経済産業省

データの越境移転に関する研究会

報告書

２０２２年2月２８日

ー 目　次ー

1．報告書のポイント

- 「Data Free Flow with Trust（DFFT）」のビジョンを制度として具体化していくためには、**基本的な価値観を共有する国同士が、プライバシーやセキュリティ、知的財産の保護などの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。
- また、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、企業、自然人、規制当局、国際機関など**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。
- このため、DFFTの具体化が目指す国際的な枠組みは、**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、以下の３つの論点に焦点を当て、企業ヒアリング及び各国の法令調査等の結果をまとめた。

① 企業によるデータの利活用において、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）

② また、企業がデータを越境移転させる場面においてどのような障壁に直面しているのか

③ 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

2．データのライフサイクルと越境移転における障壁

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

■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。

■データ管理方法

顧客から収集したデータは、一旦リージョンごとのクラウドに保存して、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される。また、エンジニア等の人材をグローバルに採用しているため、分析・開発作業等の際に、社内の「越境アクセス」が発生する。

データのライフサイクル

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。主なデータは、顧客の属性データ及び顧客の利用状況データの２つ。

B）企業の要望
- 開発拠点や本社等のクラウドに集約する、地域ごとのクラウドで管理するなどを市場環境に合わせて柔軟に選択できるのが望ましい。

C）企業から見た課題
- 国によってデータを域外移転する際の要件が異なり、同意の要件も用途によって異なる等から、定型的な対応も難しい。また、第三国提供の場合、移転先国の法令準拠も求められ、対応に苦慮。
- 法令が国毎に異なると、1国１拠点や越境前の処理対応が必要となるため、スタートアップや中小企業にとって参入障壁が高すぎる。

加工

A)データの状況
- 作業の効率化や法令遵守などの観点から、データの越境前にエンジニアが個人情報の切り分け等の処理を行う。

B）企業の要望
- 開発拠点や本社等のクラウドに集約する、地域ごとのクラウドで管理するなどを市場環境に合わせて柔軟に選択できるのが望ましい。

C）企業から見た課題
- 「個人情報」の定義や要件が法令本体だけなく、ガイドラインや申し合わせ等にまで及んでおり解釈が難しい。
- 収集データの増加すると、「個人情報」の該当判断が微妙になる。
- 国境を越えた複数リージョン間のデータ統合や越境データアクセスが「越境移転」に該当するか分からず、予防的措置が必要。

移転

A)データの状況
- データを開発拠点に集約。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、加工後のデータを保存する。

B）企業の要望
- 越境アクセスには情報通信コストがかかるので、開発等のリソースがある場所にデータを集約させたい。
- 提供サービスによって開発に「個人特定性」が必要か否かが決まる。

C）企業から見た課題
- 各国法令上、「個人特定性」の定義が分かりにくく、匿名化等しても、重要情報として規制対象になる懸念あり。
- 第三国から情報提供を受ける際の法令等の要件に対応するのが難しい。
- 複数リージョン間をまたいでビッグデータ化したくても、各国法令が異なる、その解釈が不透明等の理由から、踏み出せない。

2．データのライフサイクルと越境移転における障壁

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

■概要

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してグローバルに事業展開を行っている大企業が、海外のクラウドを利用してサービス提供しており、その一部業務を海外企業に委託（共同利用含む）している。

■データ管理方法

顧客のアプリ利用によって発生したデータは、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・サービスとの連携等に利用。ユーザーエクスペリエンスの向上等に使われるデータは、リージョン毎に収集・保存され、そこで利用・加工されるが、海外事業者に一部業務委託するために、越境アクセスもしくは越境移転が発生する。

データのライフサイクル

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。主なデータは、顧客の属性データ及び顧客の利用状況データの２つ。

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各リージョン内に保存し、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に直面している。

加工

A)データの状況

- 海外から調達したエンジニアが、各リージョン内にあるデータにアクセスして処理を行う。

B）企業の要望

- 当該業種では、専門性に沿った分業化が進み、ユーザーエクスペリエンスの観点からデータをリージョン内に保存したまま、海外に分析等の業務委託する可能性や、優秀なエンジニア確保のために、越境アクセスして作業を行う必要性が増加。

C）企業から見た課題

- 「越境移転」の条件が不明瞭。域外からのデータアクセスや社員が物理的に域外に移動してアクセス場合も該当するのか。
- 「第三国への越境移転」も定義が不明瞭。

移転

A)データの状況

- データを第三国へ越境移転する。

C）企業から見た課題

- 主要国の個人情報保護法制では、データの移転先国において、移転元国と同等の保護・管理体制の確保を要求。しかし、移転先国に法令整備の十分性や、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。
- 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。

2．データのライフサイクルと越境移転における障壁

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

（個人情報が含まれない場合）

■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。

■データ管理方法

現時点では、取得先で個別に保存されているが、今後、IoT経由で本社のクラウドサーバー等データをに集約し、利活用される予定。センサーから取得したデータは個人利用ではないIoT機器から収集されるため、個人情報を含まないが、セキュリティに係る情報として、越境移転が制限されることがある。

データのライフサイクル

生成・移転

A)データの状況・ライフサイクル

- 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。
- センサーから取得した情報を集約する。（現時点では取得先で個別に保存されているが、今後活用したい）

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、一カ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を、本社所在地にあるサーバーに直接転送したい。

C）企業からみた課題

- 「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。

2．データのライフサイクルと越境移転における障壁

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

（個人情報が含まれる場合）

■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、機器のオペレーションやそれに付随する稼働環境、エネルギー消費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。

■データ管理方法

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、機器によって多種多様データが収集可能であるため、越境移転の規制対象になり得る。これらの情報には機器の稼働上必要不可欠なものが含まれており、急な規制そのものや解釈の変更によって、一部サービス停止につながるリスクがある。

データのライフサイクル

移転

A)データの状況・ライフサイクル

- 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。
- センサーから取得した情報を集約する。IoTの性質上、データは直接本社か開発拠点に送信する。

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）企業からみた課題

- 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。

2．データのライフサイクルと越境移転における障壁
類型５：プラットフォームサービス・IaaSの提供

■概要
企業が提供するプラットフォーム上で、個人アカウントを作成し、顧客に様々なサービスを提供。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。当該プラットフォーム上では、顧客やインターネットから必要なデータを収集・蓄積し、分析・管理されとおり、分析されたデータは広告宣伝システム等に使用されることがある。

■データ管理方法
セキュリティの観点から分散管理を行っているもしくは行うことが望ましいと回答する一方、中には、顧客アカウントに紐付く情報については、法令遵守に係るコストの高さから、分散管理しないし、ビッグデータ化も行わないと回答する企業があった。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。

データのライフサイクル

生成・取得 （顧客データ）	生成・移転 （顧客のサービス利用情報）	生成・移転 （セキュリティ関連データ）
A)データの状況 ● 顧客がアカウントを作成。サービス提供に係る分析のために、顧客データや過去のクッキー情報や閲覧記録等を取込む。 ● データは現地で管理・分析するものと、本社・開発拠点に直接集約するものとある。	A)データの状況 ● 顧客のサービス利用により、サービス関連デやサポート関連データが発生。 ● これらのデータは「非個人情報」とみなし、越境移転して、本社もしくは開発拠点に集約。	A)データの状況 ● 顧客のサービス利用により、サービス生成データが発生。 ● これらのデータは「非個人情報」とみなし、越境移転して、本社もしくは開発拠点に集約。
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、分散管理が最善。 ● グローバルで対応するためには、シンプルな対応で、定義・分類等が明らかな制度が望ましい。	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、分散管理が最善。 ● グローバルで対応するためには、シンプルな対応で、定義・分類等が明らかな制度が望ましい。	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 ● 越境移転で制限されるデータの定義等が不明瞭であり、それによる不利益を企業に転嫁。 ● 個人情報の移転に係る条件は、国・地域ごとに異なるため、システム上も個別対応が必要。 ● 越境移転の条件が非常に複雑であるため、顧客に多種多様な同意を求める必要がある。 ● 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。	C）企業から見た課題 ● 越境移転で制限されるデータの定義等が不明瞭であり、それによる不利益を企業に転嫁。	C）企業から見た課題 ● 越境移転で制限されるデータの定義等が不明瞭であり、それによる不利益を企業に転嫁。

2．データのライフサイクルと越境移転における障壁

類型６　：サイバーセキュリティサービスの提供

■概要

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。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。

■データ管理方法

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個人情報を除去してから送信されるケースがある。情報の管理については、効率性の観点から一ヵ所に集約する方が望ましいが、事業継続性の観点から最低二箇所程度に分散管理し、常に情報が同期される必要あり。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。

データのライフサイクル

移転

A)データの状況・ライフサイクル

- 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・加工する。
- 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）企業からみた課題

- 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。また、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。加えて、英語で利用可能な情報が限られる国も多い。
- 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。
- セキュリティ関連情報の取扱いについては、グローバルな規定だけでなく、地域・国独自の認証の取得を要求されることがあり、取得等にかかるコストが多大である。

2．データのライフサイクルと越境移転における障壁（まとめ）

- 企業がビジネス上、越境移転の際に直面する障壁として、各国において、国内規制当局間のデジタルサイロ等によると思われる**規制の重複**、規制の具体的要請・要件が多層的に定められ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**法的安定性の問題**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**、**データの取扱いに関する認証の取得に多大なコストがかかる**こと、**「越境移転」の定義が明確になっていない国がある**こと、などがあげられた。

企業から見た課題（抜粋）

- 「個人情報」の定義や要件が、法令本体だけなく、ガイドラインや申し合わせ等にまで及んでいる国もあり、解釈が難しい。加えて、英語で利用可能な情報が限られる国も多い。（類型１、類型６）
- 各国の法令が異なることから、国境を越えた複・数リージョン間のデータ統合や越境データアクセスが「越境移転」に該当するか分からない。（類型１、類型２）
- 「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出てきているが、規制対象の範囲が極めて曖昧かつ、急な変更も増加している。（類型４、類型５）
- 「個人情報」以外のデータに関する規制が増え続けており、国内から持ち出すことを禁止する場合があるが、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。（類型３）

→ **透明性の確保 -Transparency-**

- 第三国へ越境移転時に、データの移転先国においても、移転元国と同等の保護・管理体制の確保を要求され、その責任が企業に課せられているため、対応に苦慮している（類型１、類型２）
- 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を標準化や定型化できないか。（類型４）
- セキュリティ関連情報の取扱いについては、グローバルな規定だけでなく、地域・国独自の認証の取得を要求されることがあり、取得等にかかるコストが多大である。（類型６）

→ **技術と標準化 - Technology and Standardization -**

3．各国データ関連規制の現状①

- 各国で順次導入されているデータ関連規制について、越境移転規制や国内保存・国内保管義務にかかる規定を整理した。**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、国内保存・国内保管義務の有無や内容といった各国法令における規定ぶりが国によって大きく異なっており、**グローバルに事業展開を行う**企業の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**状況。
- 一方で、「データ」という存在自体、多面的な性質を持っているため、目的や文脈によって様々な分類が可能でありながら、その境界線には常に解釈の問題が存在しており、シンプルかつ履行しやすい形で一般的なタクソノミー（定義・分類）することは困難。

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
EU	GDPR	個人データ（識別され又は識別可能な自然人に関する情報）	管理者又は処理者	可能（十分性認定）	可能（SCC、ad hoc契約）	可能	拘束力ある社内規程、公的機関の認証、契約の履行の確保、重大な公益・生命の保護等	個人情報保護法制上は、規制なし			
米国	個人情報保護法制上は、規制なし							個人情報保護法制上は、規制なし			
カナダ	個人情報保護法制上は、規制なし							個人情報保護法制上は、規制なし			

3．各国データ関連規制の現状②

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
中国	個人情報保護法	個人情報（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）	個人情報取扱者	他の手続（本人同意）と組み合わせて可能（※）	他の手続（本人同意）と組み合わせて可能（※）	他の手続（安全評価等）と組み合わせて可能	安全評価、法令の定めるその他の条件（※）	個人情報保護法	個人情報	①国家機関、②重要情報インフラ運営者、③一定数に達する個人情報の取扱者	国内保存義務・安全評価
										個人情報取扱者	国外の政府機関への提供につき主管機関の認可
	サイバーセキュリティ法	①個人情報（自然人の身分を識別可能な氏名等の情報）、及び②重要データ（国の安全、経済発展等に密接に関連するデータ）	重要情報インフラ運営者	（規定なし）	（規定なし）	（規定なし）	安全評価	サイバーセキュリティ法	個人情報及び重要データ	重要情報インフラ運営者	国内保存義務・安全評価
	データセキュリティ法	国の安全・利益や国際的義務の履行の維持に関連する管理品目のデータ	（規定なし）	（規定なし）	（規定なし）	（規定なし）	輸出管理	データセキュリティ法	重要データ	重要情報インフラ運営者	国内保存義務・安全評価
										その他のデータ処理者	別途法令で定める
		重要データ	重要情報インフラ運営者	（規定なし）	（規定なし）	（規定なし）	安全評価		（規定なし）	中国国内の組織又は個人	国外の政府機関への提供につき主管機関の認可
			その他のデータ処理者	（規定なし）	（規定なし）	（規定なし）	別途法令で定める				

※重要情報インフラの運営者又は取り扱う個人情報が一定数に達する個人情報取扱者に該当する場合には依拠不可

3．各国データ関連規制の現状③

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
インド	個人情報保護法制上は、規制なし							支払システム情報の保存に関する政令	支払システム情報（エンドツーエンドの取引詳細及び情報）	認可対象となる支払システムの提供者	国内のみでの保存義務
								電気通信分野における統一ライセンス法	サービス利用者の財務情報及び利用者情報	電気通信サービス事業者	国外への移転禁止
ベトナム	個人情報保護に関する政令案	個人情報（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）	個人情報に関係する機関、組織及び個人	他の手続（同意、国内保存等）と組み合わせて可能	（規定なし）	他の手続（国内保存、当局承認等）と組み合わせて可能	（規定なし）	サイバーセキュリティ法	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	ネットワーク上のサービス提供事業者	国内保存義務及び国内拠点設置義務
								政令72号	（規定なし）	オンラインサービス事業者	国内サーバー設置義務
インドネシア	2019年政令及び2016年省規則	個人情報（直接又は間接に個人を識別できる情報）及び個人データ（保管・管理され、秘密性が保護されなければならない情報）	電子システム提供者	（規定なし）	（規定なし）	（規定なし）	通信情報大臣との連携	2019年政令	（規定なし）	公的機関から任命された電子システム提供者	国内での管理・処理・保存義務
	個人データ保護法案	個人データ（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るべき情報）	管理者	（規定なし）	可能	可能	移転先国の規制の同等性、国家間同意の存在	金融庁規則	（規定なし）	ノンバンク金融機関、商業銀行等	国内保存義務

注：水色部分は法案段階のもの

４．まとめ

- これまでの検討結果を踏まえ、今後の検討方針として、以下の**DFFT具体化に向けて核となる５つの領域**を特定。

透明性の確保 – Transparency

データの越境移転に関する規制について、透明性確保に関する課題を共有するとともに、その改善に向けた国際協力の内容（例えば、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）の検討を行う。

技術と標準化 - Technology and Standardization

第三国へデータを移転する際にプライバシーやセキュリティ等を確保する上で、目安となるような技術や、その技術の実装に係る標準について、国際的な理解と議論を喚起し、産業界等のステイクホルダーに対して連携・関与を求める。

相互運用性 – Interoperability

データの越境移転に係る各国国内制度が異なることを前提に、既存の認証制度を含め、「相互運用性」を確保するための政策オプションの調査・検討を行う。

関連する制度との補完性 – Complementarity

データの越境流通に係る既存の通商ルールや一般原則に加え、プライバシーやセキュリティ分野におけるデータ取扱いに係る議論などとの相互補完的かつ調和した形で検討を進める。

DFFT具体化の履行枠組みの実装 – Implementation

DFFTのビジョンに賛同が得られた国との間で、例えば、透明性確保のため各国の法改正に関する通報制度や関連する取り組みに係るレビューなど、DFFTに親和的な政策を推進するための協力枠組みのあり方を検討する。