、デジタル市場を、既存の

EU域内市場に影響を与える規模である	欧州経済領域（EEA）における直近３会計年度の年間売上高が65億ユーロ以上、または直近会計年度の平均時価総額またはそれに相当する公正な市場価値が650億ユーロ以上であり、少なくとも３つの加盟国で中核となるプラットフォームサービスを提供している
ビジネスユーザーから最終消費者に向けた重要なゲートウェイをコントロールする立場にある	中核となるプラットフォームサービスを運営しており、直近の会計年度において、EU域内に設立または所在する月間アクティブエンドユーザー数が4,500万人以上、EU域内に設立された年間アクティブビジネスユーザー数が１万人以上である場合
定着した永続的な地位にある	過去３年間の各会計年度において、上記２つの基準を満たしていれば、これに該当する

図表Ⅱ-７．ゲートキーパー基準

2 https://www.bruegel.org/2021/02/regulating-big-tech-the-digital-markets-act/
3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

ゲートキーパーがしなければならないこと	
相互運用性	サードパーティが、ゲートキーパーのサービスと相互運用できるようにしなければならない。
データアクセス／ポータビリティ	ビジネスユーザーは、ゲートキーパーのプラットフォーム上での活動によって生成されたデータにアクセスできる。
広告主とパブリッシャーのための透明性	ゲートキーパープラットフォーム上の広告主に、パフォーマンス測定ツールやその他の関連情報へのアクセスを提供し、広告主がパフォーマンスを検証できるようにする。
価格の透明性	広告主とコンテンツパブリッシャーに、広告主が支払う価格とパブリッシャーに支払われる報酬の情報を提供する。

ゲートキーパーがしてはならないこと	
自社を優先する行為	ゲートキーパーが、検索結果のランキングで自社の製品やサービスを優先的に表示してはならない。
ビジネスデータの悪用	ゲートキーパーはビジネスユーザーから得た非公開データを使って、当該ビジネスユーザーと競争してはならない。
データ収集	ゲートキーパーは、自社のプラットフォームから取得した個人データを、ゲートキーパーが提供する他のサービスから取得した個人データと結合してはならない。
最恵国待遇条項（MFN）の適用	ゲートキーパーは、ビジネスユーザーが他のチャネルでより良い価格や条件を宣伝、契約、提供することを妨げてはならない。
バンドリング	ゲートキーパーは、ユーザーに対して、ゲートキーパープラットフォームにアクセスする条件として、他のコアプラットフォームサービスへの加入または登録することを要求してはならない。
ソフトウェアのアンインストールを妨害	ユーザーが、プレインストールされたソフトウェアやアプリケーションをアンインストールすることを妨害してはならない。
スイッチング	ゲートキーパーは、エンドユーザーが異なるソフトウェアやアプリケーションにスイッチ／サブスクライブする能力を技術的に制限することはできない。

図表Ⅱ-8．ゲートキーパーに課せられた義務

ライバルや将来のライバルにとって、競争力のある公正なものにすることを目的としている。

DMAの第５条から第13条では、データ利用の制限、データ開示要件、相互運用性など、広範囲にわたる義務をゲートキーパーに課している。これらの義務を要約すると、図表Ⅱ-８のとおりである。

2021年11月23日、欧州議会域内市場・消費者保護委員会は、ターゲティング広告の禁止を盛り込んだDMAの修正案を賛成42、反対２で可決した。今回の修正案では、「ターゲットを絞った広告やマイクロターゲティング[4]広告を配信する目的でデータ結合をしない」ことを企業に要求するとともに、未成年者に対するターゲティング広告を厳しく禁止している。本法案は2021年12月13日に開かれる欧州議会本会議で投票にかけられる予定である。

4　マイクロターゲティングとは、年齢や性別、住んでいる地域などのデータを細分化し、効率的に広告配信や情報提供を行うこと。

2．米カリフォルニア州法

アメリカでは、2018年６月28日に成立したカリフォルニア消費者プライバシー法（California Consumer Privacy Act: CCPA）を皮切りに、2020年11月３日にはCCPAを改正するカリフォルニアプライバシー権利法（California Privacy Rights Act: CPRA）が可決、同州に続いて、バージニア州、コロラド州も州レベルのプライバシー法を成立させている。

なかでも、CPRAは消費者の権利の拡大、有効な「同意」基準の詳細化など多くの点で注目に値する。以下に、CCPAから大きく変更された点を概説する。

CCPAとCPRAの適用範囲は、図表Ⅱ-９のとおりである。CPRAは、中小企業に配慮し、対象となる販売、共有する個人情報の数が５万から10万に変更されている。

CCPA		CPRA
年間総収入が2,500万ドル以上の企業	→ 変更なし	年間総収入が2,500万ドル以上の企業
５万以上の個人情報を商業目的で購入、受領し、商業目的で販売、共有する。	→ 変更あり	**10万以上**の個人情報を商業目的で購入、受領し、商業目的で販売、共有する。
消費者の個人情報を販売することで、年間収益の50％以上を得ている。	→ 変更あり	消費者の個人情報を販売**または共有**することで、年間収益の50％以上を得ていること。

図表Ⅱ-９．CCPAおよびCPRAが適用される事業者

また、CCPAでは使用されていなかった「センシティブな個人情報（sensitive personal information）」という用語を図表Ⅱ-10のとおり定義し、他の個人情報と明確に区別している。

社会保障番号、運転免許証番号、州の身分証明書、またはパスポート番号
アカウントのログイン、金融口座、デビットカード、またはクレジットカードの番号と必要なセキュリティコード、アクセスコード、パスワード、またはアカウントへのアクセスを許可する認証情報との組合わせ。
精密な位置情報
人種や民族、宗教や哲学的信条、組合員であること。
通信の意図する受信者でない限り、消費者のメール、電子メール、テキストメッセージの内容
遺伝子データ
消費者を一意に識別する目的で、生体情報を処理すること。
消費者の健康に関する個人情報の収集と分析
消費者の性生活や性的指向に関する収集・分析された個人情報。

図表Ⅱ-10．CPRAのセンシティブな個人情報の定義

CPRAは、消費者に対し、（１）「共有」を拒否する権利、（２）特定の状況下でのセンシティブな個人情報の使用を制限する権利、という2つの新しいオプトアウト権を与えた。つまり、該当する企業は、現在の「販売」に対するオプトアウトと同様に、消費者が企業の「ホームページ」上のリンクから新しい権利を行使することができるよう対応しなければならない。該当する企業は、現行のCCPAの「個人情報を売らないでください」というリンクを「個人情報を売らないでください、または共有しないでください」という内容に更新することになる。

また、CPRAでは、「同意とは、自由に与えられた、具体的で、情報に基づいた、消費者の望みが明確に

ユースケース	CCPA	CPRA
消費者がオプトアウトの権利を行使した後の個人情報の販売または共有（§1798.120(d)）	明示的な承認	新しい同意基準
未成年者の個人情報の販売または共有（§1798.120(c)-(d)）	積極的な承認または明示的な承認	新しい同意基準
経済的インセンティブプログラムへの参加（§1798.125(b)(3)）	オプトイン同意	新しい同意基準（「オプトイン・コンセント」への言及は引き継いだものの）
消費者が使用または開示を制限する権利を行使した後の「センシティブな個人情報」の追加使用または開示（§1798.121(b)）	n/a	新しい同意基準
研究の適用除外	インフォームドコンセント	新しい同意基準

図表Ⅱ-11．CCPAとCPRAの有効な同意の比較

示されたもの」[5]という、GDPRとほぼ同様の同意基準を新たに導入している。

さらに、CPRAは、1974年以降、連邦政府に適用されてきた公正情報行動原則（Fair Information Practice Principles: FIPPs）のうち、データの最小化、目的の特定、セキュリティ、透明性、正確性、説明責任といった原則が民間企業にも適用されるように成文化した法律という点でも注目されている。

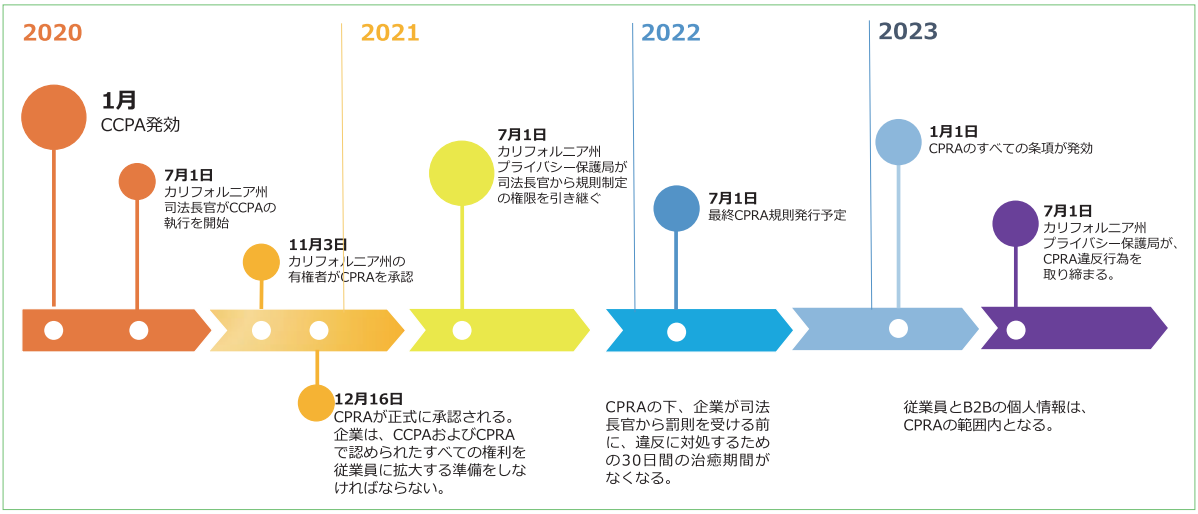
5　“Consent” means any freely given, specific, informed, and unambiguous indication of the consumer’s wishes（後略）

カテゴリー	トピック	CCPA	CPRA
適用範囲	未成年者に対する特別な保護	✓	✓
	B2Bおよび従業員データ	×[1]	×[2]
	センシティブデータに対する制限	×	✓
消費者の権利	知る権利（消費者に関する情報の収集）	✓	✓
	アクセス権	✓	✓
	訂正権	×	✓
	消去権	✓	✓
	処理を制限する権利	×	✓
	データポータビリティ権	✓	✓
	処理に異議を唱える権利	×	✓
	センシティブな個人情報の利用を制限する権利（位置情報を含む）	×	✓
	自動的な意思決定およびプロファイリングを拒否する権利	×	✓
	ポップアップなしの閲覧または個人情報の販売	×	✓
	差別されない権利	✓	✓
事業者の義務	プライバシーポリシーの開示	✓	✓
	データ保護バイデザイン・バイデフォルト	×	✓
	処理者／サービスプロバイダー／請負業者／第三者との書面による契約	✓	✓
	処理活動に関する記録の維持	×	✓
	権利要求への対応	✓	✓
	オプトアウトリンク[3]	✓	✓
	合理的なセキュリティ対策の実施	✓	✓
	セキュリティ侵害の通知	✓	✓
	データ保護影響分析	×	✓
	データ保護オフィサー	×	×
	保管制限とデータ最小化要件	×	✓
	越境データ移転規則の遵守	×	×
執行	専門のデータプライバシー保護機関	×	✓
	罰則（民事上の罰金）	✓	✓
	罰則（私的訴訟権－違反）	✓	✓

1．2022年１月１日までB2Bおよび従業員情報が免除される。
2．2023年１月１日までB2Bおよび従業員情報が免除される。
3．CCPAでは、「私の情報を売らないでください」というリンクが必要。CPRAでは、「私の個人情報を販売または共有しないでください」というリンクと、「私のセンシティブな個人情報の使用を制限してください」というリンクが必要。

図表Ⅱ-12. CCPAとCPRAの比較

CPRAの全条項が発行するのは2023年1月1日である。　CPRAの発効スケジュールは図表II-13のとおりである。



図表Ⅱ-13. CPRAの発効スケジュール

Ⅱ-2 中国個人情報保護法と最新の動向

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　客員研究員　柊 紫央璃
主席研究員　寺田 眞治

2021年11月１日、中華人民共和国个人信息保护法（以下、「中国個人情報保護法」という。）が施行された。また、これを補完するネットワークセキュリティ管理条例（草案）、データ越境移転安全評価弁法（草案）が11月にパブリックコメントにかけられている。現在の状況は、中国における個人情報保護の基本的な体系がほぼ完成し、実務面での行政法規やガイドラインの整備が急速に進められている段階である。本稿では、中国個人情報保護法と補完する最新の行政法規等について概要を説明するとともに、日本企業が検討すべき事項について若干の示唆を加えている。

１．制定の経緯

中国でプライバシー保護や個人情報保護が法制度として整備し始められたのは、比較的最近のことである。個人情報保護を明確に示したのは、2009年に可決された刑法改正案（七）にて「個人情報の販売・不正提供罪、個人情報の不正入手罪」を定めたのが端緒と考えられる。その後、2015年の刑法改正案（九）で改正案（七）の２つの罪を個人情報侵害罪として合併し、情報セキュリティ管理義務履行拒否罪を追加している。この頃からさまざまな国の行政機関や地方行政が独自に個人情報保護を目的とする規制を短期間に次々と制定するが、個人情報の定義も微妙に異なり、個別の問題への対処といった面が強いものであった。

体系化の動きは、まず2017年10月に施行された民法総則に表れる。第111条において「自然人の個人情報は、法律による保護を受ける。他者の個人情報を取得する必要がある組織及び個人は、法令に従って個人情報を取得し、個人情報の安全を確保しなければならず、他人の個人情報を違法に収集、利用、処理、又は譲渡することは禁止される。」と規定された。さらに上位となる中華人民共和国民法典は、2021年１月施行においてプライバシー及び個人情報保護（第６章）という章が新たに設けられ、プライバシー権の定義が初めて規定される。

今回施行された個人情報保護法は、この民法典における個人情報保護の考えを受け継いで、個人情報処理規則、個人情報越境移転、個人の権利および個人情報処理者の義務などに対してさらに具体的に整理、規定したものとなっている。さらに草案第２稿からの変更点として、第１条に「憲法に基づき、本法を制定する」との記述が追加されており、中国における個人情報保護制度の体系化が一通り整ったと考えられる。

２．概要

2.1　適用対象

中国国内において自然人の個人情報を取り扱う活動に対し適用される。また、中国国外においても、中国国内の自然人の個人情報を取り扱う活動が、以下のいずれかに該当する場合は適用される。

（一）国内の自然人に向けて商品又はサービスを提供することを目的としている。
（二）国内の自然人の行為を分析し、評価する。
（三）法律又は行政法規の規定するその他の状況。

ただし、自然人は個人または家庭の事務により個人情報を取り扱うことに関しては、本法を適用されない。

2.2　基本的定義

個人情報	電子的又はその他の方法で記録された、既に識別され又は識別可能な自然人に関する各種情報をいうが、匿名化処理後の情報を含まない。
センシティブ個人情報	一旦漏えいし又は不法に使用されると、容易に自然人の人格的尊厳が侵害され、又は人身、財産安全に危害を受けやすい個人情報を言い、生体識別、宗教信仰、特定身分、医療健康、金融口座、行方所在等の情報、及び14歳に満たない未成年の個人情報を含む。
個人情報の取扱い	個人情報の収集、保存、使用、加工、伝達、提供、公開、削除等を含む。
個人情報取扱者	個人情報の取扱活動において、自らが取扱目的、取扱方法を決定する組織、個人をいう。
匿名化	個人情報が処理を経て、特定の自然人を識別できず、かつ元に復元することをできないようにする過程をいう。

2.3　個人情報の取扱いにかかる原則とルール：

個人情報保護法の第５条から第10条にかけて、個人情報の取扱いに関する以下の基本原則が定められている：合法性、正当性、必要性及び信義誠実（第５条）、明確かつ合理的な目的及び目的との直接関連（第６条第１項）、本人の権利利益への影響が最小となる方法・範囲の収集（第６条第２項）、公開及び透明性の原則（第７条）、個人情報の質と正確性の保証（第８条）、セキュリティの保障（第９条）、法令遵守・国家安全・公共利益保護（第10条）

具体的な取扱いルールとして、下記の７つの正当化事由のいずれかに該当しない限り個人情報の取扱いはできないとしている。

（一）本人の同意を取得している場合	
（二）～（七）本人の同意が不要な場合	本人が当事者の一方となる契約の締結若しくは履行に必要な場合、又は適法に制定された労働規章制度及び適法に締結された集団的契約に基づく人事管理を実施する上で必要な場合。
	法定の職責又は法定の義務の履行に必要な場合。
	突発的な公衆衛生上の事案に対応し、又は緊急状況下において自然人の生命、健康及び財産の安全の保護のために必要な場合。
	公共の利益のためメディア報道、世論監督等の行為を実施し、合理的範囲内で個人情報を取り扱う場合。
	本法の規定に基づき合理的な範囲で本人が自ら公開し又はその他適法に既に公開済みの個人情報を取り扱う場合。
	法律、行政法規の規定するその他の状況。

また、個人情報の取扱いに際し、センシティブ個人情報を取り扱う場合や個人情報の越境移転の場合など、本人の個別的同意または書面による同意を得なければならないと法律または行政法規が規定する場合には、当該規定に従わなければならない。

さらに、同意の必要の有無にかかわらず告知の義務が課せられている。「目立つ方式で、明確かつ理解しやすい表現を用いて、本人に対し、真実で、正確でかつ完全に」以下の事項を告知しなければならない。

共通	個人情報取扱者の名称又は姓名及び連絡先
	個人情報の取扱目的、取扱方法、取り扱う個人情報の種類及び保存期限
	本人が本法の規定する権利を行使する方法及び手続
	法律及び行政法規が告知すべきと規定するその他の事項
個人情報取扱者の合併、分割、解散、破産宣告等によって個人情報の移転が発生する場合	移転先の名称又は姓名及び連絡先
他の個人情報取扱者に個人情報を提供する場合	受領者の名称又は姓名、連絡先、取扱目的、取扱方法及び個人情報の種類
センシティブ個人情報を取り扱う場合	センシティブ個人情報を取り扱う必要性及び本人の権利利益への影響
越境移転の場合	移転先の名称又は姓名、連絡先、取扱目的、取扱方法、個人情報の種類及び本人が域外移転先に対する権利を行使する方法及び手続等の事項

このように、同意、告知の要件として、いずれも「法律、行政法規の規定するその他の状況」のようなバスケット条項が設けられているため、今後法律等によって追加されるかをウォッチしておく必要がある。

たとえば、2021年11月にパブリックコメントが開始されたネットワークセキュリティ管理条例（草案）において、本人の同意に基づき個人情報を取り扱う場合の要件を以下のとおり具体的に提示している（第19条）。

（一）取り扱う個人情報は、サービスの提供に必要であり、又は法律、行政法規で定める義務の履行のために必要である。

（二）取扱いの目的を達成するための最短期間、最低頻度に限定し、個人の権利・利益への影響が最小となる方法を用いる。

（三）サービスの提供に必要な個人情報以外の情報の提供を拒否したことを理由に、サービスの提供を拒否し、又は本人のサービスの正常な利用を妨げてはならない。

同意と告知についても、個人情報の第三者移転の場合は「個人情報を提供する目的、種類、方法、範囲、保管期間、保存場所を本人に告知し、かつ本人の同意を個別に取得する」としている。

2.4　センシティブ個人情報の取扱いに関する特則

センシティブ個人情報の取扱いの要件として、「特定の目的及び充分な必要性」および「厳格な保護措置」が定められている。同意および告知に関しては2.3で整理したとおりに通常の事項に加えて特則がある。

特に注意したいのは、草案第２稿からの変更点として14歳未満の情報がセンシティブ個人情報に含まれるようになったことであり、その場合はさらに父母またはその他の監護者の同意を取得し、かつ専門的な個人情報取扱ルールを設けなければならないという点である。

3．その他の主な特徴

3.1　域外適用

中国個人情報保護法は、中国国内の自然人に製品、サービスを提供し、または中国域内の自然人の行為を分析し評価する中国国外における個人情報の取扱いを適用範囲としている。これはGDPRの域外適用規定にきわめて近い考え方で、たとえば日本のゲーム会社がアプリストアを通じて中国国内の自然人にゲームを提供し、個人情報の取扱いを行う場合、直接適用されることになる。域外適用規定が置かれていることから、中国に関連会社がある企業に留まらず、自社またはグループ会社の非中国企業が適用を受けないかについて確認する必要が出てくる。

3.2　自動的決定の規制

自動的決定は、コンピュータプログラムを通じて自動的に本人の行為習慣、興味、嗜好または経済、健康、信用状況等を分析、評価し、決定を行う活動をいう。

これは、草案第２稿を審議した際に殊に条項の強化を指示された部分で、APIによる過剰な個人情報収集や、それに伴うビッグデータによる差別的な取引価格などの不合理な取引の実施が、近年中国で問題となっていることが背景にある。GDPR第22条１項の自動化された意思決定およびプロファイリングの規制に類似している。

個人情報取扱者が個人情報を利用して自動的決定を行う場合には、「決定の透明度及び結果の公平性・公正性を保障しなければならない。本人に対し、取引価格等の取引条件において不合理な差別的待遇を実施してはならない。」との原則を据えた上で、「自動的決定の方法によって本人に対し、情報配信、商業的マーケティング活動を実施する場合には、同時に当該本人の特徴に基づかない選択項目を提供し、又は本人に対し簡便な拒絶方法を提供しなければならない。」としている（第24条）。

3.3　データポータビリティ権

第45条３項のデータポータビリティに関する規定も最終稿に新たに加えられた内容である。本人が指定する個人情報取扱者へ当該本人の個人情報を移転するよう請求した場合、それが国家インターネット情報部門の定める条件に合致していれば、個人情報取扱者は移転方法を提供しなければならないとされている。しかし、対象となる個人情報の範囲や具体的な条件、実務面における移転方法の提供をどのように実現するかについては記載されていない。ただし、前述のネットワークセキュリティ管理条例（草案）において、以下のようにある程度の規定が提示されている（第24条）。

（一）移転請求がなされた個人情報が同意に基づく場合、又は契約の締結、履行のために収集が必要な個人情報である場合。

（二）移転請求がなされた個人情報が本人の情報又は請求者が合法的に入手した他人の情報であり、かつ他人の意思に反していない場合。

（三）請求者の合法的な身分を検証できるデータ取扱者は、個人情報を受領する他のデータ取扱者が個人情報を不正に取り扱うリスクを発見した場合は、個人情報の移転請求に対して合理的なリスク提示を行わなければならない。

3.4　域外移転のルールとデータ国内保存義務

すべての個人情報取扱者を対象とした一般的な移転のルールとしては、必要事項の告知、個別の同意の取得に加え、以下の条件のいずれかを満たさなければならないとされている。

（一）国家インターネット情報部門による安全評価に合格した場合。

（二）国家インターネット情報部門の規定に基づく専門機構による個人情報保護の認証を得ている場合。

（三）国家インターネット情報部門が制定する標準的契約を域外の移転先と締結し、双方の権利及び義務を約定する場合。

（四）法律、行政法規又は国家インターネット情報部門の規定するその他の条件。

（一）の安全評価に関しては、さっそくデータ越境移転安全評価弁法（草案）がパブリックコメントに出され、11月28日まで意見募集が行われた。（二）の個人情報保護の認証はまだ詳細が明かされていない。（三）の「標準契約」もまだ策定中のようだが、GDPRのSCCとの類似点についても注目したい。

さらに、重要情報インフラ運営者および取り扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者を対象に、第40条では中華人民共和国域内で収集し、または発生した個人情報を国内で保存しなければならず、たしかに域外に提供する必要がある場合には、原則的に国家インターネット情報部門による安全評価に合格しなければならないとしている。重要情報インフラについて個人情報保護法では定義の扱いがないが、2017年６月施行のサイバーセキュリティ法によると「公共通信・情報サービス、エネルギー、交通、水利、金融、公

共サービス、電子政府等の重要な産業及び分野、並びにひとたび機能の破壊、喪失又はデータの漏えいに遭遇した場合、国の安全、国民経済と民生、公共の利益に重大な危害を与え得るその他の重要情報インフラの運営者」とされている（第31条）。また、規定する数量は、前述のデータ越境移転安全評価弁法を見ると「取り扱った個人情報が100万人に達した個人情報取扱者が越境移転する場合」（第４条第３号）、「累計で10万人以上の個人情報又は１万人以上の機微な個人情報を越境移転した個人情報取扱者」（第４条第４号）とあり、これが目安となると考えられる。

ネットワークデータセキュリティ管理条例（草案）でも、データ越境移転安全評価に合格しなければならない対象者を「越境データに重要データが含まれている場合（第37条第１号）、重要情報インフラ事業者、及び100万人以上の個人情報を取り扱うデータ取扱事業者（第37条第２号）としている。

さらにデータ越境移転セキュリティ管理の章（第５章）が設けられており、個人情報の越境移転に際し、国外のデータ受領者の関連情報などを本人に通知するだけでなく、個別の同意を得なければならないとしている。また、同管理条例の草案では、データ越境移転する場合のデータ取扱者の義務が明確に規定されており（第39条、40条）、国によって「データ越境移転セキュリティゲートウェイ」を設置する（第41条）コンセプトが打ち立てられていることにも注目したい。

４．今後の動向と日本企業の対応

中国個人情報保護法は基本的な方向性と原則を定めたものであり、外形的にはEUのGDPRに類似している。すでにGDPR対応をしている企業にとっては比較的整合性を取りやすいように一見思われるが、実態としては排他的傾向が強いものとなっている。それは本法律のバスケット条項に基づき別途策定される法律や行政法規に表れており、いわゆるデータローカライゼーションと言われるデータの国内保存義務や越境移転について、厳しい規定が多くみられることからも明らかだ。ただし、これらは必ずしも国外の事業者の締出しを図るためのものではなく、国内の事業者による無秩序なデータの流出を阻止する意味合いの方が大きいと考えられている。特に最近締付けを厳しくしている中国国内のプラットフォーム事業者や新興の大企業をターゲットにしていると思われる。したがって、ただちに日本企業に対して取締まりが行われるかと言えば、その可能性は現時点ではさほど大きくはないと見られている。しかし、法律制定時の見せしめ的な一斉取締まり、対外環境の悪化などさまざまな不確実性を勘案すると、あまり良い言い方ではないが「不運な」状況に陥る企業が出てくるのも避けられないだろう。

法律の遵守は当然のことなので、本来「不運」とは言えないが、この法律だけで具体的で明確な対応を行うことは現実的には困難である。今後策定される補完的な、あるいは領域別、場合によっては地域別の法律、行政法規、さらにはガイドラインが出てくるまでは想定されるリスク範囲を大きく設定して対応するしかないのが実態である。過去に制定されたさまざまな規定も参考にはなるが、本法律に合わせて改定されたり無効にされたりするものもあると思われるので、実効性を十分に見極める必要がある。

また、現地の政策動向や国際環境変化などの外部の情報に注意を払うことは当然のことではあるが、現地従業員に対する教育や個人情報を扱う委託事業者の管理など、ガバナンスの強化も必須である。中国サイバーセキュリティ法が2017年６月に施行されて以降、個人情報を含むデータセキュリティに関する規定やガイドラインが大量に策定されている。同様に今回の個人情報保護法に合わせて、本稿でも触れているように個人情報の安全管理措置に該当するセキュリティに関連する規定の策定が相次いで予定されている。企業は取扱いのルールを策定するだけではなく、これを遵守できる体制の確立が喫緊の課題となるであろう。

中国のプライバシー保護、個人情報保護に関する基本的な法体系の確立が、今回の個人情報保護法の施行で一応の完成に達したと考えられる。今後は、この法体系の下にあらゆる領域において実効的な整備が急速に進められることが想定される。中国の法制度の普及や執行のスピードはきわめて速いことから、各企業もこれを見越した対応が必要であり、リスクマネジメントの最大のポイントになるであろう。

Ⅱ-3 OECDが進めるデジタル経済政策とデータトラストへの取組み

一般財団法人日本情報経済社会推進協会　電子情報利活用研究部　主席研究員　**水島 九十九**

1．はじめに

デジタル化が急速に加速しており、コミュニケーションや生活スタイル、仕事のやり方などを大きく変化させてきた。企業はグローバルでの競争力強化のために、DX（デジタルトランスフォーメーション）を推進し、イノベーションを促進してサービス改善を進めている。その際、デジタル化されたデータとデータを扱うためのデジタル技術が重要となってきている。

2011年のダボス会議（世界経済フォーラム）にて、「パーソナルデータはインターネットにおける石油」であると報告され、それ以来、「データ＝石油」と表現されることが増えた。データが石油以上の価値を持つ資源になることが示唆された。しかし、石油と異なりデータには最初から国境がなく、元来自由に国境を移動することが可能である。そのため、目に見えないデータの利用や管理においては、プライバシーやセキュリティなどトラスト（信頼）を高めることが重要になってきている。

今回は、国際社会の先頭に立って新たな課題に取り組むOECD（経済協力開発機構、Organisation for Economic Co-operation and Development）において、議論が進められている「OECDが進めるデジタル経済政策とデータトラストへの取組み」について解説する。

2．OECDが考えるデジタル経済

OECDは、国際経済の課題を協議することを目的とした国際機関である。先進国による自由な意見交換を通じてグッドプラクティスを共有し、各種政策に関して先見性を高める論議を交わしている。「世界最大のシンクタンク」とも呼ばれて、現在のOECD加盟国は38カ国である。OECD全体で約30の委員会がさまざまな分野で活動している。[1]

その中で、CDEP（デジタル経済政策委員会、Committee on Digital Economy Policy）はデジタル経済の課題を検討する付属機関である。デジタル技術の発展により生じた課題に対して、必要な政策や規制対策を促進している。OECDにおける政策提言（勧告、recommendation）という方法により、原則やガイドラインが示されることも多く、事実上の先進国標準となるケースも多い。プライバシーガイドライン（1980年策定、2013年改定）、セキュリティガイドライン（2002年策定、2015年改定）などの勧告が公開されている。[2]

OECDが考えるデジタル経済は、「デジタル技術やデータ利用によって向上するすべての経済活動」と定義されている。デジタル経済の進展により、現実世界のあらゆる場所で生成された膨大なデータが、インターネットを経由してサイバー空間に蓄積される。蓄積されたデータはAIなどによって解析され、得られた結果は現実世界にフィードバックされる。データやデジタル技術を有効に活用することにより、イノベーションを創出し、新たな付加価値を提供することが期待されている。[3]

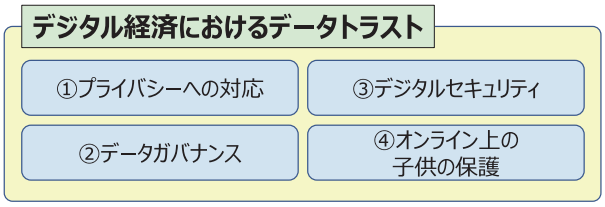
3．デジタル経済におけるデータトラスト

OECDは、デジタル経済において社会的な拡大を促進するために、経済政策を取りまとめ政策提言を公開している。特に、EC（電子商取引）やシェアリングエコノミーを含むオンラインビジネスを成長させるためには、利用者に関する課題解決が重要と考えら

1　https://www.oecd.org/about/
2　https://oecdgroups.oecd.org/Bodies/ShowBodyView.aspx?BodyID=1837&Lang=en
3　https://www.oecd.org/digital/ieconomy/

れている。OECDではステークホルダーのトラストを得ることは、デジタル経済において重要な役割であり、複雑なグローバル環境における「強力なツール」になると捉えている。今日のデジタル経済において、成功した多くの企業は社会や環境の課題に迅速対応しており、ガバナンスを維持・強化し、ステークホルダーの期待に応えることで市場価値を最大化していると認識されている。OECDでは、トラストを高めることがビジネスの成功への重要な要素であると捉え、トラストの強化に取り組む企業や組織は、長期的な価値が保証されるとして政策提言を取りまとめている。

OECDでは、データトラストを高める重要な施策を４つのカテゴリーで区分している。[4]



図表Ⅱ-14. OECDデータトラストの重要施策

3.1 プライバシーへの対応

OECDは、数十年にわたってプライバシーの尊重を基本的な価値として向上させ、国境を越えた個人データの自由な流れを促進する上で重要な役割を果たしてきた。基本的人権を尊重し、国内のプライバシー法制と調和させ、国際的なデータの流れを中断させないために有効なガイドラインが必要であると考えている。プライバシー対応と越境する個人データ移転について、OECDのプライバシーガイドラインの見直しが進んでいる。これは、プライバシーに関するOECDの取組みの基礎となっている。[5]

1980年、OECDプライバシーガイドラインと呼ばれる「プライバシー対応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」は、世界共通となる個人情報保護の基本原則を規定した指針として公開された。OECD８原則は、個人情報保護やプライバシー対応に関して、グローバルの法規制の規範となっている。

2013年、OECDは初めてプライバシーガイドラインを改訂した。OECDの提言内容を見直し、プライバシー法制における執行協力を強化した。特に下記の２テーマが特徴となっている。[6]

①プライバシー対応におけるリスク管理アプローチ
②相互運用性向上によるグローバルなプライバシー対応

さらに現在、OECDプライバシーガイドラインの改訂や勧告附属文等の追記が検討されており、追加的なガイダンスを提供することを目指している。AIやIoTなどの新たなデジタル技術を踏まえて、個人データの収集や利用目的、安全管理措置などを規定した追加的な指針が必要であると考えられている。

具体的には、①説明責任、②データローカライゼーション、③民間部門の個人データへのガバメントアクセス、④規制のサンドボックス制度が取り上げられている。

3.2 データガバナンス

データガバナンスは一般的には、効果的かつ効率的に使用するためにデータマネジメントのすべての活動を統制することを意味する。ビジネスで利用するデータの品質とセキュリティを保証し、そのプロセスにおいて責任を確立することである。特にOECDにおいては、データへのアクセスと共有を強化することをデータガバナンスの課題として取り組んでいる。

データへのアクセスと共有は、コロナ感染症への対策やSDGs（持続可能な開発目標）の達成など社会的課題の解決に重要な役割を果たすと考えられている。しかし、データへのアクセスと共有はリスクを伴うため、デジタル経済と実社会がデータを十分に活用できなくなる可能性を示唆している。また、データアクセスを制限することは、共有することを躊躇させることにつながる。

2021年、EASD（Enhancing access to and sharing of data）の実現に向けて、「データへのアクセスと共有の強化の理事会勧告」が採択された。この勧告は、政府が一貫性のあるデータガバナンス

4 https://www.oecd.org/sti/ieconomy/information-security-and-privacy.htm
5 https://www.oecd.org/digital/ieconomy/privacy.htm
6 https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

ポリシーとフレームワークを策定し、国や組織などコミュニティにおいてデータの潜在的なメリットを引き出し、サポートすることを目指している。データ利用においてトラストを向上させ、データへのアクセスと共有を促進して、効果的かつ責任あるデータガバナンスを実現することを狙いとしている。[7]

3.3　デジタルセキュリティ

デジタルセキュリティに対するOECDの取組みは、デジタル技術の可能性を阻害することなく、トラストを高める政策提言を策定することを目指している。「サイバーセキュリティ」ではなく「デジタルセキュリティ」としているのは、サイバーセキュリティが技術的な側面や法執行も含めた国際的なセキュリティの側面に着目しているのとは対照的に、デジタルセキュリティはサイバーセキュリティの経済的および社会的側面を主に対象としていることが理由である。デジタルセキュリティへの取組みは、デジタル技術の恩恵を最大化させ、トラストを向上させることで、ステークホルダーとの間で有効な情報共有を図るものである。[8]

2015年、「デジタルセキュリティのリスク管理に関するOECD勧告」が採択された。これは2002年に採択された「情報システムとネットワークのセキュリティに関するOECDガイドライン」に代わるものである。経済的および社会的な繁栄を目指し、デジタルセキュリティリスク管理に関する提言がなされた。この勧告は経営者に対して、デジタルセキュリティリスク管理を技術的な問題として扱うのと同時に、経済的および社会的な意思決定を体系的に実行することを要求している。イノベーションを促進するために、デジタル技術の可能性を阻害することなく、デジタルセキュリティに対処する方法として８つの原則が示された。[9]

【一般原則】①意識・スキル・エンパワーメント、②責任、③基本的人権、④協力
【運用原則】⑤リスク評価と対応サイクル、⑥セキュリティ対策、⑦イノベーション、⑧継続性

現在、2022年末に向けて勧告の改訂作業が進んでいる。

3.4　オンライン上の子供の保護

2021年、「OECDオンライン上の子供の保護勧告」が採択された。勧告は、インターネット上の青少年保護について、保護者の役割や官民一体での取組み、国際的な目標の必要性について規定している。オンラインのリスクから子供を保護し、デジタルの世界が提供する機会と利益をバランスさせることを目指すものである。特に重要なテーマについて、２つの課題が提起されている。[10]

①子供のプライバシーとオンラインデータ
②子供に安全で有益なデジタル環境を確保するためのステークホルダーの役割

昨今、多くの子供はスマートフォンを所有しており、生活時間の多くをオンラインで過ごすようになった。デジタル環境は子供に多大なメリットをもたらし、コミュニケーションや教育など新しいツールを提供することにつながった。しかし同時に、ネットいじめ、プライバシー侵害など深刻なリスクも大きな課題となっている。これらのリスクは、コロナ感染症により従来以上に深刻になってきている。子供にとって安全で有益なデジタル環境の構築を促進するため、国際協力の重要性を強調している。

4．おわりに

企業活動のグローバル化において、データとデジタル技術を活用することにより、特にクラウドサービスなど国境を越えた情報の流通が容易になった。グローバル事業を成長させるために、ステークホルダーのトラストを得ることは社会的にも経済的にも重要な役割になってきている。今まで以上に、国際的な調和のとれた自由な情報流通の仕組みや、プライバシーに配慮することへの取組みが求められている。

7　https://www.oecd.org/sti/ieconomy/enhanced-data-access.htm
8　https://www.oecd.org/digital/ieconomy/digital-security/
9　https://www.oecd.org/digital/ieconomy/digital-security-risk-management.htm
10　https://www.oecd.org/sti/ieconomy/protecting-children-online.htm

Ⅲ データの利活用

Ⅲ-1 準天頂衛星システム「みちびき」を活用した位置情報

一般財団法人日本情報経済社会推進協会　電子情報利活用研究部　主査　**松下 尚史**

1．はじめに

2021年10月26日、準天頂衛星「みちびき初号機後継機」を搭載したH-IIAロケット44号機の打上げが成功したと報じられた。本誌を読まれる方々においては、準天頂衛星はあまり馴染みのない話題かもしれないが、当協会では、わが国独自の測位衛星である準天頂衛星システム（愛称：みちびき）に関する取組みも行っている。

人類初の人工衛星は、1957年10月４日に、ソ連（当時）が打ち上げた「スプートニク１号」であり、96分で世界を一周することに成功した。その後、人類初の宇宙飛行が、1961年４月12日、ソ連の「ボストーク１号」に搭乗したソ連のユーリー・ガガーリンによって実現され、1969年７月20日には、アメリカの「アポロ11号」に搭乗したニール・アームストロング船長とバズ・オルドリン月着陸船操縦士２名が、人類で初めて月面に降り立った。わが国では、1970年２月11日、東京大学宇宙航空研究所が鹿児島宇宙空間観測所からL-4Sロケット５号機により打ち上げられた「おおすみ」が最初の人工衛星である。

「スプートニク１号」から半世紀以上が経過し、世界の宇宙産業の市場規模は、2019年時点で3,660億ドル[1]、2040年までには１兆ドル以上に拡大する[2]と言われる成長産業となっている。わが国においては、2017年時点の市場規模は約1.2兆円とされており、市場拡大のポテンシャルが高いことから、2030年前半までに宇宙産業の市場規模を倍増することを目指し、さまざまな取組みが進められている[3]。

宇宙基本計画[4]において、宇宙システムは、「位置・時刻・画像情報や通信機能を提供するなど、その実現に不可欠な社会のデジタル化・リモート化を、安全を確保しつつ実現する基盤であり、より一層経済社会への明確な貢献が求められる」ものとされている。

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

2．準天頂衛星システムの概要

準天頂衛星システムは、2006年から文部科学省・宇宙航空研究開発機構（JAXA）、総務省、経済産業

1　http://uchuriyo.space/snet/aichi2021/assets/pdf/snet2021aichi_cao.pdf
2　https://www.morganstanley.com/Themes/global-space-economy
3　宇宙政策委員会「宇宙産業ビジョン2030」
　https://www8.cao.go.jp/space/vision/mbrlistsitu.pdf
4　宇宙基本計画（令和２年６月30日 閣議決定）
　https://www8.cao.go.jp/space/plan/kaitei_fy02/fy02.pdf

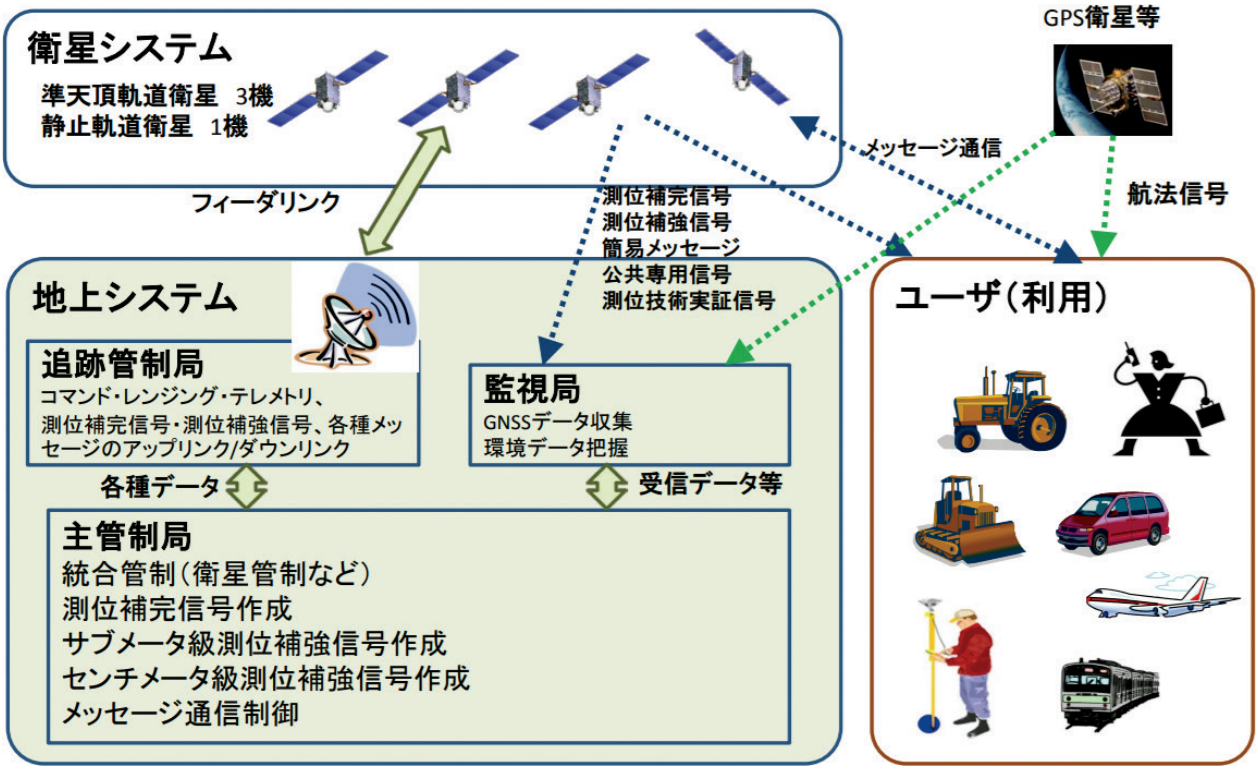
省、国土交通省が連携し、世界初のセンチメートル級衛星測位の実現を目指して、開発が開始された。2010年９月の初号機打上げ後、「実用準天頂衛星システム事業の推進の基本的な考え方」（平成23年（2011年）９月30日閣議決定）に基づき、2017年２月28日をもって、JAXAから内閣府に運用が移管された。その後、2017年に２号機、３号機、４号機の打上げに成功し、現在４機体制となり、2018年11月１日よりサービス提供を開始した。初号機開発から12年を経て、センチメータ級測位を実現している。

現在の準天頂衛星システムは、衛星系システムと呼ばれる宇宙空間に配備された３機の準天頂軌道衛星と１機の静止軌道衛星からなる４機の準天頂衛星と、地上系システムと呼ばれる地上に配備された主管制局、監視局、追跡管制局から構成される。

準天頂衛星は、静止衛星軌道[6]を45度傾けた準天頂軌道を周回する衛星を中心として構成することから準天頂衛星と呼ばれており、準天頂軌道衛星の軌道高度は日本上空で約40,000km、オーストラリア上空では約32,000km[7]となるような軌跡を辿る。これは日本の天頂（真上）付近（おおむね仰角70度以上）で約８時間の滞在時間を確保するためである。

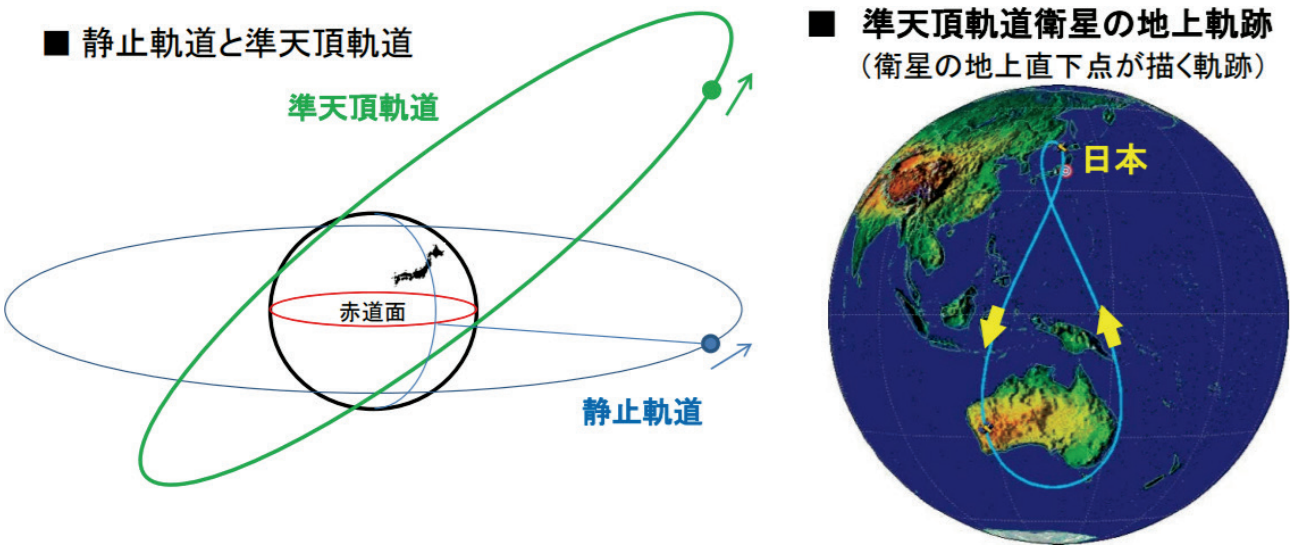
また、準天頂衛星の地上直下点が描く軌跡が８の字であることも特徴である。これはGPS（米国）、Galileo（欧州）、GLONASS（ロシア）、BeiDou（中国）が全世界を対象にしたものであるのに対し、準天頂衛星はRNSS（Regional Navigation Satellite System、リージョナルナビゲーションサテライトシステム、地域航法衛星システム）であり、特定地域を対象にしたものであることから、このような８の字の軌跡を描き、日本を中心としたアジア・オセアニア地域をサービス提供範囲としている。

2023年度をめどとして、準天頂衛星システムの７機体制が確立されると、日本上空に必ず衛星４機が存在する状態を維持できるようになり、米国のGPSに依存せず、持続測位が可能となる。



図表Ⅲ-１．準天頂衛星システムの全体概要[5]

5　https://www.mlit.go.jp/road/ir/ir-council/keizai_senryaku/pdf01/5.pdf
6　静止軌道衛星は、赤道上空約36,000kmの周回軌道（静止軌道）を、地球の自転と同じ速度で運行しており、地上からは常に上空の１点に止まって見える。
7　米国が運用するGPS（Global Positioning System）は、約20,200kmとされている。



図表Ⅲ-２．準天頂軌道と静止軌道、および準天頂軌道衛星の地上軌跡[6]

３．準天頂衛星システムが提供するサービス

準天頂衛星システムが提供している主なサービスは、以下のとおりである。

①衛星測位サービス[9]

準天頂衛星システムからGPSと同一周波数・同一時刻の測位信号（L1C/A、L2C、L5）を送信し、GPSと一体となって、測位精度を向上するサービス

②測位補強サービス

■サブメータ級測位補強サービス（SLAS）[10]

国内監視局（13局）での観測データを用いて、電離圏遅延や軌道、クロック等の誤差の軽減に活用できる情報を準天頂衛星システムから送信し、誤差を軽減することによって、誤差１ｍ以内での測位を実現するサービス

■センチメータ級測位補強サービス（CLAS）[11]

国土交通省国土地理院が全国に整備している電子基準点のデータを利用して補正情報を計算し、現在位置を正確に求めるための情報を準天頂衛星システムから送信し、誤差数cmの測位を実現するサービス

図表Ⅲ-３．準天頂衛星システムが提供する主なサービス[8]

8　https://www.mlit.go.jp/road/ir/ir-council/keizai_senryaku/pdf01/5.pdf
9　https://qzss.go.jp/overview/services/sv04_pnt.html
10　https://qzss.go.jp/overview/services/sv05_slas.html
11　https://qzss.go.jp/overview/services/sv06_clas.html

③メッセージサービス

■災害・危機管理通報サービス「災危通報」[12]

サブメータ級測位補強サービスと同じくL1S信号を使用し、気象庁が提供している防災気象情報などを独自のフォーマットに変換して、４秒間隔で送信するサービス

■衛星安否確認サービス「Q-ANPI」[13]

災害時における避難所の情報（避難所の位置、開設情報、避難者数などの避難所の状況など）を準天頂衛星システム経由で管制局に送信するサービス

④その他

L6E信号を用いた海外向けサービスであるMADOCA（Multi-GNSS Advanced Demonstration tool for Orbit and Clock Analysis）[14]や、L1Sb信号を用い、航空機などに対して測位衛星の誤差補正情報や不具合情報を提供するSBAS（衛星航法補強システム）信号を配信するサービス[15]なども提供している。

４．準天頂衛星システムの活用事例

「みちびき（準天頂衛星システム）」においても、多くの活用事例が紹介されている[16]。それらの活用事例の中で代表的なものとしては、以下のようなものが挙げられる。

■物流分野での活用

▶準天頂衛星システムのセンチメータ級測位補強サービスをドローンの自律飛行制御に活用し、ドローンによる個人宅などへの貨物輸送の実現を図る。

▶サブメータ級測位補強サービス対応の無線ICタグモジュールと管理者向けアプリにより、コンテナやシャーシの駐車位置情報をスマートフォンアプリで管理し、コンテナを探す手間を省力化することで物流の効率化を図る。

■自動運転分野での活用

▶センチメータ級測位補強サービスを車載センサーや高精度３次元地図と組み合わせることで、道路と自車の正確な位置関係や先の道路の曲率、勾配などの道路形状を把握し、高速道路のナビ連動ルート走行やハンズオフ走行の実現を図る。

▶センチメータ級測位補強サービスを活用して、オペレーターの運転操作を支援する除雪作業支援システムの実証実験を開始している。

■農業分野での活用

▶センチメータ級測位補強サービスを活用したトラクターの自動走行の実現を図る。（某ドラマのモデルにもなっている[17]。）

このようなドローン、自動運転車、自動運転トラクターなどの自車位置推定のために、高精度地図や車載センサー等と組み合わせて、GPS等とともに準天頂衛星システムも活用されている。GPSのみの測位では、誤差が５ｍ～10mと言われており、自動走行での利用は非常に困難であったが、準天頂衛星システムの提供するサービスを活用することにより、測位精度が格段に向上する。衛星測位で得られる位置情報は、特に絶対位置の推定には必要不可欠であるため、みちびきによる測位が高精度化・安定化することは大きなメリットとなっている。2021年には国土交通省より自動運転レベル３の型式認定を取得した世界初量産車が発売されるなど、その実装が進んでいる[18]。

また、こうした衛星測位の高度化を受け、国土地理院においては2021年４月１日より新しい解析手法によって、電子基準点日々の座標値[19]が最新の衛

12 https://qzss.go.jp/overview/services/sv08_dc-report.html
13 https://qzss.go.jp/overview/services/sv09_q-anpi.html
14 https://qzss.go.jp/info/information/madoca_171206.html
15 https://qzss.go.jp/overview/services/sv12_sbas.html
16 https://qzss.go.jp/usage/userreport/index.html
17 北海道大学リサーチタイムズ https://www.hokudai.ac.jp/researchtimes/2018/12/post-3.html
18 https://qzss.go.jp/info/archive/honda_210517.html
19 地図は過去のある時点の情報であり、その時点から地殻変動等によって、地図と現在の状態にズレが生じることから、電子基準点における日々の変動を把握するために提供している。
https://www.gsi.go.jp/eiseisokuchi/eiseisokuchi61007.html

星や測地基準座標系等に対応した、より高精度な位置情報として提供されるようになり、また、国土交通省主導の下、Society5.0の基盤として期待される世界水準の3D都市モデルがオープンデータとして順次公開[20]されるなど、地図の高度化に資する取組みも進み、衛星測位との高度な組合わせを用いたサービスの実現が期待される。

さらに、準天頂衛星システムでは、信号認証技術の整備が進んでいる。信号認証は測位信号に含まれる航法メッセージが本物であることを「電子署名」技術により証明するものであり、2023年度までに実施することが計画されている[21]。取得できる位置および時刻情報の信頼性が高まることから、ドローンや自動運転車両の運行管理、食品・医薬品等のトレーサビリティ、盗難品の追跡などへの活用の他、ブロックチェーンと組み合わせてサプライチェーンにおける品質管理の活用にも考えられる。また、シェアリングサービスにおいても、利用者IDとシェアされるモビリティ（たとえば自動車）のIDを紐付けることで、利用者がシェアしたモビリティをどのように使ったかというような利用状況が信頼性の高い情報として確認できるようになることも考えられる。そのような情報を、自動車保険などにおいても活用することが考えられる。

5．おわりに

準天頂衛星システムを活用した精度の高い位置情報、高精度な地図（３次元含む）データなどの活用は、Society5.0の基盤となるものである。現在は、実証実験段階の取組みが多く、実装された取組みはまだ少ない。また、われわれが身近なサービスとして、生活の中で触れることができるものはさらに少ない。

デジタルデバイドなSociety5.0の実現のためにも、多くの方々がこのような取組みに触れ、そこから多くのアイデアが生まれてくることが期待されている。

20　PLATEAU
https://www.mlit.go.jp/plateau/
21　https://qbic-gnss.org/wp-content/uploads/2021/05/21_wg4_01-02.pdf

Ⅲ−2 消費者視点のデータ利活用

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　グループリーダ　**奥原 早苗**

1．はじめに

2020年から本格化したコロナの世界的なパンデミックにより私たちの生活様式はこれまでとは大きく異なった。たとえば、マスク、手洗いが手放せなくなるなど、日常に支障をきたすような消費生活や、物品の購入等の消費行動にも大きな変化をもたらしている。要因の一つは、外出機会の減少により、店舗購入からオンライン経由で購入する等の消費行動が年代を問わずに増加、拡大したことであり[1]、オンラインによる消費行動は、デジタルプラットフォームを経由した取引が利用者の市場アクセスを大幅に向上させたこと等に後押しされ、生活インフラの一部になりつつある。他方、デジタルプラットフォームに関しては取引の透明性および公正性の低さ等の懸念が指摘されている。2021年２月１日に「取引透明化法[2]」が施行された経緯からも、デジタルプラットフォームとそれを利用する事業者間における取引の不透明さは社会課題の一つと見ることができる。なぜなら、デジタルプラットフォームを利用する事業者間における取引の不透明さは消費者取引のリスクに直結する可能性があるだけでなく、そのリスクがどのような影響を及ぼすかを予測することが困難であり、消費者個人が容易に解決できないトラブルに直面することになるからである。

消費者相談件数の商品・サービス別では、デジタルコンテンツが年代を問わず上位を占めており、販売購入形態別では「通信販売」の割合が増加する中、特にインターネット通販に関する相談件数は2018年から2020年の２年間で1.3倍となっている[3]。また、66.7％にのぼる消費者がインターネット上での商品・サービス購入で心配なこととして、「個人情報が漏えい・悪用されている」を挙げており[4]、オンライン取引に伴い提供が求められる個人情報の取扱いに不安を抱える消費者は少なくない。

個人情報保護法の令和２年改正（以降、「改正法」という。）では、データ利活用に関する施策の在り方としてイノベーションを促進する観点から新しい概念が導入された[5]。改正法の全面施行と同時期に施行される成年年齢引下げ[6]も相まって、契約行為のみならず契約時に提供することとなる個人情報に対する若年層の認識不足も大いに危惧されるところである。本項では、進展するデジタル社会で期待されるビッグデータの活用において、国内外の法制度も概観しながら、情報の提供主体である消費者（個人）の視点で留意すべき点を整理する。

2．令和２年改正個人情報保護法 ～個人の権利の拡大～

改正法は、消費者の権利または正当な利益の拡大が伴う重要なものであることは言うまでもないが、改正の背景として、次の事項が挙げられる[7]。特に、①、④、⑤は、自らが権利を行使する主体として、

1　消費者庁「令和３年版消費者白書」【特集】第１部第２章第１節新型コロナウイルス感染症の感染拡大と消費（２）「家計支出とインターネットを利用した支出の推移」
2　「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」経済産業省ホームページ https://www.meti.go.jp/policy/mono_info_service/digitalplatform/index.html（最終アクセス：12月１日）令和２年５月27日に成立し、同年６月３日に公布された。
3　前掲１ 第１部第１章第３節・第４節　最近注目される消費者問題（４）
4　前掲１ 第１部第２章第２節「新しい生活様式」と消費者の意識・行動
5　個人情報保護委員会ホームページ https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/（最終アクセス：12月１日）
6　平成30年６月13日、民法の成年年齢を20歳から18歳に引き下げること等を内容とする民法の一部を改正する法律が成立した。「民法の一部を改正する法律（成年年齢関係）」について　法務省ホームページ（最終アクセス：12月１日）
7　「個人情報保護法いわゆる３年ごと見直し制度改正大綱」令和元年12月13日（個人情報保護委員会）を元に筆者が要約。

消費者自身が「何が新たにできるようになったのか」、概要だけでも理解することが求められる。

①個人自らの情報の取扱いに対する関心や期待が高まっており、「個人の権利利益を保護」するために必要十分な措置を整備する必要がある。

②「保護と利用のバランス」をとるために、個人情報等を巡る技術革新の成果が、経済成長等と個人の権利利益の保護との両面で行き渡るような制度を目指すことが重要である。

③デジタル化された個人情報を用いた多様なサービスがグローバルに展開されており、国際的な制度調和や連携に配意した制度とする必要がある。

④海外事業者によるサービスの利用や、国境を越えて個人情報を扱うビジネスが増大し、個人が直面するリスクの変化に対応する必要がある。

⑤AI・ビッグデータ時代を迎え、個人情報の活用が一層拡大し、本人が自身の個人情報の取扱いを網羅的に把握することが困難になる中、事業者が本人の予測可能な範囲内で適正な利用がなされるよう権利利益における説明責任を果たし、環境を整備していくことが重要である。

3．プライバシーへの対応と消費者

2020年７月に、総務省と経済産業省が「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」の策定を公表した[8]。社会全体のデジタルトランスフォーメーション（DX）が進む中、イノベーションの創出による社会課題の解決とともに、プライバシー保護への要請が高まっていることが策定の背景である。ビジネスモデルの変革や技術革新が著しく、イノベーションの中心的役割を担うDX企業は、イノベーションから生じるさまざまなリスクの低減を自ら図っていかなければならない。企業にとってプライバシーに関わる問題に取り組むことは、消費者からの信頼を獲得し、企業価値の向上につながるとしている。

プライバシーに関する問題は、個人情報保護法を遵守していても、ビジネスモデルの複雑さや目に見えない情報やデータの取扱いによる不利益、そして、取扱われ方やリスクがどれぐらいなのかがわからないことへの不安が募り、炎上してしまうケースも少なくない。ひとたび炎上すると、批判や意見が集中し、メディアが過剰に不安を煽る現象も見受けられる。その場合、適正に情報を取捨選択し、冷静に自らのリスクを判断できる消費者はどれぐらいいるだろうか。仮に、企業が消費者やステークホルダーに対して、積極的に説明責任を果たしたとしても、誰もが一義的に情報を整理して理解できるわけではない。プライバシーガバナンス[9]に着目し、企業が能動的に消費者への説明責任を果たすことで社会の信頼獲得（向上）を図ろうと考えるのであれば、そもそも「消費者とは何か？」という重要な問いに目を向ける必要があると考える。

4．消費者の定義と脆弱性

消費者主権が成り立つ市場は、事業者と消費者に情報の非対称性がなく、消費者が合理的な判断の下で消費行動を行えるという条件が必要となる。しかし、DXが進展する社会では、情報の入手が容易になる反面、膨大な情報から自らに必要な情報を適切に収集し、判断する能力が不可欠となるため、消費者の定義は個人差によりさまざまなケースが考えられる。

わが国における消費者法では、消費者を明確に定義しているものとされていないものが混在しており、個人情報保護法でも明確に定義されていない。脆弱性の定義のうち、特に年齢については、未成年者も考慮した年齢別のルールが規定されていないため、わが国においても注視していく必要がある。

8　経済産業省ホームページを元に筆者が要約。
https://www.meti.go.jp/press/2021/07/20210719001/20210715009.html（最終アクセス：12月１日）

9　「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の向上に向けて、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う。前掲７より

「消費者（個人）」とは一体どのような主体を想定しているのか、「消費者の定義と脆弱性」は、今後議論が進むであろう“適正な同意の在り方”のみならず欠かすことのできない要件である。この要件をめぐる国外の事例として、欧州連合（EU）と米国の法制度を紹介する。

4.1　欧州連合（EU）

GDPR[10]では、すでに脆弱性要件のうち、年齢については16歳未満の子どもの個人データの取扱いにおいて親権者の同意を義務づけているが、ここではEUの欧州議会から出されている「脆弱な消費者[11]」より、プライバシーや個人情報の取得主体となる“消費者”について概観したい。

「脆弱な消費者」はEU指令でも規定されており、最良の取引を見つけて競争市場から利益を得ることができる、いわゆる合理的な選択をすることが可能と考えられている平均的な消費者と比較した場合、脆弱な消費者は、さまざまな理由でそうすることができないと考えられている。

脆弱な消費者を特定するには、主に２つのアプローチがあり、一つは、社会経済的地位の低さ、教育レベルの低さ、特定の言語を話す、マイノリティであるなど、脆弱になる（理論上の）リスクを高める消費者固有の特徴である。もう一つは、個々の特性間の相互作用により、すべての消費者が脆弱になる可能性があるとする見方である。これらの見方によれば、消費者は個々の状態に応じて脆弱な消費者になったり、そうでなかったりするという状況が生まれる。EUの消費者調査（2018）によると、EU市民の43％が消費者として脆弱であると報告していることからも、消費者の脆弱性は年齢やデジタルデバイドといった事柄に固定されるものではないことがわかる。つまり、わが国でも今後議論が活発化することが期待されている同意の在り方を検討する上でも、現行法の中でビッグデータの利活用を推進していく上でも、脆弱性は一部の消費者や個人を対象とするのではなく、消費者あるいは個人の誰もが脆弱性を持ち合わせる可能性があるといった、大きな枠組みで捉えた柔軟な対応が求められる。

EU法における脆弱な消費者のイメージは、学術文献に見られるものよりも狭いとされている。消費者が製品またはサービスを購入する以前の、商品開発の企画段階で、特に子どもの情報について考慮すべきである等、事業者の消費者に対する不公正な取引方法に関する指令（2005/29/EC: OJ 2005 L149/22）（以下、表記する場合は「不公正取引方法指令」という。）で定義されている。それは、「精神的または肉体的な弱さ、年齢または軽信性のために特に脆弱である消費者」のために、特別な保護が必要というものである。この定義は、消費者を脆弱にする可能性のあるさまざまな変数を考慮に入れるが、脆弱な消費者を保護する規定は、他の消費者法や、特定のセクターに関する法律、たとえばエネルギー、金融、食品等の分野で考慮されている。

電子商取引や人工知能の開発等においても、消費者の脆弱性に対する懸念が指摘されており、データの利活用を推進する場面では重要な視点となる。EUの消費者機構（BEUC）は、オンラインでのいくつかの慣行として、「平均的な」消費者と「脆弱な」消費者の概念の再考を求めている。消費者を操作してデータを収集する場合、すべての消費者が脆弱な消費者となる可能性が高まることから、すべての消費者を平等に保護する必要がでてくると指摘している。一方、欧州議会は、脆弱な消費者を定義する上で、より広い概念を提唱し、消費者をより強力に保護してきた。

しかし、どちらの概念も、消費者法の他の分野で明示的および暗黙的に使用されており、また、定義されている平均的な消費者の基準が高すぎて（操作されてデータを取得された消費者が、必ずしも合理的ではなく、平均的な消費者基準を下回り、多くの消費者が脆弱性を伴う）、実際の消費行動に対応していない。その結果、「脆弱な消費者への適切な保

10　GDPR（General Data Protection Regulation: 一般データ保護規則）。
EU域内の個人データ保護を規定する法として、2018年5月25日に施行された。
11　欧州議会 EPRS｜欧州議会研究サービス「脆弱な消費者」PE 690。619 – May 2021を元に筆者が要約。
https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690619/EPRS_BRI(2021)690619_EN.pdf

護を目的として、消費者の概念を再考すべきではないか」という議論は、今後私たちにとっても有益なユースケースとなるだろう。

4.2　米国

１）カリフォルニア州消費者プライバシー法（CCPA）[12]

海外の法制度として、米国カリフォルニア州消費者プライバシー法（以下、「CCPA」という。）に消費者の年齢を規定したルールがあるので触れておきたい。

CCPA第1798.120条（ｃ）項では、若者の年齢について次のように規定している。消費者が16歳未満であるという認識を事業者が実際に有していた場合、その事業者は、消費者が13歳以上16歳未満の場合には当該消費者自身が、又は消費者が13歳未満の場合には当該消費者の親又は保護者が、積極的に消費者の個人情報の販売を認めていない限り、消費者の個人情報を販売してはならない。事業者の要件は、①年間総収益2,500万ドル超、②５万件以上の消費者、世帯又はデバイスの個人情報を商業目的で取得・売買・共有等し、③年間収益の50％以上を個人情報の販売で得ていることのいずれか一つ以上を満たす事業者（第1798。140条（ｃ））としており、小規模事業者は除外されている。また、事業者には、事業者が提供を求められる通知および情報が、平均的な消費者により容易に理解され、障害のある消費者にアクセス可能であり、消費者とのやりとりに主として使用される言語で利用できるように提供されることを確保するために必要なルール、手続き、および例外を、成立後１年以内に、またその後は必要に応じて設けなければならないと規定している。

２）児童オンラインプライバシー保護法（COPPA[13]）他

COPPAは、米国の大手情報通信事業者が告発され、当該法では過去最大の和解金を支払ったことでも有名となった米国連邦取引委員会による米国連邦法である。COPPAは、13歳未満の子どもから個人情報を収集するウェブサイトまたはオンラインサービスを運営している事業者を対象として、いくつかのルールを設定している。たとえば、COPPAに準拠したプライバシーポリシーの公表や13歳未満の子どもから個人情報を収集する際は、保護者に通知し、検証可能な保護者の同意を得ることを義務づけている。

１）で触れたCCPAの強化版と言われるカリフォルニアプライバシー権利法（California Privacy Rights Act: CPRA）も動き始めており、人種または民族に関する情報、生体認証情報、性的志向に関する情報、位置情報等、「機微（センシティブ）情報」というカテゴリーが個人情報に加わった。

II章「各国のプライバシー保護施策」の「II-３．OECDが進めるデジタル経済政策とデータトラストへの取組み」で、OECDの取組みとして2021年に採択された「OECDオンライン上の子供の保護勧告」を紹介している。教育やインターネット、コミュニケーションツールを介して、子どもが気づかないうちに日常生活でデータの利活用が欠かせないものとなっているが、子どもをどのように保護していくのかを考慮する際、消費者教育だけで適正な利活用とリスクについて理解が深まるかと言えば、カバーできる範囲は限定的である。

６．おわりに

冒頭でも触れたコロナのパンデミックは、新規変異株である「オミクロン株」が世界各地で確認される等、新たな脅威となっている。わが国でもすべての国を対象として当面の間新規入国者を原則停止することが発表され、予断を許さない状況である。今後も引き続き、人との接触を抑えるという意味でも

12　個人情報保護委員会ホームページ https://www.ppc.go.jp/enforcement/infoprovision/laws/CCPA/
「California Consumer Privacy Act of 2018（仮日本語訳：カリフォルニア州消費者プライバシー法（2018年））」（最終アクセス：12月１日）

13　COPPA（Children's Online Privacy Protection ACT）FTCホームページを元に筆者が編集。
https://www.ftc.gov/（最終アクセス：12月１日）

オンラインを利用した消費行動の増加が見込まれ、取得される膨大なデータの利活用により得られるメリットは計り知れない。他方、企業は、新たな取引類型や決済手段の多様化に伴い、目に見えない取引の不透明さによる消費者取引のリスクが及ぼす影響がどのようなものか、説明責任がより一層求められることとなるだろう。消費者にとっても、自身の情報がいつどのように利活用されるのか、またはしないのかを理解し、自らどの情報をどこまで提供するのかを選択していかなければならない。

脆弱性は、製品の設計段階から始まり、利活用を終えて廃棄のフェーズを通し、顧客対応（苦情や問い合わせ）も含め、お客様の消費者としての行動のさまざまな段階で発生する可能性がある。脆弱性が発生する可能性をできるだけユースケースとして共有し、課題になり得るものは早めに潰しこみを行うことが必要である。今後、わが国でも「消費者」の誰もが持つ脆弱性を考慮した法整備の必要性が高まるものと思われる。ビッグデータの利活用は、個人情報の適正な取扱いによる安心・安全が担保され、その結果得られる信頼（トラスト）によって拡大していくものと考える。一義的なルールづくりではなくキメ細やかな配慮と共に、真に「“誰一人取り残さない”デジタル化」の実現を期待したい。

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

国　内	年	海　外	
特定個人情報保護委員会発足（1/1） APEC越境プライバシールール（CBPR）システムに参加（４月）	2014		
「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） 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）	2016	EU	欧州本会議「一般データ保護規則（GDPR）」を正式可決（4/14）
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ver. 2.0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）
	2021	米バージニア州	米国で２番目の消費者データ保護法制定（３月）
		中国	中華人民共和国の個人情報保護法成立（8/20）

〈資料2〉情報化に関する動向（2021年４月～2021年９月）

国　内	海　外
2021年４月	
・経済産業省、巨大IT企業６社を取引条件開示義務の規制対象に設定。 ・NTTコミュニケーションズ、欧州データ規制「GAIA-X」との相互接続の基盤開発に成功。 ・LINE、2021年３月に発覚した海外委託先企業に対する個人データのアクセス権限付与について、金融庁、総務省、個人情報保護委員会らが行政指導。 ・日本IBM、2010年受注の野村HDのシステム開発作業遅延に伴う契約解除による未払い報酬請求訴訟で勝訴。野村に履行作業分の報酬1.1億円の支払い命令。 ・東京都、コロナワクチン接種予約サイト登録の医療従事者27万人の情報が閲覧可能な状態に。 ・デジタル市場会議、巨大IT企業のデジタル広告の規制強化。取引条件などの情報開示義務付け。	・米最高裁、自動テキストメッセージ送信は電話消費者保護法に違反しないとして、Facebookへの支持判決。 ・サイバー犯罪フォーラムで、Facebookが2019年に流出した利用者情報5.3億件分が閲覧可能に。アイルランドデータ保護委員会が調査開始。F社は不正アクセスを否定。あわせてLinkedInやClubhouseの情報公開の報道あり。 ・Google、Oracleとの10年にわたるJavaの著作権侵害訴訟で勝訴。 ・中国国家市場監督管理総局、取引先への圧力が独禁法違反に当たるとしてアリババに3,000億円の罰金。 ・EU、AIの利用規則案発表。重要インフラ、顔認証利用に事前審査制導入。最大約39億円の罰金の可能性。

国　内	海　外
2021年５月	
・Sales Force、利用者側の公開設定ミスにより、国内38自治体、企業の保有する個人情報が外部から閲覧可能に。一部の組織で不正アクセスの痕跡あり。 ・デジタル改革関連法成立。デジタル庁を中心に行政のデジタル化、データ利活用促進を目指す。 ・眼鏡チェーンZoff運営会社、不正アクセスで9.7万件の顧客・取引先情報流出。 ・セイコーソリューションズ他、電子認証の共通基盤開発に着手。事業者間でのサービスの相互利用を可能に。 ・婚活マッチングアプリ「Omiai」、不正アクセスで会員情報171万件流出を報告。	・Amazon偽レビュー詐欺関与の20万人超の個人情報が流出。 ・IBM、世界初の「2nmプロセスチップ」製造。エネルギー消費75％削減可能に。 ・米コロニアル・パイプライン、サイバー攻撃で全業務停止。ハッカー集団ダークサイドに身代金５億円超を支払い復旧。その後、FBIが2.5億円を回収。 ・イタリア独占禁止局、GoogleにOS、アプリの独占的地位の悪用として1.2億ドルの支払い命令。 ・Facebook、アイルランドデータ保護委員会によるEU － 米国間のデータ移管禁止仮命令への不服申立て。データを活用したビジネス展開への弊害を主張するも認められず。 ・大手保険グループAXA、ランサムウェア被害で契約者情報など3TBのデータ盗難。 ・印航空会社Air India、乗客情報を扱うサービスプロバイダへのサイバー攻撃の影響で450万人分の顧客情報流出。

国　内	海　外
2021年６月	
・政府、契約書のデジタル化（電子契約）を盛り込んだ「特定商取引法・預託法」改正。 ・「押印を求める手続の見直し等のための経済産業省関係政令の一部を改正する政令」閣議決定。一部の手続きにおいて、押印／署名が不要に。 ・東芝、量子暗号通信で世界最長級の通信距離600㎞実証。2026年までの実用化を目指す。 ・KDDI他、世界初の「水空合体ドローン」開発。空中ドローンに映像伝送、音波での測位可能な水中ドローンを搭載。 ・政府、IT基本法の見直し、デジタル庁設置に対する政府の基本的方針を示した「デジタル社会の実現に向けた重点計画」閣議決定。 ・中日新聞社、委託先の不正アクセスで14.3万件の個人情報漏えいの可能性。 ・JIPDEC、標準企業コード登録をデジタル化。登録証にeシール（発行元証明）付与。	・ハッカー集団ノベリウム、24カ国150超の政府、組織にサイバー攻撃。昨年も大規模攻撃に関与。 ・ブラジル食肉最大手JBS、サイバー攻撃で北米、豪で操業停止。約12億円の身代金支払い。 ・仏競争委員会、広告掲載サービス市場での支配的地位の乱用でGoogleに290億円の制裁金。 ・米Webコンテンツ配信会社fastly、大規模なシステム障害で世界各国の政府、企業サイト数千件が一時利用不可に。原因は未発見のソフトウェアのバグ。 ・独フォルクスワーゲン、販売業者へのハッキング被害で顧客300万人分の連絡先情報流出。 ・中国政府、企業のデータ統制強化を図る「データ安全法」成立。データ収集から保存などすべての過程を当局が管理。 ・欧州司法裁判所、加盟国のデータ監視当局は監督外でもデータ規制違反企業への提訴が可能と判断。Facebookのベルギー当局による管轄範囲をめぐる訴訟が契機。 ・ヘルスケア会社CVS Health、10億件ものデータがクラウド上に公開、閲覧可能に。 ・米下院委員会、巨大IT企業規制強化の反トラスト法改正案６本を可決。 ・米連邦地裁、Facebookに対する米連邦取引委員会（FTC）の反トラスト法違反訴訟を棄却。SNS市場でのF社の独占的地位証明できず。 ・EUと英国、個人データ移転合意。全EU加盟国が英国の十分性を認定。

国　内	海　外
2021年７月	
・NTTぷらら、委託先が不正アクセス被害で最大800万件の個人情報流出の可能性。 ・みずほ銀行、システム障害で取引停止。2021年２月から複数回障害発生。金融庁が業務改善命令。 ・東京大学とIBM、ゲート型商用量子コンピュータシステム稼働開始。東大がシステム占有使用権を保有、企業や研究機関で活用。	・EU、世界初のデジタル健康証明書導入開始。コロナワクチン接種済ならEU域内の旅行が可能に。 ・米Kaseya、ランサムウェア攻撃被害で世界約1,500社に影響。身代金請求額は約77億円。 ・G20、巨大IT企業の課税逃れを規制する法人課税ルール見直しで合意。今後制度を見直し、2023年運用開始を目指す。 ・仏競争委員会、ニュース記事のコンテンツ使用に関する配信会社との交渉方法に従わないとして、Googleに５億ユーロの制裁金。 ・中国政府、インターネットサービスの管理規定発表。セキュリティ上問題があったネットサービス企業を当局の指導下に。

国　内	海　外
2021年８月	
・富士通、５月発生の情報共有ツールへの不正アクセスで、官庁など129組織の情報流出が判明。ツールの脆弱性を突き、正規のID／パスワードでログイン。 ・ニップン、７月に起きたグループ会社を含む大規模なサイバー攻撃によりデータが暗号化され、復旧困難。四半期報告書提出できず。	・エストニア国家情報システム庁、国民IDカードの顔写真データ約29万人分が不正ダウンロード。 ・分散型金融DeFi運営会社Poly Network、サイバー攻撃被害で暗号資産約660億円が不正流出。その後ほぼ全額がハッカーから返還。 ・中国政府、重要インフラ施設のデータ保護のための「重要情報インフラ施設安全保護条例」９月施行発表。国内からのサイバー攻撃への対策強化へ。 ・仮想通貨取引所運営QUOINE、ハッカー攻撃被害で約108億円の暗号資産流出。 ・中国、「個人情報保護法」成立、11月施行。個人データの海外持出し規制。 ・FTC、６月の訴状棄却を受けFacebookを独占禁止法違反で再提訴。新興企業買収で競合他社との市場競争阻害を訴え。 ・スイス研究チーム、スパコンで円周率計算。62.8兆桁目まで計算し、世界記録更新。 ・Microsoft、アプリ開発ツールの設計ミスで3,800万件の個人情報流出。 ・英政府、個人データの国際的移転に関し、「英国版一般データ保護規則（UK GDPR）」で十分性認定に向けたパートナーシップ締結の優先的な国・地域に、米、豪、韓国など６カ国・地域を指定。

国　内	海　外
2021年９月	
・デジタル庁、９月１日付発足。中央省庁、国、地方のシステム統一、行政手続きのオンライン化に着手。 ・公正取引委員会、独占禁止法違反に抵触するとして2016年以降Appleを審査。外部課金サイトへの一部誘導を認める対応を受け、審査終了。 ・Amazon、クラウドサービスAWS障害で、日本国内の航空会社、証券会社などに影響。 ・政府、「サイバーセキュリティ戦略」を閣議決定。「DX with Cybersecurity」を掲げ、デジタル庁を中心にDXとセキュリティ対策を推進。 ・フィッシング対策協議会とJIPDEC、メーラーの「S/MIME」対応状況を調査。S/MIME電子署名メールを送信できるメーラーは、Outlook等６種類。	・中国政府、データ安全法（データセキュリティ法）施行。中国初のデータ取扱いを規制する法律。 ・アイルランド個人情報保護当局、Facebook傘下のWhatsAppに約290億円の制裁金。個人情報の利用に関する説明の不透明性を指摘。 ・エルサルバドル政府、ビットコインを法定通貨として世界初の採用。 ・Epic Games、Appleに対する反トラスト法訴訟で、A社が反トラスト法への抵触を否定する米連邦地裁判決を受けて上訴。 ・韓国公正取引委員会、競合するソフト開発会社に対する優越的地位の乱用に対し、Googleに約195億円の課税金納付命令と是正措置命令。 ・Google、EUから競争法違反で過去最大額43.3億ユーロの制裁金命令に対する異議申立て訴訟審理開始。OS市場独占に対し、G社は市場競争を機能させる上で大いに役立ってきたと主張。 ・豪競争・消費者委員会、Googleのオンライン広告独占がメディア、広告会社、消費者に悪影響を与えるとし、ターゲット広告のための利用者情報の使用規制権限の必要性を指摘。

JIPDEC IT-Report 2021 Winter

2021年12月24日発行（通巻第18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：03-5673-0560

制　作　株式会社ウィザップ