2022 年 2 月 28 日

経済産業省

# データの越境移転に関する研究会

# 報告書

# 目次

## はじめに

個人や企業が生成したデータが共有されることで、新たな経済的価値が創出され、社会問題等に対する画期的な解決を生み出す経済社会がグローバルに発展しつつある。ビッグデータは世界経済のあらゆる部門において不可欠なインフラであるとともに、人工知能などの革新的な技術革新を牽引する資源でもある。このようなデータが生み出す経済的・社会的な価値を最大限に引き出すためには、国境を越えた自由なデータフローの確保が重要である。一方で、データローカライゼーションと一般的に呼ばれる・データの国内保存・国内保管義務やその他の越境移転の制限、ガバメントアクセス、データ主権など、領域内で生成・保存されるデータに対する領域国のコントロールを強化する動きが国際的に広がり始めている。

このような動きに対し、これまでは経済価値の源泉をデータに求める経済システム（「データ資本主義」）の視点から、いわば 20 世紀における「石油」のように、データという「財」を巡る国際競争が熾烈化しているとの認識が支配的であった。この視座からは、データの自由流通に向けた国際通商ルールの整備が既に始まっている。他方で、データ・情報は、経済的な価値を持つとはいえ、物品やサービスとは根本的に性質が異なり、更に近年はデータの持つ公共財的な性質を強調する考え方も広がりつつある。データは扱われる用途や文脈によって、多様かつ重複した分類が可能であり、ライフサイクルあるいはバリューチェーンの中で構造化や断片化あるいは統合などによって変化していく。またデータは非競合的（non-rivalrous）であり複製が容易である。もちろんデータへのアクセスを制限することで一定の排除可能性（excludability）を付することは可能であるが、データの種類・利用法によっては、個人の人格的尊厳や国家安全保障に対する重大な脅威につながるものもある。さらに、データの「越境」を観念するに当たっても、データが別地域のサーバーに複製される場合や、国境を超えてデータにアクセスする場合など様々なパターンが想定される。このパターンは、技術の発展や新しいビジネスモデルに伴い増え続けており、これら全てを包有する概念として「データの越境移転（国際データフロー）」が認識されている。

日本政府は、データの越境移転が生み出す経済的・社会的価値や効用を広く世界に分配し、健全な世界経済と社会の発展を促進していくために何が必要なのか、という原点に立ち戻り、データの自由流通を成立させる基盤としての「信頼」に基づく自由な国際データフローのビジョン「Data Free Flow with Trust（DFFT）」を提唱した。いかにデータの共有がもたらす経済的・社会的な利益や効用が明らかであったとしても、個人情報の保護やセキュリティ保全など、データを越境移転することに対する「信頼」がなければ、データは国際的に流れていかない。そして、この「信頼」の確保のためには、価値や概念の共有のみならず、データを越境移転する際に必要な「信頼」を担保する具体的な仕組みや制度を国際的に作っていく必要がある。

これまで日本政府は、国際通商ルールの整備や二国間の円滑な個人データ移転を図るための相互認証や対話を通して、データの越境移転における「信頼」を担保してきた。例えば、日米デジタル貿易協定及び日英 EPA(Japan-UK Comprehensive Economic Partnership Agreement) といった

二国間協定や、CPTPP(Comprehensive and Progressive Agreement for Trans - Pacific Partnership) 及び RCEP(Regional Comprehensive Economic Partnership Agreement)といった多国間協定において、データの自由な越境移転を含め、電子商取引に関するルールを実現してきた。DFFTを具体化する通商協定は、各国に一定の政策余地を残しながらデータの自由な越境移転を可能とするため、幅広い国々の参加が可能であり、引き続き、日本が共同議長を務めるWTO(World Trade Organization) での電子商取引交渉等を通じ、その拡大を追求する。また日本はEUと英国との間で円滑な個人データ移転を図るための相互認証を行っている。

さらに、通商協定以外にも、DFFTが希求するような信頼を確保していくために、国際社会は様々な取り組みを行っている。例えばOECDでは、プライバシーガイドラインのレビュープロセスにおいて、政府による民間企業が保有する個人情報へのアクセスに関する共通原則策定に向けて議論が進んでいるほか、デジタル貿易に関する各国国内規制や国際枠組みなどの政策オプションを整理するインベントリプロジェクト[1]が進行している。また2021年のG7デジタル・技術閣僚会合では、DFFT ロードマップ[2]を策定し、①データローカライゼーションの影響評価、②越境データ移転に関する各国政策の比較分析、③信頼性のあるガバメントアクセスのための指針策定、④データの相互共有の促進、の4つの分野横断的な領域における行動計画を定めたところである。

いわゆるデータローカライゼーションやガバメントアクセスについては、様々な機関や国際フォーラムでその許容されるべき範囲について検討が進んでいるものの、セキュリティなどを理由とした措置は各国それぞれ斟酌するべき事情も多く、正当な合意にたどり着くためには長い時間がかかる。また既存の検討事項以外にも、データの越境移転については残された課題も多い。既存の取り組みを踏まえ、まずは基本的な価値観を共有する国の共通理解の下で、各国のデータ関連制度に関して詳細な制度間比較を通じたデータ越境移転制度の構築が可能であれば、DFFTのメリットをより強く示すことができる。DFFTを提唱した我が国は、既存の国際社会の取り組みと連携し、各国の固有の事情を踏まえながら、データの越境移転に必要な主体間の「信頼」を確保する枠組みや制度、その他の政策措置の内容を検討し、G7などの国際的な場での提案を通して、DFFTの具体化を推進していく。このため、経済産業省は、2021年11月に有識者や企業関係者等で構成されるデータの越境移転に関する研究会（以下、「DFFT研究会」）を立ち上げた。

DFFTを具体化していく上で、DFFT研究会が最初に取り組んだ課題は、データの国際的なフローを促進する政策的措置の前提として、そもそもデータが「どこ」を「誰」の手を経て旅していくのかという「ライフサイクル」に関する知見が、個社レベルや個別の産業部門を超えてあまり共有されておらず、したがってDFFTについて議論をするときに、現実のビジネスの現場で「データが流れない」具体的な状況を想定した議論があまりなされてこなかったことである。

---

[1] OECD Trade Policy Paper - Mapping commonalities in regulatory approaches to cross-border data transfers

[2] G7 Digital and Technology Ministerial Declaration Annex2- Roadmap for cooperation on data free flow with trust

データは物理媒体やサイバー空間を行き来しながら、生成、加工、複製、保存、集約、分析などの様々な過程（ライフサイクル）を経て利用されていくが、その各過程には様々な主体が関わり、各過程におけるデータのマネジメントや意思決定は、そこに関与する主体自身の条件（経営資源、知識など）と主体が置かれた「場」の条件（規制など）によって定義されていく。データの越境移転は、このライフサイクルの一部として発生する。この視座から、本報告書では、企業が流したいデータのライフサイクル、発生する越境移転の様々な状況、そして、各国の規制がデータのマネジメントや意思決定に与える影響について調査を行った。その結果、各国法制度の違いや、規定の明確性、相互性の粒度といった観点で残された問題は多く、依然として企業がデータの越境移転を行う上で、ビジネスにおける意思決定の自由度を著しく下げる、あるいは萎縮的な効果を与える障壁が大きいことが明らかになった。また、多数国間で自由なデータの越境移転を確保していくために、異なる規制当局間やデータ利用主体等のステークホルダー間における「信頼」を担保する仕組み作りが必要であることも浮き彫りになった。

- 企業は、データの越境移転にかかる要件の不透明性や予見可能性の欠如、各国法令の下で求められる安全基準を履行する上で、取引先である第三国企業のデータガバナンスやセキュリティ体制に関する共通基準の不備や認識の相違などの問題によって、多大な調整コストを払う必要があるという問題に直面している。
- データに関する規制権限は多くの国で複数の機関に分散しているが、個別分野の規制当局がデジタル経済の複雑な構造を必ずしも理解しているわけではない。当局間や業界間で情報が分断される「サイロ化」の問題が散見され、その結果として規制の重複や、複数の法令間でデータローカライゼーションや法定手続の要件が極めて分かりにくくなるなどの現象が発生している。
- データ主体である個人と企業の関係性についても、個人が自身に関わる情報の収集や利用において、相互的な「信頼」を担保するべきであるという考え方が主流になりつつある。日本政府はSociety 5.0の中でデータに関する「人間中心（human centric)」アプローチを推進しているが、これは越境移転における「信頼」確保に対する考え方に通底する。特に越境移転が含まれるデータのライフライサイクルに関する体系的な情報は限られており、これは「信頼」を担保する上での大きな障壁となる。

本報告書では、まず第1章で国際的なデータの利活用の実態と、データのライフサイクルにおける具体的な越境移転の状況を類型化し、現在あるいは潜在的に生じ得る障壁を特定する。第2章では、各国におけるデータの越境移転に制限的効果を持つ法令を概説する。第3章では、データの越境移転を実現するための、「信頼」を担保する仕組みについて、今後の方向性や残された課題を考察する。

# 第１章　データのライフサイクルと越境移転における障壁

第１章では、「データの越境移転」という用語で指し示される多種多様な実態が、どのようなデータを対象に、どのような行為によって構成されているのかを具体的に把握し、データのライフサイクルの中で、企業などのデータ利活用を行う主体がどのような障壁に直面しているのかを整理する。

そのために、越境移転の実態を把握する上で、本報告書では「データ・マネジメント・フレームワーク（仮）」[3]の考え方を下敷きにして、データがどのような過程を経て企業等に利活用されているのかを、データの生成を起点とするライフサイクルとして把握し、各過程における関係する主体、データの所在、越境移転と観念し得る移動などを調査した。本報告書では、データの越境移転がビジネスモデルの前提となる、あるいは今後そうなることが明確な企業にヒアリング調査を行い、集めた事例を6つの類型に分類している。ヒアリングを行ったのは、主にアプリケーション・サービスに関わる企業、Infrastructure as a Service （IaaS）などミドルウェアを提供する企業、オンライン・プラットフォームを提供する企業、IoTの利活用がビジネスモデルに組み込まれている企業、セキュリティなどネットワークの脅威に関わる情報を扱う企業である。これらの企業の選定は、個人情報、セキュリティ関連情報、そしてその他の非個人情報の越境移転を網羅すること、データの利活用につき代表的なビジネスモデルであるという観点から選択された。類型化においては、特に企業の多様なニーズを拾う観点から、ビジネスモデルの代表例を選定したもの（類型1、3、4、5）、代表的なビジネスモデルで扱われないセキュリティ情報を主に扱う事例（類型6）、そして越境移転が第三者企業との間に発生する事例（類型2）を選び、本報告書で取り上げている。調査において分析の視座となる、データのライフサイクルの「イベント」には大きく分けて、生成、加工、利用、保管、廃棄などがありうる。これらはそれぞれ重複する性質を持つ場合があり、事例に応じて適切に「イベント」を捉え、データの越境移転の状況を可視化していく必要があるため、事例によってイベントの定義は変わりうる。現に存在する各国の規制によって、データの越境移転に関する経営上の選択は変化していくが、本報告書では、特に遵守のコストや市場の状況に即したビジネスモデルの構築などに関し、個社レベルでは対応が困難といえる事例を集めている。

本章はデータの越境移転に関する障壁を包括的に指し示すものではなく、あくまで代表的な事例におけるデータのライフサイクルと企業が直面している障壁の性質を明確にすることで、今後の更なる議論を喚起するものである。

---

[3] 経済産業省が提唱する、データを軸として、データの生成・取得から廃棄に至るライフサイクル全体を視野に入れたデータマネジメントの在り方に関する枠組み。

## １．類型１：オンラインアプリ企業の商品開発におけるデータの利活用

### （１） 概要

顧客の基本データと当該顧客のアプリ利用実績から、顧客のタイプごとに利用傾向などを分析し、公的データなどの外部から入手したデータと組み合わせ、アプリの改善や新規サービスの開発に利用する。また第三国の企業からデータ提供を受けることもある。

商品開発に関連して収集されるデータには、大きく分けて利用登録時に提供されるデータ（顧客の属性：性別、年齢、居住地域など）、顧客のアプリの利用から生成されるデータ（アクセス頻度、選択される情報の傾向など）がある。個人情報などの越境移転について、厳しい条件を課している国・地域に対する対応や規制の違い・フラグメンテーション（細分化）の拡大などの理由から、一旦各市場の商用クラウドにデータを保存し、データを「リージョン」（データセンターが設置されているエリア単位）内である程度構造化・統合した上で、開発拠点がある国のクラウドに移転するとの回答が多かった。またエンジニアを始め人材採用をグローバルに行い、分析や開発にかかる作業や社内の打ち合わせを完全にオンライン化している企業も多く、このような社内の「越境アクセス」について各国法令との関係を懸念する声が上がっている。一方で、ユーザーエクスペリエンス向上のために必要なデータは、リージョンあるいは国毎に管理するほうが望ましいと回答する企業もあった。

データの管理については、特にアプリ提供会社は中小企業やスタートアップが多いことから、ほぼ全ての社から、市場ごとにサーバーを設置し、個人情報を除去するなど情報を加工するプロセスを配置することはコストの観点から非常に難しいとの回答があった。またセキュリティの観点からミラーサーバーへのバックアップは必須であるが、越境移転に関する条件が厳しくなることで、日常的なバックアップが困難になることを懸念する意見もあった。更にサーバー拠点の数を限定する場合、世界中に散らばっているエンジニアがサーバーにアクセスすることが必要になるが、これが越境移転に当たるのか、など法的不透明性を懸念点として上げる企業もあった。各国で、個人情報のみならず、セキュリティなどの観点から多様なデータを対象とした規制が導入されつつあるため、新たな地域への事業拡張や臨機応変なデータ・情報の統合・分割を行うための法令遵守やリスクマネジメントにかかるコストが増大しており、ビジネスモデルを構築していく上での障壁になっているとの声もあった。（一部の社は、法的不透明性が極めて高い国からのアクセスは完全に遮断していると回答）。

### （２） データのライフサイクルにおける越境移転の状況

#### ⅰ. データの生成・取得

A）　データの状況：

- **顧客のアプリ利用に関して、データが発生する。**顧客の属性を示すデータと、利用により生成されるデータが主なデータである。

B)　企業の要望：

- 開発拠点や本社のクラウドに直接送信するか、社のリソースに合わせて地域ごとにあるクラウドに集約管理するなど、市場環境を踏まえて柔軟な対応をしたい。

C)　企業から見た課題：

× 「個人情報」や「重要情報」など、国によってデータを域外に持ち出す上で様々な要件が定められている。事前の個人同意や標準契約条項（Standard Contractual Clauses、以下、「SCC」）などの当事者間の契約条項によりで定型的に対応可能であれば、アプリ自体に許諾などの処理を組み込むこともできるが、現実には同意の要件が用途ごとに細かく異なる上、ガイドラインなどが次々制定されることから、解釈の余地が大きい。またアプリ連携など第三者提供が含まれる場合は、第三国にいる相手方企業に対して、データ移転元国（データオリジン）の法令準拠を求められることも多く、対応に苦慮している。

× 法令が国ごとに大きく異なるようになると、現状のままでは１国１拠点が必要になり、越境させる前にデータを加工し、個人特定性がない形にするなどの体制を組まなければいけなくなる。新しいアイデアを持ったスタートアップや中小企業の参入障壁が高すぎる。

### ii. データの加工[4]

A) データの状況：

・ **データを加工する。**作業の効率化や法令遵守などの観点から、データを越境させる前にデータをエンジニアが処理する。

B) 企業の要望：

- 開発拠点や本社のクラウドに直接送信するか、社のリソースに合わせて地域ごとにあるクラウドに集約管理するなど、市場環境を踏まえて柔軟な対応をしたい。

C) 企業から見た課題：

× データを加工する際に「個人情報」を切り分けるが、そもそもの定義や要件が法令本体ではなくガイドラインや申し合わせをも読まなければ理解できない建て付けであることが多く、解釈が困難である。

× どこまで抽象化すれば「個人情報」でなくなるのか。収集するデータが増えるに従い、「個

---

[4] データの加工には大きく分けて、以下の３つがある。
① 構造化：収集の時点である程度構造化されているデータもあるが、情報の検索履歴などは、パラメーター（例:性別、年齢、居住地域、職業など）に従い構造化する。サービスによって、顧客関連データと公的データを組み合わせることもあるが、日本の場合は、様式や前提などが機関ごとに異なることから、データを収集した時点では非構造化データとして扱い、各社のパラメーターに従い構造化する（公的データがある程度標準化されていないと、利用者側に非常に大きなコストとなる）。
② 統合：構造化されたデータは、用途によって、組み合わせ・統合。
③ 切り分け：各国の法令によっては、個人情報（個人特定性のある情報）にならないように切り分けをして越境する。

人情報」に該当するか否か微妙なケースが増えてきている。

× 商品開発や加工の用途に応じて、国境を超えて複数リージョン間のデータの統合を行う場合、あるいは国境を越えてデータのアクセスを行う場合、それが「越境移転」に当たる可能性があるのか不明。したがって、安全をとった予防的措置を執らざるをえない。
  - 日本の個人情報保護法との関係では、中国子会社から日本国内に保存するデータへのアクセスは遮断しているが、これも明確に法令で求められているというよりは、予防的措置である。

### iii. データの移転

A) データの状況：

・ **データを開発拠点に集約する。**開発チームがいる地域のクラウドにデータを移転するか、開発チームが利用可能な環境に、加工したデータを保存する。

B) 企業の要望：

- 商品・サービス向上や開発については、集約することに意味がある。分析・開発リソースの位置によってデータの越境移転（データの移動）が発生する。物理的に距離がある場所からアクセスするのは、情報通信のコスト（通信のスピードやセキュリティコストなど）、開発がいる地域のクラウドにデータを移したい。
- 現時点で提供しているサービス（ニュースアプリやフリマアプリ、ゲームアプリなど）では、個人情報が必要なユーザーエクスペリエンスに関わる情報はリージョンあるいはローカルのクラウドに保存している。提供する/したいサービスによって、開発に「個人特定性」がある情報が、必要か否かが決まってくる。

C) 企業から見た課題：

× 各国の個人情報保護法制において、何をもって「個人特定性」がないといえるのかわかりにくい。しかし匿名化し、さらに統合して「情報化」されたものであっても、重要情報として規制対象となる可能性もある。

× 第三国の企業から情報提供を受ける際に、データオリジンの法令遵守にかかる様々な要件を契約上求められることがある。この対応が非常に煩雑であり、かつ現地法令を確認しようにも英語で利用可能な条文や資料が限られていることもある。

× 複数リージョンをまたいでデータ収集・管理・統合をしてビッグデータの恩恵を受けようと思っていても、現状は法令の違いや法令解釈の不透明性・情報不足などの問題で、それらに対処するリソースがなく踏み出せていない。
  - データを移動させる場合（A 国/B 国から集めた情報をさらに C 国にいるエンジニアがアクセスする場合、あるいは D 国エリアのクラウドに移動させる場合など）、現在は関係国の法令に関して、言語の壁や条文の曖昧さなどによって、適法な越境移転の条件を把握しきれない。

## ２．類型２：収集したデータを業務委託のために海外の第三国企業に移転

### （１） 概要

この類型のデータ越境移転については、具体的なビジネス事例を用いて、データのライフサイクルと障壁について概説する。

当該企業は、モバイルペイメントサービスとオンラインブッキングプラットフォームサービスを提供する。海外のクラウドを利用してサービス提供しているが、一部業務を海外企業に委託（共同利用含む）している。社の規模は大企業で、グローバルに事業を展開している。

取り扱う情報のうち、特に法令との関係で取扱いに注意が必要であるのが、個人情報に関わるもので、利用登録時に提供されるデータ（顧客の属性、すなわち性別、年齢、居住地域など）、顧客のサービスの利用から生成されるデータがある。データの利用方法は、ユーザーエクスペリエンスの向上、サービス改善・開発、及び支払いアプリの連携による他社アプリ・サービスとの連携が主な用途。ユーザーエクスペリエンスの向上などに使われるデータは、クラウドにリージョン毎に収集・保存され、そこで利用・加工される。開発目的で個人情報そのものを集約することは、現時点では殆ど行っていない。海外事業者が委託業務において収集したデータを取扱う場合には、データが収集された地域から別地域のクラウドへ越境移転、あるいは越境アクセスする。

### （２） データのライフサイクルにおける越境移転の状況

#### ｉ．データの生成・取得

A)　データの状況：

- **顧客のアプリ利用に関して、データが発生する。**顧客の属性を示すデータと利用により生成されるデータが主なもの。

B)　企業の要望：

- ユーザーエクスペリエンス向上に関するデータは基本的にはリージョン内で保存し、同地域で加工や分析を行う。ただし、当該企業は多くの業務を海外事業者に委託していることから、越境移転に関する法令制度の不透明性（下記）に直面している。

#### ｉｉ．データの加工

A)　データの状況：

- **データを加工する。**データをリージョン内でエンジニアが処理するが、その際に同地域のエンジニアのチームを編成するのではなく、海外から調達する。

B)　企業の要望：

- 当該企業の業種では、専門性に沿った分業化が進んでおり、ユーザーエクスペリエンスの

観点からデータを地域から動かさなくても、分析などの業務を国際的に委託することが今後増えてくる可能性がある。また優秀なエンジニアの確保は年々難しくなっており、越境アクセスによって作業を行う必要性が増している。

C)　企業から見た課題：

× 「越境移転」の条件が分かりにくい。例えば、域外からデータにアクセスすることは「越境移転」なのか、分からない法令も多い。同じ社内の人間であっても、物理的所在が域外の場合には「越境移転」になるのか。また複数国にまたがってクラウドが存在する場合に、データがクラウドに入った瞬間に「越境移転」になる可能性があるため、少なくも顧客に対しては、事前にシステム上で合意を得るようにしている。

× 「第三国への越境移転」の定義が不明瞭。

### iii. データの移転

A)　データの状況：

・**データを第三国へ越境移転する。**

B)　企業から見た課題：

各国の法令に照らし、「第三国への越境移転」であることが確実な場合にも以下のような問題があり得る。

× 第三国への移転について、主要国の個人情報保護法制では、データの移転先となる者の所在する国（移転先国）において、データオリジンと同等の保護・管理体制を確保することを求めている。しかし、移転先国の法令におけるデータの取扱いや安全管理について、移転先国の法令とデータオリジンの法令の十分性や、GDPR で求められるような取引先企業の管理体制などの調査・確認の責任は企業に課せられている。

- 現実に法の保護水準が同等であるか、移転先企業（他社）でデータが安全に管理されるなど、一企業が「何を基準に」「どう確認したらいいのか」現時点では国際的に合意されたスタンダードがない。
- データの保存場所として、商用クラウドサービスが採用されている場合、安全管理体制について、一企業と取引先が利用しているクラウドベンダー（多くはグローバル企業）の間に個別の契約交渉の余地があることは稀である。

× 規制の範囲に影響のある「委託先」の定義が各国の法令上曖昧であり、自社の体制では「子会社」としている 組織が、当該国の法令では「委託先」になってしまうこともある。

## ３．類型３：IoT を介して海外からリアルタイムにデータを収集・分析（個人情報が明らかに含まれない場合）

### （１） 概要

グローバルに販売した機器等について、IoT プラットフォームを活用し、稼働状況やそれに付随する稼働環境、修理等に係るデータを海外からリアルタイムに収集・分析することで、故障の発生予測やそれを元にメンテナンス計画の最適化などを行う。

ほとんどの企業が、現時点では機器のセンサーから集約したデータは、現地の事業者ないし代理店のサーバーに保存（現地のリージョンクラウドかオンプレミスに取得・保存）している。顧客データも含めて、代理店が管理していることが多く、その場合はデータを本社に移転させる整理になっていない。今後 IoT 経由で収集したデータを活用していく際の分析は本社で行うことを想定していることから、代理店との契約関係などの見直した上で、データは本社所在地にあるクラウドサーバーに保存することを考えている。

IoT データは、収集された時点では、テキストメッセージや音声データなど加工が必要なものから、重量やスピード、温度などの定量情報など多岐にわたるが、個人利用ではない IoT 機器から収集されるデータは「個人情報」を含まない。他方で、法制度によっては、個人情報が含まれない情報であってもセキュリティなどに関わる情報として、越境移転が制限されることがある。

### （２） データのライフサイクルにおける越境移転の状況

#### ⅰ. データの生成・移転

A)　データの状況：

- 販売した機器に備え付けられた**センサーから、データを取得する。**
- **センサー情報を集約する。**

B)　企業の要望：

- ● マーケティング以外の目的で、IoT 機器から得られた情報について地域ごとの差異を分析することはあまりない。製品開発や故障の発生予測やシステム構築など、一ヵ所に集約して分析を行いたい。
- ● 分析などの拠点を本社に置くことを検討しているため、センサーから取得された情報は基本的には個人情報ではないことから、本社所在地にあるサーバーに直接転送したい。

C)　企業から見た課題：

× 「個人情報」以外のデータに関する規制が増え続けており、国によっては個人情報とのリンクが全くない情報（特定の駅の人の流れの情報など）であっても、国内から持ち出すことを禁止する場合があるが、越境できる情報とそうでないものを個別に精査する工程を入れ

ると、IoT の特性であるリアルタイムモニタリングの利点などが損なわれる。

## ４．類型４：IoT を介して海外からリアルタイムにデータを収集・分析（個人情報が含まれ得る場合）

### （１） 概要

グローバルに販売した機器から IoT プラットフォームを活用し、機器のオペレーションやそれに付随する稼働環境（標識などのインフラや、位置情報、人の流れなどカメラなどの多種多様なセンサーから集約される情報）、エネルギー消費、決済にかかる情報、搭載ソフトウェアの稼働状況、修理等に係るデータを海外からリアルタイムに収集・分析することで、顧客のニーズを踏まえた商品システムの提供、故障の発生予測、現地環境への適合などを行う。

この類型で取得される IoT データは、個人所有の機器からの情報収集であり、品質解析などの観点から顧客自身の ID などの個人情報を含み得る。また機器の稼働環境に関する情報は、機器の種類によっては、収集できるデータが多種多様（標識・インフラなどの写真・映像、位置情報、事故・ヒヤリハット情報、道路情報、渋滞情報、エネルギー消費、気温、人の流れ、決済情報など）であることから、様々な法令によって越境移転の規制対象になり得る。これらの情報は、製品開発や現地の環境適合性を高めるために必要な情報であることから、急に規制が変わる、あるいは解釈が変更になると、一部サービスを停止しなければならなくなるリスクがある。

規制が短期間で不透明な形で変更されることが続くと、情報収集・解析・商品開発までを１国内で実施する圧力となる。しかしグローバルにサービスを展開していく以上、データは複数拠点に置いて常に全世界で同期しておくことで、分析・開発業務やトラブル対応を 24 時間 365 日実施できるようにしておくことが望ましい。

### （２） データのライフサイクルにおける越境移転の状況

#### ⅰ．データの移転（集約）

A)　ライフサイクルの状況：
- 販売した機器に備え付けられた**センサーから、データを取得する。**
- もしくは、**センサー情報を集約する。**

B)　企業の要望：
- 顧客のシステムから拠点のサーバーに直接・自動的に収集した情報を送信できるようにすることが望ましい。
- 現地環境に適応させるための情報収集もあるが、特にビジネスモデルとの関係で重要な情報は、機器の稼働一般にかかる情報（機器・ソフトウェアのエラー、事故・ヒヤリハット、

決済情報、エネルギー消費など）で、データは複数拠点に置いて常に全世界で同期しておくことで、分析・開発業務やトラブル対応を24時間365日実施できるようにしておくことが望ましい。

C)　企業から見た課題：

- × 越境移転規制に対して、個人情報のみならず、「セキュリティ情報」「重要情報」など非個人情報を含む新しいデータ区分が登場しているが、規制対象の範囲が極めて曖昧かつ、申し合わせなどの関連文書によって対象となる情報が急に追加されることが増えている。
- × IoTの特性を生かしたリアルタイムモニタリングを行う上で、越境移転にかかる法令要件の遵守にかかる手続は、ある程度標準化・定型化できることが望ましい。

## ５．類型５：プラットフォームサービス・IaaSの提供

### （１）　概要

企業が提供するクラウドなどのプラットフォーム上で、個人アカウントを作成した顧客に、様々なサービスを提供をする。あるいは顧客が消費者に提供するサービスに必要なネットワークリソースを提供する。サービスの提供において、プラットフォーム上で、必要なデータを顧客やインターネットから収集・蓄積して、分析・管理を行う工程が含まれる。ここで分析されたデータは広告宣伝システム（ターゲティング広告など）などにも用いられることがある。

このビジネスモデルにおいて、最も厳格な個人情報保護法制度であるGDPRの規定をふまえ、データポータビリティの担保の観点などから、個人情報である顧客データや顧客が提供しているネットワーク上に保有するデータは原則として顧客自身が管理していると回答する企業がほぼ100%であった。このような企業では、法令適合性や十分性の確認は、一次的には顧客自身が調査・検討するべきであると整理している。事業目的によっては、個人の顧客に対する事前同意やSCCによるデータの越境移転を行う場合があるが、同意の真正性などの要件は年々厳格になり、また目的ごとに同意が必要である。他方でサービス提供に関連するその他のデータとして、社内のポリシーに従って「非個人データ」として扱われる、「サービス関連データ（提供サービスをどの日時にどれくらいの頻度で使っているかなど）」、「セキュリティ関連データ（サイバーセキュリティなど）」、「サポートサービスデータ（不具合の報告など）」の情報がある。これらの非個人データは、本社か開発拠点がある地域に集約して分析し、サービス向上のために利用される。ただし個人情報保護以外の法制度によって、非個人データに関するコントロールが強める国も増えており、サービス展開の方針決定やデータセンター等のリソース配分の決定における考慮事項は複雑性をますます深めている。

データの管理方法については、セキュリティの観点から分散管理（ミラーリング含む）を行っている、行うことが望ましいと回答する企業が多かった。ただし法令遵守のコストの高さから、顧

客アカウントに紐付く情報は分散管理しない、ビッグデータ化も行わないと回答する企業もいた。他方で、ユーザーエクスペリエンス向上に必要なデータは、ローカルで管理するほうが望ましいと回答する企業もあった。

### （２） データのライフサイクルにおける越境移転の状況

#### ⅰ. データの生成・取得（顧客データ）

A) データの状況：

・ 顧客がアカウントを作成する。**顧客データが発生。**

・ サービス提供にかかる分析のため、顧客データ、その他の個人情報（e.g.顧客の情報 - 過去のクッキー情報、過去の行動・閲覧記録など）の取り込みを行う。

B) 企業の要望：

- ● セキュリティや継続的なサービス提供の観点から、本来は分散管理を行い24時間365日データの同一性と一貫性を維持できるようにすることが最善。
- ● グローバルで対応するにはシンプルな対応が望ましく、定義や分類（タクソノミー）が明確になった制度が望ましい。

C) 企業から見た課題：

× 越境移転が制限されるデータは多岐に渡るが（「個人情報」「重要情報」「セキュリティ情報」など、定義や一般概念がない、定義の不明瞭さから来る不利益が企業に転嫁されている。

× 個人情報の移転にかかる条件は、法令や利用目的ごとに様々であるため、国・地域ごとに異なる利用条件の設定・表示やシステム設計を行わねばならない。

  - 国・地域ごとに多様な規制が導入されつつあり、それぞれ対応するためには、各国の法令を分析するのみならず、それをテクノロジーに反映するエンジニアリングなどの工数がかかるため、ビジネスとして対応できるようになるには相当時間がかかる。
  - 企業によっては、個別対応ではなく、最も厳しい法令（GDPR 又は米国の California Consumer Privacy Act）に基づくグローバル・リスクベースアプローチで対応し、差分に対して設定や条件を適宜拡張する方針をとる場合もある。この場合も現地の法務チームと本社の密な連携が不可欠である一方で、全ての国・地域に法務チームを置けるわけではない。

× 越境移転の条件が非常に複雑であることも多く、サービス提供に際して、顧客に対して多種多様な同意を求めなければならない。顧客からするとサービス利用において許諾を求める大量のポップアップに煩わされる事態が発生している。個人情報保護については、個人の同意の真正性など要件が厳格化される一方であり、個人情報の移転をサービス利用の条件にすることができない場合もある。規制の変化により、データ主体である個人による主体的な関与が求められるが、関与を確保するエンジニアリングコストは、企業の側にある。

× 主要国の法令が、第三国移転において「安全確認」や「十分性確認」の義務を企業に課して

いる。

- どのような条件を満たせば、「安全」なのか、「十分」なのかについて、企業の日々のビジネス実態に寄り添った具体的なガイドラインや定義がない。
- グローバルでリスクベースアプローチをとるのであれば、広く安全保障に関連する「NIST800-171」や「NIST CSF」などの米国政府が出している基準やISO等のグローバルな基準、又はCSマークやISMAPといった地域・特定国の標準も取得することは1つの選択肢だが、このような標準を取得するためには、監査を受けるための社内の技術的な対応準備に加え、監査法人から承認を受けるために莫大な費用が掛かる場合もある。

### ii. データの生成・移転（顧客のサービス利用情報）

A)　データの状況：

・**顧客がサービスを利用することで、サービス関連データやサポート関連データが発生。**このデータは地域ごとの法令における「非個人情報」であるとみなし、越境移転して本社または開発拠点などに集約される。

B)　企業の要望：

- セキュリティや継続的なサービス提供の観点から、本来は分散管理を行い24時間365日データの同一性と一貫性を維持できるようにすることが最善。
- グローバルで対応するにはシンプルな対応が望ましく、定義やタクソノミーが明確になった制度が望ましい。

C)　企業から見た課題：

× 越境移転が制限されるデータは、国・地域ごとに多岐に渡るが（「個人情報」「重要情報」「セキュリティ情報」など）、定義や一般概念がないことも多く、不明瞭さから来る不利益が企業に転嫁されている。

  - 「個人情報」と「非個人情報」の境界線が曖昧な事例や（特にIDとサポート関連情報などがリンクされる場合など）、セキュリティなどの観点から越境移転が制限される情報の範囲は多岐にわたり得る。定義が不明瞭な場合、企業側は安全策として最大限に厳しい解釈に併せて、サービス展開の方針決定やデータセンター等のリソース配分の決定を行わざるを得ない。

### iii. データの生成・移転（セキュリティ関連データ）

A)　データの状況：

・サイバー空間の状況を把握するための**セキュリティ関連データが発生。**このデータは地域ごとの法令に照らし「非個人情報」であると見なされ、越境移転して本社または開発拠点などに集約される。

B)　企業の要望：

- セキュリティや継続的なサービス提供の観点から、本来は分散管理を行い 24 時間 365 日データの同一性と一貫性を維持できるようにすることが最善。
- グローバルで対応するにはシンプルな対応が望ましく、定義やタクソノミーが明確になった制度が望ましい。

C)　企業から見た課題：

× 越境が制限されるデータは、国・地域ごとに多岐に渡るが（「個人情報」「重要情報」「セキュリティ情報」など）、定義や一般概念がないことも多く、不明瞭さから来る不利益が企業に転嫁されている。

## ６．類型６：サイバーセキュリティサービスの提供

### （１） 概要

ハードウェアやスマホなどの機器向けのセキュリティソフトや、クラウド環境のセキュリティ保守・保全の提供などを中心に、サイバー攻撃の探知、対処、予防的な措置をサービスとして提供している。世界中で同様のソフトウェアを使用している全ての顧客に対して、同じシステムでサイバー攻撃に対応する仕組みになっていることから、脅威の分析や対応ソフトウェア開発などのために必要な情報は集約し一元管理をしている。脅威と判定された情報はデータベースに保存され、提供されるソフトウェアに反映する。

取り扱うデータには、顧客や外部機関から提供される情報と自社が独自に収集するセキュリティ関連情報があり、顧客から提供される情報が個人情報を含み得る。開発拠点に送られるデータには、顧客に提供したシステムから直接送信されるケースと、各リージョンで解析して脅威ありと判定された場合に、送信されるケースがある。個人情報については、ある程度社内で決まった運用があり、例えばメールについては、リージョンのある国のエンジニアのみがアクセスし現地で解析する（越境アクセスはない）ようにしているとの回答があった。解析後に送信される脅威情報は、個人情報を除去している。現地の規制で個人情報の取扱いに対しては、特に第三国移転に厳しい要件や複雑な要件を課している国（日本、EU 加盟国、インド、カナダなど）があるが、そのような国に対しては、リージョンに設置しているサーバーに情報を集約し、個人情報を含まないように処理した上で、脅威情報を開発拠点のある国のサーバーへ送信する必要があるとの回答が多かった。このような企業では、規制があまり厳しくない国では、顧客のシステムから開発拠点のある国のサーバーに直接送信されるが、国・地域の法令にかかわらず、一般的に顧客の同意を得た（システム上はチェックを入れた）上で、送信している。

効率性を考えると、情報は常に一ヵ所に集約する方が望ましいが、万が一のサイバー攻撃や事故に備え、事業継続性の観点から最低二ヵ所程度に分散管理し、常に情報が同期されることも必要

である。他方で情報を全てのリージョンごとに精査し分析することは、設備投資等のコストがかかる。現時点では、各リージョンの状況について報告・アップデートミーティングを行い、各国制度の差分をマトリックスに整理し、毎回更新している。サーバーの設置場所についても常時検討を行っている。

### （２） データのライフサイクルにおける越境移転の状況

#### ⅰ. データの移転

A)　データの状況：

- ・ 顧客のシステム・クラウドから、**脅威関連情報が開発拠点のサーバーに直接送信される。**
- ・ 各リージョンで情報を収集・分析・加工し、**開発拠点に脅威関連情報を送信する。**

B)　企業の要望：

- ● 顧客のシステムから開発拠点のサーバーに直接・自動的に脅威関連情報を送信できるようにすることが望ましい。

C)　企業から見た課題：

- × 個人情報に関する法令は国ごとに大きく異なり、かつ移転の要件が利用目的ごとに細かく分かれている場合もある。そもそもの要件の中身が、法令本体だけでなく、ガイドラインや申し合わせを合わせて読まなければ理解できない建て付けになっており、解釈が困難であることが多い。
  - － 外国にある第三者への移転における「第三者」の定義について、子会社であっても外部委託扱いとなり「安全管理義務」がかかり得る。
  - － 「安全管理義務」における担保するべき安全の基準が不明瞭であり、これが個別企業のリスクで解釈を行うことになっている。
  - － 個人情報の定義に関わる「容易照合性」や「個人特定性」の条件が不明瞭で、結局のところ、どの範囲までの情報が容易照合性や個人特定性があるものとして扱われるのか分かりにくい。
- × 法令上の要件が厳しい・不明瞭な国については、リージョンごとに情報を一旦集約して、個人情報を適宜除去した上で脅威情報を送信することにしているが、設備投資や人件費といったコストがかかる。
- × グローバルにデータの取扱いに関する法令の情報を収集・分析をした上で、各国制度の差分を整理しているが、英語で利用可能な法令情報が限られる国も多い。
- × 法令の条文ではなく、ガイドラインや申し合わせなどに具体的なルールが落ちているなど、当地の法文化を反映したガバナンスの違いや、セキュリティ関連情報の取扱いに関してISOなどのグローバルな規定のみならず、地域・国で発行する特定の認証の取得を要求されることもある。認証規格同士は重複する内容もあるが、地域・国ごとに求められる認証規格は全て取得しなければならないため、対応する際のコストが多大である。

# 第２章　各国データ関連規制の現状

第 2 章では、日本企業にとって対応が必要となる可能性が比較的高い、越境移転に制限的効果を持つ法令についての現状を整理するべく、各国における背景事情を可能な限り踏まえつつ、規律の概説を行う。具体的には、各国のデータ関連規制を中心とした主要な法令のうち、越境移転そのものに制約を課す規律に加え、データの自由な越境移転に影響を与える国内保存・国内保管義務を定める規律についても紹介する。本報告書において紹介する国・地域は、経済産業省が 2021 年に実施した企業アンケート[5]において「制度への対応で重視すべき国・地域」としてニーズが高かったものからピックアップしている。なお、本章においては、全体として、2021 年末の情報を整理している。

## １．EU

### （１） 対象となる法令

EU 全体としては、2018 年 5 月 25 日に施行された General Data Protection Regulation（GDPR）[6]44 条ないし 50 条に、越境移転の規律が定められている。

当該規律については、GDPR の前身である EU データ保護指令（Data Protection Directive 95）[7]から継承されてきたものであり、個人データを EU 内外に流通させることは国際取引や国際協力の拡大のために必要ではある一方で、GDPR で保障する自然人の保護レベルを脅かすべきではなく、GDPR を遵守したデータ移転のみが許容されているとの趣旨である（GDPR 前文（101）項参照）。

### （２） 越境移転の規律

#### ⅰ. 規律される行為

GDPR44 条では、①EEA 域外の第三国又は国際機関に対する個人データの移転、及び②当該第三国又は国際機関からさらに別の第三国又は国際機関への個人データの転送（Onward Transfer）に関するものについて、同条以下の規律の対象になると定めている。

このうち、①については、同じ国の中での個人データの移転であっても、EEA 域外の国にある第三者内の移転（例えば、GDPR が適用される米国法人 A から米国法人 B への移転）であれば、越境移転規制の対象となる。また、②については、例えば、EEA 域内の企業が、米国のベンダーに個人データを移転し、当該ベンダーが EEA 域外にある再委託先に個人データを移転する場合が含まれる。

---

[5] 経済産業省 「国際的なデータの移転・活用に関する企業アンケート」（https://www.meti.go.jp/press/2021/05/20210531001/20210531001-1.pdf）

[6] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

### ii. 規律の対象となるデータの種類

GDPRの関連規定において越境移転規制の対象となる個人データとは、識別された自然人又は識別可能な自然人（データ主体）に関する情報を意味し、識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す1つ又は複数の要素を参照することによって、直接的又は間接的に識別され得るものと定義されている（同法4条1項）。

### iii. 規律の対象となる者の定義・範囲

GDPR上の管理者（自然人、法人、公的機関、部局又はその他の組織であって、単独又は他の者と共同で、個人データの処理の目的及び方法を決定する者、同法4条7項）及び処理者（管理者のために個人データを処理する自然人、法人、公的機関、部局又はその他の組織、同法4条8項）が、越境移転規制の対象とされている（同法44条）。管理者から委託を受けて個人データを処理する者は処理者に該当し、例えば、管理者が利用しているクラウドサービスプロバイダや給与計算代行会社等が処理者に含まれ得る。

### iv. 規律の内容

GDPR上、個人データをEEA域外に移転することは原則として禁止されている（同法44条）が、次のいずれかを満たす場合には、例外的に個人データのEEA域外への移転が可能になる。

(ア)まず、欧州委員会が、十分なデータ保護の水準を確保しているとの認定（十分性認定）を行った国、地域又は国際機関[8]へのデータ移転については、追加して特段の対応を行わずに個人データをEEA域外に移転することが許容される（GDPR45条1項）。

(イ)移転先国が十分性認定を取得していない場合、GDPR46条に規定された以下の保護措置に準拠して個人データをEEA域外に移転することが可能である。

① 公的機関又は公的組織の間の法的拘束力・執行力のある文書
② 拘束的企業準則（Binding Corporate Rules：BCR）[9]
③ 欧州委員会が採択したSCC[10]
④ 監督機関が採択し、欧州委員会が承認したSCC
⑤ GDPR40条所定の行動規範（管理者や処理者の業界団体が制定する自主ルール）
⑥ 管理者や処理者のデータ保護措置がGDPRを遵守していることの認証[11]

---

[8] この認定を受けているのは、日本の他、アンドラ、アルゼンチン、カナダ（商業組織のみ）、フェロー諸島、ガーンジー、イスラエル、マン島、ジャージー、ニュージーランド、スイス、ウルグアイ、英国、韓国である。

[9] 企業グループあるいは共同経済活動に従事する事業者のグループの構成企業同士で、1ヵ国又は複数の第三国における管理者又は処理者に対して個人データ移転又は一連の個人データ移転のため、策定・遵守される個人データ保護のためのグループ内規をいう（GDPR4条20号）。同法47条2項所定の事項を当該内規に定めておくことが求められる。

[10] 個人データをEEA域外に移転するための契約の雛形であり、https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=ENの別紙として掲載されている。SCCは条項の内容の変更を行うことができず、データ移転の類型に応じたバリエーションを選択し、必要事項を記入して用いることになる。

[11] GDPR42条に定められており、権限ある監督機関又は認証を行うことが正当に認可された機関によって付与される認証である。

⑦　監督機関の個別的な承認を受けた契約条項又は取決め

（ウ）上記（ア）の十分性認定を取得しておらず、かつ、上記（イ）の適切な保護措置を講じることができない場合には、GDPR49条に規定された例外事由（Derogations）[12]を満たす場合に限り個人データをEEA域外に移転することができる。

## ２. 米国

### （１） 対象となる法令

米国においては個人情報の保護に関する包括的な連邦法は存在せず、個別法として以下に代表される法令が存在する。

①　Electronic Communications Privacy Act of 1986（ECPA）[13,14]
②　Gramm Leach Bliley Act（GLBA）[15,16]
③　Health Insurance Portability and Accounting Act（HIPAA）[17,18]

また、州法としては、カリフォルニア州（California Consumer Privacy Act of 2018（CCPA）[19]）[20]、ヴァージニア州（Consumer Data Protection Act[21]）及びコロラド州（Colorado Privacy Act[22]）には個人情報の保護に関する包括法が存在する。また、個別的な法令で個人情報保護に関連する規律を定めているものとしては、例えば、ニューヨーク州のNew York Stop Hacks and Improve Electronic Data Security（SHIELD）Act[23]やNew York Department of Financial Services Cybersecurity Regulation[24]、イリノイ州のIllinois Biometric Information Privacy Act[25]や

---

[12] 以下の例外事由が規定されている。
① 適切な保護措置が講じられていないことに伴うリスクについてデータ主体が情報提供を受けた上で、個人データのEEA域外への移転に明示的に同意している場合
② データ主体との間の契約の履行又はデータ主体が要請する契約締結前の措置の実施のために必要である場合
③ 第三者との間の、データ主体の利益になる契約の履行又は締結のために必要である場合
④ 公共の重大な利益のために必要である場合
⑤ 法的主張の立証又は攻撃・防御のために必要である場合
⑥ データ主体が物理的又は法的に同意できない場合で、データ主体又は第三者の生命に関する利益を保護するために必要である場合
⑦ EU法又はEU加盟国の国内法に従う一定の登録機関からの移転である場合

[13] https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

[14] このうち、Title II、Stored Communications ACT（SCA）及びその修正版である Clarifying Lawful Overseas Use of Data Act. 18 U.S.C. § 2510, 2701-2713.（CLOUD法）が個人情報保護関連の規定である。

[15] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

[16] このうち、the Privacy Rule and the Safeguards Rule. 15 U.S.C. §§ 6801-6809, 6821-6827が個人情報保護関連の規定である。

[17] https://www.cdc.gov/phlp/publications/topic/hipaa.html

[18] このうち、the Privacy Rule and the Safeguards Rule. 41 U.S.C.§§ 1320Dが個人情報保護関連の規定である。

[19] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[20] カリフォルニア州においては、Californian Consumer Privacy Act Of 2018よりも規制を強化するCalifornia Privacy Rights Actが2023年１月１日に発効する予定である。

[21] https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392

[22] https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

[23] https://www.nysenate.gov/legislation/bills/2019/s5575

[24] https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)&bhcp=1

[25] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Personal Information Privacy Act[26]が存在する。
しかしながら、これらの連邦法及び州法のいずれについても、越境移転特有の規律を定めた規定や、データの域内保存・域内保管を義務づける規定は存在しない。

## ３．カナダ

### （１） 対象となる法令

カナダでは、個人情報の保護に関する包括的な連邦法として、①2001 年から 2004 年にかけて段階的に施行された民間部門に適用される連邦法である Personal Information Protection and Electronic Documents Act（PIPEDA）[27]と、②1983 年 7 月 1 日に施行された公的部門に適用される連邦法である Privacy Act[28]が存在する。
しかしながら、これらのいずれの法律についても越境移転特有の規律を定めた規定や、データの国内保存・国内保管を義務づける規定は存在しない。
ただし、カナダの個人情報保護当局（the Office of the Privacy Commissioner of Canada）は越境移転に関するガイドライン（Processing Personal Data Across Borders Guidelines[29]）を公表しており、カナダ国内でのデータ移転と同様、移転元と同等のレベルの保護が移転先においても要求されること等が求められてきた。
なお、個別の州法では越境移転の規律について定めているものも存在し、プライバシーノーティスを要求する例（アルベルタ州[30]）や合理的な措置を要求する例（ケベック州[31]）が含まれる。

## ４．中国

### （１） 対象となる法令

中国では、個人情報の保護に関する包括的な法令として、2021 年 11 月 1 日に施行された個人情報保護法[32]が存在し、越境移転特有の規律を定めた規定や、データの国内保存・国内保管を義務づける規定が存在する。
その他、関連する規定が存在する法令として、2017 年 6 月 1 日に施行されたインターネット領域のセキュリティに関する基本法であるサイバーセキュリティ法（又はネットワーク安全法とも言われる）[33]及び 2021 年 9 月 1 日に施行されたデータとそのセキュリティの監督管理や利活用策を定めるデータセキュリティ法[34]が存在する[35]。

---

[26] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67
[27] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
[28] https://laws-lois.justice.gc.ca/eng/acts/P-21/
[29] https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf
[30] Personal Information Protection Act（SA 2003 C P-6.5）section 6(2))
[31] Act Respecting the Protection of Personal Information in the Private Sector（CQLR c P-39.1）section 17
[32] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[33] https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf
[34] http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml
[35] なお、2021 年 10 月 1 日より試験的に施行されている、自動車データセキュリティ管理の若干の規定においても、自動車産業固有の越境移転規制や国内保存義務の規定が存在する。

ただし、これらの法令における規律の対象となる各要件の解釈が必ずしも明確ではないことから、各企業においては中国からのデータの越境移転を行わないようにする方向での動きも見られるとの情報も存在するところである。

越境移転特有の規律を定めた規定及びデータの国内保存・国内保管を義務づける規定の目的は国家の安全保障と考えられる。

## （２） 越境移転の規律

### ⅰ. 規律される行為

(ア) 内容が確定していない[36]ものではあるが、サイバーセキュリティ法の下位法令と位置付けられる、2017年4月11日に公示された個人情報及び重要データ越境移転安全評価弁法案（以下、「2017年弁法案」）17条においては、ネットワーク運営者が中国国内運営[37]において収集し、発生した個人情報及び重要データ[38]を、中国国外にある機構、組織又は個人に対し提供することが規律されることと定められている。

(イ) また、同じく内容が確定していないものではあるが、データ越境移転安全評価ガイドライン案[39]3.7条においては、ネットワーク運営者がネットワーク等の方法により、中国国内運営において収集し、発生した個人情報及び重要データを、中国国外にある機構、組織又は個人に対し、直接提供又は業務展開、サービス・製品提供等の方法により提供する一回限りの又は継続的な活動を規律しており、以下の場面も越境移転規制の対象とされると定め

---

[36] 中国においては、内容が未確定の法令であっても解釈の参考となり得ることがあるため、本報告書では参考情報として紹介している。

[37] データ越境移転安全評価ガイドライン案においては、外国企業が中国国内で登記をしているか否かにかかわらず、中国国内において何らかの経営活動を行い、又は中国国内に製品若しくはサービスを提供する場合には、中国国内の「運営」に該当するとされている（同ガイドライン案3.2条）。この中国国内の運営の該当性の判断要素としては、①取引における中国語の使用の有無、②決済通貨としての人民元の使用の有無、③中国国内への配送・物流の有無等が存在する。

[38] 2017年弁法案17条によれば、重要データとは、国の安全、経済発展、並びに社会的及び公的利益に密接に関連するデータをいい、その具体的な範囲は国の関連基準及び重要データ識別ガイドラインを参照するとされている。加えて、データ越境移転安全評価ガイドライン案の別紙Aによれば、重要データとは、政府、組織、個人が中国国内において収集し、又は発生する、国家機密には該当しない国の安全、経済発展、又は公共の利益に密接に関連するデータ（原始データ及び派生データを含む）であり、かつそのデータが同意なしに公開、紛失、濫用、改竄若しくは廃棄され、又は分析等を経た後、①国家の安全や国防利益を害すること、国際関係の破壊、②国有財産、公共の利益及び個人の合法的な利益を害すること、③産業スパイや軍事スパイ活動、組織犯罪等に対する国家の予防・取締りに影響すること、④行政機関による違法、汚職行為に対する調査に影響すること、⑤政府の行政活動の妨害、⑥国家の重要インフラ、重要情報インフラ、政府システムの情報システムの安全を害すること、⑦経済及び金融の秩序を害すること、⑧国家機密又はセンシティブデータにアクセスし得ること、⑨その他国家の安全事項を害することをもたらす可能性があるものをいう。なお、同ガイドラインでは、通信、鋼鉄、金融、電子商取引、食品薬品等27のカテゴリーが設けられ、業界分野ごとに重要データの範囲が規定されている。
また、同じくサイバーセキュリティ法を前提とする2019年5月28日に公示されたデータセキュリティ管理弁法（意見募集案）の38条においては、重要データとは、漏洩により国家安全、経済安全、社会安定性、公共健康及び安全に直接に影響を及ぼし得るデータをいい、具体的には未公開の政府情報、広範囲の人口、遺伝子健康、地理、鉱物資源等が含まれるとされている。
これらの2017年及び2019年に公示されたいずれの弁法案の内容が確定していくのかは未定である。
さらに、データセキュリティ法において、重要データのデータ分類制度を確立し、経済社会発展におけるデータの重要度並びに改ざん、破壊、漏洩又は不法取得及び不法利用にひとたび遭遇した場合における国家安全、公共利益又は個人若しくは組織の適法な権益にもたらす危害のレベルに基づき、重要データ目録を国が制定する旨が規定されている（同法21条）ため、今後、重要データ目録の制定・公布動向に注目しておく必要がある。

[39] https://www.tc260.org.cn/file/20170830203000000004.docx

られている。

① 中国の司法管轄に属さず又は中国国内[40]で登記されていないものの、中国国内にある機構、組織又は個人（すなわち中国から見て外国企業や外国人）に対し、個人情報及び重要データを提供する場合

② データが中国国外の地域に移転・保存されないものの、中国国外の機構、組織又は個人がアクセスして閲覧できる場合（公開情報、ホームページのアクセスを除く）

③ 企業グループ内部におけるデータの移転であっても、中国国内運営において収集し、発生した個人情報及び重要データに関わる場合

他方で、同条の規律は、以下の場面には及ばないこととされている。

① 中国国内運営において収集しておらず、又は、中国国内運営において発生したものではない個人情報及び重要データを、変更や加工処理を経ずに中国を経由して中国国外に移転する場合

② 中国国内運営において収集し、発生したものではない個人情報及び重要データが中国国内での保存･加工処理を経てから中国国外に移転されるものの、中国国内運営において収集し、発生した個人情報及び重要データに関わらない場合

### ii. 規律の対象となるデータの種類

（ア）個人情報保護法の越境移転規制の対象となる個人情報は、電子又はその他の方法により記録される、既に識別され、又は識別可能な自然人に関する各種情報であり、匿名化処理後の情報を含まないものと定義されている（同法4条）。

（イ）サイバーセキュリティ法の越境移転規制については、個人情報及び重要データが規律の対象となる。このうち個人情報とは、電子又はその他の方式で記録した単独又はその他の情報と組み合わせて自然人（個人）の身分を識別することができる、自然人の氏名、生年月日、身分証番号、個人の生体認証情報、住所、電話番号等を含むがこれらに限らない各種情報をいう（同法76条5号）。

（ウ）データセキュリティ法においては、国の安全と利益の維持、国際的義務の履行の維持に関連する管理品目[41]に該当するデータ（同法25条）及び重要データ（同法31条）が越境移転規制の対象となる。

### iii. 規律の対象となる者の定義・範囲

（ア）個人情報保護法の関連規定においては、個人情報取扱者が越境移転規制の対象となる。個人情報取扱者とは、個人情報の取扱活動において、取扱いの目的及び方法を自主的に決定する組織又は個人をいうものと定義されている（同法73条1号）。

---

[40] 香港、マカオ、台湾を含まない中国本土の意。「国外」はその逆である。

[41] 両用品目、軍需品、核並びにその他の国の安全及び利益の維持・保護、拡散防止等の国際義務の履行に関連する貨物、技術、サービス等の品目を指し、品目関連の技術資料等のデータを含むが、管理品目に該当するデータであるか否かは、国所定の規制リストや基準をもって判断することになる（輸出管理法2条、4条）。

（イ）サイバーセキュリティ法の関連規定においては、重要情報インフラ[42]の運営者[43]が越境移転規制の対象となる。

（ウ）データセキュリティ法の関連規定においては、データ処理者（同法 27 条以下）が越境移転規制の対象となる。

### iv. 規律の内容

（ア）個人情報保護法においては、個人情報取扱者が業務等の必要性により、個人情報を中国国外に提供する必要が確実にある場合については、次の条件のいずれかを満たす場合のみ認められるものとされている（同法 38 条）。ただし、個人情報取扱者のうち、重要情報インフラの運営者又は国家ネットワーク情報部門の定める数量[44]に達する個人情報取扱者は、次の②～④の根拠に拠ることはできず、越境移転の必要がある場合、法律・行政法規又は国家ネットワーク情報部門により免除がなされている場合を除き、事前に国家ネットワーク情報部門による安全評価に合格する必要がある（同法 40 条後段）。

① 同法 40 条の規定に従い、国家ネットワーク情報部門による安全評価に合格すること
② 国家ネットワーク情報部門の規則に従い、専門機構による個人情報保護の認証を得ること
③ 国家ネットワーク情報部門の制定する標準契約に従って中国国外の移転先と契約を締結し、双方の権利及び義務を約定すること
④ 法律・行政法規又は国家ネットワーク情報部門の規定するその他の条件

また、これに加え、個人情報取扱者は、中国国外への個人情報の提供に際しては、中国国外の受領者の名称又は氏名、連絡方法、取扱いの目的、取扱方法、個人情報の種類、並びに個人情報主体から中国国外の受領者への個人情報保護法に定める権利の行使方法・手続等の事項を個人情報主体に告知し、かつ、個別の同意を取得しなければならない（同法 39 条）。

（イ）サイバーセキュリティ法においては、重要情報インフラの運営者は、中国国内での運営に

---

[42] 公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務等の重要な業界及び分野、並びにその他の一旦破壊され、機能を喪失し、又はデータが漏洩すると国の安全、国の経済と人民の生活、公共の利益に深刻な危害が及ぶおそれのあるその他の重要情報インフラをいうとされている（サイバーセキュリティ法 31 条）。その更に具体的な内容は、重要情報インフラセキュリティ保護条例案 18 条が定めており、①政府機関及びエネルギー、金融、交通、水利、衛生医療、教育、社会保険、環境保護、公的事業等の業界・領域の組織機構、②電気通信ネットワーク、ラジオ・テレビ放送ネットワーク、インターネット等の情報ネットワーク及びクラウド、ビッグデータその他大型の公共情報ネットワークサービスの組織機構、③国防・科学技術工業、大型装備、化学工業、食品薬品等の業界・領域における科学研究・生産の組織機構、④ラジオ局、テレビ局、通信社等のマスメディア、並びに⑤その他の重要な組織機構が運営し、管理するネットワーク施設及び情報システムで、一旦破壊され、機能を喪失し、又はデータが漏洩すると国の安全、国の経済と人民の生活、公共の利益に深刻な危害が及ぶおそれのあるものとされている。

[43] 2017 年弁法案においては、越境移転の規律の適用対象となる者を重要情報インフラの運営者から、全てのネットワーク運営者（サイバーセキュリティ法 76 条 3 号に基づき、ネットワークの所有者、管理者及びインターネットサービスプロバイダをいうこととされている）に拡大している。かかる規定が実現すると、中国国内のネットワークを利用する事業者が広く規律の対象となることとなる。

[44] 現行法上は明確な基準は定められていないものの、国家ネットワーク情報部門が 2021 年 10 月 29 日に公表したデータ越境安全評価弁法（意見募集稿）の 4 条 1 項（データ取扱者が中国国外にデータを提供する際、国家ネットワーク情報部門による安全評価が必要となるケースを定めている）に定める以下の内容が参考になる。
①100 万人以上の個人情報を取り扱う個人情報取扱者が中国国外に個人情報を移転する場合
②累計して 10 万人以上の個人情報又は 1 万人以上のセンシティブ個人情報を中国国外に移転する場合

おいて収集し、生じた個人情報及び重要データを、中国国内で保存しなければならず、業務上の必要により、中国国外に提供する必要が確実にある場合は、国家インターネット情報部門が国務院の関係部門と共に制定した規則に従って安全評価を行わなければならないとされているが、法律・行政法規に別途規定がある場合は、当該定めに従うこととされている（同法 37 条）。

（ウ）データセキュリティ法においては、国の安全と利益の維持、国際的義務の履行の維持に関連する管理品目に該当するデータについては、法に基づき輸出管理を実施することとされている（同法 25 条）。また、重要データのうち、①重要情報インフラの運営者が中国国内での運営において収集し、生じた重要データの越境移転の際の安全管理については、サイバーセキュリティ法の規定が適用されるが、②その他のデータ処理者が中国国内での運営において収集し、生じた重要データについては、データセキュリティ法において、国家ネットワーク情報部門が国務院の関係部門と共同して、越境移転の際の安全管理に係る弁法を制定する旨が定められている（同法 31 条）。

### （３）　データの国内保存・国内保管義務を定める規律

#### ｉ. 規律の対象となる者の定義・範囲

（ア）個人情報保護法においては、①国家機関（同法 36 条）、②重要情報インフラの運営者（同法 40 条）、③取り扱う個人情報が国家ネットワーク情報部門の定める数量に達する個人情報取扱者（同法 40 条）及び④中国国内に保存された個人情報を外国の司法又は法律執行機関に対して提供する個人情報取扱者（同法 41 条）がデータの国内保存・国内保管義務を定める規律の対象となる。

（イ）サイバーセキュリティ法においては、重要情報インフラの運営者[45]がデータの国内保存・国内保管義務を定める規律の対象となる（同法 37 条前段）。

（ウ）データセキュリティ法においては、①重要情報インフラの運営者及びその他のデータ処理者（同法 31 条）、並びに②中国国内の組織又は個人（同法 36 条）がデータの国内保存・国内保管義務を定める規律の対象となる。

#### ｉｉ. 規律の内容

（ア）個人情報保護法においては、国家機関が処理する個人情報は、中国国内で保存しなければならず、国外に提供する必要が確実にある場合には、安全評価に合格しなければならないこととされている（同法 36 条）。（２）iv.（ア）記載の同法 40 条、すなわち重要情報インフラの運営者及び取り扱う個人情報が国家ネットワーク情報部門の定める数量に達する個人情報取扱者は、法律・行政法規又は国家ネットワーク情報部門により免除がなされている場合を除き、中国国内において収集し、生じた個人情報を国内において保存しなければ

---

[45] 2017 年弁法案においては、越境移転の規律の適用対象となる者を重要情報インフラの運営者から、全てのネットワーク運営者（サイバーセキュリティ法 76 条 3 号に基づき、ネットワークの所有者、管理者及びインターネットサービスプロバイダをいうこととされている）に拡大している。かかる規定が実現すると、中国国内のネットワークを利用する事業者が広く規律の対象となることとなる。

ならず、中国国外に提供する必要が確実にある場合には、国家ネットワーク情報部門が組織する安全評価に合格しなければならない旨の定めは、越境移転に関する規律であるとともに、データの国内保存・国内保管義務を定める規律ともとらえることが可能である。また、主管機関は、関連する法律及び中国が締結し、若しくは参加する国際条約若しくは協定に基づいて、又は平等互恵原則に従い、外国の司法又は法律執行機関による国内に保存された個人情報の提供に関する請求を処理することとされ、主管機関の認可を経ていない場合には、個人情報取扱者は外国の司法又は法律執行機関に対して中国国内に保存されている個人情報を提供してはならないとされている（同法41条）。

（イ）（２）iv.（イ）記載のサイバーセキュリティ法37条の規律は、越境移転に関する規律であるとともに、データの国内保存・国内保管義務を定める規律ともとらえることが可能である。

（ウ）データセキュリティ法においては、重要情報インフラの運営者が中国国内での運営において収集し、生じた重要データの安全管理には、サイバーセキュリティ法の規定を適用することとされ（その結果、上記のとおり安全評価が必要となる）、その他のデータ処理者が中国国内での運営において収集し、及び発生した重要データの安全管理のための弁法については、国家ネットワーク部門が国務院の関係部門と共に制定する旨が定められている（同法31条）。また、主管機関は、関連する法律及び中国が締結し、若しくは参加する国際条約若しくは協定に基づいて、又は平等互恵原則に従い、外国の司法又は法律執行機関によるデータ提供に関する請求を取り扱うこととされ、主管機関の認可を経ていない場合には、中国国内の組織又は個人は、外国の司法又は法律執行機関に対し、中国国内に保存されているデータを提供してはならないとされている（同法36条）。

## ５．インド

### （１） 対象となる法令

インドにおいては施行済みの個人情報の保護に関する包括的な法令は存在せず、個別法として、2000年6月9日に施行されたInformation Technology Act, 2000（情報技術法）[46]及び2011年4月11日に施行されたInformation Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011（セキュリティ規則）[47]が存在する。しかしながら、これらの法令においては、越境移転特有の規律を定めた規定や、データの国内保存・国内保管を義務づける規定は存在しない。

他方で、特定の業種についてはデータの国内保存・国内保管を義務づける規定が存在し、インド中央銀行については支払システム情報の保存に関する政令（DL政令）[48]及びDL政令に関するFAQ[49]

---

[46] https://www.meity.gov.in/writereaddata/files/itbill2000.pdf

[47] https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf

[48] https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[49] https://m.rbi.org.in/scripts/FAQView.aspx?Id=130#:%7E:text=The%20entire%20payment%20data%20shall,except%20in%20cases%20clarified%20herein.&text=The%20data%20should%20include%20end,of%20a%20payment%20message%20%2F%20instruction

（DL 政令と併せて「DL 規則」と呼称する）が存在する。また、電気通信サービス事業者については電気通信分野における統一ライセンス法[50]が存在する。

加えて、未確定の内容ではあるが、個人情報の保護に関する包括的な法律として、2019 年 12 月 11 日に国会に提出された個人情報保護法の法案（Bill No.373 of 2019）[51]を一部修正する提案を行う、2021 年 12 月 16 日に提出された同法案関連の報告書[52]が存在する[53]。

個人情報保護法の法案におけるデータの国内保存・国内保管義務を定める規定については、セキュリティ確保、犯罪捜査に資する目的で立案されており、当局（The Joint Parliamentary Committee）がこれをデータ保護の不可欠な要素であると考えている旨の情報[54]が存在する。

## （２） データの国内保存・国内保管義務を定める規律

### ⅰ. 規律の対象となる者の定義・範囲

DL 規則については、インド中央銀行による認可の対象となる支払システムの提供者（仲介者、ペイメントゲートウェイ提供者、第三者ベンダー等を含む）がデータの国内保存・国内保管義務を定める規律の対象となる。

統一ライセンス法については、同法に基づき電気通信省（Department of Telecommunications）からライセンスを受けた電気通信サービス事業者がデータの国内保存・国内保管義務を定める規律の対象となる。

### ⅱ. 規律の内容

(ア)DL 規則については、デジタル決済の健全な発展とデータブリーチによるリスクを低減するために、決済データの監視、監督を行うことを目的とし、インド中央銀行による認可の対象となる支払システムの提供者（仲介者、ペイメントゲートウェイ提供者、第三者ベンダー等を含む）は、支払システムに関連する全ての情報をインドにおいてのみ保存することを義務づけられている。

(イ)規制の対象となる支払システム情報とは、インド国内のサーバーに保存されるか、メッセージ、支払指示の一部として収集、伝達又は処理されたエンドツーエンドの取引詳細及び情報と定義されており（DL 政令 2 条(i)）、氏名、携帯電話番号、電子メール、Aadhaar 番号（国民マイナンバー情報）、PAN（納税者番号）を含む顧客情報、顧客及び受益者の口座情報を含む支払センシティブ情報、ワンタイムパスワード、PIN、パスワード等の支払クレデンシャル、システムへの入退出情報、取引参照情報、タイムスタンプ、取引金額を含む取引情報が包含されると規定されている（DL FAQ 3 条）。

(ウ)DL 政令はエンドツーエンド情報を原則としてインド国内にて保存することを義務づけてい

---

[50] https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf

[51] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[52] http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[53] 当該報告書の提案内容が法案として採択されるか否かが 2021 年末時点では不明であるため、本報告書にて同法案に係る内容の紹介は行わないが、関連動向は引き続き注視が必要である。

[54] https://sflc.in/summary-jpc-recommendations-personal-data-protection-bill-2019

るが、DL FAQ の定める一定の外国の要素を持つ取引についてはその限りではないとされている（DL 政令 2 条(i)）。すなわち、インド国内と国外双方の側の情報を取り扱うこととなる国際取引の情報については、必要に応じてインド国内側の情報についても、インド国外にてコピーを保存することが許容されている。

(エ)統一ライセンス法においては、同法に基づき電気通信省（Department of Telecommunications）からライセンスを受けた電気通信サービス事業者に対して、サービス利用者の財務情報（国際ローミング及び料金情報を除く）及び利用者情報（ローミングでインドの事業者のネットワークを利用しているインド国外の契約者等に係るものを除く）をインド国外に移転することを禁じている（同法 39.23 条(viii)）。

## ６．ベトナム

### （１） 対象となる法令

ベトナムにおいては施行済みの個人情報の保護に関する包括的な法令は存在せず、個別法として、2019 年 1 月 1 日に施行されたサイバーセキュリティ法[55]や 2013 年 9 月 1 日に施行されたインターネットサービス及びオンライン情報の管理、提供及び利用に関する政令 72 号[56]（以下、「政令 72 号」という）といった法令が存在する。

これに加え、2021 年 2 月に公表された個人情報保護について詳細な規定を包括的に定める個人情報保護に関する政令案[57]が存在する。同政令案においては、未確定の内容ではあるが、越境移転特有の規律を定めた規定や、データの国内保存・国内保管を義務づける規定が存在する。

### （２） 越境移転の規律

#### i. 規律される行為

個人情報保護に関する政令案 21 条においては、ベトナムの国境及び領土外に移転する行為が規律されるものとしている。

#### ii. 規律の対象となるデータの種類

個人情報保護に関する政令案の関連規定において越境移転規制の対象となる個人情報は、個人に関する情報、又は特定の個人の識別し若しくは識別可能な情報[58]と定義されている（同政令案 2 条 1 項）。

#### iii. 規律の対象となる者の定義・範囲

個人情報保護に関する政令案は、個人情報に関係する機関、組織及び個人に適用され（同政令案 1 条 2 項）、ベトナムで事業を行っている国内外の全ての組織、企業及び個人が同政令違反の

---

[55] https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx

[56] https://thuvienphapluat.vn/van-ban/cong-nghe-thong-tin/nghi-dinh-72-2013-nd-cp-quan-ly-cung-cap-su-dung-dich-vu-internet-va-thong-tin-tren-mang-201110.aspx

[57] http://www.bocongan.gov.vn/van-ban/van-ban-du-thao/du-thao-nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-240.html#parentHorizontalTab4

[58] 「個人情報」は、さらに「基礎個人情報」と「センシティブ個人情報」に区分される（同政令案 2 条 2 項）。

責任を負うと規定されている（同政令案4条2項）。

### ⅳ. 規律の内容

個人情報保護に関する政令案は、ベトナム市民の個人情報は、以下の①から④の要件が全て満たされた場合、ベトナムの国境及び領土外に移転することができるものと定めている（同政令案21条1項）。

① データ主体が移転に同意する
② オリジナルの情報がベトナムで保存される
③ 情報を受領する国、領土又は当該国若しくは領土内の特定の地域が、本政令に定める水準と等しい又はそれ以上の水準の個人情報保護に関する規制を有していることを証明する書類が付与される
④ 個人情報保護委員会の書面による承認を得る

これに加え、同政令案は、次の場合には上記①から④の要件を満たさずとも個人情報をベトナム国外に移転することができるとも定めている（同条3項）。

⑤ データ主体が移転に同意する
⑥ 個人情報保護委員会の書面による承認を得る
⑦ 個人情報を保護するための情報処理者のコミットメントが存在する
⑧ 個人情報保護手段を実施するための個人情報処理者のコミットメントが存在する

上記の二種類の規律は文言としての共通性が多いものであるが、同政令案の文言は現状趣旨不明瞭な部分があり、上記の21条1項及び3項の適用関係や各要件の詳細についての解釈は不明確である。

以上の規律はデータの国内保存・国内保管義務を定める規律ともとらえることが可能である。

## （３） データの国内保存・国内保管義務を定める規律

### ⅰ. 規律の対象となる者の定義・範囲

（ア）サイバーセキュリティ法上のデータの国内保存・国内保管義務を定める規律は、ベトナムにおいて電気通信ネットワーク又はインターネット上のサービスその他サイバー空間上の付加価値サービスを提供する国内外事業者[59]に適用されるものとされている（同法26条3項）。

（イ）また、政令72号のデータの国内保存・国内保管義務を定める規律は、以下のオンラインサービス事業者に適用される（同政令72号24条2項、25条8項、28条2項及び34条2項）。

① 一般ウェブサイト[60]を開設する団体及び企業（所謂ニュース配信サービス等がこれに該

---

[59] 同法上の文言だけを見れば、全てのオンラインサービス事業者が含まれるかのようにも読み得るところであるが、当該義務は詳細な施行規則を政令で定めることとされている（同法26条4項）ため、当該政令で定められることとなる内容も踏まえて注視が必要である。

[60] 政令72号上、「一般ウェブサイト」とは「機関、団体又は企業のウェブサイトであって、正確に公式の情報源を引用し、か

当すると考えられる）
② ソーシャルネットワーキングサービスを提供する団体及び企業
③ 移動電気通信ネットワークにおいて情報コンテンツサービスを提供する団体及び企業（携帯電話網を用いて SMS 等で情報を配信するサービス等がこれに該当すると考えられる）
④ オンライン電子ゲームサービス事業者

**ii. 規律の内容**

（ア）サイバーセキュリティ法においては、i.（ア）で記載のサービス提供事業者は、ベトナムにおける個人情報に関するデータ、サービス利用者の関係に関するデータ又はサービス利用者の作成したデータの収集、利用、分析又は加工を行う場合、ベトナム政府の定める一定期間中は、そのデータをベトナムで保管する義務が定められている（同法 26 条 3 項）。また、当該要件を満たすベトナム国外企業は、ベトナムに支店又は駐在員事務所を設けることが義務づけられている（同条項）。

（イ）政令 72 号においては、i.（イ）で記載のオンラインサービス事業者は、情報通信省が定めるとおりサービス提供に関する顧客の苦情に対応するため、管轄行政当局による情報の検査、確認、保管及び提供の要求に対応可能なサーバーシステムを少なくとも 1 台ベトナムに設置することが義務づけられている（同政令 72 号 24 条 2 項、25 条 8 項、28 条 2 項及び 34 条 2 項）。

（ウ）なお、（２）において越境移転規制として紹介している個人情報保護に関する政令案における規律は、越境移転に関する規律であるとともに、データの国内保存・国内保管義務を定める規律ともとらえることが可能であることは上述のとおりである。

## ７. インドネシア

### （１） 対象となる法令

インドネシアにおいては施行済みの個人情報の保護に関する包括的な法令は存在せず、個別法として、2019 年 10 月 10 日に施行された電子システム及び電子取引の実施に関する 2019 年政令第 71 号（Government Regulation No.71 of 2019 on the Administration of Electronic Systems and Transactions、以下、「2019 年政令」）[61]及び 2016 年 12 月 1 日に施行された電子システムにおける個人情報に関する 2016 年通信情報省規則第 20 号（Minister of Communications and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System、以下、「2016 年省規則」）[62]が存在する。

---

つ、その著者の氏名又は公式の情報源の機関の名称及び掲載又は放送の時期を明示した上で、一般的な情報を提供するもの」と定義されている（政令 72 号 20 条 2 項）。

[61] https://jdih.kominfo.go.id/produk_hukum/unduh/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019

[62] https://jdih.kominfo.go.id/produk_hukum/unduh/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016

また、2020年1月24日に国会に提出された、個人データ保護に関する統一的な法令としての個人データ保護法案[63]が存在する。同法案においては、GDPRに類似した規律も多く存在し、未確定の内容ではあるが、越境移転特有の規律を定めた規定が存在する。

当該規定については、データの越境移転が行われることにより、個人の保護レベルが損なわれることがないようにするという、GDPR類似の趣旨を有する。

## （２） 越境移転の規律

### ⅰ. 規律される行為

2016年省規則においては、個人データのインドネシア国外への移転が規律されている。

### ⅱ. 規律の対象となるデータの種類

2019年政令の関連規定において越境移転規制の対象となる個人情報は、電子システムを通じたものか否かにかかわらず、単独又は他の情報と共同して、直接又は間接的に個人を識別できる情報と定義されている（同政令1条）。

また、2016年省規則の関連規定において越境移転規制の対象となる個人データは、保管及び管理された一定の個人データであって、その秘密性が保護されなくてはならない情報と定義されている（同規則1条1項）。

### ⅲ. 規律の対象となる者の定義・範囲

（ア）2019年政令、2016年省規則ともに、電子システム提供者に適用される（2019年政令1条4項等）。

（イ）個人データ保護法案においては、越境移転規制は個人データの管理者に適用される（同法案49条）。

### ⅳ. 規律の内容

（ア）2016年省規則においては、通信情報大臣との連携により実施されることとされている（同規則22条1項a）。当該連携においては、①移転先国、移転の相手方、移転日、移転の理由を最低限内容に含む報告の実施、②必要に応じた支援の要請、及び③移転の結果報告の実施を行うことが規定されている（同条2項）。

（イ）また、個人データ保護法案においては、越境移転に際して、以下の条件のいずれかに拠るものとされている（同法案49条）。

① 移転先国にインドネシアと同等以上の個人データ保護規則があること

② インドネシアと移転先国の間の国家間同意があること

③ 移転元の個人データ管理者と移転先の個人データ管理者の間に個人データの処理に関する契約があること

---

[63] https://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf

④ データ主体の同意が得られていること

### （３） データの国内保存・国内保管義務を定める規律

#### ⅰ. 規律の対象となる者の定義・範囲

2019年政令上のデータの国内保存・国内保管義務を定める規律は、公共部門の電子システム提供者に適用されるものとされている（同政令20条2項）。

他方で、民間部門の電子システム提供者は、インドネシア国外で電子システム及び電子データを管理、処理又は保存することができるものである（同政令21条1項）が、同政令上、公共部門は中央及び地方の政府機関（金融サービス庁は除く）並びに政府機関から任命された者が該当することとされ（同政令2条3項、4項）、民間部門は、政府機関により規制又は監督される電子システム提供者で、特定の目的[64]に利用するウェブポータル、ウェブサイト又はアプリケーションを保有する者とされている（同政令2条5項）。

#### ⅱ. 規律の内容

（ア）2019年政令においては、公共部門の電子システム提供者がインドネシア国内に電子システム及び電子データを管理、処理又は保存することが義務づけられている（同政令 20 条 2 項）。ただし、当該義務の例外として、保管技術がインドネシア国内で利用できない場合には、公共電子システム運営者は、インドネシア国外でデータの保存を行うことができる（同政令20 条3項）。この「利用できない」場合に該当するか否かの基準は、通信情報省等の関連省庁により構成される委員会によって決定されることとされているが、当該基準は公表されていない。

（イ）この他、金融分野に関しては、インドネシア金融庁が制定する規則（OJK Regulation No.4/POJK.05/2021 on Application of Risk Management During the Use of Information Technology by Non-bank Financial Service Institutions、OJK Regulation No. 38/POJK.03/2016 on the Application of Risk Management in the Use of Information Technology by Commercial Banks（OJK Regulation No. 13/POJK.03/2020 により改正）等）により、インドネシアのノンバンク金融機関、商業銀行等はデータの国内保存・国内保管義務を負う。

---

[64] 以下の目的をいうものとされている（同政令2条5項）。
① 物又はサービスの申込み又は取引の提供、管理又は運営
② 金融取引サービスの提供、管理又は運営
③ ウェブポータル、ウェブサイト、電子メール、その他のアプリケーションを通じて利用者のデバイスにダウンロードすることによる資料又は有料コンテンツの配布
④ ショートメール、音声通信、ビデオ電話、電子メール、チャットルーム、ネットワーキングサービス、ソーシャルメディア等のコミュニケーションサービスの提供、管理又は運営
⑤ サーチエンジンサービス又はテキスト、音声、画像、アニメーション、音楽、ビデオ、映画、ゲーム若しくはこれらの組み合わせの形式における電子情報の提供サービス
⑥ 電子取引活動に関する公共の利益に資する活動のための個人データの処理

## ８．全体像

表１：各国法令上のデータ関連規制

| | 越境移転規制 | | 国内保存・国内保管義務 | |
|---|---|---|---|---|
| EU | **General Data Protection Regulation（GDPR）** 本文脚注6 | | 個人情報保護法制上は、該当なし | |
| | 規制の対象となる情報 | 識別され又は識別可能な自然人に関する情報（個人データ） | | |
| | 規制の対象となる者 | 管理者又は処理者 | | |
| | 規制の内容 | 越境移転は原則禁止だが、以下の条件のいずれかを満たせば例外的に可能<br>①移転先国が十分性認定を受けている場合<br>②GDPR46条にある保護措置（Binding Corporate Rules、Standard Contractual Clauses、当局の認証等）に準拠している場合<br>③GDPR49条の例外事由（データ主体の同意、データ主体の利益となる契約に必要、公共の重大な利益のために必要等）を満たす場合 | | |
| 米国 | 個人情報保護法制上は、該当なし | | 個人情報保護法制上は、該当なし | |
| カナダ | 個人情報保護法制上は、該当なし | | 個人情報保護法制上は、該当なし | |
| 中国 | **個人情報保護法** 本文脚注32 | | **個人情報保護法** 本文脚注32 | |
| | 規制の対象となる情報 | 識別され又は識別可能な自然人に関する匿名化していない情報（個人情報） | 規制の対象となる情報 | 識別され又は識別可能な自然人に関する匿名化していない情報（個人情報） |
| | 規制の対象となる者 | 個人情報取扱者 | 規制の対象となる者 | ①国家機関<br>②重要情報インフラの運営者<br>③取り扱う個人情報が国家ネットワーク情報部門の定める数量に達する個人情報取扱者<br>④国外の政府機関に個人情報を提供する個人情報取扱者 |
| | 規制の内容 | データの越境移転は以下の条件を満たす場合のみ可能<br>ア）データ主体からの同意取得<br>＋<br>イ）<br>①重要情報インフラの運営者、又は②取り扱う個人情報が国家ネットワーク情報部門の定める数量に達する個人情報取扱者：安全評価の実施<br>③その他の個人情報取扱者：(i)安全評価、(ii)当局認証、(iii)所定の標準契約の締結又は(iv)法令の定めによるその他の条件のいずれか | 規制の内容 | ①②③：国内保存義務・安全評価<br>④：国外の政府機関への提供にあたっては主管機関の認可が必要 |
| | **サイバーセキュリティ法** 本文脚注33 | | **サイバーセキュリティ法** 本文脚注33 | |
| | 規制の対象となる情報 | 国内で収集・生成した、(i)自然人の身分を識別可能な氏名等の各種情報（個人情報）及び(ii)国の安全、経済発展等に密接に関連するデータ（重要データ） | 規制の対象となる情報 | 国内で収集・生成した、(i)自然人の身分を識別可能な氏名等の各種情報（個人情報）及び(ii)重要データ |
| | 規制の対象となる者 | 重要情報インフラの運営者 | 規制の対象となる者 | 重要情報インフラの運営者 |
| | 規制の内容 | 安全評価 | 規制の内容 | 国内保存義務・安全評価 |
| | **データセキュリティ法** 本文脚注34 | | **データセキュリティ法** 本文脚注34 | |
| | 規制の対象となる情報 | (i)国の安全と利益の維持、国際的義務の履行の維持に関連する管理品目のデータ、及び(ii)国内で収集・生成した重要データ | 規制の対象となる情報 | 以下①②：国内で収集・生成した重要データ（③は限定なし） |
| | 規制の対象となる者 | (ii)について<br>①重要情報インフラの運営者<br>②その他のデータ処理者 | 規制の対象となる者 | ①重要情報インフラの運営者<br>②その他のデータ処理者<br>③国内の組織又は個人 |
| | 規制の内容 | (i)について<br>輸出管理の実施<br>(ii)について<br>①：サイバーセキュリティ法と同様<br>②：国家ネットワーク部門が国務院の関係部門と共に制定する弁法に従う | 規制の内容 | ①：サイバーセキュリティ法と同様<br>②：国家ネットワーク部門が国務院の関係部門と共に制定する弁法に従う<br>③：国外の政府機関への提供にあたっては主管機関の認可が必要 |

| | 越境移転規制 | | 国内保存・国内保管義務 | |
|---|---|---|---|---|
| インド | 個人情報保護法制上は、該当なし | | 支払システム情報の保存に関する政令本文[脚注48,49]【金融分野】 | |
| | | | 規制の対象となる情報 | 国内サーバに保存されるか、メッセージ、支払指示の一部として収集、伝達又は処理されたエンドツーエンドの取引詳細及び情報（支払システム情報） |
| | | | 規制の対象となる者 | 中央銀行の認可対象となる支払システムの提供者 |
| | | | 規制の内容 | 国内のみでの保存義務 |
| | | | 統一ライセンス法[本文脚注50]【電子通信分野】 | |
| | | | 規制の対象となる情報 | サービス利用者の財務情報及び利用者情報 |
| | | | 規制の対象となる者 | ライセンスを受けた電気通信サービス事業者 |
| | | | 規制の内容 | 国外への移転禁止 |
| ベトナム | 個人情報に関する政令(案)[本文脚注57] | | サイバーセキュリティ法[本文脚注55] | |
| | 規制の対象となる情報 | 個人に関する情報、又は特定の個人を識別し若しくは識別可能な情報（個人情報） | 規制の対象となる情報 | 個人情報に関するデータ、サービス利用者の関係に関するデータ又はサービス利用者の作成したデータ |
| | 規制の対象となる者 | 個人情報に関係する機関、組織及び個人 | 規制の対象となる者 | 国内情報通信ネットワーク又はインタネット上でサービス等を提供する事業者 |
| | 規制の内容 | 次の①～④の全てを満たす場合のみ越境移転可能（①～④を満たさない場合も一定の条件を満たせば可）<br>①データ主体の同意<br>②オリジナルデータの国内保存<br>③移転先国の個人情報保護規制の存在証明<br>④個人情報保護委員会からの書面承認 | 規制の内容 | 個人情報に関するデータやサービス利用に関するデータ等を収集・利用・分析・加工する場合、一定期間の国内保存義務及び国内拠点設置義務 |
| | | | 政令72条[本文脚注56] | |
| | | | 規制の対象となる者 | オンラインサービス事業者 |
| | | | 規制の内容 | １台以上の国内サーバー設置義務 |
| インドネシア | 2019年政令[本文脚注61]及び2016年省規制[本文脚注62] | | 2019年政令[本文脚注61] | |
| | 規制の対象となる情報 | (i)直接又は間接的に個人を識別できる情報（個人情報）<br>(ii)保管・管理され、秘密性が保護されなければならない情報（個人データ） | 規制の対象となる者 | 公的機関から任命された電子システム提供者 |
| | 規制の対象となる者 | 電子システム提供者 | 規制の内容 | 保管技術が国内で使用できない場合を除き、国内に電子システム・電子データを管理、処理及び保存する義務 |
| | 規制の内容 | 情報通信大臣への移転先国、移転の相手方、移転日、移転理由、移転結果を報告する義務等の連携が必要 | | |
| | 個人データ保護法(案)[本文脚注63] | | 金融庁規則【金融分野】 | |
| | 規制の対象となる情報 | 個人データ | 規制の対象となる者 | ノンバンク金融機関、商業銀行等 |
| | 規制の対象となる者 | 個人データの管理者 | 規制の内容 | 国内保存義務 |
| | 規制の内容 | 越境移転は以下の条件のいずれかを満たす場合のみ可能<br>①移転先国の個人データ保護規制がインドネシアと同等以上であること<br>②移転先国との国家間同意の存在<br>③移転元・移転間の個人データ処理に係る契約の存在<br>④データ主体の同意 | | |

# 第３章　まとめ

DFFT研究会では、2021年11月2日に開催された第1回の会合以降、3回にわたって、データの越境移転に係る相互運用可能な枠組みについての議論を深めてきた。「信頼」に基づく自由な国際データフローのビジョン「Data Free Flow with Trust（DFFT）」のもと、必要な「信頼」を確保するための具体的な仕組みや制度を検討していくために、DFFT 研究会の検討対象は、抽象的な制度論や規範形成ではなく、「経済成長や社会的繁栄を持続していくために、必要なデータを越境移転させる」というゴールから逆算して障壁を特定し、それを解消する具体的な政策オプションを提案していくことである。

DFFT のビジョンを制度として具体化していくためには、データの越境移転に関して基本的な価値観を共有する国同士で、プライバシーやセキュリティ、知的財産の保護など、データの利活用によって生じる脅威を軽減する規制的要請を踏まえた上で、相互運用可能な仕組みを構築・提案していくことが重要である。また、「はじめに」でも述べたように、国際的なデータ流通を円滑にするためには、政府間の「信頼」のみならず、データのライフサイクルに関わる全てのステークホルダーの間に「信頼」が存在することが必要である。データのライフサイクルは、物理空間とサイバー空間の双方に拡張した膨大なネットワークに依拠し、そこには企業（データ利用主体、データのプロセッサー（クラウドプロバイダー）、ネットワークプロバイダー等を含む）、自然人、規制当局、国際機関など様々な主体が関わっている。したがって、DFFTの具体化が目指す国際的な仕組みは、政府間の「信頼」のみならず、ボトムアップな視座から、このような様々な主体の間に現在存在する障壁を特定し、それを解消することも射程に含めていくべきである。

本報告書では、企業などデータを利活用する主体が、データを越境移転させる際の障壁を特定する観点から、以下の 3 つの論点に焦点を当てた企業ヒアリングや各国の法令調査の結果をまとめている。

- 企業によるデータの収集・利用において、越境移転がどのように行われているのか（データのライフサイクル、ライフサイクルに関わるステークホルダー、越境移転のパターンの特定）
- 企業が越境移転の場面においてどのような障壁に直面しているのか
- 各国のデータ関連規制が主にどのような観点から行われているのか

まず、第1章では、データのライフサイクルを特定し、企業のヒアリングなどから収集された情報を比較可能な形で検証することで、データの越境移転に関する障壁の「見える化」を目指した。データが収集・生成、加工、分析、統合、と様々なイベントを経ていく過程、すなわちライフサイクルの中で、異なるステークホルダーが関わり、様々なパターンの「越境移転」が生じている。

そして、このデータのライフサイクルの中で、データの越境移転に対する何らかの障壁が存在することにより、企業のビジネスにおける選択肢が分岐していく。この分岐を、本報告書では「企業の要望」と「企業からみた課題」として整理している。データが各国の経済社会構造の中でどのように扱われ、越境移転をする際にどのようなステークホルダーが関わり、規制によるコストが誰にどのように転嫁され得るのかについて、このデータのライフサイクルに関わる全ての主体がある程度共通した理解を有することは、DFFT のビジョンの具体化を進めていくために必要な素地である。もちろん、このようなデータの利活用主体からみた「障壁」は、データに関するプライバシー保護やセキュリティなど領域国の正当な法益を確保するための制度も含まれ得る。そのため、本報告書では、データの取扱いに関する多種多様な規制ニーズと、データの国際的な共有が生み出す経済的・社会的価値を両立させる観点から、障壁自体の性質にも着目している。

データの越境移転について、企業がビジネスオペレーション上で日常的に直面する障壁としては、これまでは一部の国の法令が極めて広範囲のデータの持ち出しを制限するなど、各国間のデータガバナンスに関する根本的な方針の対立が注目されてきた。しかし、越境移転の具体的な状況を特定し、より掘り下げた調査を行うことで、法令の運用にかかる障壁など、国際的な政策協力やキャパビルなどを通して、ビジネスへの萎縮効果やオペレーションのコストを大幅に下げることが可能な事例も多く浮かび上がってきた。例えば、国内規制当局間のデジタルサイロなどに起因すると思われる過規制や、規制の具体的な要請・要件が多数の履行規則や解釈準則に依拠していることに起因する法的透明性の問題、それらが頻繁に変更されることに伴う法的安定性や関連する企業側の調査コストの問題、データの第三国移転に関するビジネス実態への理解不足に起因する問題、「安全」、「信頼」の国際的な共通理解の不足、あるいは地域や特定国におけるデータの取扱いに関する認証や標準の取得が煩雑かつ高額の費用が要求されることなどが挙げられる。

また、データの「越境移転」という用語が包有し得る様々な活動について、明確性が確保されていないという声もあった。企業ヒアリングの中で、伝統的な領域間の物品・サービスの移動（貿易）と観念しにくいが、ビジネスモデルに応じた様々な越境移転となり得る様々な状況が特定されている。

＜例＞

- 本社所属の社員が、出張先から本社のクラウドにアクセスしたら越境移転になるのか。本社が提供する VPN ネットワークを介した場合とそうでない場合で評価が変わるか。
- 社員をグローバルに採用している企業で、社員の所在地から業務上必要な情報が格納されているデータベースやクラウドのアクセス（同地域に蔵置されていない）は越境移転になるのか。
- 海外子会社の社員を含むオンラインの社内会議での資料共有は越境移転になるのか。

次に、現時点における「越境移転」の具体的な定義は、各国の法令解釈の問題に帰結すること等を踏まえ、第2章では、各国のデータ保護法制を中心とする規制制度について関連情報を整理した。なお、各国の規制制度といってもプライバシー保護法やセキュリティ法など目的の異なる法令がデータの越境移転に対して制限を設けていることから、比較が困難である場合もある。順次導入されつつある各国の規制制度において、越境移転規制の対象となる情報や越境移転が許容されるための要件に加え、国内保存・国内保管義務の名宛人や要件設定等にかかる規定ぶりに各々異なるところがあり、データの越境移転を行うグローバル企業における各国法令への対応コストは、近年ますます大きくなってきている。

そのような状況を踏まえ、多くの企業からはシンプルで国際的に通用する共通定義・分類（タクソノミー）を求める声も上がった。しかしながら、「はじめに」においても述べたように、データという存在自体が多面的な性質を持っており、目的や文脈によって様々な分類が可能である一方で、その境界線には常に解釈の問題が存在する。各国の規制制度においてその対象となるデータを「個人情報」と設定している法制も存在するところであるが、例えば個人情報と非個人情報を分類するに当たって、匿名化された情報であったとしても、一定の条件下で個人特定性を有していたり、他のデータと組み合わせることで個人の行動パターンなどを特定したりすることが可能である場合がある。また、国・地域によっては、暗号化された個人情報（ハッシュなど）を個人情報として定義上扱うこともある。他の代表的な分類である公的データと私的データの区分も、同様の問題をはらんでいる。このようなデータの性質上、シンプルで履行しやすい形で国際共通定義・分類を制定することは困難であるが、各国それぞれの定義・分類を明確にする努力は継続するべきであり、企業負担軽減の観点から、運用レベルでのハーモナイゼーションを確保するために検討を進めていくことが重要である。

以上の検討を踏まえ、DFFT研究会は、以下の5つの要素をDFFTの具体化の核となる領域として特定し、各領域で検討するべき要素を提案した。

### １）透明性の確保（Transparency）

本報告書で実施した企業ニーズの分析によって明らかになったのは、企業等によるデータの越境移転に対して、抑制的効果を持つ法令が一般法や業所管法など重複して存在すること、それらの規制の具体的な要請・要件が多数の履行規則や解釈準則に依拠すること、頻繁な改正などが報告されており、データの越境移転に関する規制及びそれらの運用について透明性が確保されていないといえる状況があることである。透明性の確保は、全ての政府とデータのライフサイクルに関わるステークホルダーに資することから、基本的な価値観を共有する国との間で、透明性確保に関する認識や課題を共有し、改善に向けた働きかけや国際協力の中身（情報共有、通報制度、ガイドラインやベストプラクティスの共有など）を検討していくことが求められるのではないか。

### ２）技術と標準化（Technology and Standardization）

透明性の欠如に並んで、データの越境移転に関して企業が置かれた状況として明らかになったのは、第三国へのデータの移転において、企業が確保することを要求されるプライバシー保護やセキュリティ保全について、個別具体的なビジネスの状況に照らし、どのような運用であれば十分なのか、企業にとって明確ではないことである。このため、プライバシーやセキュリティ等を確保していく上で目安となる、データの保存や分析その他のデータ処理に関する具体的な技術や規制遵守コストを引き下げる技術実装のあり方、そのような技術の実装にかかる標準の必要性などについて、国際的な理解と議論を喚起し、産業界を中心に、マルチステークホルダー間の連携強化と関与を求めていく必要があるのではないか。

### ３）相互運用性（Interoperability）

透明性の確保や技術･標準による運用の改善など、早急に対処が求められる課題と並行して、各国の様々な規制によって求められる保護基準の同等性や差分が明確ではないことは、データの越境移転における障壁として多くの企業が強調してきた。この相互性は標準化された技術によって担保することもできるが、二国間の個人データに係る相互認証や、第三者の認証機関による多数国間の認証スキームなど、様々な相互性にかかる試みもこれまで存在してきた。データの越境移転に関する各国の国内制度が違うことを前提に、「相互運用性」を確保していくための様々な政策オプションを調査していく必要があると考えられる。その際には、セキュリティやプライバシーの確保の観点から、国・地域別に取得が求められる認証が既に存在する場合もあるが、それらの基準の相互性の確保の可能性なども検討の射程に入れるべきではないか。

### ４）関連する制度との補完性（Complementarity）

DFFTの具体化に向けて、G7などの国際的な場で政策・制度の提言を目指していく視座からは、データの自由な越境流通にかかる既存の通商ルールや一般原則（G7 デジタル貿易原則など）、またプライバシーやセキュリティ分野等におけるデータの取扱いに関する議論を踏まえ、それらの取り組みとの間で相互補完的かつ調和した形で検討を進める必要があると考えられる。その前提として、DFFT研究会の検討要素として提案する「透明性」などは、通商法、個人情報保護法、セキュリティ法など、データの取扱いに関する様々なアプローチの全てに共通して必要とされる要素であるが、存在する障壁の全てを解決するものではない。特に第二回の研究会でも議論があったように、一部の国の規制では、企業にとって製品・サービスそのものの提供ができなくなるほど深刻な制限を課している、あるいは課している懸念があるものがある。DFFT はデータの越境移転を巡る様々な利害に対して、可能な限り調和的な解決法を模索するアプローチであるが、データの越境移転に制限的効果を持つ規制について、それ自体の是非を問う通商法などとも、本研究会で明確にしてきたDFFT具体化の前提（データのライフサイクルと多様な主体間に確保するべき信頼の性質など）や検討内容を共有し、共通の前提の下で議論を進めていくべきではないか。

### ５）DFFT 具体化の履行枠組みの実装（Implementation）

DFFT のビジョンについて賛同を得られた国の間で、DFFT に親和的な政策を推進していく協力枠組みのあり方を検討する必要があるのではないか。なお、このあり方は DFFT を具体化するための政策（例えば、透明性を確保するために、各国の法改正にかかる通報制度や各国の取り組みのレビューなど）にも依拠する。

最後に、2021 年 11 月に発足した DFFT 研究会では、3 回の研究会を通して、特に企業がデータを越境移転する際の「実際の国際データフロー」 と、そのフローに関わる様々な「主体」 を特定するとともに、越境移転に対して制限的な効果を持つ各国の法令を紹介し、このような企業が日常的に直面する主要な越境移転に対する障壁を明らかにした。次期の DFFT 研究会では、以上の５つの領域について、DFFT の精神にのっとり、国際データフローを実践的かつ現実的に確保していくために、このような障壁を解消する効果的な政策提言に向けた議論を深めていく。