

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ム、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。

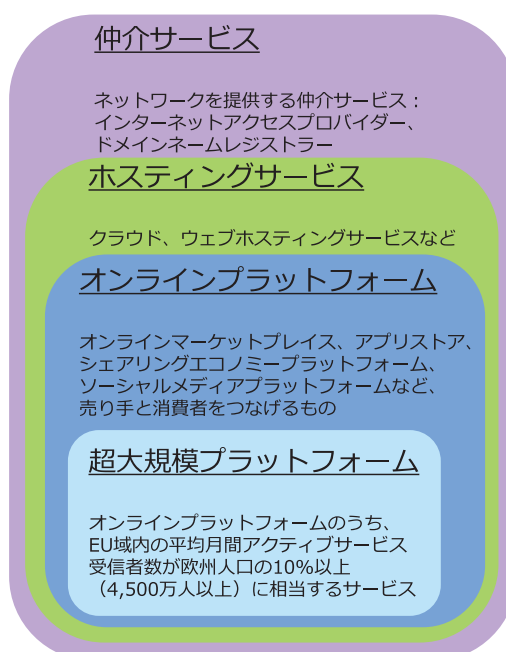
	DMA	DSA
包括的な目的	新しいプラットフォームが市場に参入しやすくすることで、競争を可能にする。	透明性、ユーザーの安全性、およびプラットフォームのアカウントビリティを実現する。
対象	ゲートキーパー（図表 II-7 参照）	仲介サービスプロバイダー、オンラインプラットフォーム。 ※月間アクティブユーザー数が4,500万人以上の「超大規模」オンラインプラットフォームに関する特別ルールあり。
箇条の種類	競争を阻害しないために、ゲートキーパーが必ずしなければならないことと、してはならないことを定める。	責任規定、透明性報告義務、デューデリジェンス義務。
施行方法	EUレベルで、通信ネットワーク・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」の制裁金を課することができる。	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ムに対して、オンライン上の透明性とアカウント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ムごとに異なる（図

表II-5）。特に、影響力が大きい超大規模プラットフォームに対しては、より一層の透明性とアカウント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トビリティ				●
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¹。

また、近年の巨大プラットフォームの市場にお

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ムによるオンライン市場の支配的地位を背景に、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。

コア・プラットフォームサービス（例）

- オンライン仲介サービス
- オンライン検索エンジン
- SNS
- 動画共有プラットフォームサービス
- メッセージサービス
- OS
- クラウドコンピューティング

ゲートキーパー

- EU域内市場に影響を与える規模である
- ビジネスユーザーから最終消費者に向けての重要なゲートウェイをコントロールする立場にある
- 定着した永続的な地位にある

図表Ⅱ-6. DMAにおけるコア・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ム、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ン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み合わせ。
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。

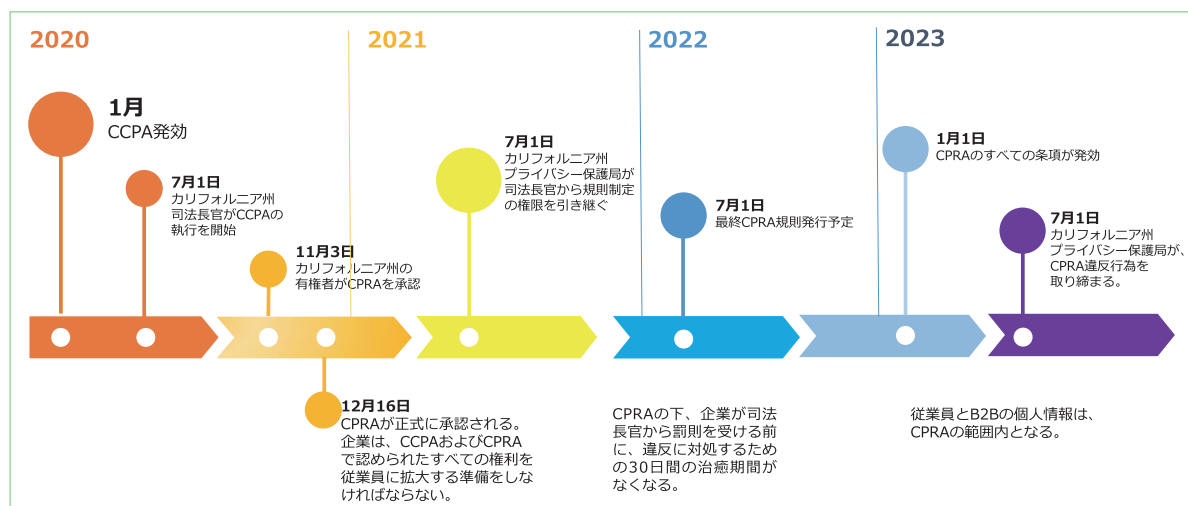
5 “Consent” means any freely given, specific, informed, and unambiguous indication of the consumer’s wishes（後略）

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）	✓	✓

- 2022年1月1日までB2Bおよび従業員情報が免除される。
- 2023年1月1日までB2Bおよび従業員情報が免除される。
- 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