



RIETI Discussion Paper Series 24-J-007

データ・ローカライゼーションに関する考察： 企業に与える影響と政策目的を踏まえたアプローチを中心に

今野 由紀子

長島・大野・常松法律事務所



Research Institute of Economy, Trade & Industry, IAA

独立行政法人経済産業研究所

<https://www.rieti.go.jp/jp/>

データ・ローカライゼーションに関する考察：企業に与える影響と政策目的を踏まえたアプローチを中心に¹

今野由紀子（長島・大野・常松法律事務所）

要 旨

データ・ローカライゼーション措置は、国際的なデータ流通の問題の一つとして広く認識されており、今後データ量が増大するにつれて益々大きな問題になりうる。一部の新興国では、さまざまな政策ツールを用いてデータ・ローカライゼーション措置が提案されており、グローバルに事業を展開する企業にとって、経済的な負担を伴う課題となっている。本稿では、データ・ローカライゼーション措置の導入目的を整理し、その多様性を明示するとともに、企業への影響についても俯瞰する。また、データ・ローカライゼーションが必ずしも特定の政策目的に貢献しないことや、より制限的でない代替策が存在する可能性についても議論する。データ・ローカライゼーションに対する政策アプローチとしては、引き続き、通商ルールにおける関連規定との整合性を志向し、データ・ローカライゼーション政策の導入に厳格な姿勢を維持することの重要性に触れる。一方で、データ・ローカライゼーション措置がもたらす事業者への影響の観点から、政策目的を達成するための実効性について検証するとともに、より制限的でない代替案を示すことの重要性についても、提言する。

キーワード：デジタル、越境データ移転、DFFT、電子商取引、OECD、貿易協定

JEL classification: K22, K24, K33, L52, L88

RIETI ディスカッション・ペーパーは、専門論文の形式でまとめられた研究成果を公開し、活発な議論を喚起することを目的としています。論文に述べられている見解は執筆者個人の責任で発表するものであり、所属する組織及び（独）経済産業研究所としての見解を示すものではありません。

¹ 本稿は、独立行政法人経済産業研究所（RIETI）におけるプロジェクト「現代国際通商・投資システムの総合的研究（第VI期）」の成果の一部である。本稿の原案は、経済産業研究所（RIETI）のディスカッション・ペーパー検討会で発表を行ったものである。検討会参加者からの有益なコメントに感謝したい。また、本稿の作成にあたっては、川瀬剛志教授（RIETI／上智大学）、渡辺翔太様（株式会社野村総合研究所）から多くの有益なコメントを頂いた。ここに記して、感謝の意を表したい。なお、本稿の見解は筆者が所属する法律事務所の見解を示すものではない。

1. はじめに

データ・ローカライゼーションは、国際的なデータ流通の課題の一つであり、DFFT²の文脈において、ガバメントアクセスの問題と並ぶ重要なテーマとして広く認識されている。データ・ローカライゼーションの確立した定義はないものの、たとえば、特定のデータを特定の地理的範囲（自国であることが多い。）内において保存又は処理することを要求する措置をいう（なお、CPTPP³では、コンピュータ関連設備利用・設置要求という態様で規定されている（CPTPP 第14.13条）。）。

データ・ローカライゼーションは、各国の法令上、罰則を伴う法的拘束力のある義務として事業者には課せられることが多い。したがって、ガバメントアクセスの問題と比較しても、企業にとっては、より直接的な課題であると言える。そうであるにも関わらず、不公正貿易報告書⁴等一部の文書を除き、日本語でデータ・ローカライゼーション措置について分析した文献は多いとは言えない。

かかる状況を踏まえ、本稿では、データ・ローカライゼーションに関する基本的な内容を整理する。具体的には、データ・ローカライゼーションを取り巻く環境を概観した後（第2章）、データ・ローカライゼーションの定義と多様性（第3章）、データ・ローカライゼーション措置を導入する国・地域における政策目的（第4章）を整理する。その上で、データ・ローカライゼーションがもたらす企業への影響を考察し（第5章）、近年のデータ・ローカライゼーション措置の例として、ベトナム、中国、インドにおける例を紹介する（第6章）。次に、データ・ローカライゼーションに対するアプローチの在り方について私見を述べる（第7章）。最後に、貿易協定におけるデータ・ローカライゼーション措置として、CPTPP 及び日米デジタル貿易協定の例を挙げる。

他方で、日本政府がデータ・ローカライゼーションに関して行ってきた取り組みについては、本稿のメインテーマではないため、取り上げない。例えば、日本が議長国を務めた2023年のG7の議論を踏まえ、日本政府は、DFFTを具体化させるための新たな国際的な枠組み「Institutional Arrangement for Partnership (IAP、相互運用のための制度的取り決め)」の設立を目指していることを公表した⁵が、こうした日本の政策は詳しくは取り上げない。

2. データ・ローカライゼーションをとりまく状況

（1）2000年以降のデータ・ローカライゼーションの高まり

以下の表に示されるとおり、データ・ローカライゼーションを含むデータ流通規制は、増加傾向にある。OECDのデータによれば、2023年初めの時点で、40か国で96の関連する措置が採

² 信頼性のあるデータの自由な流通 (Data Free Flow with Trust)

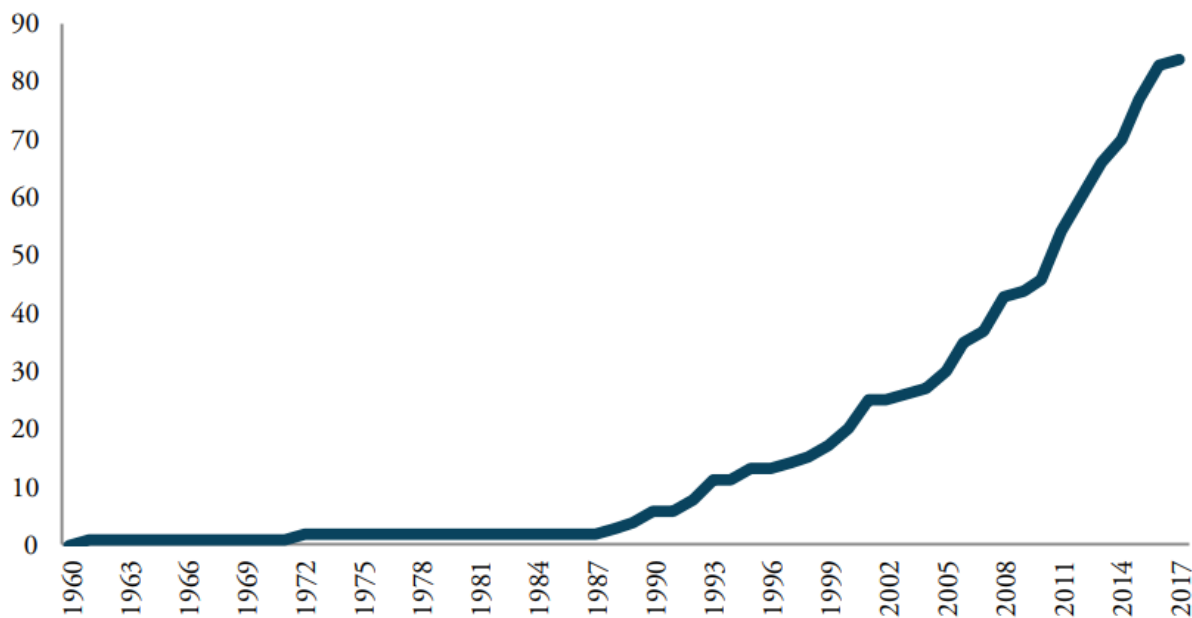
³ 環太平洋パートナーシップに関する包括的及び先進的な協定

⁴ 2023年版不公正貿易報告書 第二部補論デジタル貿易

https://www.meti.go.jp/shingikai/sankoshin/tsusho_boeki/fukosei_boeki/report_2023/pdf/2023_02_19.pdf

⁵ METI ジャーナルオンライン「G7の論点②「デジタル化」データの自由な流通と信頼を確保」（2022年12月21日）<https://journal.meti.go.jp/p/24752/>（2023年12月8日最終アクセス）

用されている⁶。データ・ローカライゼーションが各国で導入されたのは、2000 年以降からであると言われている。こうした 2000 年以降のデータ・ローカライゼーションの増加は、取引のクロスボーダー化、デジタル化（に伴うデータの越境移転量の増加）と密接に結びついている。今後、取引のデジタル化、AI といった振興技術の進展に伴い、ますます導入が加速される可能性がある。



図表 1：越境データ移転に対する規制の累積数（1960 年～2017 年）⁷

（2）国際的なデータ流通の重要性とその課題

ア 国際的なデータ流通の重要性

データ・ローカライゼーションは国際的なデータ流通促進における課題の一つである。ここで、データ・ローカライゼーションの検討に入る前に、データ流通の重要性について、コネクテッドカーとスマート建設機械の例をもとに、具体例を示してみたい。

i 自動車会社のコネクテッドカーの例

例えば、日本の自動車会社が海外でコネクテッドカーを展開する例では、データの国外移転が不可欠である。コネクテッドカーは、車両に搭載されたセンサーを通じて様々なデータを収集する。コネクテッドカーサービスを提供する事業者は、収集したデータ（走行データや車両識別番号、周囲の道路の状況など）を本社で一括管理し、事故の解析や、新しいビジネスの研

⁶ Del Giovane, C., J. Ferencz and J. López González (2023), "The Nature, Evolution and Potential Implications of Data Localisation Measures", OECD Trade Policy Papers, No. 278, OECD Publishing, Paris, <https://doi.org/10.1787/179f718a-en>.

⁷ Martina F. Ferracane (2017), "Restrictions on Cross-Border data flows: a taxonomy", ECIPE WORKING PAPER No. 1/2017, <https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf>.

究開発に利用するニーズがある。データの国外移転は、データの一括管理やサービスの向上をもたらすものであり、利用者にとっての利便性にもつながる。

ii 建設機械会社のスマート建機の例

次に、日本の建設機械会社が海外でスマート建設機械を展開する例でも、データの国外移転は不可欠である。センサーを搭載した建設機械は、様々なデータ（稼働情報、位置情報や消耗品の交換時期といった情報）を収集し、当該データにユーザーの本社所在地からアクセス・閲覧することで、ユーザーによる稼働管理やメンテナンス管理が実現される。このようなサービスを提供する企業にとって、データを国外に移転させることや、国外からアクセスすることが容易でなければ、他のサービスとの差別化を図ることができなくなる可能性もある。

このように、特に海外で事業（とりわけ IoT 製品やサービス）を展開する日本企業にとっては、データ流通の重要性が高まっており、データ量の増大とともに、今後ますますデータを国外に移転させることに関するニーズが高まると思われる。

しかし、データ・ローカライゼーション措置によって、進出先国から日本に事業活動において収集したデータを容易に持ち出せないという問題が生じている。

イ 国際的なデータ流通の課題

国際的なデータ流通に関する課題として近年特に注目されているものは、以下の二つである。

一つは、本稿のテーマである、データ・ローカライゼーションの問題である。近年では、中国、ベトナム、インドを含む国々が措置を導入している。特に、2021 年、中国ではデータセキュリティ法をはじめとするいわゆるデータ 3 法が制定され、同法の下位法令のもとで、コネクテッドカーが収集するデータを国外に持ち出すことが難しくなっていると言われる。

二つ目は、ガバメントアクセスの問題である。2022 年 12 月、OECD のデジタル経済政策委員会（CDEP）閣僚会合において、「民間部門が保有する個人データに対するガバメントアクセスに関する宣言」⁸が採択された。同宣言は、法的根拠や透明性といったガバメントアクセスに関する共通原則を盛り込んでおり、G7 広島サミットの首脳宣言においても言及された⁹。なお、データ・ローカライゼーションには第 3 章で後述する通り多様な措置を含みうるが、特に国内保存義務はガバメントアクセスの目的を達成するためのツールになりうるとも言われており、ガバメントアクセスとデータ・ローカライゼーションとは密接に関連していると言える。

3. データ・ローカライゼーションの定義と多様性

⁸ 個人情報保護委員会 https://www.ppc.go.jp/enforcement/cooperation/international_conference/OECD_0412/

⁹ G7 広島首脳コミュニケ（2023 年 5 月 20 日）39 パラ、<https://www.mofa.go.jp/files/100507035.pdf>（2023/12/08 最終アクセス）

(1) データ・ローカライゼーションの定義を論ずる必要性

現時点において、データ・ローカライゼーションに関する確立した定義はない。データ・ローカライゼーションに関する定義は多数の文書に見られるが、それらの多くは、「データの処理（保存を含む。）を自国領域内に限る措置」と定義している。他方で、データ・ローカライゼーションを国内保存要求と同義であるかのように議論したり、あるいは、条件付きでデータの越境移転を認める越境移転規制まで（広義の）データ・ローカライゼーションに含めるものも存在する。国内保存要求、すなわち、特定のデータを国内に保存することを要求する措置はデータ・ローカライゼーションの代表的な例であり、最もよく知られている措置と言えるが、国内保存要求はデータ・ローカライゼーションの一態様にすぎず、同義ではない。そこで、公表されている文書におけるデータ・ローカライゼーションの定義を紹介したうえで、本稿で前提とするデータ・ローカライゼーションについて言及する必要がある。

データ・ローカライゼーションに関する定義については、様々な文書において確認することができる。以下に、主なものを紹介する。

総務省 情報通信白書（平成30年度版）※3

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。

阿部教授※4

狭義のデータローカライゼーション措置とは、国家が自国内で行われる事業活動に関するデータを国内で保存することを要求したり（国内保存義務）、データを処理するサーバー等を国内に設置することを求めたりする規制（国内設備設置義務）を指す。他方で、広義のデータローカライゼーション措置には、狭義のデータローカライゼーション措置だけではなく、国民のプライバシー・個人情報を保護する目的で、それらのデータの越境移転を規制する措置も含まれる。

Svantesson, 2020

A mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction (和訳：特定の領域内でデータを保存又は処理することが、直接的又は間接的に、排他的又は非排他的に、義務付けられる法的又は行政上の要件)

CPTPP 14.13第十四・十三条コンピュータ関連設備の設置

2いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならない。

「コンピュータ関連設備」とは、商業上の利用のために情報を処理し、又は保存するためのコンピュータ・サーバー及び記憶装置をいう。

EU regulation on the free flow of non-personal data^{※1}

“data localisation requirement” means any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State;

(和訳:「データローカライゼーション要求」とは、特定の加盟国の法律、規制、又は行政規定に規定されているか、又は公共の法に基づく一般的で一貫した行政慣行から派生するか、又は公共調達分野を含む、Directive 2014/24/EUに影響を与えることなく、データの処理を特定の加盟国の領土内に義務付け、他のどの加盟国でのデータ処理を妨げるものである義務、禁止、条件、制限、その他の要件をいう。)

OECD, 2022^{※2}

An explicit requirement that data be stored and/or processed within the domestic territory

(和訳: データが国内領域内で保存及び/又は処理されるという明確な要件)

Cory and Dascoli, 2021

Forced local data-residency requirements that confine data within a country's borders, a concept known as “data localization”. (和訳: データを特定の国の境界内に制限する必要があるという強制的な要件)

総務省情報通信白書平成30年版は、サーバやデータ自体の国内設置・保存を求める規制とし、越境移転規制はデータ・ローカライゼーションに含まれないとしている。

これに対し、阿部克則教授¹⁰は、狭義のデータ・ローカライゼーションと広義のデータ・ローカライゼーションという概念を用いた上で、広義のデータ・ローカライゼーションには「データの越境移転を規制する措置」が含まれるとしている。

Svantesson 教授による定義¹¹は、データ・ローカライゼーション措置の態様を幅広くカバーした網羅的な定義である。例えば、定義に含まれる「exclusively or non-exclusively (排他的に又は非排他的に)」は、データの国外保存を認めないという排他的な措置と、国内にデータ(のコピー)を保存すれば、国外において保存・処理することを認める(非排他的な)態様をいずれも含む趣旨とも読める。また、「directly or indirectly (直接的に又は間接的に)」の文言は、直接的な国内保存・処理要求だけでなく、間接的に国内にデータを保存させる措置を含む趣旨と読める。いかなる措置が間接的な国内保存・処理要求に該当するかは明らかではないものの、例えば、データの国外移転(越境移転)を禁止したり、厳しい要件のもとでのみ越境移転を許容したりする措置がデータ・ローカライゼーションに含まれる可能性がある(越境移転規制の問題については、第6章(4)参照)。

CPTPP では、自国領域におけるコンピュータ関連設備の利用・設置要求という態様で言及され

¹⁰ 阿部克則 『データローカライゼーション措置と国際経済法上の規律 ―WTO と TPP における法的位置づけ―』(財務省財務総合政策研究所「フィナンシャル・レビュー」令和元年第5号(通巻第140号)2019年11月)
https://www.mof.go.jp/pri/publication/financial_review/fr_list7/r140/r140_03.pdf

¹¹ Svantesson, D. (2020), “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, OECD Digital Economy Papers, No. 301, OECD Publishing, Paris,
<https://doi.org/10.1787/7fbaed62-en>.

ている（CPTPP 第 14.13 条）。ここでいうコンピュータ関連設備（computing facilities）とは、商業上の利用のために情報を処理し、又は保存するためのコンピュータ・サーバー及び記憶装置と定義されている（CPTPP 第 14.1 条）。この定義は、データ・ローカライゼーションに関し、データを保管・処理するための設備に対する要求とする点で、データの国内保存・処理要求とする他の定義と異なっている。しかし、国内保存義務のように、国内のコンピュータ処理施設の設置が明文上義務づけられていない場合であっても、国内保存義務によって、結果として当該義務の対象となるデータを処理するための施設を国内に設置する（あるいは第三者が当該国内に設置した設備を利用する）必要が生じるため、このような文言上の違いによって、必ずしも有意な差が生じるとは考えられていない（データの国内保存・処理要求を導入する加盟国の措置と CPTPP との整合性が問題になる文脈においても、CPTPP14.13 条が問題になると考えられている。）。

EU 非個人データ流通規則（EU Regulation on the free flow of non-personal data¹²⁾）は、行政機関による事実上の要求も含まれ、幅広い態様を含む点で、Svantesson 教授による定義と同様である。定義上、国内保存要求は明示されていない（国内「処理」要求のみが明示されている）が、国内処理要求は国内保存要求を含むという整理であるように思われる。

López González ら¹³⁾の定義は国内保存要求及び国内処理要求を含む点で一般的であり、かつ、「明示的な要求」としていることから間接的な措置は含まれない。結果として、越境移転規制による間接的な国内保存要求を含まない可能性がある。

Cory による定義¹⁴⁾は、国内保存要求や国内処理要求といった態様を定義に含めていないことから、態様にかかわらず、広くデータを特定の領域に制限する措置を含みうる。

（２）データ・ローカライゼーションの多様性と分類

ア データ・ローカライゼーション措置の多様性

上記で紹介したデータ・ローカライゼーションの定義からわかるように、データ・ローカライゼーションの定義や規制態様は多様であり、国内保存要求や国内処理要求のみならず、自国内におけるコンピュータ関連設備（データを保存するためのサーバを含む。）の利用・設置要求とするもの、越境移転規制を含めるもの、さまざまある。

さらに、データ・ローカライゼーションに関する政策ツールとしては、法令上国内保存義務のように法的拘束力を伴う形で義務づけられる場合が多いが、許認可を付与する要件として課されるといった、行政機関による要求（administrative requirements）であることもある。

¹²⁾ REGULATION (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>

¹³⁾ López González, J., F. Casalini and J. Porras (2022), "A Preliminary Mapping of Data Localisation Measures", OECD Trade Policy Papers, No. 262, OECD Publishing, Paris, <https://doi.org/10.1787/c5ca3fed-en>.

¹⁴⁾ Cory, Nigel & Dascoli, Luke. (2021) "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>

イ データ・ローカライゼーション措置の分類

データ・ローカライゼーションの多様性を踏まえ、データ流通に対する制約となりうる措置（このうち、本稿においてデータ・ローカライゼーション規制に分類されるもの）¹⁵のバリエーションは大きく以下のように整理することができる。

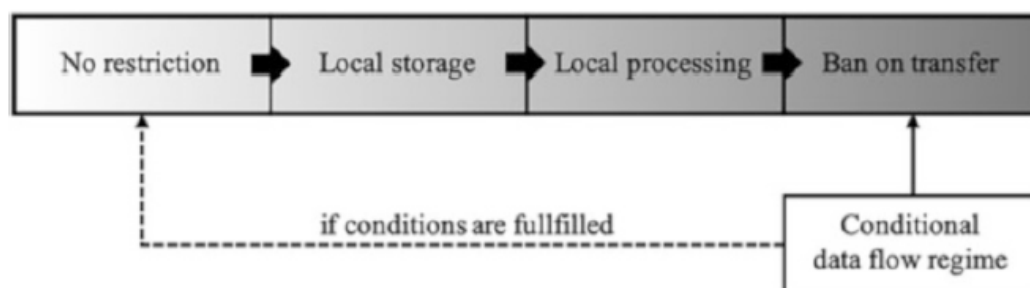


Fig. 4.1 Taxonomy for restrictions on transborder data flows

図表 2 越境データ流通に対する制約の分類（出典：Tobias Naef, “Data Protection without Data Protection The right to protection of personal data and data transfers in EU law and international trade law”（2023 年））

一つ目は、国内保存（Local Storage）要求であり、データの保存場所を指定するものである。これは、データのコピーを国内に保存すれば、国外に移転し、処理することを認める場合を念頭に置いている。

二つ目は、国内処理（Local Processing）要求であり、データの（主要な）取扱い場所を指定するものである。一般的に、「保存（storage）」よりも処理「(processing)」の方が概念としては広いと考えられており（例えば、欧州一般データ保護規則（GDPR）では、「処理」

（processing）は、保存（storage）だけでなく、使用、編集、変更といった幅広いデータの取扱いが含まれる。GDPR4 条(2)号参照）、国内保存要求よりも厳しい制約であると考えられる。国内保存要求はデータのコピーを国内に保存すれば、国外に移転し、処理することを認める場合を念頭に置いていたが、国内処理要求の場合には、国外における処理は認められない場合を念頭に置いている。なお、国外処理禁止措置と、国外にデータを移転することを禁止する、越境移転禁止規制との区別についてはどのように考えるべきかが問題になる。これについて明示的に議論された文献は見当たらないが、国内処理要求は、（国内処理要求における「処理」の内容及び定義次第ではあるものの）国外からのアクセスまでは禁止されておらず、他方、越境移転規制は、国外からのアクセスも禁止されるという違いが一般的に考えられる。

なお、国内保存・処理要求は、データの保管や処理に対する地理的制約ではなく、自国内におけるコンピュータ処理設備（サーバを含む。）の利用・設置要求という形態をとることもある。

¹⁵ データ流通に対する制約には、条件付きで越境移転を認める規制（越境移転規制）も含まれうるが、制約の大きさの観点からは同等に論じる必要はないため、本稿では含めていない。

三つ目は、越境移転「禁止」規制である。二つ目の国内処理要求と越境移転禁止規制とは、一見すると後者がデータ流通を直接禁止する効果を伴うものであり、越境移転禁止規制を国内処理要求の延長と捉えることについて議論の余地がありうる。しかし、前述したとおり、国内処理要求は、国外における処理を認めないことの裏返しとして、データを国外に移転することを事実上禁止する措置を念頭に置いている（両者の違いは、国外からのアクセスを禁止する効果を伴うかどうかの違いにしか存在しない場合もある）ことから、データ流通に対する制約としては、連続的なものとして整理することも可能と思われる。

ウ 条件付きで越境移転を認める規制（越境移転規制）

上記のとおり、条件付きで越境移転を認めるものについてもデータ・ローカライゼーションの一部として整理する見解もある。条件付きで越境移転を認める措置の代表例は、個人情報保護法第 28 条のいわゆる越境移転規制である。

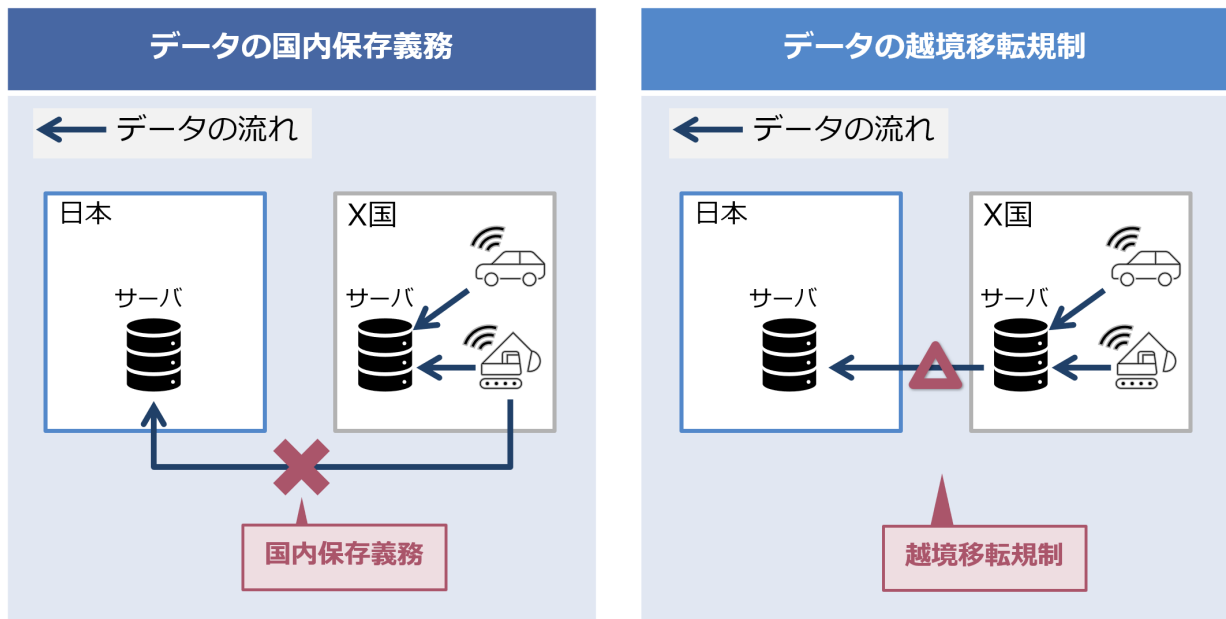
しかし、個人情報保護法や GDPR にみられるいわゆる越境移転規制は、上記イで述べた規制（すなわち、国内保存要求、国内処理要求、越境移転禁止措置等）とは異なり、条件付きで越境移転を認めるものであるため、当該条件が客観的であり、かつ、必要最小限であると認められる限りは、上記で述べた規制に比べてデータ流通への制約が大きいとは言えない。

他方、当該条件が恣意的で予見可能性が低いものについては、事実上の越境移転禁止規制と評価できる場合がありうる。例えば、越境移転が当局による許可制であり、客観的な許可基準が定められておらず、当局に与えられた裁量の幅が広い場合には、事実上の越境移転禁止措置に相当するとして、データ・ローカライゼーションに分類されるという議論もあり得ると思われる。しかし、後述するように、中国データ 3 法における越境移転規制の一部についてそのような懸念はあるものの、事実上の越境移転禁止措置に相当するかどうかは、今後示される越境移転の要件に関する細則や、実際の運用状況によるため、現時点でそのような評価を下すことは困難である。このように、事実上の越境移転禁止措置と条件付きで越境移転を許容する規制を区別する明確な基準を設けることは現時点では難しいことから、越境移転規制については一律に本稿の対象としない。

（3） 本稿が対象とするデータ・ローカライゼーション措置

上記を念頭におき、本稿でいうデータ・ローカライゼーションは、国内保存要求や国内処理要求を含むが、越境移転規制（条件付きで越境移転規制を認める措置）を含まない前提で議論する。他方で、越境移転の条件を充足するかどうかについて当局の大幅な裁量が認められるなどの理由で、予見可能性を欠く場合には、事実上の越境移転禁止措置となる場合がある。今後、このような事実上の越境移転禁止措置をデータ・ローカライゼーションに含めて（あるいはデータ・ローカライゼーションと同列に）論じることにも検討に値する。

（４）データの国内保存義務と越境移転規制のイメージ



図表 3：データの国内保存と越境移転規制のイメージ

出典：総務省

（<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc123120.html>）をもとに筆者作成

国内保存義務と越境移転規制を明確に区別することは難しいが、わかりやすさの観点から、イメージを示しておきたい。

図表 3 の左側は、国内保存義務を示している。「X 国に所在するコネクテッドカーが収集したデータを、X 国内のサーバに保存しなければならない。逆に、日本のサーバに保存してはいけない」とする要求が、国内保存義務である。

次に、図表 3 の右側は、越境移転規制を示している。「X 国に所在するコネクテッドカーが収集したデータを、X 国の現地法人のサーバから、日本の親会社のサーバに移転してはならない」とする要求が、越境移転規制である。越境移転については、越境移転禁止措置と、条件付きで越境移転を認める場合があり、後者は、条件の内容や運用によってはデータ流通に対する過度な制約とはならないこともある。そのため、越境移転禁止と越境移転に条件を付す場合とで区別することも必要な場合がある。一方で、第 6 章（４）で述べるとおり、実務上これらを区別することが困難である場合もある。

4. データ・ローカライゼーションの政策目的（導入目的）

（1）OECD による整理

データ・ローカライゼーションを導入する政策目的は、様々である。この点、OECD が 2022 年 6 月に公表したマッピング資料¹⁶が詳細に整理しており、参考になる。

プライバシー・ 個人情報保護	政府は、国内のプライバシーとデータ保護の原則、および個人の権利が尊重される手段として、データの国内保存を要求することがある
法執行・監督目的	政府は、規制目的を達成するため、情報へのアクセスを確保するために、データを国内で保存することを義務付けることがある。例えば、税務当局が税務目的に必要な情報にアクセスできるようにしたり、電気通信、銀行、または保険規制当局が当該セクターの活動を監督するために必要な情報を提供できるようにする
国家安全保障	政府は、国家安全保障の観点から機密と見なされる情報を保護する手段としてデータのローカライゼーションを求めることがある。これは、国家安全保障機関によるデータへのアクセスとレビューを可能にするため、または信頼されていない機関や政府からのデータへのアクセスを防止または保護するためである
セキュリティ	データは、国内で保存・処理される場合に最もその安全性が保証される
国内産業保護	いくつかの国では、デジタルと密接に関連するセクターでの国内の能力を開発するのにデータ・ローカライゼーション措置が役立つと考えられており、産業政策やデジタル保護主義の文脈で推進されることがある

（2）データ・ローカライゼーション措置国における整理—インド

¹⁶ López González, J., F. Casalini and J. Porras (2022), "A Preliminary Mapping of Data Localisation Measures", OECD Trade Policy Papers, No. 262, OECD Publishing, Paris, <https://doi.org/10.1787/c5ca3fed-en>.

OECD の整理のほか、実際にデータ・ローカライゼーション措置を導入している国において、どのように政策目的が整理されているかについては、(少なくとも英語で公表されている範囲では) 資料が少ない。

2017 年 12 月、インド政府は、個人情報保護法案の起草時に立ち上げたインドデータ保護フレームワークに関する有識者委員会が作成したホワイトペーパー¹⁷を公表し、意見公募手続を実施した。同ペーパーでは、データ・ローカライゼーションに関係する政策目的を①データ主体の権利保護、②他国のガバメントアクセスからの保護、③法執行・国家安全保障のためのデータへの容易なアクセスの 3 つに整理しており、参考になる。注目すべき点としては、外国政府によるガバメントアクセスからの保護が含まれている点である。

Protecting Rights of Data Subjects (データ主体の権利保護)	Enacting a data localisation law may help in ensuring the protection of the rights of data subjects in some circumstances. (和訳: データの国内保存は、データ主体の権利保護に役立つことがある)
Preventing Foreign Surveillance (他国のガバメントアクセスからの保護)	- One of the primary reasons for enacting a data localisation law is to prevent foreign surveillance. - It is grounded in the belief that placing data abroad would allow foreign governments to impinge upon the privacy and security of the data of domestic nationals. - This has led to some countries attempting to keep data from leaving their shores, in order to protect it from falling into the hands of other governments. - While, a data localisation mandate may be effective in reducing foreign surveillance as data will be stored locally, such a mandate may increase the risk of local surveillance by law enforcement agencies. (和訳) - データ・ローカライゼーションを定める主な理由の一つは、(外国政府による) ガバメントアクセスを防ぐことにある

¹⁷ White Paper Of The Committee Of Experts On A Data Protection Framework For India,
https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

	- これは、データを国外に置くことにより、外国政府が国内の国民のデータのプライバシーやセキュリティを侵害する可能性があるという考えに基づいている - こうした考えにより、一部の国はデータが自国を離れないようにしようとし、他国の政府の手に落ちることを防ごうとしている - データ・ローカライゼーション要求は、データが国内に保存されるため、外国政府によるガバメントアクセスを減少させる効果があるかもしれないが、同時に法執行機関による現地のガバメントアクセスのリスクを増加させる可能性がある
Easy Access of Data in Support of Law Enforcement and National Security (法執行・国家安全保障のためのデータへの容易なアクセス)	Currently, jurisdictional claims against foreign entities are enforced through Mutual Legal Assistance Treaties. The presence of personal information in the territory of a country could trigger the territorial basis for jurisdiction, thus giving additional powers to police and other law enforcement agencies. If data is locally stored in India, enforcement agencies will have access to a larger pool of data. This data could aid counter-terrorism efforts and may help protect national security. Further, local storage of data will ensure easier access to data in contradistinction to foreign storage of data wherein the sovereign power may choose not to grant access to Indian law enforcement agencies. (和訳) 現状、外国の事業者に対する管轄権は、刑事共助条約（MLAT）を通じて行使されている。ある国の域内に個人情報が存在することが、当該領域内の管轄権を生じさせる可能性があり、それにより警察その他の法執行機関に権限が与えられる可能性がある データがインド国内で保存されている場合、インドの法執行機関はより多くのデータにアクセスできる。このデータはテロ対策の取り組みを支援し、国家安全保障を守るのに役立つ。さらに、国外に保存されるデータに対し、インドの法執行機関がアクセスを許可されない可能性がある

が、国内に保存される場合には、データへの容易なアクセスを確保することができる

5. データ・ローカライゼーションが企業に及ぼす影響

データ・ローカライゼーション措置は、企業にどのような影響を及ぼすか。以下のとおり、企業にとっては、データセンター設置費用とセキュリティへの懸念が大きいといわれることが多い。

(1) データセンター設置費用

データ・ローカライゼーション措置、特に国内保存・処理要求の帰結として、事業者は、自らデータを保存するためのサーバを当該国に設立したり、当該国のローカルベンダーを起用する（あるいは、市場から撤退する）ことを余儀なくされる。

筆者が経済産業省の職員として実施した企業ヒアリングにおいては、ある日系企業から、中国におけるデータセンター設置費用の試算を行ったところ、2桁億円を要することがわかったという報告を受けた。また、マスターカードはインドのデータセンターの建設費用に350百万USドル（約500億円）を投じると報じられている¹⁸。さらに、アマゾンのように大規模かつ大量にデータを処理する事業者の場合、データセンターの開発コストは8億USD規模（約1,100億円）にのぼるとの分析もある¹⁹。

(2) セキュリティ上の懸念

ある進出先国において国内保存要求が課せられる場合、当該国で収集したデータは、第三国で収集したデータと別の場所で保管することを余儀なくされる。その場合、セキュリティ投資が増加するだけでなく、データの保存場所が追加されることによって新たなセキュリティホールとなり、サイバー攻撃の対象になるリスクが想定される。また、分散管理によるインシデント時の早期回復が困難になる。さらに、セキュリティ対策としてローカルベンダーを起用しなければならないことによって、セキュリティ対策が十分に講じられない事態も想定される。

(3) 事業継続性に与える影響

第2章(2)で紹介したとおり、コネクテッドカーやスマート建設機械を海外展開する企業は、進出先国において収集したデータを国外でも利用できることが、自社製品・サービスの不可欠の要素となっていることがある。国内保存義務や国内処理義務は、こうした国外におけるデータの

¹⁸ The Times of India, “Mastercard to invest \$1 billion in India” (May 7, 2019)
<https://timesofindia.indiatimes.com/business/india-business/mastercard-to-invest-1bn-in-india/articleshow/69208868.cms>

¹⁹ Institute of International Finance, “Data localization: costs, tradeoffs, and impacts across the economy” (December 2020)
https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf

取扱いを制限することにつながり、自社製品の国際競争力（特に、現地企業との競争における優位性）が限定的となる懸念がある。

（４）個人情報保護法との抵触

令和２年個人情報保護法改正では、個人データ国外移転時の情報提供義務が課され、提供先国における国内保存義務に係る制度がある場合には、当該制度について情報提供することになった²⁰。改正時の議論では、データ・ローカライゼーションによる影響として、「例えば、データ・ローカライゼーション政策との関係から、本人による個人データの消去の請求に越境移転先の事業者が対応することができないおそれ」が指摘されている²¹。

６．諸外国のデータ・ローカライゼーション²²

以下では、諸外国において導入・検討されたデータ・ローカライゼーションのうち、とりわけ 2017 年以降に導入・検討された比較的新しい措置について紹介する。

（１）ベトナム

ベトナムはサイバーセキュリティ法において、国内保存義務を定める。サイバーセキュリティ法 26 条には、以下の国内保存義務に関する定めがある。

Article 26. Guarantees relating to information security in cyberspace

3. Domestic and foreign service providers on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [cyberspace service providers] carrying out activities of collecting, exploiting [using], analysing and processing data [being] personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a [specified] period [to be] stipulated by the Government. Foreign enterprises referred to in this clause must have branches or representative offices in Vietnam.

4. The Government shall provide detailed regulations on clause 3 of this article.

（仮訳）

第 26 条 サイバースペースにおける情報セキュリティに関する保証

²⁰ 個人情報保護法 28 条 2 項、個人情報保護法施行規則 17 条 2 項 2 号、ガイドライン（外国にある第三者提供編 5-2(2)（エ）の事例 2 参照。

²¹ 個人情報保護委員会「個人情報保護法いわゆる 3 年ごと見直し制度改正大綱」第 3 章第 6 節 3。

https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf

²² なお、日本においても法的拘束力を伴わない形でデータの保管場所に関する留意点が定められている例がある。具体的には、「医療情報システムの安全管理に関するガイドライン第 6.0 版」に関する Q&A 44 頁、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 1.1 版」51 頁、「政府機関の対策基準策定のためのガイドライン」（令和 5 年度版）143 頁、170 頁等がある。

3. ベトナムのサイバースペースにおける電気通信ネットワークおよびインターネット、その他の付加価値サービスを提供する国内外のサービスプロバイダー（以下、「サイバースペースサービスプロバイダー」という。）は、ベトナムにおける個人情報、サービス利用者の関係性に関するデータ、およびサービス利用者によって生成されたデータの収集、利用、分析、又は処理の活動を行う場合、政府が定める一定期間は、これらのデータをベトナムに保存しなければならない。本条項において言及される外国企業は、ベトナムに支社または代表事務所を置かなければならない。

4. 政府は、本第3条に関する詳細な規定を提供する。

サイバーセキュリティ法上、当該義務の詳細は政令で定めることとされており（同法26条4項）、これを受けて2022年8月に制定された政令53号（Decree 53/2022/ND-CP）は、ベトナムにおいて設立されオンラインサービスを提供する事業者（国内事業者。日本企業のベトナム子会社を含む。）に対して、無条件にかつ幅広くデータ・ローカライゼーション義務を課すものになっている。なお、外国事業者については、その提供するサービスが違反行為に利用された場合など例外的な場合に限って国内保存義務が課せられることになった²³が、上記国内事業者には日本企業のベトナム子会社を含むこととなっているため、例えば日本企業のベトナム法人がオンラインEコマース事業を行う場合には、特定のユーザーデータをベトナムのサーバに保存しない限り罰則の対象となりうる。

なお、ベトナムでは、2023年7月に個人情報保護政令が施行開始した。同法は2021年公表時の草案では、越境移転時の条件としてデータ・ローカライゼーション（データの国内保存義務）を要求していたが、成立した個人情報保護法では、この国内保存義務は削除された点が注目される。

（2）中国

中国では、いわゆる中国データ3法のもとで国内保存義務が化せられているが、国内保存義務の対象者の範囲及び当該義務の対象となるデータの範囲それぞれについて、予見可能性が低いことが指摘されている。

2021年8月、中国では初の個人情報保護法が成立し、同年11月から施行開始した。2021年9月からは、データ安全法（データセキュリティ法とも呼ばれる。）が施行されている。これら2つの法律が成立したことにより、2017年6月から施行されているサイバーセキュリティ法（「ネットワーク安全法」とも呼ばれる。）とあわせて「中国データ3法」などと呼ばれ、中国のデータ保護法制が整ったと言われている。この中国データ3法において、データ・ローカライゼーション措置が定められている。

²³ すなわち、特定の規制業種（電気通信サービス、電子商取引を含む。）を営む場合で、かつ、当局、その提供するサービスがサイバーセキュリティ法の違反行為に利用されたことを通知し、当局への協力等を要請したにもかかわらず、外国事業者がこれに従わない場合等に限られる。

ア サイバーセキュリティ法における国内保存義務

サイバーセキュリティ法（2017年6月）はネットワーク安全法とも呼ばれるように、ネットワークの保護を目的とした法律である。具体的には、ネットワークをサイバー攻撃や物理的な破壊、データ漏えい、改ざん、滅失、不正利用などから保護することを意味する。サイバーセキュリティ法は、ネットワークを保護することを基本に、特に重要なネットワークに関するものを「重要情報インフラ」と定義して規制を強化している。そのため、「重要情報インフラ」の運営者に対して義務が加重される仕組みをとっている。

重要情報インフラの義務は主に3つあるが、その1つが「個人情報」及び「重要データ」の国内²⁴保存義務である。サイバーセキュリティ法 37 条は以下のとおり定める。

第 37 条 重要情報インフラ運営者が中華人民共和国国内での運営中に収集及び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。（略）

イ 個人情報保護法上の国内保存義務

個人情報保護法においても、重要情報インフラの運営者に対して個人情報の国内保存義務が課されている（個人情報保護法 40 条）。サイバーセキュリティ法は、個人情報に加えて、「重要データ」についても国内保存義務が定められているという違いがある。

個人情報保護法

第 40 条 重要情報インフラ運営者及び処理する個人情報が国家インターネット情報部門が規定する数量に達した個人情報処理者は、中華人民共和国国内で収集及び発生した個人情報を国内に保存しなければならない。（略）

上記のうち、個人情報の内容についてはガイドライン等により明確化されているため、「重要情報インフラ」と「重要データ」の内容が企業の関心事になっている。

「重要データ」は、ひとたび改ざん、破壊、漏えい又は不正取得、不正利用がされた場合、国家安全、公共利益に危害を及ぼす可能性がある電子的データ」をいう（情報安全技術重要データ識別ガイドライン（2022 年 1 月 13 日付意見募集稿）参照）。具体的には政府機関が定義することとされているが、現時点では重要データの目録や識別について定めた国レベルの法令・ガイドライン等は公開されていない。この例外として、国内保存義務の対象となる自動車関連のデータについてはデータセキュリティ法の下位法令である「自動者データセキュリティ管理の若干規定（試行）」（2021 年 10 月）において定義されている。また、工業情報化分野についても「工業情報化分野データセキュリティ管理弁法」（試行）で工業情報化分野の重要データが定義されている。

²⁴ 香港、マカオ、台湾を含む。

「重要情報インフラ」とは、「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、電子行政、国防科学技術工業等の重要業界及び分野の、並びにその他のひとたび破壊、機能喪失またはデータ漏えいを受けた場合に、国の安全、国の経済と人民の生活、公共の利益を著しく脅かすおそれのある重要ネットワーク施設、情報システム等」をいうとされている（重要情報インフラ保護条例）。業界及び分野ごとの主管機関等が所管の重要情報インフラを認定し、事業者に通知することとされたため、今後の運用次第では、予見可能性が担保されたとも言える。また、列挙されている産業は、エネルギーや水利、公共サービスなど中国の重点産業分野として外商投資が制限されている場合が多いため、日本企業を含む外国企業が「重要情報インフラ」の運営者に該当する場面は実務上限定的と思われる。もっとも、これらは限定列挙ではないため、国が今後追加的な分野を指定する余地がある。現に、2021年10月に施行された「自動車データセキュリティ管理の若干の規定」によって、外商投資が必ずしも禁止されていない自動車関連産業に対して「重要情報インフラ」運営者と同等の義務（国内保存義務等）が課せられているなど、今後の業種別の指定に留意する必要がある。

ウ データセキュリティ法上の国内保存義務

データセキュリティ法上、明文の国内保存義務の定めはない。しかし、同法の下位法令において、特定の産業分野のデータが国内保存義務の対象となっているものがある。例えば、「自動車データセキュリティ管理の若干規定（試行）」（2021年10月）においては、自動車関連の重要データが国内保存義務の対象とされている（同規定11条）。

中国における国内保存義務の問題点としては、誰が対象であり、どのデータが対象となるかについて未だ詳細な下位規則やガイドラインが公表されていないため、予見可能性が低い点が挙げられる。

（3）インド

インド準備銀行の通知（Reserve Bank of India's Directive 2017-18/153（2018年4月6日））において、国内保存義務の定めがある。

2. It is observed that not all system providers store the payments data in India. In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries/ third party vendors and other entities in the payment ecosystem. It has, therefore, been decided that:

i. All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the

transaction, if any, the data can also be stored in the foreign country, if required.

(和訳)

システムプロバイダーのすべてが支払いデータをインドに保存していないことが確認されている。より効果的な監視を確保するために、これらのシステムプロバイダーが保存するデータに対して制約のない監督アクセスを持つことが重要である。そのため、以下のことが決定された：

- i. すべてのシステムプロバイダーは、自らが運営する支払いシステムに関連するすべてのデータがインド内のシステムに保存されることを確保しなければならない。このデータには、メッセージや支払い指示の一部として収集、運搬、処理される完全なエンドツーエンドの取引詳細/情報が含まれる。取引に外国の要素を含む場合、必要に応じ、当該データを国外保存することができる。

すべての支払いシステムに関するデータを対象としていることから、システムの脆弱性に関する情報も国内保存しなければならない可能性がある。その結果、インシデントを検知した場合に、インドの支払いシステムについて対応するのが遅れる恐れがある。

(4) 越境移転規制の問題

本稿でいうデータ・ローカライゼーションは、国内保存要求や国内処理要求を含むが、越境移転規制（条件付きで越境移転規制を認める措置）を含まない前提で議論することは前述した。他方で、越境移転規制といっても、条件を充足するかどうかについて当局の大幅な裁量が認められるなどの理由で、事業者にとって予見可能性が著しく低いような場合には、事実上の越境移転禁止措置に相当すると評価しうるケースも考えられる。この点、中国サイバーセキュリティ法は、重要情報インフラ運営者に対し、国内保存義務に加えて個人情報越境移転時に政府による安全評価を実施する義務を課しており、日本の個人情報保護法やGDPRと異なり、政府による許可制となっていることから、以下でその概要と問題点について説明する。

中国サイバーセキュリティ法（2017年6月）第37条

重要情報インフラ運営者が中華人民共和国国内での運営中に収集及び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、国外提供の必要が確かにある場合には、国家ネットワーク情報部門が国务院の関係部門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規程がある場合には、当該規程に従うものとする。

中国サイバーセキュリティ法上、「重要情報インフラ」の運営者は、一定の場合を除き、政府の安全評価を受けなければ国外に重要データ及び個人情報を提供することができないこととされている。

また、個人情報保護法は、個人情報を国外移転する際の越境移転規制を定める。対象となる事業者のうち、重要情報インフラ運営者及び「処理する個人情報が国家インターネット情報部門により定められる数量に達した個人情報処理者」に対しては、国内保存義務に加えて個人情報越境移転時に政府による安全評価を実施する義務を課している（個人情報保護法 40 条後段）²⁵。なお、中国においては、国外から中国国内²⁶に保存された個人情報にアクセスする場合（アクセス権限を有する場合を含む。）には、個人情報が物理的に国外に転送されなくても、越境移転に該当することとされている²⁷。

中国個人情報保護法（2021 年 11 月施行）第 40 条

重要情報インフラ運営者及び処理する個人情報が国家インターネット情報部門が規定する数量に達した個人情報処理者は、中華人民共和国国内で収集及び発生した個人情報を国内に保存しなければならない。国外に提供する必要がある場合、国家インターネット情報部門が組織した安全評価を通過しなければならない。法律、行政法規及び国家インターネット情報部門が安全評価を行わなくてもよいと規定している場合、その規定に従う。

サイバーセキュリティ法及び個人情報保護法等の下位法令に基づき、越境移転時の安全評価が必要な場合は、以下のとおりとされている（データ越境移転安全評価弁法 4 条）。

①重要データを中国国外に提供する場合

②重要情報インフラ運営者又は 100 万人以上の個人情報を扱っているデータ処理者が個人情報を中国国外に提供する場合

③前年 1 月 1 日から起算して、累計 10 万人以上の個人情報または 1 万人以上の機微な個人情報を中国国外に提供しているデータ処理者が個人情報を中国国外に提供する場合

④主管当局が定めるデータ越境移転安全評価の申告が必要であるその他の事由がある場合

政府機関による安全評価項目は 2022 年 9 月施行の「データ国外移転安全評価弁法」において規定されている²⁸が、中国の法令等の遵守状況や当局が認めるその他必要事項といった包括的な項目が挙げられており、恣意的な運用がなされないか、今後の動向を注視する必要がある。

²⁵ 「重要情報インフラ」の運営者及び「処理する個人情報が国家インターネット情報機関の規定数量に達する個人情報処理者」以外の個人情報取扱者は、国外移転の必要がある場合は国外に個人情報を提供することができるが、その際の適法化根拠として、以下のいずれかの要件を満たす必要がある。①個人情報保護法 40 条の規定に基づく国家インターネット情報機関による個人情報保護認証を取得すること、②別途定められる規定により、国家インターネット情報機関による個人情報保護認証を取得すること、③国家インターネット情報機関が別途定める標準契約に従い国外の受領者と契約を締結すること、又は④法律、行政法規または国家インターネット情報機関が定めるその他の条件。加えて、(i) 国外移転時の本人通知事項を提供した上で、本人の「単独の同意」を取得すること、(ii) 国外の受領者が個人情報保護法の下で要求されるのと同レベルの保護を提供できることを保証するために必要な措置を援用すること、(iii) 個人情報保護影響評価報告書及び処理状況を 3 年間保管することが要求される。

²⁶ 香港、マカオ、台湾を含む。

²⁷ データ越境移転安全評価申告ガイドライン（第 1 版）（2022 年 9 月 1 日施行）。

²⁸ すなわち、国家インターネット情報機関によるデータ国外移転安全評価では、主に以下の事項が評価される（8 条）。(ア) データ域外移転の目的、範囲、方法等の合法性、正当性、必要性、(イ) 域外移転先が所在する国・地域のデータセキュリティ保護に関する政策法規およびサイバーセキュリティ環境が、データ域外移転の安全性に与える影響。域外移転先のデータ保護水準が、中国における関連の法律、行政法規の規定および強制性国家標準の要求に達し

上記のように、中国においては、重要データ又は個人情報等を国外移転する際には、当局による安全評価を経る必要がある場合があり、国家がデータ流通に介入する度合いが比較的高い。他方で、中国データ 3 法を所轄する機関（中国国家インターネット情報弁公室）は、データ 3 法の施行後、急ピッチで越境移転規制の要件を含む法令の要求事項を明確化するための細則やガイドラインを整備している側面もある²⁹。そのため、中国における越境移転規制が事実上の越境移転禁止措置に相当するかどうかは、今後示される越境移転の要件に関する細則やガイドラインの整備状況や、実際の運用状況によるため、今後の動向を注視する必要がある。また、かかる理由で、現時点では、越境移転規制のうち、当局の許可を条件とする措置についても、データ・ローカライゼーションに含めて検討する必要性は低いと考えている（この点については、今後の運用状況等を踏まえて検討する必要がある）。

7. データ・ローカライゼーションの政策目的に対するアプローチ

以上で見たとおり、データ・ローカライゼーションの政策目的は、個人情報保護、法執行・監督目的、他国のガバメントアクセスからの保護、国家安全保障など、様々ある。

日本政府は、これまで、通商ルール、すなわち日米デジタル貿易協定や二国間・複数国間の EPA（経済連携協定）で、DFFT（信頼性のある自由なデータ流通）を推進してきた。データ・ローカライゼーションとの関係では、コンピュータ関連設備の利用・設置強制の禁止規定に基づき、データ・ローカライゼーション措置の導入に対して厳格な姿勢をとっている。引き続き、CPTPP や RCEP を含む通商ルールにおけるデータ・ローカライゼーション関連規定との整合性を追求することが重要である³⁰。また、現状、日本政府は電子商取引に関する WTO 交渉において、データ・ローカライゼーション要求を禁止する条項を合意するために取り組んでいる。さらに、通商ルールとの抵触の懸念については、WTO のサービス貿易理事会や TBT 委員会といった政府間の対話の場も用意されており、データ・ローカライゼーション措置についても取り上げられている。

ているか否か、(ウ)データ域外移転の規模、範囲、種類、機微の度合い、域外移転中および域外移転後におけるデータの改竄、破壊、漏洩、紛失、移転または不法取得、不法利用される等のリスク、(エ)データセキュリティおよび個人情報に係る権益が、十分かつ有効な保障を受けられるか否か、(オ)データ取扱者が域外移転先と締結する予定の法律文書においてデータセキュリティ保護に関する責任義務が十分に取決められているか否か、(カ)中国の法律、行政法規、機関規則の遵守状況、(キ)国家インターネット情報機関が評価の必要があると認めるその他の事項。なお、本弁法の仮訳は、<https://www.cistec.or.jp/service/uschina/50-20220829.pdf>（2023 年 12 月 9 日最終アクセス）参照。

²⁹ 例えば、個人情報取扱事業者が個人データの越境移転時に依拠できる③の標準契約については、細則を定めた下位規則（個人情報越境標準契約弁法）が 2023 年 6 月から施行され、関連するガイドライン（個人情報越境移転標準契約届出ガイドライン（第 1 版）が同年 5 月に公表されており、同ガイドラインのなかでは上記（iii）の個人情報保護影響評価報告書等の届出書類の様式も公表されている。このように、中国国家インターネット情報弁公室が、越境移転規制に関わる事業者の予見可能性を高めるための取り組みを行っている」と評価できる側面もある。ただし、重要情報インフラ運営者による越境移転については、細目規定やガイドラインは公表されておらず、不透明な部分が残されている。

³⁰ 特に、中国との関係では、RCEP 第 12.14 条のコンピュータ関連設備の設置要求等禁止条との整合性を追求することが重要である。

以下では、まず、データ・ローカライゼーションは当該目的に必ずしも貢献しない、あるいは同じ目的を達成するために、データ・ローカライゼーション措置を講ずることよりも制限的でない方法（alternatives）がありうるのではないかという示唆を行う。その内容を簡単に整理したものは、図表4のとおりである。その上で、データ・ローカライゼーション措置への対応としては、上記の通商ルールにおける関連規定との整合性追求や将来の通商ルールにおける関連規定の合意と並行して、こうした代替措置の存在を各国に示すこともまた、重要な取り組みであることを提言する。

データ・ローカライゼーションの政策目的	アプローチ
(1) プライバシー・個人情報保護	代替措置として、個人情報保護法における域外適用規定のように、データの保存・処理場所にかかわらず、自国のプライバシー法制の適用を可能とするメカニズムがありうる。
(2) 法執行・監督目的	代替措置として、国外に保存・処理されるデータに対する捜査当局・監督当局によるアクセス確保のための国際的な枠組み作り（既存の枠組みのアップデートを含む。）がありうる。
(3) 他国政府によるガバメントアクセスからの保護	代替措置として、「民間部門が保有する個人データに対するガバメントアクセスに関する宣言」といった、共通原則策定の取り組みにより、ガバメントアクセスを行う政府に対して適切なセーフガードを要求する方法が考えられる。
(4) セキュリティ	データ・ローカライゼーションは必ずしもセキュリティ強化に貢献しない点を示す。

図表4 データ・ローカライゼーションの政策目的に対するアプローチ

(1) プライバシー・個人情報保護

データ・ローカライゼーション措置を導入する政策目的として、プライバシー・個人情報保護という考え方がある。これは、国内にあるデータにのみ、個人情報保護法による保護を与えることができるという考え方であり、逆に言えば、他国にデータを保存することで、自国の個人情報保護法の適用を免れることを前提としている可能性がある。

しかし、A国で収集したデータを国外（B国）で保存・処理しても、A国における個人データ保護法制の適用をなお及ぼすためのメカニズムを導入することは可能である。

例えば、日本の個人情報保護法及びGDPRには、域外適用規定が存在する。域外適用規定により、ある国に向けてビジネスを行っている（製品・サービスを提供する）事業者は、データ処

理の場所にかかわらず、また、当該国に事業拠点がなくとも、当該国でのプライバシー法制の適用を受けうる。

なお、域外適用規定については、国際法上の観点から、制約がある。一般に、自国に拠点を持たない事業者、あるいは自国外で行われた行為に対して立法管轄権を行使するには、国家と対象事項との間に「真正な連結 (genuine connection)」が認められる必要がある³¹と考えられているところ、日本の個人情報保護法における域外適用規定においては、「日本に向けて製品・サービスを提供していること」が連結点と捉えることが可能である。こうした連結点に関わる要件を充足する限り、当該国においてデータを保存しているかどうかに関わらず（むしろ、国外でデータを処理する場合であっても）データ保護法の適用範囲に含めることを通じて、データ保護法による保護を与えることが可能とされている。

事業者にとっては、当該国に向けて同じサービスを提供している限り、国内に所在する事業者であるかを問わず、同じルールのもとで競争できる方がメリットが大きいように思われる。したがって、国内保存義務と比べても事業者への負担が少ないと評価することも可能であるように思われる。

個人情報保護法 171 条

この法律は、個人情報取扱事業者、仮名加工情報取扱事業者、匿名加工情報取扱事業者又は個人関連情報取扱事業者が、国内にある者に対する物品又は役務の提供に関連して、国内にある者を本人とする個人情報、当該個人情報として取得されることとなる個人関連情報又は当該個人情報をを用いて作成された仮名加工情報若しくは匿名加工情報を、外国において取り扱う場合についても、適用する。

欧州一般データ保護規則 (GDPR) 3 条

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

³¹ Restatement of the Law (Fourth): Foreign Relations Law of the United States (2018)

b. the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

(和訳³²)

1. 本規則は、その取扱いが EU 域内で行われるものであるか否かを問わず、EU 域内の管理者又は処理者の拠点の活動の過程における個人データの取扱いに適用される。

2. 取扱活動が以下と関連する場合、本規則は、EU 域内に拠点のない管理者又は処理者による EU 域内のデータ主体の個人データの取扱いに適用される：

(a) データ主体の支払いが要求されるか否かを問わず、EU 域内のデータ主体に対する物品又はサービスの提供。
又は

(b) データ主体の行動が EU 域内で行われるものである限り、その行動の監視。

3. 本規則は、EU 域内に拠点のない管理者によるものであっても、国際公法の効力により加盟国の国内法の適用のある場所において行われる個人データの取扱いに適用される。

上記のとおり、域外適用規定により、データの所在場所や処理の場所に関わらず、自国の個人情報保護法の規律を及ぼすことは可能であることを示すことが考えられる。

(2) 法執行・監督目的

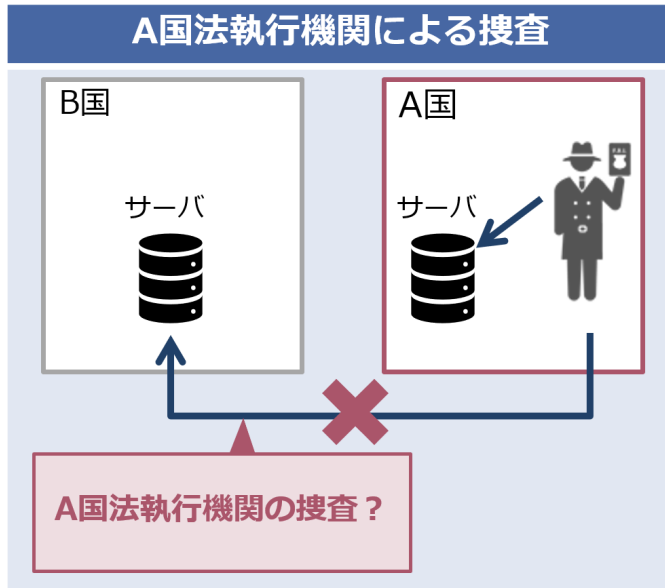
データ・ローカライゼーション措置を導入する政策目的として、法執行・監督目的を挙げる例がある。この考えは、データ・ローカライゼーション（特に国内保存）が法執行・監督目的でのデータアクセスを適法に行う唯一の（又は最善の）方法であり、国外に保存されたデータに対しては法執行・監督権限を行使できないことを前提としていると考えられる。

しかし、他国の主権を侵害せずに他国に保存されたデータを収集する方法は存在する。具体的には、大きく分けて、①他国の主権を侵害しない態様でデータを収集する方法、②他国の協力のもとで収集する方法が考えられる。

①について、例えば、対象となるデータが保存されているサーバの管理者が国内に所在する場合に、当該サーバ管理者の任意の協力のもとで、国外に所在するデータの提供を受ける場合が考えられる。国外のサーバに保存されているデータを捜査機関が捜査の対象とすることがで

³² 個人情報保護委員会が公表している仮日本語訳 (<https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf>) に依拠している。

きるかという問題に関し、「国外のサーバに保存されているデータについては、他国領域に捜査機関が立ち入り、捜査を行うような執行管轄権に基づく強制措置とは異なり、実際のデータまたはその記録媒体の提出行為が国内で行われ、国外に所在するサーバへのアクセスは命令を受けた国内にいるサーバの管理者等が行うのであれば、国際法上許容されると考えるべきである」、と指摘するものがある（クラウド研究会報告書 2.0 44 頁）。



②については、刑事相互共助条約（MLAT）を通じた手続が存在する。

この点、MLAT を通じた手続は、平均して 10 ヶ月程度の期間を要するなど迅速な証拠収集が妨げられているという批判や、データの所在国が不明である場合には対応できないといった問題が指摘されている³³。このように、使い勝手のよいメカニズムが存在しないことが、各国におけるデータ・ローカライゼーション措置の導入を加速しているとの指摘もある³⁴。

しかし、犯罪のグローバル化や、証拠がネットワークを通じてグローバルに点在する現状、クロスボーダーの証拠収集は不可避である。かかる状況下において、法執行機関は、データの保存場所ではなく、アクセス権限の確保に向けて法的枠組みをアップグレードする必要があることを強調したい。

（3）他国政府によるガバメントアクセスからの保護

データ・ローカライゼーション措置を導入する政策目的には、他国政府によるガバメントアクセスからの保護が含まれる。かかる政策目的は、国内保存要求をすることが、他国政府によるガバメントアクセスをブロックすることに役立つという考え方を前提としている。

³³ 西村高等法務研究所 CLOUD Act 研究会「報告書 2.0 企業が保有するデータと捜査を巡る法的課題の検討と提言」（2023 年 4 月）51 頁

³⁴ Cory, Nigel & Dascoli, Luke. (2021) “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them” 25 頁, <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>

確かに、国外に保存されたデータに外国の政府機関がアクセスする場合、他国の主権侵害の問題が生じうることや、MLAT による手続に相当の期間を要する問題があることは、(2) で述べたとおりである。このように、国内保存要求によって、外国政府が自国に所在するデータにアクセスすることは困難になるため、他国政府によるデータアクセスを困難にすることに役立つことは否定できない。

しかし、ガバメントアクセスの問題の核心は、政府による民間データのアクセスが無制限に行われることによって、個人のプライバシーやセキュリティを侵害するリスクにある。

こうしたガバメントアクセスへの懸念に対しては、「民間部門が保有する個人データに対するガバメントアクセスに関する宣言」といった、共通原則策定の取り組みが存在する。これは、ガバメントアクセスを実施する政府に適切なセーフガードを要求することにより、懸念に対処しようとする考え方であり、国内保存義務を課すよりも事業者への負担が少ない方向での解決策であると言える。そもそも、インドのホワイトペーパーでも整理されているように（第4章（2）参照）、国内保存義務を課せば、同時に現地法執行機関によるガバメントアクセスのリスクを増加させる可能性があるだけであり、ガバメントアクセス自体の懸念が払拭されるわけではない。

ガバメントアクセスに関する各国共通の原則を策定し、適切な運用を確保することは、各国が独自の措置（すなわちデータ・ローカライゼーション措置）を導入することを回避することにも役立つものである。日本政府としては、こうした取り組みの正当性を評価し、国内保存義務には断固として対抗する必要がある。

（4）セキュリティ

データ・ローカライゼーション措置を導入する政策目的には、セキュリティの確保が含まれる。これは、国内保存要求をすることが、対象となったデータのセキュリティを確保することに役立つという考え方、データが国内で保存及び処理される場合に最もその安全性が保証されるという考え方が土台になっている。

しかし、一方で、データ・ローカライゼーションはセキュリティの強化に貢献しないばかりか、逆に、セキュリティ上のリスクを増大させるという点が指摘されている。その理由は、データ・ローカライゼーション措置、特に国内保存・処理要求の帰結として、事業者は、自らデータを保存するためのサーバを当該国に設立したり、当該国のローカルベンダーを起用する（あるいは、市場から撤退する）ことを余儀なくされることから、セキュリティベンダーの選択肢が狭まることや、データを分散管理できないことによるインシデント発生時の復旧の遅れが発生すること等にあるとされる。そもそも、データの漏えい、滅失、毀損を防ぐための組織的・技術的・物理的措置が適切に講じられるかどうかはセキュリティ対策の不可欠の要素であって、データの取扱場所はセキュリティ向上とは関係がない。

産業団体であるBSA（ソフトウェア・アライアンス）は、「ローカル・サーバーだけにデータを保存しても、サイバーセキュリティは強化されない。一元的に保存された情報は、大規模なインフラに分散された情報よりもはるかに安全ではない。それは、無許可の第三者がこれらの

データ「ハニーポット」に侵入し、最大限の悪影響を及ぼす可能性が高まるからである。グローバルなクラウド・コンピューティングのように、データの保存場所を分散させることで、データセットを区分けし、ある場所での侵害を確実に封じ込め、他のデータセットにアクセスできないようにすることができる。」と述べている³⁵。

8. 貿易協定におけるデータ・ローカライゼーション関連条項

日本政府は、これまで、通商ルール、すなわち日米デジタル貿易協定や二国間・複数国間のEPA（経済連携協定）で、DFFTを推進してきた。具体的には、CPTPP、RCEP等³⁶には、データ・ローカライゼーション関連規制が盛り込まれている³⁷。日本が加盟国となっていない協定を含めると、2022年までに、27の協定にデータ・ローカライゼーション関連規制が盛り込まれているとのデータもある³⁸。

しかし、通商ルールにおけるデータ・ローカライゼーション関連規制には一定の限界もある。

通商ルールにおける主なデータ・ローカライゼーション規制として、CPTPP第14.13条及び日米デジタル貿易協定第12条2項におけるコンピュータ関連設備の設置要求禁止に係る規律を取り上げる。

（1）CPTPPにおけるデータ・ローカライゼーションの規律

- | |
|--|
| <ol style="list-style-type: none">1. 締約国は、各締約国がコンピュータ関連設備の利用に関する自国の法令上の要件（通信の安全及び秘密を確保することを追求する旨の要件を含む。）を課することができることを認める。2. いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならない。3. この条のいかなる規定も、締約国が公共政策の正当な目的を達成するために2の規定に適合しない措置を採用し、又は維持することを妨げるものではない。ただし、当該措置が、次の要件を満たすことを条件とする。<ol style="list-style-type: none">(a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと。(b) 目的の達成のために必要である以上にコンピュータ関連設備の利用又は設置に制限を課するものではないこと。 |
|--|

³⁵ https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf

³⁶ 地域的な包括的経済連携協定。

³⁷ CPTPP第14.13条、RCEP第12.14条、日米デジタル貿易協定第12条2項等。なお、CPTPP第14.13条と同様の規定は、2022年11月に署名された韓国・シンガポール・デジタルパートナーシップ協定（Korea-Singapore Digital Partnership Agreement、KSDPA）にも含まれている。

³⁸ Del Giovane, C., J. Ferencz and J. López González (2023), "The Nature, Evolution and Potential Implications of Data Localisation Measures", OECD Trade Policy Papers, No. 278, OECD Publishing, Paris, <https://doi.org/10.1787/179f718a-en>.

上記のとおり、CPTPP の電子商取引章（14 章）には、コンピュータ関連施設の利用又は設置要求禁止規定が存在する（14.13 条）。同条が対象とする措置は、国内保存要求や国内処理要求という形では明記されていないものの、国内保存要求や国内処理要求を一般的に含むと考えられている。

なお、同規定によって保護を受ける対象者から、金融機関等が除外されている（14.1 条）。したがって、CPTPP 締約国が金融機関に対し、自国内にコンピュータ関連施設の設置を強制しても、ただちに 14.13 条違反にはならない。また、CPTPP の金融サービス章（11 章）には、コンピュータ関連施設の設置要求等を禁止する条文は存在しない。

さらに、コンピュータ関連施設の利用又は設置要求禁止の例外として、個人情報保護目的、安全保障目的の措置については、例外規定によって正当化される余地がある（一般例外条項（29.1 条 3 項）、安全保障例外条項（29.2 条）、公共政策目的（LPP0）例外（14.13 条 3 項）、GATS 第 14 条(c)(ii)）。したがって、国家安全保障目的や個人情報保護目的のデータ・ローカライゼーション措置については、これらの例外規定によって、正当化される余地が否定できない点に留意が必要である（ただし、国家安全保障目的と言っても、措置国の無制限の裁量が認められるわけではない。例えば、GATT21 条（安全保障例外）における対象措置の「必要」性については、措置国の裁量を尊重しつつ、条約解釈における信義則（good faith）（ウィーン条約法条約 26 条、31 条）を援用する形で、措置国に一定の説明を求めるパネルもあると報告されている³⁹）。

（２）日米デジタル貿易協定におけるデータ・ローカライゼーションの規律

日米デジタル貿易協定では、金融サービス提供者をコンピュータ関連施設設置要求禁止条項から除外している（12 条 2 項）。そのうえで、金融サービス提供者については特別のコンピュータ関連施設設置要求禁止条項が設けられている（13 条）。同条では、コンピュータ関連施設設置要求禁止の前提として、金融規制当局による対象金融サービス提供者のデータへのアクセスの確保が必要とされている。金融規制当局に対して国外に保存されたデータへのアクセスが確保されていなければ、関連するデータを国内に保存させることが許容される。法執行・監督目的でのデータ・ローカライゼーションを金融サービス分野において一部許容する趣旨と思われる。

9. 結語

以上、本稿では、データ・ローカライゼーションが必ずしも特定の政策目的に貢献しないことや、より制限的でない代替策が存在する可能性について検証した。

データ・ローカライゼーションに対する政策アプローチとしては、引き続き、通商ルールにおける関連規定との整合性を志向し、データ・ローカライゼーションに関する国内措置の導入

³⁹ 「安全保障例外～GATT21 条の解釈をめぐる論点と最近の WTO 先例」2023 年版不正貿易報告書 267 頁。
https://www.meti.go.jp/policy/trade_policy/wto/3_dispute_settlement/32_wto_rules_and_compliance_report/322_past_columns/2023_04.pdf

に厳格な姿勢を見せることが重要である。一方で、データ・ローカライゼーション措置がもたらす事業者への影響の観点から、政策目的を達成するための実効性について検証するとともに、より制限的でない代替案を示すこともまた、重要と考える。データ・ローカライゼーション措置に関わる政策目的や理念は様々であり、政策目的を達成するための政策的アプローチは様々である。まずは、諸外国が重視する政策目的の正当性を尊重しつつ、その上で、同じ政策目的や理念を達成するためにより制限の少ない効果的な方法を提示し（その具体例は、第7章で述べたとおりである。）、データ・ローカライゼーション措置が政策目的を達成するための正当かつ有効な手段になりうるのかを建設的に議論することも重要であるように思われる。そして、より制限的でないかどうかの分析にあたっては、事業者の国際的なデータ流通に対するニーズや、データ・ローカライゼーション措置によって事業者が被る不利益の観点も考慮に入れることが望ましい。

最後に、本稿で言及したアプローチのために、データ・ローカライゼーション措置国との関係づくりや直接の対話の機会を確保することが肝要である。データ・ローカライゼーション措置国がその背景にある政策目的を公表する例は非常に稀であることから、公の場で背後にある政策目的を知ることは困難を伴うことが予想される。しかし、データ・ローカライゼーション措置国との直接かつ継続的な対話を通じて、当該国がいかなる政策目的を考慮しているのかについて理解を示すことは、データ・ローカライゼーション措置に代替する手段を建設的に議論するための第一歩になると思われる。

以上