第2節 日本と世界のデータ関連制度

1 法整備以降の国内動向

我が国におけるデータ流通に関わる環境整備は急速に進展しつつある。特にここ1年間程で、2017年5月の改正個人情報保護法全面施行、2016年12月の官民データ活用推進基本法公布・施行など、基盤となる法制度が整備されてきたことを受け、それらに基づく一層のデータ流通促進に向けた環境整備が進められている。本項では、最近の国内における施策と検討状況を概観する。

1 PDS・情報銀行・データ取引市場

ア 内閣官房IT総合戦略室での検討

有線・無線ブロードバンドネットワークの整備やスマートフォン・IoT機器の普及、AIの進化などにより、個人の行動履歴等を含む膨大なデータを効率的に流通させ、活用していくための技術的環境が整いつつある。法制度面では、改正個人情報保護法における匿名加工情報制度の導入による個人のデータの活用の拡大が期待されているところだが、それに加え、個人のデータをどのように安全に流通させるか、また個人に係らない産業データ等の流通をいかに進めていくかが、総合的なデータ流通環境整備にとっての課題となる。

内閣官房IT総合戦略室では、それらの課題に対応した環境整備を行うため、2016年9月から「データ流通環境整備検討会」を開催し、同検討会に設けられた「AI・IoT時代におけるデータ活用ワーキンググループ」において、PDS（Personal Data Store）、情報銀行（情報利用信用銀行）、データ取引市場という新たなデータ流通の仕組みについて集中的に検討し、2017年3月に中間とりまとめを公表した。それぞれの定義は以下のとおりである（図表1-2-1-1）。

図表1-2-1-1 PDS・情報銀行・データ取引市場の定義[*1]

PDS（Personal Data Store）	他者保有データの集約を含め、個人が自らの意思で自らのデータを蓄積・管理するための仕組み（システム）であって、第三者への提供に係る制御機能（移管を含む）を有するもの。
情報銀行（情報利用信用銀行）	個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業。
データ取引市場	データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）。

（出典）IT総合戦略本部 データ流通環境整備検討会「AI、IoT時代におけるデータ活用ワーキンググループ　中間とりまとめ」（2017）

情報銀行は、観光や金融（フィンテック）、医療・介護・ヘルスケア、人材等の様々な分野において、個人情報を本人が自らの意思に基づき活用することを支援し、その便益を本人に還元することにより、官民データ活用推進基本法第12条に定められる「個人の関与の下での多様な主体による官民データの適正な活用」の拡大に資することが期待される。データ取引市場は、情報銀行に蓄積された個人のデータや、様々な企業が保有する産業データ等の取引を活性化させ、企業や分野を越えたデータ流通の基盤となることが期待される。

イ 総務省・経済産業省での検討

データ流通環境整備検討会での検討を受け、2017年2月、総務省情報通信審議会情報通信政策部会 IoT 政策委員会基本戦略ワーキンググループの下に「データ取引市場等サブワーキンググループ（SWG）」が設置され、2017年6月に取りまとめを公表した[*2]。同SWGでは、今後情報銀行が、個人とのデータ活用に関する契約等に基づき、データ保有者に代わり第三者提供の可否を判断し実際に提供まで行う、いわゆる情報信託機能を実現していく上で、情報信託機能の信頼性を確保するための仕組みが必要であるという認識の下、経営の安定性やセキュリティ体制、データ提供者との契約内容等に関わる一定の基準を満たした事業者を認定する仕組みについて、民間団体等が任意の認定制度を構築していくことが望ましいと結論付けている。

これに基づき、2017年11月からは、総務省と経済産業省が合同で「情報信託機能の認定スキームの在り方に

＊1　内閣官房IT総合戦略本部データ流通環境整備検討会「AI、IoT時代におけるデータ活用ワーキンググループ　中間とりまとめ」（2017年3月）
https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/siryou2.pdf
＊2　情報通信審議会 情報通信政策部会 IoT政策委員会 基本戦略ワーキンググループ「データ取引市場等サブワーキンググループ 取りまとめ」
http://www.soumu.go.jp/main_content/000501149.pdf

関する検討会」を開催しており、2018年6月に、情報信託機能を担う者の認定基準、モデル約款の記載事項や認定スキーム等の民間の団体等による任意の認定の仕組みについて、指針が公表された。さらに情報銀行等を通じたデータ流通を拡大していくために、官民が保有する個人情報を、再利用しやすいデジタル形式で本人に還元したり、あるサービスから別のサービスに移管できるようにする「データポータビリティ」に関しても、同じ2017年11月から経済産業省と総務省が合同で「データポータビリティに関する調査検討会」を開催し、次項で述べるEUの施策等を参照しながら調査・検討を進めている。

ウ　データ流通推進協議会の設立

データ取引市場の形成に関しては、2017年11月にデータ流通ビジネスに積極的に取り組む企業数十社により「データ流通推進協議会[*3]」が設立され、民間主導でのデータ流通事業者認定制度構築を視野に入れた取組が開始されている。同協議会では、データ提供者・利用者の双方が安心してデータ流通に参加する上での基盤となるデータ流通事業者が満たすことが望ましい事項や、具体的な認定制度運用のあり方を検討するため、「運用基準検討委員会」「技術基準委員会」「利活用促進委員会」「認定・監査委員会」の4つの委員会が設けられ、産業界・政府・学識経験者等を交えての議論が進められている。

2　オープンデータの活用

ア　オープンデータ基本方針の策定

我が国では、2012年7月に内閣官房IT総合戦略本部が策定した「電子行政オープンデータ戦略」などに基づき、政府や独立行政法人、地方公共団体、公益企業等が保有するデータの公開と再利用の促進に向けた施策が進められてきた。特に官民データ活用推進基本法において、「国及び地方公共団体等が保有する官民データの容易な利用等（第11条）」が基本的施策として定められたことを受け、2017年5月には、内閣官房IT総合戦略本部が今後のオープンデータに関わる施策の基本指針をまとめた「オープンデータ基本指針[*4]」を公表している。同基本指針では、公共データにつきオープンデータを前提として情報システムや業務プロセス全体の企画、整備及び運用を行う「オープンデータ・バイ・デザイン」の考え方に基づき、政策企画・立案の根拠となったデータを含め、各府省庁が保有するデータはすべてオープンデータとして公開すること、各省庁のウェブサイト公開されるデータについては政府標準利用規約を適用し公開データの二次利用を積極的に促進すること、機械判読に適した構造・データ形式で掲載することなどの原則を提示している。

イ　官民の対話によるオープンデータ推進

また内閣官房IT総合戦略室では、先述の「データ流通環境整備検討会」の下に2016年10月から「オープンデータワーキンググループ」を設置し、各府省庁の施策推進や地方公共団体等におけるオープンデータ施策の支援に取り組んできたが、より民間ニーズに即したオープンデータの取組を進めるため、2018年1月からは「オープンデータ官民ラウンドテーブル[*5]」を開催し、公共データの活用を希望する民間企業等と公共データを保有する府省庁等の対話を行っている。同ラウンドテーブルでの民間企業等の具体的要望を受け、早くも各府省庁が新たなデータ公開やデータの標準化に向けた作業を進めている。

＊3　データ流通推進協議会 https://data-trading.org/
＊4　内閣官房IT総合戦略本部官民データ活用推進戦略会議決定「オープンデータ基本指針」2017年5月30日　https://cio.go.jp/sites/default/files/uploads/documents/data_shishin.pdf
＊5　実施状況については、内閣官房IT総合戦略室による以下のページを参照。
https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/kanminrt_dai1/gijisidai.html

図表1-2-1-2　国内の関連省庁におけるデータ流通環境整備に関する議論の状況

省庁	部局	会議体	公表文書等	検討事項
内閣官房	日本経済再生総合事務局	未来投資会議	未来投資戦略（2018.6予定）	第４次産業革命の推進、Society5.0実現
	IT総合戦略室	データ流通環境整備検討会	オープンデータ基本指針（2017.5）	政府全体のオープンデータに関わる施策の基本指針
		官民データ活用推進戦略会議	IT新戦略の策定に向けた基本方針（2017.12）	官民データ活用の促進
内閣府	総合科学技術・イノベーション会議	重要課題専門調査会	分野間データ連携基盤の整備に向けた方針（2018.4）	分野をまたいだデータ連携を実現するための基盤構築
総務省	情報流通行政局 └情報通信政策課	情報通信審議会 └情報通信政策部会 └IoT新時代の未来づくり検討委員会	未来をつかむTECH戦略（2018.4）	自治体・産業のデータ活用、データ流通時代の競争力強化方策
		情報信託機能の認定スキームの在り方に関する検討会（経済産業省と合同開催）	報告書（2018予定）	情報信託機能を扱う者が満たすべき要件
文部科学省	文化庁	文化審議会 └著作権分科会	著作権法改正案（2018.2）	「柔軟な権利制限規定」の導入によるデータ活用の円滑化
経産省	経済産業政策局 └知的財産政策室	産業構造審議会 └知的財産分科会 └不正競争防止小委員会	データ利活用促進に向けた検討中間報告（2018.1） 不正競争防止等改正案（2018.2）	不正競争防止法の改正によるビッグデータの保護
	商務情報政策局 └情報経済課	データポータビリティに関する調査・検討会（総務省と合同開催）	報告書（2018予定）	主要分野（医療、金融、電力等）におけるデータポータビリティの在り方
		IoT推進コンソーシアム	データ利用権限に関する契約ガイドラインVer1.0（2017.5）	事業者間の取引におけるデータ活用に関する契約の在り方
国交省	大臣官房 └技術調査課	i-Construction推進コンソーシアム	3次元データ利活用方針（2017.11）	建設生産プロセスの各段階での3次元データの利活用方法、システム構築
公正取引委員会	競争政策研究センター	データと競争政策に関する検討会	報告書（2017.6）	データの収集・利活用に関連する競争政策及び独占禁止法上の論点整理

（出典）総務省「我が国のICTの現状に関する調査研究」（2018年）

2 国際動向

1 パーソナルデータの国際流通

ア　EU一般データ保護規則の適用開始に向けた動向

1995年に成立して以来、EUのみならず世界各国の個人情報保護法制のモデルとして参照されてきたEUデータ保護指令は、2018年5月25日から、新たな「一般データ保護規則（GDPR：General Data Protection Regulation）」の直接適用に置き換えられた。GDPRは2012年1月に欧州委員会から原案が提出されて以来、欧州議会・欧州理事会での審議を経て2016年4月に成立、それから2年間の猶予期間を経ての適用開始となる。

GDPRは、EU加盟28国及び欧州経済領域（EEA：European Economic Area）3か国を含む31か国において事業を営む場合に加え、海外からEU市民に向けてサービスを提供したり、その個人情報を取得したりする場合にも適用される。2,000万ユーロか全世界連結売上高4%のいずれか高い方等を上限とする高額な制裁金などを背景に、世界各国の企業がそのコンプライアンス対応に取り組んでいる。

従来のデータ保護指令は、EU及びEEA加盟国が指令に基づく国内法を整備することで初めて効力を持つものだったが、GDPRは、適用が開始され次第、加盟国及びEU域外の対象企業に直接適用されるルールであり、それに伴い、EU域内でのデータ保護法は原則として一本化される。ただし、GDPRの執行は引き続きEU加盟国それぞれが設置するデータ保護当局（Data Protection Authority）が行うものであり、GDPRではその一貫性を確保するためのメカニズム整備なども行われているが、実際の法運用は引き続き国による相違が一定程度存在し続けることが想定される。

2016年のGDPR制定以来、各国のデータ保護当局及びEU機関のデータ保護を担当する欧州データ保護監察官から構成される合議体である29条作業部会（GDPRの適用開始以降は欧州データ保護会議と改称）は、GDPRによって導入される新たなデータ保護ルールについての解釈・執行指針を示す多くのガイドラインを策定してきた。2018年4月末現在公表されているガイドラインの一覧は、下記のとおりである（図表1-2-2-1）[*6]。GDPRへの対

*6　個人情報保護委員会ホームページ「GDPR（General Data Protection Regulation：一般データ保護規則）」を参照。
https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/

応においては、これらのガイドラインの精査が求められる[*7]。

図表1-2-2-1　ガイドライン一覧

・データポータビリティの権利に関するガイドライン
・データ保護責任者に関するガイドライン
・データ管理者又はデータ処理者の主導監督当局を特定するためのガイドライン
・データ保護影響評価及び処理活動が「高いリスクを引き起こし得る」か否かの判断に関するガイドライン
・制裁金の適用及び設定に関するガイドライン
・個人データ漏えい時の通知に関するガイドライン
・自動化された個人に関する決定及びプロファイリングに関するガイドライン
・同意に関するガイドライン
・透明性に関するガイドライン

（出典）個人情報保護委員会ホームページ

またEUには、データ保護指令を補完する形で、2002年に電子通信分野における特別なプライバシー保護のルールを定めた電子通信プライバシー指令（e-privacy directive, 2002/58/EC）が制定されており、通信の機密性や、行動ターゲティング広告等に用いられるブラウザのクッキー情報利用などについての規律が定められている。欧州委員会は2017年1月、GDPRと同時の2018年5月の適用開始を目指す形で、新たな「電子通信プライバシー規則」案を公表し、欧州議会・欧州連合理事会における審議が進められてきた。

加盟国間での意見調整の長期化などにより、同規則の成立は2018年秋以降にずれ込む見込みだが[*8]、同規則案は、GDPRと同様に従来の電子通信プライバシー「指令」を「規則」に格上げするとともに、執行主体や制裁金を含め、GDPRと一体的な運用を可能とする形での立法作業が進められている。GDPRと同等の域外適用も導入される見込みであり、日本企業としても対応を検討する必要がある（図表1-2-2-2）。

図表1-2-2-2　「電子通信プライバシー規則」案（2017年1月欧州委員会提案版）の主な内容

指令から規則へ	GDPR同様、現行の指令を規則に変更、加盟国に直接適用される。
域外適用	EU域外から域内のエンドユーザーに電子通信サービスを提供する場合や、域内の端末に関わる情報（クッキー等）の利用にも適用される。
執行協力	各国のデータ保護当局がGDPRと合わせて執行を担うと共に、制裁金も一般データ保護規則の規定が準用される。
通信の機密性	伝統的通信事業と機能的に同等なOTTサービスに通信の機密性保護義務の適用対象を拡大し、明確な同意無き通信内容利用を禁止。具体的には、SkypeやFacebookメッセンジャー、Gmail等のメッセージング・VOIP・クラウドメール等が対象になる。
クッキー規制の合理化	現行指令同様クッキーの利用は原則オプトインとし、新規則案ではサービスの提供に不可欠な場合や第三者提供を伴わないウェブ解析等は同意が不要であることを明確化すると共に、ウェブブラウザ提供事業者に簡易なクッキー拒否オプションの提供を義務付ける。

（出典）総務省「我が国のICTの現状に関する調査研究」（2018年）

イ　EUからの十分性認定と日本の個人情報保護法

EUのデータ保護法制は、グローバルなデータ流通環境においてEU市民の個人情報保護を確保するため、欧州委員会から個人情報の「十分な保護水準」を有するという認定（十分性認定）を受けた第3国以外へのEU域内からの個人データ移転を原則として禁止する、越境個人データ移転規制を有してきた。十分性認定を受けていない第3国への個人データ移転を行うためには、企業等は拘束的企業準則（BCR）や標準契約条項（SCC）などEUから認定された特別な枠組を用いるか、本人からの同意を得なければならず、そのコストが日本企業の国際的なデータ活用ビジネスを進める上での課題とされてきた。

日本においては、ここ数年来、個人情報保護委員会を中心として日EU間の双方向での個人データの越境流通の枠組の構築を目指した対応を行ってきた。現在、2018年の早い段階でGDPRに基づくEUからの正式な十分性認定を受け、また個人情報保護法第24条に基づく外国指定をEUに対して行うことを目指し、EUとの間での交渉が進められている。これにより、日本とEUの間での個人データ移転を含む国際取引は大きく拡大していくことが期待されている。

一方で、日本とEUの個人情報保護法制には一定の差異が存在することに鑑み、十分性認定の実現と合わせ、その差異を埋めるために、十分性認定により移転されたEU市民のデータを日本国内で取り扱うにあたっての規定に関わる「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ガイドラインの方向性につい

＊7　これらのうち一部は、日本貿易振興機構（JETRO）が、日本語による解説を公表している。
https://www.jetro.go.jp/world/reports/2018/01/9a90f1003bc16515.html
＊8　英国Privacy Law & Business Report“e Privacy Regulation not Ready to Coincide with GDPR implementation”（2018年1月）。
https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2018/1/e-privacy-Regulation-not-ready-to-coincide-with-GDPR-implementation/

て[*9]」が個人情報保護委員会から公表されている。要配慮個人情報の範囲や、匿名加工情報を利用する際の措置をはじめ、EU市民の個人データを取り扱う際には同ガイドラインに留意する必要がある。

また日本法においても、2017年5月に施行された改正個人情報保護法第24条において、外国にある第三者に個人情報を提供する際の規律が導入されたところだが、個人情報保護委員会は、EUからの十分性認定を受けると同時に、EU全体を同条に基づく「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国」として指定する個人情報保護委員会規則を採択する方向性が示されている。指定対象として想定されるEUには、EU加盟28か国に加え、EEA3か国（アイスランド、リヒテンシュタイン、ノルウェー）が含まれ、これらの国々には、国内と同様の要件にて個人情報の提供を行うことができる見込みである。

ウ　アジア諸国における越境個人データ移転規制の状況

インターネットの本格的な普及や電子商取引のグローバルな拡大を受け、新興国においても、ここ数年来、個人情報保護法制の整備が急速に進められてきており、EUと類似した越境個人データ移転規制を有しているものも見受けられる。例えばアジア太平洋地域では、少なくともカナダ・メキシコ・韓国・香港（当該条文未施行）・シンガポール・マレーシア・インド・オーストラリア等が広範な越境個人データ移転規制をすでに有しており、その他にもタイやインドネシア、ベトナム等が立法準備を進めている。特に日本企業にとっては、2020年東京オリンピック・パラリンピックにおけるおもてなしICTサービスの展開等において、多数のアジア太平洋諸国民の個人データを扱うことが想定されるため、これら国々の越境個人データ移転規制の状況にも注意を払う必要がある。

アジア太平洋各国の越境個人データ移転規制においても、日本やEUのように、適切な保護水準を有する外国への認定を行うことで自由な越境個人データ移転を可能とする、十分性認定制度を有している国が見受けられる。例えば2017年4月には、東アジア地域では初めて、マレーシアが十分性認定を行う国リストの草案を公表している[*10]。

EU加盟28か国＋EEA3か国で一括の十分性認定を行うEUとは異なり、これら新興国の十分性認定についてそのような国際的な枠組は現時点で存在していない。こうした複雑さを増すアジア太平洋地域における個人データの越境移転を円滑化するため、アジア太平洋経済協力（APEC：Asia Pacific Economic Cooperation）において越境プライバシー保護ルール（CBPR：Cross Border Privacy Rules）の枠組が開始されている。2018年3月現在では、正式参加国はアメリカ・カナダ・メキシコ・日本・韓国・シンガポールの6か国となっている。CBPRの枠組では、APECから認定を受けた中立的な認証機関（アカウンタビリティーエージェント：民間団体又は政府機関）が、個人情報保護に関する一定の条件を満たした事業者を認証する。日本は、2014年よりCBPRに参加しており、一般財団法人日本情報経済社会推進協会（JIPDEC）が認証機関に認定されている。

2　非個人データを含むデータローカライゼーション規制の状況と対応

前項で述べた越境個人データ移転規制と並行して、ここ数年来、特に新興国を中心に、ICTサービスの提供に用いられるサーバー設備等の国内設置を求める、「データローカライゼーション（data localization）」規制が拡大しつつある。

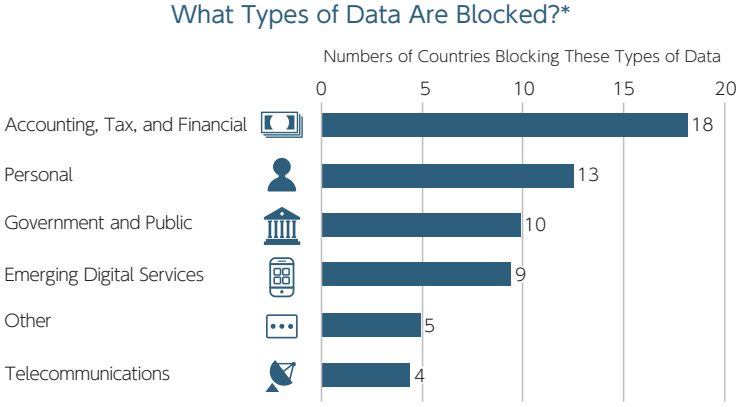
このデータローカライゼーション規制は、個人データの越境移転行為に焦点を当てる越境データ移転規制と異なり、ある国において（あるいは外国から当該国を対象に）特定の事業活動を営む場合に、当該事業活動に必要なサーバーやデータ自体の国内設置・保存を求める規制である。また、越境個人データ移転規制では原則として本人の同意があれば海外への移転が可能であるが、データローカライゼーション規制では、対象データが個人データに限られないため、本人の同意による移転は行い得ず、データの越境移転にあたっては、当該国政府の許可等が必要となることが多い。なお、米国の業界団体であるITIF（Information Technology and Innovation Foundation）が公表している、データローカライゼーション規制の対象になっているデータの種別内訳は以下のとおりである（図表1-2-2-3）。

＊9　第53回個人情報保護委員会（2018年2月9日）資料を参照。
https://www.ppc.go.jp/enforcement/minutes/2017/20180209/
＊10　マレーシアによる十分性認定に関する意見招請のための文書草案につき、以下を参照。
http://www.pdp.gov.my/images/pdf_folder/PUBLIC_CONSULTATION_PAPER_1-2017_.pdf

ア　中国サイバーセキュリティ法

データローカライゼーション規制に関して、国際的に広い関心を集めるきっかけとなったのが、2017年6月に中国で施行された、サイバーセキュリティ法（中華人民共和国網絡安全法）[*11]第37条である（図表1-2-2-4）。同条は、①何らかのネットワークを所有・運営する「ネットワーク運営者」のうち、②特に国の安全や国民経済と民生、公共の利益に与える影響が大きいと指定される「重要情報インフラストラクチャーの運営者」について、③それが保有する個人情報及び「重要データ」を中国国外に移転するにあたっては、④国が定める基準に従い「安全評価」を行わなければならないことを定めている。なお、サイバーセキュリティ法の第37条部分については、2019年1月1日の施行が見込まれている。

図表1-2-2-3　データローカライゼーション規制対象となるデータ種別内訳



（出典）ITIF “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?”（2017年）

図表1-2-2-4　中国サイバーセキュリティ法　第37条

重要情報インフラストラクチャーの運営者が中華人民共和国の国内での運営において収集、発生させた個人情報及び重要データは、国内で保存しなければならない。業務の必要性により、国外に対し確かに提供する必要のある場合には、国のネットワーク安全情報化機関が国務院の関係機関と共同して制定する弁法に従い安全評価を行わなければならない。法律及び行政法規に別段の定めのある場合には、当該定めに基づいて行う。

（出典）JETROホームページ

条文中に現れるそれぞれの用語について、サイバーセキュリティ法本文の中では明確な定義がなされておらず、今後の具体的な法執行や、現在策定が進められる各種の下位規範（日本で言う政省令）やガイドラインによって明らかにされるのを待つ必要があるが、上記①～④のステップを簡略に示すと下記のとおりである（図表1-2-2-5）。

図表1-2-2-5　中国サイバーセキュリティ法　第37条中の用語

①「ネットワーク運営者」	サイバーセキュリティ法中で「ネットワークの所有者、管理者及びネットワークサービスプロバイダ（76条3項）」と定義。多くの企業は何らかのネットワークを運営しているため、大半の企業が含まれると考えられる。
②そのうち「重要情報インフラ運営者」	「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（31条）」
③それが保有する「重要データ」	組織や個人が中国国内で収集・生成したデータで、国家の安全、経済発展、公共の利益に密接に関わるデータを指す。2017年8月に国務院が公表した「重要データ識別ガイド[*12]」案に、全27産業に渡る分野ごとの広範なデータが記載されている。例えば電子情報分野に関しては、「電子情報製品の使用過程での運行、メンテナンス、修理データ」等までもが含まれる。
④その移転の際に必要な「安全評価」	国務院が定める基準に基づき、社内評価チームによるセキュリティ評価を行うことが原則だが、50万人以上の個人情報、エネルギー産業・化学生物・国防軍事産業・健康等の領域のデータ等の場合は主管部門の安全評価が必要となる。

（出典）総務省「我が国のICTの現状に関する調査研究」（2018年）

特に個人情報・パーソナルデータに限られない、産業データを含む「重要データ」の広範な国外移転規制は、IoTビジネス全体に関わる広範なデータローカライゼーション規制として機能しうることが懸念されており、サイバーセキュリティ法の施行後、早くもAppleが中国国内にデータセンターを設置することを発表している。また中国国内でデータセンターを運営するためには、中国資本企業が過半数の株式を保有する形での合弁会社を設立することが必要となるため、2018年1月には、中国でのiCloudサービス運営を中国企業に移行させる計画を発表している[*13]。情報通信のみならず製造業等を含む中国進出企業は、今後の下位規範やガイドラインの策定動向を注視する必要がある。

＊11　JETRO「中華人民共和国網絡安全法」（仮訳）。以降の条文の邦訳は、当該仮訳を用いる。
https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf
＊12　同識別ガイドに関しては、クララオンライン社による以下の邦訳を参照。
https://www.clara.jp/wp-content/uploads/2017/10/20171030_importantdataguidelines_Claraonline.pdf
＊13「アップル、中国での「iCloud」サービス運営を中国企業に移行へ」CNET Japan（2018年1月15日）
https://japan.cnet.com/article/35113131/

イ　国際枠組におけるデータローカライゼーション規制の抑止

中国以外のアジア諸国では、例えばインドネシアは、個人データに対しデータローカライゼーションを規定する非常に厳しいデータ移転制限がある[*14]。特定の業界に対するデータ移転の包括的禁止や特定の処理及びサービス提供を対象としたデータローカライゼーション規制を議論する対象国が増加している[*15]。韓国においても、詳細地図情報の国外持ち出しを禁止する法制度の存在により、Google Maps等のサービスが韓国国内では他国同様に展開することができない。データローカライゼーション規制を設ける目的は国や分野により様々だが、①自国内の産業保護、②安全保障の確保、③法執行／犯罪捜査などの要素が複雑に関連していることが指摘されている。

広範なデータローカライゼーション規制の拡大は、国際的な電子商取引を拡大していく上での障壁として機能するため、2016年のG7香川・高松情報通信大臣会合での共同宣言[*16]や、環太平洋パートナーシップ協定（TPP：Trans-Pacific Strategic Economic Partnership Agreement）の電子商取引章などにおいて、正統な公共政策上の理由を有さない同種の規制を抑止するための国際協力体制の構築が進められてきている。TPPに関しては、2017年の米国の離脱により一時期は妥結が危ぶまれたが、米国以外の11か国（オーストラリア、ブルネイ、カナダ、チリ、日本、マレーシア、メキシコ、ニュージーランド、ペルー、シンガポール、ベトナム）で2018年3月8日に署名されたTPP11においても、データローカライゼーション規制の抑止を定めた電子商取引章の規定は凍結対象とはされず、署名国の間での国際的なデータ流通確保の基盤となることが期待されている。

さらにASEAN10か国に日本・中国・韓国・オーストラリア・ニュージーランド・インドを加えた広範な経済連携協定である東アジア地域包括的経済連携（RCEP, Regional Comprehensive Economic Partnership）においても、中国のサイバーセキュリティ法を中心としたデジタル保護主義への牽制を視野に入れ、国際的な電子商取引ルールの構築に向けた交渉が進められている（図表1-2-2-6）、（図表1-2-2-7）。

図表1-2-2-6　RCEP加盟国[*17]

（出典）外務省ホームページ

図表1-2-2-7　ASEAN関連首脳会議（2017年11月）におけるRCEP首脳共同声明（仮訳）より[*18]

電子商取引（E-commerce）：E-commerce 章は、参加国間での電子商取引を推進し、世界的に電子商取引のより幅広い利用を促進すると共に、電子商取引のエコシステムの発展に係る、参加国間の協力を強化する。E-commerce 章は、特に中小企業にとって、電子商取引を円滑化する機会を利益あるものとし、また、創出する現代的な協定としてRCEPを位置付けるのに役立つ。

（出典）外務省ホームページ

ウ　EUデジタル単一市場戦略におけるデータローカライゼーション規制への対応

EUに目を転じても、2017年1月に欧州委員会が公表した調査[*19]によれば、EU加盟国の中でも、様々なデータローカライゼーション規制が置かれていることが明らかになっている。このような状況を、欧州全体におけるデータ自由流通拡大の障壁として問題視する欧州委員会は、2017年9月、域内のデータ自由流通を推進するための「非個人データのEU域内自由流通枠組規則」の草案を公表した。

同規則案は、GDPRにおいて定められた個人データ域内自由流通ルールの対象とならない、「非個人データ」全体を対象とした上で、データローカライゼーション規制を「データ保存やその他の処理の場所を特定の加盟国の領土内とするよう義務付けたり、他の加盟国内でのデータ保存やその他の処理を妨げる、加盟国のあらゆる法令又は行政規定（第3条第5項）」と定義する。加盟国は、公共の安全（public security）を理由とした正当化が行われない限り、原則としてデータローカライゼーション規制を設けることはできず、またすでに定められている同種の規制については撤廃を行う必要があるとしている。

＊14 産業構造審議会新産業構造部会資料（2017年4月5日）
＊15 ITIF“Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?”AppendixA“Data Localization Policies Around the world”（2017年5月）
＊16 総務省「G7香川・高松情報通信大臣会合の開催結果」 http://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000083.html
＊17 外務省「東アジア地域包括的経済連携（RCEP）」 http://www.mofa.go.jp/mofaj/gaiko/fta/j-eacepia/index.html
＊18 外務省「東アジア地域包括的経済連携（RCEP）交渉の首脳による共同声明」 http://www.mofa.go.jp/mofaj/files/000307670.pdf
＊19 欧州委員会“Facilitating cross border data flow in the Digital Single Market”（2017年1月）
https://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market

ただし同規則が直接推進しようとするのは、あくまでEU域内であり、EU域外との関係性については何も言及しておらず、我が国とのデータ自由流通枠組の構築に関しては、日欧間の経済連携協定であるEPA（Economic Partnership Agreement）において検討が進められている。2017年12月の交渉妥結においては、EPAの発効後3年以内に、「自由なデータ流通」に関する条項を含める必要性を再評価することを規定することが合意された[*20]。

3 オンライン・プラットフォームとデータ流通

ア　EUデジタル単一市場戦略とオンライン・プラットフォーム

オンラインプラットフォーム（以下、OP）は、ネット広告、ネット市場、検索エンジン、SNS、アプリ市場、決済システムなど、広範なネット上の活動の基盤を指す。個人情報を含む様々なデータの流通や活用においては、国際的に高いシェアを持つプラットフォーム企業が大きな影響力を有する。GoogleやFacebookに代表される国際的なプラットフォーム企業は、データ関連サービスを生み出すための重要な基盤としての役割を果たしているが、その影響力の巨大さがゆえに、データ活用サービスの競争環境への影響に対する懸念を生み、前項で紹介したとおり、我が国においても公正取引委員会などにおいて、適正なデータ流通を実現する競争環境の整備に向けた検討が進められてきている。

EUでは、2015年5月に開始されたEU全体のデジタルサービス市場の統合を目指したデジタル単一市場戦略枠組[*21]の中で、2016年5月に「オンライン・プラットフォームとデジタル単一市場：欧州にとっての機会と挑戦[*22]」と題するコミュニケーション（以下、OP政策文書）を公表し、EUにおけるOPの健全な発展を促すための総合的な政策枠組を提示している。

図表1-2-2-8　OP政策文書の主要指針

- EU全域における可能な限りのルールの一本化
- 消費者保護とエンフォースメントの強化
- イノベーションに親和的な簡素・柔軟な規制枠組
- 原則ベースの自主規制・共同規制による実現

（出典）総務省「我が国のICTの現状に関する調査研究」（2018年）

OP政策文書では、「同等なデジタルサービスの公平な競争条件」「オンライン・プラットフォームによる責任ある行動」「信頼や透明性の増大と公正性の確保」「データ駆動型経済成長のためのオープンで非差別な市場」4つの原則に基づき、OPに関わる各種の規制枠組を現代の情報環境に適合した形で改革していくことを示しており、対象となる法規制はEUの情報通信関連法制全体に渡る。OP政策文書に沿う形でここ2年間の間に公表された新規・改正法や制度の案は、以下のとおりである（図表1-2-2-9）。

図表1-2-2-9　OP政策文書における4原則と関連する制度改革方針

原則Ⅰ：同等なデジタルサービスの公平な競争条件
・電子通信プライバシー指令の見直しによるメッセージングサービスのプライバシー保護強化（2017年1月に「電子通信プライバシー規則」案が公表）
原則Ⅱ：オンライン・プラットフォームによる責任ある行動
・視聴覚メディアサービス指令の見直しによるビデオ共有プラットフォームへの規律適用（OP政策文書と同時に「視聴覚メディアサービス指令」改正案が公表） ・電子商取引指令の見直しによるテロリズムやヘイトスピーチへの対応強化（2017年9月に「オンライン・プラットフォームの責任強化に向けたオンライン違法コンテンツへの取組」コミュニケーションが公表） ・著作権関連法制の見直しによる権利侵害対策強化と収益配分の適正化（2016年9月に「デジタル単一市場のための著作権指令」案が公表）
原則Ⅲ：信頼や透明性の増大と公正性の確保
・消費者保護法制の見直しによる国境を越えた安全なサービス利用の拡大（OP政策文書と同時に「消費者保護執行当局間の協力規則」案が公表） ・プラットフォームに関わるBtoB商取引慣行の継続的調査（2018年4月に「オンライン媒介サービスの透明性と公正性に関する規則」案が公表）
原則Ⅳ：データ駆動型経済成長のためのオープンで非差別な市場
・データの自由な流通イニシアティブによるプラットフォーム間のスイッチング促進（2017年9月に「非個人データのEU域内自由流通枠組規則」案が公表）

（出典）総務省「我が国のICTの現状に関する調査研究」（2018年）

＊20 外務省「日EU経済連携協定（EPA）に関するファクトシート（PDF）」を参照。
http://www.mofa.go.jp/mofaj/gaiko/page6_000042.html
＊21 欧州委員会「デジタル単一市場」https://ec.europa.eu/commission/priorities/digital-single-market_en
＊22 欧州委員会“Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe”（2016年5月）
https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe

イ　データ流通に関連の深い制度改革分野

OP政策文書に基づき進められる制度改革の中でも、特にデータ流通に関わりが深いのが、上記「原則Ⅳ：データ駆動型経済成長のためのオープンで非差別な市場」に関して公表された「非個人データのEU域内自由流通枠組規則」案に含まれる、非個人データの自由流通に関わる規律である。同規則案は、GDPRの対象にならない産業データ等の「非個人データ」に関して、先に触れたEU域内のデータ自由流通を阻害する加盟国によるデータローカライゼーション規制の抑止を行うと共に、クラウドサービスに関わるデータのポータビリティ促進を規定している。ここではクラウドサービスに提供したデータを、ユーザー企業が機械可読な形式で自らの手元に取り戻したり、他のクラウドサービスに移植することで、サービス間のスイッチングを容易にするための行動規範の策定を産業界に求めている。当該行動規範自体に法的な拘束力は無いが、2017年末からは欧州委員会の主催により行動規範の策定に向けたステイクホルダー・ミーティングが開催されており、規則の発効後1年間の状況を精査した上で、必要な場合にはより強制力の強い立法手段での対応を行うことも視野に入れられている。

4　サイバーセキュリティに関する国際動向

ア　諸外国のサイバーセキュリティ政策枠組

2017年9月に明らかになった米国Equifax社の個人情報漏えい（1億4,000万人分超）や、同11月の米国Uber社（5,000万人超）をはじめとした、サイバー攻撃による大規模なデータ流出が相次ぐ中、諸外国においてサイバーセキュリティ対策の構築が急がれている。

EUでは、2004年に欧州ネットワーク・情報セキュリティ庁（ENISA）を設立し、EU全体のセキュリティ体制強化を図ってきたが、2016年7月には新たなネットワーク・情報セキュリティ指令を採択している。同指令では、加盟国にコンピューター・セキュリティ・インシデント対応チーム（CSIRT）及びセキュリティ監督機関の設置を求め、各国CSIRT間での情報共有等の協力体制を構築する他、重要サービス（エネルギー、運輸、金融、医療等）やデジタルサービス（オンラインマーケットプレイス、検索エンジン、クラウドコンピューティングサービス）提供者に対して適切なセキュリティ施策を求めると共に、セキュリティ上の脅威があった場合の当局への報告を求めている。同指令は2018年5月が国内法対応期限とされており、指令の適用対象となるサービス提供者には、EU域内に本社を置かない企業も含まれるため、日本企業としても各国法に基づく対応を要する可能性がある。

イ　個人情報漏えい通知義務

サイバー攻撃等発生時の被害を最小限にとどめるため、個人情報漏えいが生じた場合の当局への報告や本人への通知義務を課す国が増加しつつある。EUのGDPR第33-34条では、個人情報漏えいが生じた場合、データ管理者はその判明後72時間以内にデータ保護当局に報告を行う義務が導入されており、当該漏えいによって生じうるリスクが高いと見込まれる場合には、個人情報の本人に対しても通知を行わなければならない。72時間以内の報告を確実に行うためには、経営陣を含めた危機管理体制の整備を行う必要があると共に、日本企業にとっては、漏えいデータにEU市民の個人情報が含まれるか否かの確認を行った上で、必要があればEUの当局に報告を行う必要が生じる可能性がある。

また米国では、個人情報漏えい通知に関しては、金融や医療等分野ごとの連邦法の他、州法ごとの規律がなされており、少なくとも48の州が法規制を有している[*23]。またEquifax社の大規模な個人情報漏えい等を受け、2018年に入ってからは、包括的な個人情報漏えい通知義務を定めた、新たな連邦法の制定に向けた作業が進められている[*24]。

ウ　Facebook社の個人情報漏えい

そのような中、2018年3月、SNS世界最大手のFacebook社から、選挙コンサルティング会社である英ケンブリッジ・アナリティカ社が大量の個人情報を不正に取得していたことが明らかになった。ケンブリッジ大学の研究者が学術目的調査を装ってFacebook上で提供していた性格診断アプリから取得したデータが、利用規約に反してケンブリッジ・アナリティカ社に渡されていたものであり、不正に取得された個人情報は8,700万人分以上にも

＊23 米国各州の法整備状況につき、以下を参照。Foley and Lardner LLP“State Data Breach Notification Laws”（2018年1月）
https://www.foley.com/state-data-breach-notification-laws/
＊24 “Data breach notification: Congress urged to pass law” Clarion Ledger,（2018年2月）
https://www.clarionledger.com/story/news/2018/02/18/retailers-ask-congress-data-breach-notification-law/347259002/

及ぶ。ケンブリッジ・アナリティカ社は、それら膨大な個人情報を分析し、同社が支援する選挙運動に利用しており、2016年のアメリカ大統領選挙や、同年の英国EU離脱国民投票にも多大な影響を与えたとされる。

この事件は、米国・EUをはじめとする世界各国に大きな衝撃を与え、2018年4月には最高経営責任者のマーク・ザッカーバーグ氏が米国議会で証言を行ない、経緯の詳細な説明を行った他、第三者が提供するアプリケーションからの情報アクセス管理強化をはじめとしたプライバシー保護措置を実施することを約束している。プラットフォームから収集される個人情報の不正な利用が民主主義のあり方にも影響を与えた事態を受け、これまでオンラインの個人情報保護や巨大プラットフォーム企業の活動に関して産業界の自主的な規制を重視する姿勢を採ってきた米国においても、議会やマスメディア等において本格的な規制強化の議論が拡大してきている。

5　PDS・情報銀行・データポータビリティに関わる国際動向

ア　本人関与の元でのデータ活用促進

前項で紹介したように、我が国においては、2016年12月に公布・施行された官民データ活用推進基本法に関連して、情報銀行やデータポータビリティなど、個人の関与の下での多様な主体による適正なデータ活用に向けた環境整備が進められている。諸外国においても、米国のエネルギー分野のグリーンボタンや医療分野のブルーボタン、英国のマイデータ（midata）イニシアティブに基づくエネルギー・モバイル・金融・小売データ分野の取組をはじめとして、様々な主体が保有するデータを再利用しやすい電子的な形式で本人に還元し、第三者のアプリケーションでの活用を可能とするなど、本人関与の元でのデータ活用を推進する施策が進められてきた。

特にEUでは、2018年5月から適用が開始された先述のGDPR第20条において、個人情報を対象とした「データポータビリティの権利」が定められ、個人は一定の要件下で、①再利用しやすい機械可読な形式で自らの個人情報を受け取ること、そして②技術的に可能な場合には、別の企業等に対して直接その個人情報を提供することを求めることができることとされた。データポータビリティの権利は、本人による自らのデータへのコントロール能力を強化すると共に、本人自らが望んだ形でのデータ活用サービスの恩恵を受けられる環境を作るために導入されたものである。

EU各国ではデータポータビリティの権利を円滑に実現するための施策が進められており、例えばフランス政府の支援を受けたFing財団では、個人が自らの個人情報を集積・管理し自らが指定した第三者に提供する基盤となるパーソナルクラウドの構築や、様々なウェブサービスから自らの個人情報をダウンロードしたり、別のサービスに移転することを可能とするための共通仕様（レインボーボタン）の策定に取り組んでいる。

イ　分野ごとの環境整備に向けた取組

EUでは、PDS・情報銀行・データポータビリティに関連する施策は、個人情報全般を対象としたGDPRの他にも、分野ごとの法制化が進められている。EUで2015年に成立した改正決済サービス指令（PSD2：Payment Service Directive 2）は、域内の銀行や電子マネー事業者等に対して、免許・登録やセキュリティなどの要件を満たした決済指図伝達サービス提供者（PISP：Payment Initiation Service Provider）及び口座情報サービス提供者（AISP：Account Information Service Provider）と呼ばれる第三者サービスとのAPI接続を義務付けている。PISPは利用者の依頼により金融機関の決済口座に決済情報を伝達するサービスである。AISPは様々な金融機関に分散する利用者の決済情報を集約するサービスであり、データ分析に基づく家計アドバイスなどを提供することが多い。AISPは、データポータビリティに基づくPDS・情報銀行サービスの、金融分野における先行的取組であるといえる。

IoTの拡大に伴い重要性を増す、様々なデバイスから収集されるデータのポータビリティ確保に関わる取組も進められている。特に通信モジュールが搭載されたコネクテッドカーから収集されるテレマティクスデータは、運転者に対する情報提供サービスや、運転行動を保険料に反映させるテレマティクス保険をはじめとして、様々な活用が進められている。EUの自動車業界では、GDPRのデータポータビリティ権に対応するため、国際自動車連盟欧州・アフリカ支部が中心となり、テレマティクスデータの本人還元や、メーカー間・第三者提供サービス間のデータ移転を可能とするための検討を進めている*25。また2018年2月には、欧州議会運輸委員会において、「協調的インテリジェント運輸システムに向けた欧州戦略」の一環として、本人の求めに応じたテレマティクスデータの第三者サービスによるリアルタイムアクセスを可能とし、プライバシーやセキュリティに配慮した上での活用を可能と

*25 “My Car My Data: EU data protection rules mean drivers control who accesses their car data” FIA Region I,（2017年8月）
http://www.fiaregion1.com/my-car-my-data-eu-data-protection-rules-mean-drivers-control-who-accesses-their-car-data/

するための新たな立法に向けた決議が可決された[*26]。

＊26 “Report on a European strategy on Cooperative Intelligent Transport Systems”（2018年）
http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2018-0036&format=XML&language=EN