博士論文

サイバー空間分裂回避のための越境的データガバナンス規範再構成

―文脈的リスク評価に基づくデータ最小化モデル（CRDM モデル）の提案と「トウキョウ効果」の展開―

Hiroshi　KATAOKA

片岡　　弘

情報セキュリティ大学院大学

情報セキュリティ研究科

情報セキュリティ専攻

2026 年 3 月

概要

本稿では、サイバー空間分裂回避のための越境的データガバナンス規範再構成について論じる。第Ⅰ部では、各国がデジタル主権の名の下に統制を拡張した結果、規範的対立やデータ保護主義が強まり、国際的統一規範の欠如と制度的非対称性が深刻化している現状を示す。米国、中国、EU といった大国の規範的衝突は、国際的データガバナンスの調和的構築を阻み、サイバー空間を制度的ブロックへと分断させつつある。越境的データ移転は、相手国制度の信頼性評価を不可避とする領域であり、GATS の基本原則をそのまま適用することはできない。さらに、国際的統一規範を策定するための多国間フォーラムも、大国間における規範的主張の対立により停滞している。こうした状況の下では、各国の主権的統制を尊重しつつ国際的相互運用性を確保し得る越境的データガバナンス規範の再構成が不可欠となる。

第Ⅱ部では、国際的データガバナンスの分断をもたらす五つの国家施策を分析し、その累積的効果として、多様な制度原理と価値観が併存・競合する多極化したデータ秩序が形成されている点を明らかにする。これらの領域はいずれも、比例原則およびリスクベースアプローチを基軸とする規範再構成を要請している。

第Ⅲ部では、DFFT を指導原理とし、文脈的リスク評価とデータ最小化原則を統合した CRDM モデルを提示する。CRDM モデルは、リスクベースアプローチに基づき、データの性質および利用文脈に基づくリスク評価により、段階的にデータ保護措置を設定し、個人データ・非個人データを問わず、柔軟かつ持続可能な越境的データ移転制度の構築を目指すものである。規範再構成にあたっては、特定の大国モデルへの依存を回避する観点から、中堅国・新興国による有志国連携が戦略的に重要となる。日本は、この連携を主導し、新たな規範を大国へと橋渡しすることで国際標準へと昇華させ得る立場にあり、その普及動態は「トウキョウ効果」の展開として位置づけられる。

キーワード

越境的データガバナンス、サイバー空間分裂、デジタル主権、規範輸出、
データローカライゼーション、ガバメントアクセス、越境的ディスカバリ、データ流入規制、
DFFT、リスクベースアプローチ、CRDM モデル、トウキョウ効果

Abstract

This thesis discusses the restructuring of cross-border data governance norms to avoid the fragmentation of cyberspace. Part I shows that, as countries extend control in the name of digital sovereignty, normative conflicts and data protectionism have intensified, and the lack of internationally unified norms and the resulting institutional asymmetry have become more serious. Normative clashes among major powers, including the United States, China, and the EU, hinder the coherent development of international data governance and divide cyberspace into institutional blocs. Cross-border data transfer is an area where the assessment of the reliability of a partner country's regulatory and institutional framework is unavoidable, and the basic principles of the GATS cannot be applied in their current form. In addition, multilateral forums for developing unified international norms have also stalled due to conflicts among major powers over competing normative claims.

Under these circumstances, it is essential to reconstruct cross-border data governance norms that can ensure international interoperability while respecting the sovereign control of each country. Part II analyzes five categories of national policy measures that lead to the fragmentation of international data governance, and clarifies that the cumulative effect of these measures is the formation of a multipolar data order in which diverse institutional principles and values coexist and compete. These developments call for a restructuring of norms based on the principle of proportionality and a risk-based approach. Part III presents a CRDM model (Contextual Risk-Based Data Minimization model) that integrates contextual risk assessment and data minimization principles, with DFFT as its guiding framework. The CRDM model adopts a risk-based approach, in which risks are assessed according to the nature of the data and the context of use, in order to apply data protection measures in stages and to build a flexible and sustainable cross-border data transfer system, irrespective of whether the data involved are personal or non-personal. In restructuring norms, it is strategically important for mid-sized and emerging countries to collaborate with like-minded partners in order to avoid dependence on specific great-power models. Japan is well positioned to lead such collaborative efforts and to elevate emerging norms into international standards by serving as a normative bridge between like-minded partners and major powers. This pattern of normative diffusion may be conceptualized as the Tokyo Effect.

Keywords:

Cross-border data governance; Fragmentation of cyberspace; Digital sovereignty; Normative export; Data localization; Government access; Cross-border discovery; Inbound data restrictions; Data Free Flow with Trust (DFFT); Risk-based approach; CRDM model; Tokyo Effect.

目次

はじめに

はじめに

サイバー空間は分裂の危機に瀕している。その背景には、越境的データガバナンスに関する国際的統一規範が存在しない状況のもとで、国家がデータ（デジタル化され一定の意味内容を有する情報をいう。以下同じ。）[1] に対する主権行使を強化していることがある。サイバー空間は本来、国境に依存しないデータ通信やデータ流通を可能とする国際的公共基盤として構築されてきたが、今日では、データの生成・蓄積・移転・利用、これを支えるデジタルサービス、さらにそれらを規律する制度や規範が結びついたデジタルエコシステムへと変容している。その結果、各国は自国の制度、価値観、主権的判断に基づき、サイバー空間を統合的に統制し得る領域として位置づけるようになった。サイバー空間の運用やアクセスは国家ごとの法制度や政策選択に左右され、本来は国境を越えて一体性を保つはずであった空間に、制度的な境界線が形成されつつある。これらの境界線は、国家の主権的統制がサイバー空間に投影される過程で生じるものであり、規範や制度の差異を通じて空間を分断する。国家がデータを安全保障、産業競争力、社会統治を支える戦略的資源として再定義し、管理・保護を強化する動きが進むなかで、サイバー空間の一体性は揺らぎ、複数の制度的ブロックへと分裂する危機が顕在化している。この構造変容は、国家の主権行使が物理的領域からサイバー空間へと拡張し、従来の領域主権の枠組みでは捉えきれない新たな統治構造が生じていることを示している。

米国、中国及び EU は、「データ大国（Data Realms）」（以下、単に「大国」ともいう。）と称されるが[2]、各国がサイバー空間に対して主権的統制を投影する際に依拠する制度原理は大きく異なる。米国は、巨大 IT 企業が形成する市場支配構造および民間主導のデジタル基盤を国家が制度的に承認・活用することを根拠とし、貿易協定を通じてこれらのルールを国際基準へと押し広げる制度モデル（市場支配モデル：Market dominant model）を構築している。EU は、個人データ保護を軸とする規範体系を国際標準として位置づけ、GDPR などの域外適用を通じて、その規範体系を国際秩序へと投射するモデル（規範統制モデル：Normative control model）を採用している。他方で中国は、国家安全保障と制度統制を最優先とする主権モデル（サイバー主権モデル：Cyber sovereignty model）を採用し、サイバー空間を国家の統治領域に組み込むことで自律的管理体制を確立している。これら三つの統制モデルは、それぞれ異なる制度原理を基盤としてサイバー空間への規範投影を行い、その結果として相互に競合している。このようにして、同一データに対して複数の法域から相反する規制要求が課される状況が生じ、制度間の非互換性は構造的に固定化しつつある。このような制度原理の不整合が大国間の調整を阻害し、国際的に統一された越境的データガバナンス規範の策定を困難なものにしている。すなわち、国際的データガバナンスの分断を生じさせる核心的要因は、各国が投影する主権的統制の非対称性にある[3]。

---

[1] 本稿では、「データ」という語を、個人データと非個人データの両者を含む意味で使用し、主として両者に共通する論点を扱うが、それらを区別して論ずる必要がある場合には、その旨を明示する。

[2] Aaronson and Leblond (2018), pp. 245–248（以下、脚注引用文献の詳細情報は、各部末尾の参考文献一覧を参照）.

[3] 本稿では、「越境的データガバナンス」という語を、国境を越えるデータ移転に伴って生じる具体的な規制措置や、その適用範囲をめぐる各国制度の相互関係を分析する文脈で用いる。これに対し、「国際的データガバナンス」という語は、国家間に存在する制度的相違や国際秩序の構築という規範形成の枠組みを示す文脈で用いる。

国家がサイバー空間の安全と信頼性を確保しようとするほど制度間の齟齬は拡大し、その累積がサイバー空間を複数の制度的ブロックへと分離させる方向に働く。このことは、国家による保護の強化が国際的公共基盤としてのインターネットの分断を加速させるという構造的現象が生じていることを意味する。こうした現状を踏まえると、サイバー空間の分裂危機は、技術的要因よりもむしろ、各国が自国中心の主権行使を強化したことに起因する制度的かつ規範的な構造問題として理解すべきである。国家の保護目的には一定の正当性が認められるものの、制度原理が相互に競合している状況では、相互運用性の維持と制度的調和の確保が、今後の国際的データガバナンスにおける核心的課題となる。

サイバー空間がこのような分裂の危機に直面している現在、越境的データガバナンス規範の再構成は、国際秩序の安定的維持に不可欠な課題である。大国の間に根源的な対立が存在し、国家ごとに異なる制度原理が競合して相互運用性が損なわれている現状では、既存の国際枠組みのみに依拠して調整機能を期待することは困難である。特に、各国が自国の制度原理に基づき越境的な規制を一方的に適用する状況では、同一データに対して複数の要求水準が衝突し、制度間の不整合が構造的に拡大するという問題が顕在化している。この不整合は、各国が相反する規範要求の狭間で、いずれの制度的ブロックの規範に従うかという選択を迫られ、国際協調を一層困難にしている。したがって、こうした摩擦を緩和するためには、各国の制度原理そのものを統一しようとするのではなく、データの種類や利用文脈に応じて求められる保護の必要性を評価し、その評価に基づいて移転条件を調整するための共通の判断枠組みが必要となる。すなわち、越境的データガバナンス規範再構成は、いずれかの制度的ブロックの規範に全面的に依拠するのではなく、各国の主権的統制の多様性を尊重しつつも、相互運用性を確保するための共通原理を提示するものでなければならない。

越境的データガバナンス規範の再構成とは、国家の統治権限を否定する作業ではなく、サイバー空間全体の安定性と持続可能性を確保するために、国家間の主権的統制の関係を調整する取組である。各国がサイバー空間に対する非対称的な主権的統制を強める現状を放置すれば、分断は一層深化し、相互不信と制度的不確実性が累積的に増幅する。他方、制度間の相互運用性を回復するための共通基準や協調的手続を整備すれば、国家間の規範競合を抑制し、データ流通の予見可能性を高めることができる。こうした枠組みは、サイバー空間の一体性を維持し、国際社会全体の利益に資する安定的なデータ秩序の形成に向けた基盤となる。

以上の観点に基づき、本稿では、第 I 部で越境的データガバナンス規範再構成の必要性と課題を検討し、第 II 部で国際的データガバナンスの分断をもたらす五つの国家施策（大国による規範輸出、データローカライゼーション、ガバメントアクセス、ディスカバリの越境的適用、国家によるデータ流入規制）を分析する。これらの検討を経て、第 III 部では越境的データガバナンス規範再構成の在り方を提示する。その具体的方策として、各国の主権的統制の多様性を尊重しつつ国際的相互運用性を確保し得る越境的データガバナンス規範再構成に向けて、リスクベースアプローチを基盤とする CRDM モデル（Contextual Risk-Based Data Minimization model）の導入と、その実装に向けた方策を示す。さらに、再構成された規範を日本が主導して大国を取り込む「トウキョウ効果（Tokyo Effect）」を展開することにより、国際的に統一された越境的データガバナンス規範を確立し、サイバー空間分裂の回避を図るための戦略について検討する。

第Ⅰ部

越境的データガバナンス規範再構成の必要性と課題

第Ⅰ部　越境的データガバナンス規範再構成の必要性と課題

第Ⅰ部では、国際的データガバナンスにおいて深刻化する制度的分断を分析し、サイバー空間の分裂を回避するための越境的データガバナンス規範再構成の必要性と課題を検討する。

デジタル技術の進展に伴い、個人・企業・政府の諸活動はサイバー空間に再配置され、そこで生成・処理されるデータは国家の社会運営、行政サービス、経済活動、安全保障を支える不可欠の基盤となった[4]。他方、データは瞬時に国境を越えて移動し、複数法域にまたがり分散的に保存・利用されるため、従来の領域主権に基づく統治枠組みではその保護と利用を十分に制御することが難しくなっている[5]。その結果、各国はデータという非領域的対象をめぐってデジタル主権の名の下に自国の統制をサイバー空間へ拡張し、国家間の規範的主張がサイバー空間上で衝突する構造が生じている[6]。こうした国家間の制度的摩擦は、サイバー空間の規範的・制度的連続性を損ない、国際的なデータ流通の相互運用性を著しく低下させる要因となっている[7]。データの越境移転に対する各国の要求水準が相互に異なれば、同一のデータに対して異なる法域で相反する義務が課される可能性が生じ、国際的なデジタルエコシステムの一体性は長期的に脅かされ得る[8]。データ流通が地政学的境界線に沿って断片化すれば、サイバー空間全体が制度的ブロックごとに分裂するリスクが拡大する[9]。

現在の越境的データガバナンス規範は、国際的な共通原則の不在と調整メカニズムの欠如により、断片的かつ不均衡な構造を呈している。多国間フォーラムにおいても統一ルールの策定は模索されてきたものの、各国の利害対立は大きく、制度的調和には至っていない。その帰結として、各国は自国の価値観、制度、経済的利益、安全保障上の懸念に基づき独自の規制を展開し、制度間の非対称性はむしろ拡大している[10]。これに加えて、法制度の成熟度、デジタル基盤、技術能力、行政能力といった領域での構造的非対称性が、国際的データガバナンスの断片化を一層進行させている[11]。このような非対称性は制度的公平性・透明性・予見可能性の確保を困難にし、サイバー空間分断の回避に不可欠な国際協調の基盤を弱体化させている[12]。

したがって、サイバー空間の分裂を回避し、持続的な国際協調を可能とするためには、国家による主権的統制の多様性を尊重しつつ国際的な相互運用性を確保し得る越境的データガバナンス規範を再構成する必要がある。そのためにも、国家が行使するデジタル主権の限界と正統性の基準を整理し、国際社会全体として共有可能な原則を提示することが不可欠である[13]。

以上を踏まえ、第Ⅰ部では、第 1 章において国家のデジタル主権行使による国際的データガバナンスの分断を指摘し、第 2 章で伝統的基本原則の実効性喪失と国際的統一規範の欠如に

---

[4] OECD (2022a), pp. 9–12.
[5] Chander and Lê (2015), pp. 680–688, 704–712, 715–720; Cory and Dascoli (2021), pp. 6–14.
[6] Jiang (2024), pp. 728–736; von Scherenberg et al. (2024), pp. 5–7.
[7] Aaronson and Leblond (2018), pp. 245–252; Cory and Dascoli (2021), pp. 6–14.
[8] Cory and Dascoli (2021), pp. 8–9, 13–14; von Scherenberg et al. (2024), pp. 3–5.
[9] Fratini et al. (2024), pp. 3–6, 18–22; Kaya and Shahid (2025), pp. 220–224, 228–231.
[10] Aaronson and Leblond (2018), pp. 245–248, 259–265; UNCTAD (2021), pp. 85–90.
[11] Cory and Dascoli (2021), pp. 12–16; UNCTAD (2021), pp. 83–90.
[12] Aaronson and Leblond (2018), pp. 257–260.
[13] Aaronson and Leblond (2018), pp. 245–247, 257–260; Cory and Dascoli (2021), pp. 12–16.

ついて検討する。これらの検討を通じて、サイバー空間分裂の構造的要因を分析し、越境的データガバナンス規範再構成の必要性と課題を提示する。

第 1 章

国家のデジタル主権行使による国際的データガバナンスの分断

第 1 章　国家のデジタル主権行使による国際的データガバナンスの分断

現代社会においてデータは、通信や経済活動の手段としてだけではなく、各種イノベーション、個人のプライバシー、社会的秩序、さらには国家の安全保障に関わる戦略的資源として位置づけられている[14]。データの急速な越境流通が進むなかで、国家は、自国民の権利保護と公共利益の確保という固有の統治責務を果たすため、越境的データ移転に一定の規制的関与を行う必要に直面している[15]。この際に行使される国家権限は、伝統的な領域主権の単純な延長ではなく、その構造的再編ともいえる展開を示しており、物理的領域に限定されてきた主権概念が、データという非領域的対象をめぐってサイバー空間へと拡張しているという点に特徴がある[16]。個人情報保護、重要インフラ防護、サイバー攻撃対策といった領域において国家が監督権限を行使することは、制度的安定性と国民の権利保障を確保するうえで不可欠であり、このような活動は「デジタル主権」の実践として理解され得る[17]。また、国家が自国法制の下でデータ処理の安全性と透明性を確保することは、国際的データ流通における信頼の基盤であり、サイバー空間の連続性を確保するための本質的要素である[18]。

越境的データガバナンスとは、国境を越えて移動するデータについて、責任ある管理と統制を可能とする国際的な法的・制度的枠組みをいう[19]。サイバー空間が分裂の危機に直面している背景には、越境的データガバナンスをめぐる国際的な統一規範が整備されていないことがあり[20]、複数の国家が自国の制度と安全保障上の論理に基づき、データに対する主権的統制を拡大させている点が重要である[21]。これにより、サイバー空間において国家間の規範的対立が先鋭化し、データ流通の経路、保存先、アクセス基準が地政学的境界線に応じて断片化し、非対称性をさらに深化させる現象が進行している[22]。

国家によるデータ保護のための主権行使については、正当な規制措置の発動と認められる一方で、その延長線上で閉鎖的な「データ保護主義（data protectionism）」が急速に拡大し[23]、国家の産業政策や地政学的利益と結びつきながらサイバー空間の制度的連続性を深刻に損ないつつある。データ保護主義は国際的データ流通の相互運用性を低下させ、各国の規制差を固定化することによって、サイバー空間の分裂を加速させる構造的要因となっている[24]。このような状況においては、正当なデータ保護とデータ保護主義的措置との境界が曖昧化し、どの規制が公共利益に基づく正当な介入であり、どの規制が国際秩序を分断する手段なのか、その判断基

[14] Aaronson and Leblond (2018), pp. 245–247; UNCTAD (2021), pp. 15–22.
[15] OECD (2022a), pp. 17–19.
[16] Pierucci (2025), pp. 3–7, 10–12.
[17] Jiang (2024), pp. 728–732; Pierucci (2025), pp. 3–7.
[18] Kaya and Shahid (2025), pp. 223–226.
[19] Aaronson and Leblond (2018), pp. 245–247; OECD (2022a), pp. 17–19.
[20] Aaronson and Leblond (2018), pp. 257–260; Cory and Dascoli (2021), pp. 12–16.
[21] Fratini et al. (2024), pp. 14–16; Gu (2024), pp. 594–605; Jiang (2024), pp. 728–732.
[22] Aaronson and Leblond (2018), pp. 257–260; Fratini et al. (2024), pp. 20–23; Kaya and Shahid (2025), pp. 219–221.
[23] Aaronson (2019), pp. 545–552; Cory and Dascoli (2021), pp. 6–12.
[24] Aaronson and Leblond (2018), pp. 245–247, 257–260; Aaronson (2019), pp. 548–555; Cory and Dascoli (2021), pp. 6–12; UNCTAD (2021), pp. 85–92; Kaya and Shahid (2025), pp. 223–226.

準が不透明となる[25]。結果として、国際的合意形成は一層困難となり、サイバー空間の分裂回避に向けた共通規範の形成は著しく阻害されている[26]。

以上のように、サイバー空間の分裂は、統一的な越境的データガバナンス規範の欠如と、国家による主権的統制の拡大が複合的に作用した結果として顕在化している[27]。本章では、第 1 節において現代国家によるデータ保護の必要性とデジタル主権行使について整理し、第 2 節ではデータ保護主義の弊害と正当なデータ保護との区別の必要性を検討する。さらに第 3 節では越境的データガバナンスにおける非対称性の深化とその弊害を分析する。以上を踏まえ、第 4 節で越境的データガバナンス規範再構成の必要性を論じる。

[25] Aaronson (2019), pp. 545–552, 556–558; Cory and Dascoli (2021), pp. 6–12; UNCTAD (2021), pp. 83–92.
[26] Burri (2017), pp. 67–75, 120–132; UNCTAD (2021), pp. 83–89.
[27] Aaronson and Leblond (2018), pp. 245–266; OECD (2022a), pp. 34–36.

第 1 節　現代国家によるデータ保護の必要性とデジタル主権行使

現代国家におけるデータ保護の責務は、行政上の義務や技術的課題の解決にとどまらず、国家が基本的人権を保障し、公共の信頼を維持するための中核的な統治機能として位置づけられる。デジタル技術の進展により、行政、医療、教育、金融、治安などの領域で膨大なデータが日常的に収集・処理され、国家はその適正な管理と利用を制度的に確保する責務を負うようになっている。現代のデータ保護は、もはやプライバシーの問題だけではなく、国家の統治的正当性および国際秩序の安定を支える制度的責務として再定義されつつある[28]。

国家がこのようなデータ保護の責務を果たそうとする過程では、他国の主権や法秩序との衝突を回避することは容易ではない。自国民のデータを保護するために、国家が自国法を国外に及ぼしたり、外国企業や国外サーバーに法的義務を課したりする場合、それは他国の管轄権との競合を引き起こす。このような域外的規制の行使は、自国民の権利保護という制度的正当性に基づく一方で、他国の法秩序に対する干渉ともなり得る[29]。

国家安全保障、個人情報保護、経済競争力の強化といった政策領域において、各国は国家主権の名の下に、政策的かつ戦略的手段を用いて越境的データの統制を図っている。しかし、これらの措置は、伝統的な国際管轄権秩序との緊張を高める一因となっている。越境的データ流通における主権衝突の根底には、領域主権概念そのものの限界という構造的問題がある。データは物理的な国境を越えて生成・移転・保存され、同一のデータが複数の法域にまたがって存在する。したがって、国家の統治権を領域に基づいて画定するという近代国際法の原理では、もはや十分に説明・対応することができない。

このように領域主権の概念が機能不全に陥る中で、各国は自国の統制権を再定義する手段としてデジタル主権を掲げるようになった。それは、各国が自国領域内で生成されたデータをサイバー空間において自らの規範的支配の下に置こうとする動きとして具体化している[30]。しかし、デジタル主権の強調は、領域主権の限界を克服するどころか、むしろ国家の統制をサイバー空間全体に拡張させ、結果として越境的データガバナンス規範の衝突や対立を助長している。自国の安全保障上の要請や文化的価値観を根拠に各国がデータへの統制や介入を強化すれば、国際的なデータガバナンスは断片化し、主権間の摩擦が制度的に増幅される。そのため、デジタル主権の主張は、領域主権の延長としてではなく、主権相互の調整と協働を前提とした新たなガバナンス原理の中で再構築される必要がある[31]。

デジタル主権の行使は、他国の法制度や企業活動との衝突を生むリスクを有するため、越境的データガバナンス規範については、国際協調や相互承認など、多国間枠組みによるバランスの取れた調整が不可欠となる。デジタル主権は、領域主権の限界を補う一方で、新たな法的・政治的課題を提起している。これまで、デジタル主権の概念は、多くの国において異なる制度的形態によって具体化されてきた。米国は、民間企業のグローバル展開を通じて事実上の規範的影響力を保持し、民間契約と企業支配力を通じた市場支配モデル（Market dominant model）を構

[28] Viljoen (2021), pp. 580–605.
[29] Chander and Lê (2015), pp. 690–705; Kuner (2017a), pp. 883–889, 900–917.
[30] Pierucci (2025), pp. 3–7, 10–12.
[31] Mayer and Nock (2025), pp. 3–7.

築している[32]。一方、中国は、国家安全保障を根拠にサイバー空間を国家の統制下に置くサイバー主権モデル（Cyber sovereignty model）を構築し、越境的データ移転を原則的に規制する体制を採用している[33]。EU は、GDPR（General Data Protection Regulation）[34]などの規範の越境的適用を通じ、個人データやプライバシーを越境的に保護する規範統制モデル（Normative control model）を志向しており、EU 域外の国にもその規範的影響力を及ぼすことを意図している[35]。これらのモデルは、国家がいかなる原理に基づいてサイバー空間を統治するかという点で顕著に異なり、統治権限の源泉・対象・正当化根拠において本質的な相違を有している[36]。

このようなデジタル主権の制度的相違は、デジタル技術の非対称的発展と、国家にとっての戦略資源としてのデータの位置づけの差異に基づくものである[37]。今日では、越境的なクラウドサービスやプラットフォームの利用を通じて、国外の事業者や外国政府が国家内部の個人情報や産業データにアクセスし得る状況が常態化している[38]。現代の技術環境の下で国家が国内における権利保護や制度的自律性を確保するには、従来の領域主権の枠組みだけでは不十分であり、サイバー空間を統治対象に含めるような主権概念の再定義が不可避となっている。しかし、デジタル主権の興隆は、同時に国際的な格差と分断を深める要因ともなっている。米国・中国・EU といった大国が、それぞれ異なる価値観と制度論理に基づく主権モデルを競合的に展開するなかで、越境的な相互運用性や信頼の構築は一層困難になっている[39]。そのような大国の一国主義的展開が進む中で、中小国の発言機会や交渉能力は制限されている[40]。そして、技術的能力や制度的インフラが脆弱なグローバルサウス諸国にとっては、デジタル主権の行使それ自体が困難であり、強い制度設計力と技術インフラを有する大国による一方的な規範輸出（後記第 3 章参照）に従属せざるを得ない構造が生まれている。その結果、実質的に一部国家に制度的影響力が集中するという構造的格差が生じている[41]。

デジタル主権の問題は、現代国家における主権再構築の帰結の一つといえる[42]。しかし、その行使が国際的分断と制度的不均衡をもたらす以上、規範概念の調整のみでは統一的な国際的データガバナンスを確立することはできない。技術的アーキテクチャと法的制度設計が相互補完的に機能し、各国の自律性と国家間の信頼を両立させる越境的データガバナンス規範の再構築が求められている[43]。

---

[32] Aaronson and Leblond (2018), pp. 248–254; Aaronson (2019), pp. 548–557.
[33] Creemers (2017), pp. 85–97; 石本茂彦（2022）37–68 頁; 小野寺良文（2022）171–193 頁; 松尾剛行・胡悦（2022）69–107 頁.
[34] Regulation (EU) 2016/679, General Data Protection Regulation, OJ L 119, 4 May 2016, p. 1.
[35] Kuner (2017a), pp. 882–887, 892–894; Bradford (2020), pp. 25–65.
[36] Gu (2024), pp. 591–597; Jiang (2024), pp. 728–734; Mayer and Nock (2025), pp. 2–7.
[37] Mayer and Nock (2025), pp. 2–7; Pierucci (2025), pp. 3–13.
[38] Creemers (2017), pp. 85–97; Schwartz (2018), pp. 1682–1699, 1708–1732.
[39] Musoni et al. (2023), pp. 2–18, 21–28; Bradford (2023), pp. 1–52.
[40] Musoni et al. (2023), pp. 21–33; Bradford (2023), pp. 1–40.
[41] Heeks (2021), pp. 4–10.
[42] Pierucci (2025), pp. 3–7.
[43] Fratini et al. (2024), pp. 18–22.

第 2 節　データ保護主義の弊害と正当なデータ保護との区別の必要性

データ保護主義とは、国家が自国の経済的利益や戦略的優位性を確保するため、越境的データ移転に対して規制的・技術的制限を課す政策的傾向を指す[44]。これには、自国のデータを領域内にとどめるデータローカライゼーション措置や越境的データ移転制限（後記第 4 章参照）のほか、自国のデータ保護規範を他国に及ぼす規範輸出（後記第 3 章参照）などが含まれる[45]。これらの措置は、名目上は国家安全保障や個人情報保護を掲げつつも、実質的には規範的影響力や産業上の優位性を確保する機能を果たすことが指摘されている[46]。たとえば、EU の GDPR による「ブリュッセル効果」[47]は域外に対する規範的影響力の拡大をもたらし、他国の企業や政府に GDPR 準拠を事実上強いる作用を持つ。また、中国が掲げる「サイバー主権」に基づくデータ統制政策[48]も、国家安全保障や社会統制を基軸とする強固な主権的運用に依拠し、国外主体にも法的・規範的効果を及ぼし得る性質を伴っている。

国家による正当なデータ保護とデータ保護主義的措置はしばしば重なり合い、その境界は形式的基準のみでは判別しにくいが、越境的データガバナンスの文脈では、両者を厳密に区別する必要がある。この区別を欠けば、国家間の制度的断絶や規範的非対称性が拡大し、信頼に基づく越境的データ流通と国際的相互運用性の確保は一層困難となる。

第 1 項　データ保護主義の弊害

経済の開放性、規制の自律性、そしてデータに対する主権的統制という相互に競合する政策目標のもと、各国は越境的データガバナンスに関し、多様でしばしば相反する制度的アプローチを採用している。個人情報、国家安全保障、公共の利益といったデータ保護の目的は、近代国家にとって正当かつ不可欠な責務である。しかしながら、デジタル貿易の自由化を掲げながらも、厳格なデータの国内保存義務や国外移転制限を導入する政府が増えている（後記第 4 章参照）。これらの措置はプライバシー保護や安全保障を根拠としつつも、運用がその目的に必ずしも限定されず、ときに過剰または不均衡に適用され、正当な目的の範囲を逸脱してデータ保護主義へと転化する[49]。

データ保護主義は、国家安全保障や個人情報保護といった公共目的を根拠として正当化されることが多いが、その実際の運用は、多くの場合、以下のように国際経済秩序、技術革新、制度的協調に深刻な影響を及ぼしている[50]。

---

[44] Chander and Lê (2015), pp. 679–681; Castro (2022), paras. 1–3.
[45] Chander and Lê (2015), pp. 682–708; 三浦秀之（2022）33–40 頁.
[46] Aaronson (2019), pp. 545–552; Castro (2022), paras. 1–4（データ保護主義は、機微情報の漏洩防止やプライバシー保護だけではなく、国外の主体がデータを利用し価値を創出する機会を制限することを主な目的とする政策であると指摘する。）.
[47] Bradford (2020), pp. 1–6.
[48] Hung (2025), pp. 1–10.
[49] Burri (2017), pp. 87–99, 126–132; Aaronson (2019), pp. 548–552; Jiang (2024), pp. 728–734.
[50] Burri (2017), pp. 119–132; Aaronson (2019), pp. 550–557; 福山章子（2021）1–8 頁.

第一に、越境的経済活動を阻害し、企業の業務効率や市場アクセスを制限する。データの越境移転の制約により、企業は現地に独自のインフラや運用体制を構築せざるを得ず、中小企業や新興国にとっては重大な参入障壁となり得る[51]。

第二に、データの囲い込みは国際的な技術協働を困難にし、AI 開発や疫学研究など、広域的なデータ利活用を前提とする領域における研究開発の停滞を招く[52]。

第三に、各国が自国法の域外適用や独自基準を強化することで制度間の相互運用性が低下し、国際的な規範調和の実現が困難となる[53]。

第 2 項　正当なデータ保護とデータ保護主義の区別の必要性

一般に、「データ保護主義」という語は、他国事業者に対して不当または過剰に制限的なデータ規制が課されていると評価される場合に、批判的文脈で用いられることが多い。とはいえ、国際的なデータガバナンスをめぐる議論においては、各国が他国の厳格なデータ保護規制を「保護主義」と批判する一方、自国でも類似の措置を国家安全保障や主権的統制の名の下に正当化し導入するという、二律背反的状況がしばしば見られる。たとえば米国は、GDPR について、データの自由な流通を不当に妨げ、他国企業に過大なコンプライアンス負担を課すものとして批判しているが[54]、他方で米国自身も「懸念国（countries of concern）」に対する情報通信機器・クラウドサービスの利用制限や、政府関連データの国内保存義務化といった、同様に制限的な措置を採用している[55]。これは、概念としての「データ保護主義」が、価値一貫性というよりも、実利的かつ戦略的判断に基づいて用いられる傾向を示している。このような傾向は、国家によるデータ保護の正当性とデータ保護主義的運用との境界を曖昧にし、国際的なデータガバナンスの分断を助長する[56]。

急速に進行する地政学的変動に伴い、国際的データガバナンスの制度的分断は一層深刻化している。問題は、その分断が必ずしも実質的なリスク低減に基づいておらず、経済的・政治的目的を帯びた保護主義的措置として拡大している点にある。こうした措置は、制度間の相互運用性を損ない、国際的協働と域内経済の発展を阻害する。したがって、公共目的に基づく正当なデータ保護と、過度のデータ流通制限を伴う保護主義的措置とを峻別することが、均衡的かつ相互運用可能なガバナンス体制を構築する前提となる[57]。この峻別は、リスクを中立的かつ公平に評価し、その程度に応じて比例的で透明性のある保護措置を設計することによってはじめて実効性を持つ[58]。

他方、こうした基準が不明確なままでは、国家が自国中心の判断を正当化する制度的誘因が高まり、越境的データ移転規制は恣意性を帯びやすくなる。個別措置の妥当性を客観的に評

---

[51] Aaronson (2019), pp. 541–544.
[52] UNCTAD (2021), pp. 41–45; OECD (2022b), pp. 5–6, 14–17.
[53] Burri (2017), pp. 87–93, 126–132; 加藤紫帆（2024）145–154 頁.
[54] Archick (2021), pp. 2–4, 10–12; Aaronson (2019), pp. 548–552.
[55] Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern, 90 Federal Register 1010, 1010–1012 (Jan. 8, 2025). https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern
[56] Ferracane (2021), pp. 66–80.
[57] Aaronson and Leblond (2018), pp. 245–248; Castro (2022), paras. 1–5.
[58] OECD (2020), pp. 25–28, 135–140, 163–169; EDPB (2020b), paras. 3–7, 18–27, 41–44; OECD (2022b), pp. 5–17.

価する枠組みを欠く状況では、各国の法制度は互いに乖離し、データ移転の法的根拠やアクセス要件は法域ごとに異なる方向へ発展する。こうした構造は、次節で検討する制度的非対称性を拡大させる直接的要因となる。

第 3 節　越境的データガバナンスにおける非対称性の深化とその弊害

データガバナンス規範は各国の国内法や政策原則に基づき発展してきたが、データが国境を越えて流通する現代においては、国家間の制度差が直ちに国際的不整合として顕在化する。各国がデータ保護主義的施策を強化する状況の下では、相互運用性を欠いた複数の枠組みが並立し、統一的な規範秩序の形成が困難となっている。

越境的データガバナンスの構造は、地政学的力学、技術的進展、さらには社会規範の変容といった外的要因に強い影響を受けるが[59]、現状では国際的共通原則や制度的調整の欠如により、極めて断片的かつ不均衡な状態にある。各国はそれぞれの法制度、価値観、経済的利益、安全保障上の懸念に基づき独自の規制を展開しており、統一的な国際規範は存在せず、既存の枠組みも限定的な調整機能しか有していない。この拘束力と執行力の脆弱性は、越境的データガバナンスの制度的弱点を構造的に形成している。その結果、越境移転に関する判断は国家の政策裁量や政治的判断に左右され、国際的な相互運用性や法的予見可能性が著しく損なわれている。制度的信頼の基盤形成も十分に進まず、各国の制度は事実上、接続性を欠いた複数の独立した規制圏として分立している[60]。

第 1 項　越境的データガバナンスにおける「ヨコの非対称性」と「タテの非対称性」

米国、中国、EU は、いずれも自らの制度理念に基づく独自のデータガバナンスモデルを展開し、自国のデジタル主権を軸に戦略的優位の確立を図るため、越境的データ移転に関する規制強化を進めている[61]。このような大国間の制度的対立は妥協や収斂を困難にし、国際規範の形成を大きく阻害している。他方、多くの非大国は、技術的・制度的依存や交渉力の弱さにより、自律的な制度設計が困難であり、ガバナンス格差が拡大しつつある[62]。非大国の間でも、自国の統制権強化や保護的経済戦略を背景に、独自のデータ保護主義的措置が拡散しており、規範的・制度的非対称性は一層深刻化している。なかには、統治効率の向上や国民監視の強化を目的としてデータの国内保存義務や越境移転規制を強める開発途上国も存在し、非対称性の構造を複雑化させている[63]。

こうした状況により、越境的データガバナンスにおける非対称性は深刻化し、「ヨコの非対称性」と「タテの非対称性」という二つの層の構造的問題が顕在化している。

(1)　「ヨコの非対称性」

越境的データガバナンスにおける「ヨコの非対称性」とは、主要国・地域ブロック間における法制度と価値観の断絶を指す。国際的統一規範が存在しない状況では、各ブロックが自らの制度と価値観を軸に独自のデータガバナンス体系を形成するため、制度的互換性が欠如した複数のモデルが併存する構造が生じる。

---

[59] Aaronson and Leblond (2018), pp. 245–248; Pierucci (2025), pp. 1–4.
[60] Meltzer (2014), pp. 96–102; Cory and Dascoli (2021), pp. 6–20; OECD (2023a), pp. 11–18.
[61] Bradford (2020), pp. 7–15; Bradford (2023), pp. 1–6, 33–45, 82–96, 105–120; Hung (2025), pp. 3–5.
[62] Aaronson and Leblond (2018), pp. 245–251; UNCTAD (2021), pp. 8–15.
[63] UNCTAD (2021), pp. 43–46, 55–60; Jiang (2024), pp. 731–734.

現在、米国・中国・EU は、自国の規範モデルを国際的に押し広げるため、域外適用、市場力、規範輸出などの複合的手段を組み合わせ、他国のデータ取扱いに実質的制約を加える制度運用を行っている。これらの多くはデータ保護主義的性質を帯びており、デジタル主権の名の下で国際的主導権を確保する戦略に位置づけられる[64]。

米国は、圧倒的な産業競争力と市場支配力を背景に、民間主導で形成された運用基準や慣行を国際的標準として定着させてきた。これらは、地域貿易協定の電子商取引章に組み込まれることにより条約上の義務として制度化され、国際規範としての拘束力を獲得している[65]。さらに、外国情報監視法（FISA）[66]および CLOUD 法[67]は、外国情報収集や刑事捜査の目的で米国の管轄権下にある事業者にデータ開示を命じ得る制度を整備し、当該事業者を通じてデータの所在国を問わずアクセスを可能にする法的基盤となっている[68]。米国はこのように、法制度と市場力を結合する市場支配モデル（Market dominant model）を通じ、国際的制度設計に強い影響力を及ぼしている[69]。

中国は「サイバー主権」の理念を中心に、国家情報法[70]や「中国データ三法」（サイバーセキュリティ法[71]、データセキュリティ法[72]、個人情報保護法[73]）を体系化し、国家安全保障を優越的価値とする越境的データ移転規制を構築してきた。この枠組みは、サイバー主権モデル（Cyber sovereignty model）として理解され、データ保護主義を制度的に固定化し、その域外的波及を可能にする基盤となっている[74]。

EU は、GDPR に基づく厳格な保護制度を域外適用し、第三国に EU 基準の受容を促す規範統制モデル（Normative control model）を推進している。EU 法の域外適用と厳格なデータ移転条件の設定を通じて各国に制度的収斂を促すことにより、国際規範形成に大きな影響力を行使している[75]。

これらの大国間では、価値体系や政策目的を異にする規範が相互に対立しており、相互理解や歩み寄りによって統一的な枠組みを形成することは現時点では極めて困難である。そのため、互換性を欠く規範体系が並立し、データ移転、AI、クラウド基盤などの分野で国際的な相互運用性が失われ、制度的ブロック化が進行している。この「ヨコの非対称性」は、政策選択の差異だけではなく、価値体系の相克として構造的に定着しつつあり、WTO など既存の多国間フォーラムでは調整困難な分断を生んでいる[76]。

---

64 Bradford (2020), pp. 7–24; Hung (2025), pp. 3–7.
65 Aaronson and Leblond (2018), pp. 245–251; Cory and Dascoli (2021), pp. 6–12.
66 Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § § 1801–1885c (as amended).
67 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 18 U.S.C. § § 2713, 2523 (2018).
68 Daskal (2018), pp. 186–195, 221–226; 有本真由（2019）24–34 頁; 藤井康次郎（2020）56–74 頁.
69 Aaronson and Leblond (2018), pp. 251–256; Bradford (2023), pp. 1–6, 33–45.
70 中華人民共和国国家情報法（National Intelligence Law, NIL）（2017 年 6 月 27 日制定、同日施行）.
71 中華人民共和国サイバーセキュリティ法（Cybersecurity Law, CSL）（2016 年 11 月 7 日制定、2017 年 6 月 1 日施行）.
72 中華人民共和国データセキュリティ法（Data Security Law, DSL）（2021 年 6 月 10 日制定、2021 年 9 月 1 日施行）.
73 中華人民共和国個人情報保護法（Personal Information Protection Law, PIPL）（2021 年 8 月 20 日制定、2021 年 11 月 1 日施行）.
74 Creemers (2017), pp. 85–97; 石本茂彦（2022）37–68 頁; 松尾剛行・胡悦（2022）69–107 頁; 小野寺良文（2022）171–193 頁; Bradford (2023), pp. 1–6, 69–88.
75 Kuner (2017a), pp. 882–885, 892–894; Bradford (2020), pp. 25–65; Bradford (2023), pp. 1–6, 105–121.
76 Aaronson and Leblond (2018), pp. 245–256; Bradford (2023), pp. 1–6, 149–164.

(2) 「タテの非対称性」

越境的データガバナンスにおける「タテの非対称性」は、大国と非大国との間に生じる規範的・経済的支配構造を指す。これは、技術的リソース、データ処理能力、法的影響力の格差が複合的に作用し、大国が規範や技術標準の設定段階を主導することで形成されたものであり、「もう一つのデジタル格差（another digital divide）」とも称されている[77]。

大国間で異なる規範が併存する状況の下で、非大国は制度面および技術面において従属的立場に置かれ、以下の機序により、いずれか一方の大国の規範に従うか、あるいは事例ごとに異なる大国の規範を用いるかという選択を迫られている[78]。

第一に、多くの非大国は自国内で完結する技術インフラやプラットフォームを独自に構築することが困難であり、米中の巨大企業が提供するクラウドサービスや OS に依存する結果、技術的主権の確保が制約されている[79]。

第二に、EU や中国の域外適用型制度に準拠しなければ市場アクセスの拒否や制裁リスクを伴うため、受動的な制度的同調を余儀なくされる[80]。

第三に、多くの非大国では規範制定力や執行力が十分ではなく、自国独自のデータガバナンス制度を構築する能力が脆弱である[81]。

さらに、非大国相互の間でも、国際的な共通基準や相互運用性が確立していないため、個人データの定義、越境移転の許可条件、監督当局の権限といった要件が国ごとに食い違い、相互承認の成立が困難である。その結果、同一取引であっても適用される規範が国により異なり、コンプライアンス負担とリスクが不均衡に配分される。このような規範構造の連鎖作用により、越境的データ流通の方向性や条件は大国のモデルに沿って設定されやすくなり、国際的データガバナンスの均衡を欠く状態が持続する[82]。

こうした大国による規範的影響はグローバルサウス諸国に限られず、一定の制度的基盤を有する日本のような国にも及んでいる。そのため、現行の国際秩序下では、支配的データ保護モデルとの整合性を前提とした制度設計が事実上不可避となる。新興国・途上国の多くは、大国の法制度や技術基準に適合しなければ国際取引に参加できず、自国の政策的裁量や技術主権を実質的に喪失している[83]。さらに、大国が自国法を域外適用することにより、表向きは普遍的価値を掲げながらも、実質的には非大国に規制負担を転嫁し、従属的な制度秩序を固定化している。この「タテの非対称性」は、国際経済のデジタル依存関係を深化させ、規範の一方向的流通と経済的価値の片方向的集中という二重のメカニズムを通じて、非大国の構造的従属を持続的に強化している。その結果、越境的データ流通の制限は保護主義的措置の性質を帯びながら正当化されやすくなり、自律的かつ公平な越境的データガバナンスの構築は構造的に制約され、国際的分断は一層深化している[84]。

---

[77] Aaronson and Leblond (2018), pp. 245–251; UNCTAD (2021), pp. 28–31.
[78] Aaronson and Leblond (2018), pp. 245–256; Ferracane et al. (2018), pp. 13–22, 51–61.
[79] Stürmer et al. (2021), pp. 7–8, 12–14, 23–24; UNCTAD (2021), pp. 22–24, 39–41.
[80] Bradford (2020), pp. 25–65; Gao (2021), pp. 252–267.
[81] Aaronson and Leblond (2018), pp. 245–248; Bradford (2020), pp. 131–169.
[82] Aaronson and Leblond (2018), pp. 248–251; Ferracane et al. (2018), pp. 27–35.
[83] Aaronson and Leblond (2018), pp. 245–248; Bradford (2020), pp. 131–169; Stürmer et al. (2021), pp. 4–7.
[84] Aaronson and Leblond (2018), pp. 245–256; Bradford (2023), pp. 1–36.

今後の国際的議論においては、大国の一国主義的措置の抑制と、非大国による自立的ガバナンス体制の構築を可能にするため、越境的データガバナンス規範に柔軟性と段階的適応可能性を組み込んだ制度設計が求められる。分野別・段階的な協定、共通の評価基準、義務的紛争処理制度を組み合わせ、主権的統制と国際的相互運用性の均衡を制度的に担保することが不可欠である。

第 2 項　非対称性による弊害

越境的データガバナンスにおいては、国際的に統一された規範が欠如するなかで、「ヨコの非対称性」と「タテの非対称性」が重層的に作用し、各国が自国の制度的・価値的枠組みに基づいてデータ統制を強化することにより、相互運用性と信頼に基づく国際的秩序が揺らいでいる。その結果、インターネット利用に関する不平等の拡大、学術データの閉鎖化・イノベーションの停滞、さらには規範的・経済的従属構造の固定化という深刻な現象が進行し、越境的な知識共有と技術協働の基盤が損なわれている。

(1)　インターネット利用に関する不平等の拡大

インターネットは、技術的中立性と普遍的接続性を基礎理念として発展してきたが、急激な地政学的変動、国家によるデジタル主権行使の強化、サイバー安全保障政策の拡大を背景として、各国・地域が独自の規制枠組みを形成する動向が顕著となっている[85]。今日のインターネットは、単一のグローバル空間としてのまとまりを失い、法域・価値体系・技術基準ごとに区分された複数のネットワーク群として機能する構造へと変容し[86]、「スプリンターネット（Splinternet）」と揶揄されるまでになっている[87]。この語は、splinter（分裂・断片化）と internet を組み合わせた造語であり、国家的規制や地政学的対立によりインターネットが断片化する状況を象徴的に表現したものである。現時点では世界規模の接続性が形式的には維持されているものの、利用者がどのデータにアクセスできるか、どの程度の通信品質が確保されるか、どのサービスを利用できるかといった要素が、国家・地域によって大きく異なりつつあり、インターネット利用に関する不平等が拡大している[88]。国家によるアクセス制限や検索結果の地域差、通信経路への介入、特定サービスの提供地域限定、クラウド基盤の分断などの要因により、利用者が到達し得る領域や享受できる機能が制度的ブロックごとに差異化されつつある[89]。こうした不平等により、利便性の差にとどまらず、国家境界ごとに利用者が接触し得る領域が異質化し、越境的な知識共有と協働を支える基盤が揺らぎつつある[90]。インターネット利用に関する不平等が固定化すれば、形式上の接続が残っていても、実質的には複数の閉じた領域が並立する構造が生じ、やがてはサイバー空間の実質的分裂を招来するおそれがある[91]。

---

[85] Aaronson (2018), pp. 2–4, 7–12; Arcesati et al. (2023), pp. 13–20; Nocetti (2024), pp. 8–16.
[86] Drake et al. (2016), pp. 10–15.
[87] Drake et al. (2016), pp. 7–9; Lemley (2021), pp. 1399–1406.
[88] Aaronson and Leblond (2018), pp. 245–259; Gao (2021), pp. 256–267.
[89] Drake et al. (2016), pp. 31–41; Del Giovane et al. (2023), pp. 5–12.
[90] Aaronson (2018), pp. 8–12; UNESCO (2022), pp. 73–85, 91–106.
[91] Weber (2014), pp. 6–7, 11–12; Drake et al. (2016), pp. 15–19; Lemley (2021), pp. 1399–1415.

(2)　学術データの閉鎖化・イノベーションの停滞

非対称なデータ統制は、知識と叡智の共有を阻害する。各国がプライバシー保護や国家安全保障の名目でデータ移転を制限することにより、学術研究や科学技術分野における越境的な知識循環が著しく制約されつつある。たとえば、GDPR の厳格な域外移転規制は、医療、AI、環境科学などの分野で国際共同研究に必要なデータ共有を困難にしているとの指摘がある[92]。さらに、中国、ロシア、インドなどが国家安全保障上の理由で研究データの国外提供を制限していることも、国際的な学術協働の障壁となっている[93]。これらの規制は、自国の科学的基盤を保護する意図を有しつつも、国際的なデータエコシステムの分断を招き、知識の再利用・再検証や透明性の確保を困難にしている。結果として、研究成果の地域的偏在が進み、世界的な課題―パンデミック、気候変動、AI 倫理など―への協働的対応能力が低下している[94]。換言すれば、データガバナンスにおける制度的非対称性は、知識を共有財として管理・利用するための制度的枠組み（knowledge commons governance）を弱体化させ、知識へのアクセスや再利用を支える制度的均衡を損なっている[95]。こうした閉鎖化の進行は、叡智の越境的循環を断絶し、イノベーションを停滞させ、人類全体としての学術的・技術的進歩の基盤を脆弱化させるものである[96]。

(3)　規範的・経済的従属構造の固定化

越境的データガバナンスの非対称性は、国家間における規範的・経済的従属構造の固定化を促進している。データが経済成長と技術革新の中核的資源として位置づけられる現在、データへのアクセスおよびその利用能力の格差は、経済的のみならず制度的不均衡を再生産する主要因となっている。米国・中国・EU といった大国は、グローバル・プラットフォームやクラウドインフラの支配を通じて、データの収集・分析・応用に至る全過程を統制し、国際的デジタル経済の上流を掌握している。一方で、多くの新興国・途上国は、大量のユーザーデータ・社会データの提供源となっているにもかかわらず、その価値を自国の経済循環や政策形成に十分に還元できず、データ依存型経済のなかで大国の従属的地位に置かれている[97]。

さらに、先進国によるデータ保護規制の域外適用は、表面的には普遍的価値の実現を標榜しつつも、実際には発展途上国に対し技術的・法的コストの負担を転嫁し、規範的従属を強化する作用を有している。このような構造的非対称性は、市場支配の問題に加えて、デジタル主権および制度的自律性の喪失を引き起こし、国際経済秩序における不均衡を構造的なものとしている。その結果、データを媒介としたグローバルな富と知識の流通は一部の大国に集中し、国家間における規範的・経済的従属構造が固定化されることにより、制度的格差と価値の偏在が構造的に深化している[98]。

---

[92] Aaronson and Leblond (2018), pp. 245–259; UNESCO (2022), pp. 73–85, 91–106; Lalova-Spinks et al. (2024), pp. 1–3.
[93] Arcesati et al. (2023), pp. 13–20; Nocetti (2024), pp. 19–27.
[94] Verhulst and Young (2022); Tenopir et al. (2020), pp. 4–9.
[95] Madison (2020), pp. 29–43.
[96] Verhulst and Young (2022).
[97] Aaronson and Leblond (2018), pp. 245–251; UNCTAD (2021), pp. 81–85.
[98] Aaronson (2018), pp. 4–12; Bradford (2020), pp. 221–231; UNCTAD (2021), pp. 81–85.

第 3 項　　非対称性克服への方向性

越境的データガバナンスにおける「ヨコの非対称性」は、大国間における規範的対立に起因し、「タテの非対称性」は大国と非大国との間に存在する権力およびガバナンス格差に基づいている。両者は相互に補強し合う関係にあり、規範のブロック化が進展することで、各ブロック内の大国が主導的地位を強め、垂直的な従属構造が固定化される。このように、越境的データガバナンスの非対称性は、横断的な規範の断絶と縦方向の支配構造が交錯する多層的構造として理解する必要がある。この構造的非対称性を克服するためには、越境的データガバナンス規範を再構成し、ブロックの壁を越えた相互運用性と、大国・非大国間における規範的衡平性を確保することが不可欠である[99]。その際、各国の主権的統制の多様性を尊重しつつ、制度的成熟度に応じた柔軟な調整を可能とする仕組みを導入することが求められる。具体的には、比例原則およびリスクベースアプローチを基盤とし、データ保護やセキュリティに関する規範を段階的に調整することで、相互運用性を現実的に確保することができる。さらに、信頼と透明性を制度的基盤とする新たな国際秩序の形成を目指し、各国が協調的に関与できる枠組みを構築することが重要である。これにより、規範の断絶と支配構造の固定化を乗り越え、より公平かつ持続可能な越境的データガバナンスの実現が可能となる。

[99] Aaronson (2018), pp. 12–17; OECD (2019a), pp. 17–19, 87–94; UNCTAD (2021), pp. 111–115, 147–158.

第 4 節　越境的データガバナンス規範再構成の必要性

越境的データガバナンスについては、国家間の制度差および大国による規範的支配の影響を受け、非対称性が一層深化している。越境的データガバナンスの非対称性が国家間の主要課題となるのは、データの移転や利用が国境を越えて行われる際に、各国の法的・規範的体系の相違が必然的に摩擦を生じさせるためである。ある国で適法とされるデータ処理が、他国の枠組みの下では制限または禁止の対象となる場合もあり、この構造的齟齬は、各国制度間の整合性が求められる国際的課題として顕在化している。さらに、規範の分断が進めば、相互運用性や透明性が損なわれ、データ流通の安定性と予見可能性が低下する。

現状では、各国が異なる価値体系や安全保障上の論理に基づき独自のデータ規制を強化することで、世界のインターネット空間はもはや単一の相互接続的ネットワークではなく、政治的・法的領域ごとに分断された構造に変容しつつある。この現状を放置すれば、国際社会に深刻な法的・経済的・技術的亀裂をもたらすおそれがある[100]。しかし、このような状況は、各国が単独で克服できるものではなく、国際的な協調と制度間の整合性の確立を通じて対応する必要がある。

国際的な共通原理に基づく秩序を形成するためには、技術基準の整合だけではなく、分断された枠組みを再編し、データ移転の正当化原理とリスク評価を調和させることが不可欠である。越境的データガバナンス規範の再構成は、次の四つの理由から要請される。

第一に、分断された法制度の整合である。現在の国際秩序では、米国・中国・EU といった大国が、それぞれ自国の法制度と価値観を基礎として異なる規範を提示しており、共通のルールや翻訳可能性を欠いている。その結果、同一のデータ処理行為に対して法域ごとに異なる法的評価が下され、越境的取引の安定性が損なわれている。したがって、越境的データガバナンス規範の再構成により、こうした断片を接続し得る共通の評価基準を確立し、仕組み全体の相互運用性を回復することが必要となる[101]。その中心となるのが比例原則およびリスクベースアプローチであり、これらを基礎に相互運用性のある共通規範を整えることが求められる。

第二に、データ保護主義の拡大と国際的分断の克服である。各国が主権や安全保障を根拠としてデータの囲い込みを強化することで、自由で信頼に基づくデータ流通が損なわれている。この傾向は、特に新興国や中小事業者に不均衡な負担を課し、新たな依存関係を生み出している。したがって、規範再構成は自由化のみを目的とするものではなく、DFFT（Data Free Flow with Trust）の理念を具体化し（後記第 9 章第 1 節参照）、衡平で実効的に運用可能な国際枠組みを築くものであることが必要となる[102]。

第三に、技術的および制度的変化への適応である。クラウド、AI、IoT、それにフェデレーテッド・ラーニングなどの分散型技術が急速に発展し、データはもはや一国の領域内に固定されず、ネットワーク全体で生成・分析・再利用されている。従来の領域主権を前提とする規制構造では、こうした分散的処理を十分に制御できない。リスクの程度と利用文脈に応じて規制の範囲を比例的に調整する柔軟な統治原理の確立が求められる[103]。

---

[100] Aaronson and Leblond (2018), pp. 245–251; OECD (2023a), pp. 7–17.
[101] Aaronson and Leblond (2018), pp. 245–251; OECD (2023a), pp. 7–17.
[102] Aaronson (2018), pp. 12–17; OECD (2023a), pp. 7–22.
[103] McMahan et al. (2017), pp. 1273–1282; OECD (2023a), pp. 19–22.

第四に、国際的ルール形成の空白を補う必要がある。WTO や地域貿易協定は、電子商取引やデジタル貿易の基本原則を定めているが、非個人データを含む各種のデータ保護、ガバメントアクセスの要件、越境的データ移転と司法手続との調整といった領域については、統一的かつ実行性のある制度枠組みを提供しているとは言い難い。このため、越境的データガバナンスに関する紛争解決や政策調整を包括的に扱う仕組みは依然として欠如している。したがって、規範再構成により、この空白を埋めるための新たな国際協調原理と手続的保障を整備する必要がある[104]。

以上のとおり、越境的データガバナンス規範再構成とは、国家主権の多様性を尊重しつつ、断片化した制度間の齟齬を是正し、国際的相互運用性を回復するための取組である。規範再構成を実効的なものとするためには、データの性質や利用文脈に応じて、規制と保護の水準を段階的かつ柔軟に調整し得る仕組みを整え、分断された国際秩序を再接続する基盤を確立することが求められる。これにより、信頼を基盤とする合理的で持続可能な越境的データ流通秩序の確立へと道が拓かれる[105]。

[104] OECD (2023a), pp. 7–22; WTO (2024), pp. 2–3, 6–12; Dimitropoulos et al. (2025), pp. 2–22.
[105] McMahan et al. (2017), pp. 1273–1282; Aaronson (2018), pp. 12–17; OECD (2023a), pp. 7–22.

第 2 章

伝統的基本原則の実効性喪失と国際的統一規範の欠如

第 2 章　伝統的基本原則の実効性喪失と国際的統一規範の欠如

越境的データガバナンス規範は、主としてデータの越境移転に関する統制のルールを定めるものである。越境的データ移転に関する国際的統一規範の策定をめぐっては、国際フォーラムのなかでも WTO における取組が最も先行してきた。WTO 体制は、第二次世界大戦後の国際経済秩序のなかで、無差別・自由化・予見可能性などの基本原則を確立し、各国が市場アクセスと制度的安定性を共有するための普遍的枠組みを構築してきた。これらの原則は、貿易政策の一貫性と均衡的な競争環境を確保することにより、国家間の経済的相互依存を制度的に支えてきた点に歴史的意義を有する。

WTO は、GATT（関税及び貿易に関する一般協定）[106]のほか、サービス貿易の自由化と無差別原則を中核とする包括的な法的枠組みである GATS（サービスの貿易に関する一般協定）[107]を有しており、その制度基盤を活用してデジタル貿易やデータ流通を扱うことが可能と考えられてきた。さらに、WTO は拘束力のある紛争処理制度（DSU）を備え[108]、加盟国間で合意されたルールの履行を制度的に担保できる唯一のグローバルな貿易フォーラムであることから、デジタル経済分野においても最も信頼性および正統性の高い交渉の場として位置づけられてきた。加えて、WTO は 160 を超える加盟国を擁し[109]、グローバルサウスを含む新興国も幅広く参加しているため、包摂的かつ普遍的な国際規範形成を可能とする制度的基盤を備えている。

純理論的には、GATS が定める基本原則である最恵国待遇・内国民待遇・市場アクセス義務・透明性義務を越境的データガバナンスに全面適用すれば、国家が特定国だけに不利な移転条件を課したり、独自の閉鎖的ブロックを形成したりする行為が制度的に抑制され、各国はデータ移転に関して均質かつ非差別的な基準を採用せざるを得なくなるため、国境をまたぐデジタルサービスの相互接続性が高まり、結果としてサイバー空間が複数の制度的ブロックへと分裂する誘因は理論上大幅に低減されるはずである[110]。

しかし、GATS の基本原則をそのまま適用しようとするだけでは、データ規制が国家安全保障や個人情報保護、ガバメントアクセスといった主権的統治領域と密接に結びついている現実に対応できず、米国・EU・中国が異質な規範モデルを相互に競合させている状況から生じる制度的非対称性を調整することもできない。そのため、サイバー空間は依然として分断の圧力に晒される構造から抜け出せない[111]。

現状では、WTO における越境的データ移転に関する国際的統一規範の策定をめぐる議論も、大国間の主権・安全保障をめぐる利害の対立によって停滞している。その結果、WTO の制度的正統性は維持されつつも、実質的規範形成力は大きく制約されている。また、GATS による統制

---

[106] General Agreement on Tariffs and Trade (GATT), Oct. 30, 1947, 55 U.N.T.S. 194. https://www.wto.org/english/docs_e/legal_e/gatt47_01_e.htm

[107] General Agreement on Trade in Services (GATS), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183. https://www.wto.org/english/docs_e/legal_e/26-gats.pdf

[108] WTO (1994), Arts. 2(1), 3(2).

[109] 2024 年 8 月 30 日現在、WTO には 166 の国・地域が加盟している。WTO, Members and Observers. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (accessed 22 February 2026).

[110] Mitchell and Mishra (2019), pp. 405–408; Naef (2021), pp. 233–252.

[111] Mitchell and Mishra (2019), pp. 402–408; UNCTAD (2021), pp. 86–116; Christakis (2024a), Introduction, Part I, Part II.2, Conclusions; Yakovleva (2024), pp. 111–120.

は、デジタル経済への制度的対応の遅れや例外規定の広範な適用などから、越境的データガバナンスに関する国際的統一規範としての実効性を喪失している[112]。さらに、他の多国間フォーラムにおける議論も、各国の法制度や政策目的、デジタル主権や国家安全保障に対する認識の差異が大きく、拘束力を有する合意形成には至っていない。そのため、現行の枠組みは理念的・宣言的な性格にとどまり、各国の主権的判断を超えた法的拘束力および紛争処理機能を備えた実効的な規範調整の実現は構造的に困難な状況にある[113]。

本章では、まず第 1 節において越境的データガバナンスにおける WTO 基本原則の実効性喪失を分析し、次に第 2 節において WTO その他の多国間フォーラムにおける統一規範策定の限界を検討したうえで、第 3 節で越境的データガバナンス規範再構成に向けた課題を提示する。さらに、第 4 節では先行研究の潮流と本稿の位置づけを確認する。

[112] 東條吉純（2020a）35–52 頁.
[113] Aaronson (2018), pp. 7–16; Dimitropoulos et al. (2025), pp. 7–15.

第 1 節　越境的データガバナンスにおける WTO 基本原則の実効性喪失

WTO 事務局が公表している「Principles of the Trading System」においては、国際取引体制を支える基本理念として、無差別取引、貿易の自由化、予見可能性、公正な競争の促進、および開発と経済改革の奨励の五つが掲げられている[114]。本節では、これらのうち越境的データガバナンスと密接に関連する三つの原則[115]—無差別、自由化、予見可能性—に焦点を当て、その実効性喪失の構造的要因を検討する。

デジタル化の進展により、経済取引の中核がデータ流通へと移行するなかで、これらの規範原則は従来の形では越境的データ移転の規範としての機能を喪失している[116]。データは、財やサービスとは異なり、国家主権、安全保障、個人の権利保障と密接に関わる多層的性質を有するため、単純な市場自由化の文脈では整理しきれない複雑性を内包する。各国はデータの取扱いを公共政策や国家安全保障の観点から制約する方向へと傾斜しており、越境的データ移転に対して従来の無差別原則や自由化原則を適用することが困難となっている[117]。

さらに、データガバナンスにおいては、国内外の法制度、技術基準、監督体制が国によって大きく異なり、越境的データ移転に関する予見可能性が著しく低下している。予見可能性を担保するための透明性確保の要請も、データローカライゼーションなどによるデータの囲い込みのほか、企業によるソースコードやアルゴリズムの保護によって形骸化しつつある[118]。

このように、WTO 体制下で培われた三つの基本原則は、国際経済秩序の根幹的理念として制度的には継承されているものの、越境的データガバナンスの領域においては、制度面と実質面の双方においてその実効性を喪失している。WTO の諸原則は依然として条約上存続しているとはいえ、データという新たな規律対象を前に、その規範的拘束力の限界を露呈しており、理念と現実との乖離は一層深刻化している[119]。本節では、これらの基本原則の実効性喪失という構造的問題を分析する。

第 1 項　越境的データ移転への GATS の適用可能性

WTO 基本原則の実効性喪失についての分析の前提として、GATS の規定が越境的データ移転に適用され得る点を確認する。現代の国際取引においては、越境的データ移転が国際経済活動の中核的要素となっており、データの自由な流通は国際貿易の実効性と密接に結びついている[120]。GATS は国際サービス貿易の自由化を目的として構築された多国間協定であり、データ移転やデジタル手段によるサービス提供が国際取引の主要形態となった現代においては、その適用範囲には越境的データ移転もサービス提供の不可欠な構成要素として含まれ得る[121]。

---

[114] WTO (n.d.b).
[115] WTO (n.d.b), sections “Trade without discrimination,” “Freer trade: gradually, through negotiation,” and “Predictability: through binding and transparency.”
[116] Burri (2017), pp. 93–101; Aaronson (2018), pp. 5–12.
[117] Burri (2017), pp. 87–93; Aaronson (2018), pp. 4–12; Chander (2020), pp. 142–166.
[118] Aaronson and Leblond (2018), pp. 245–254; Aaronson (2019), pp. 544–565; OECD (2022b), pp. 6–14, 17.
[119] Burri (2017), pp. 87–99; Aaronson and Leblond (2018), pp. 246–255; Dimitropoulos et al. (2025), pp. 7–14, 17.
[120] Aaronson and Leblond (2018), pp. 245–248; OECD (2020), pp. 27–28, 135–137.
[121] Mitchell and Mishra (2019), pp. 399–403.

GATS 第 1 条第 1 項は、「サービスの貿易に影響を及ぼす加盟国の措置」を対象とし、第 2 項では「サービスの貿易」を四つのモードに分類している。すなわち、①越境取引（第 1 モード）、②国外消費（第 2 モード）、③商業拠点（第 3 モード）、④自然人の移動（第 4 モード）である。このうち第 1 モード（越境取引）は、「いずれかの加盟国の領域から他の加盟国の領域へのサービスの提供」を指し、クラウド、AI、電子金融、教育、医療などのデータの越境移転を前提とするデジタルサービスが典型的に該当する。したがって、これらのサービスを対象とする限り、GATS の基本的義務を定めた規定が原則として適用される[122]（以下、参照条文は各項末尾に掲載する。）。

他のモードも、デジタル経済において一定の関連性を有する。第 2 モード（国外消費）は、オンライン教育や遠隔医療の利用者が国外のサービスを消費する場合に実質的に重なり合うことがあり、第 3 モード（商業拠点）は、外国のクラウド事業者やプラットフォーム企業が現地法人を設立してデータ処理を行う場合に該当する。また、第 4 モード（自然人の移動）は、越境的データ管理や AI 開発の専門家が物理的に他国へ移動してサービスを提供する形態として関係する[123]。

このように、GATS の四つのモードのうち、第 1 モードが越境的データ移転との関連で最も中心的であるものの、デジタル経済の特質上、複数のモードが相互に重複し得る。したがって、GATS の規律構造全体は、越境的データガバナンスの制度的文脈においても適用される。

【参照条文】

GATS（サービスの貿易に関する一般協定）

第 1 条（適用範囲及び定義）

1. この協定は、サービスの貿易に影響を及ぼす加盟国の措置について適用する。
2. この協定の適用上、「サービスの貿易」とは、次の態様のサービスの提供をいう。
   (a) いずれかの加盟国の領域から他の加盟国の領域へのサービスの提供
   (b) いずれかの加盟国の領域内におけるサービスの提供であって他の加盟国のサービス消費者に対して行われるもの
   (c) いずれかの加盟国のサービス提供者によるサービスの提供であって他の加盟国の領域内の業務上の拠点を通じて行われるもの
   (d) いずれかの加盟国のサービス提供者によるサービスの提供であって他の加盟国の領域内の加盟国の自然人の存在を通じて行われるもの
3. この協定の適用上、
   (a) 「加盟国の措置」とは、次の措置をいう。
      (i) 中央、地域又は地方の政府及び機関がとる措置
      (ii) 非政府機関が中央、地域又は地方の政府又は機関によって委任された権限を行使するに当たってとる措置

   加盟国は、この協定に基づく自国の義務及び約束を履行するに当たり、自国の領域内の地域及び地方の政府及び機関並びに非政府機関による当該義務及び約束の遵守を確保するため、利用し得る妥当な措置をとる。

[122] Willemyns (2018), pp. 4–7; 中川淳司（2019）207–217 頁.
[123] Willemyns (2018), pp. 4–7; 中川淳司（2019）207–217 頁.

(b)「サービス」とは、政府の権限の行使として提供されるサービス以外のすべての分野におけるすべてのサービスをいう。

(c)「政府の権限の行使として提供されるサービス」とは、商業的な原則に基づかず、かつ、一又は二以上のサービス提供者との競争を行うことなく提供されるサービスをいう。

第 2 項　無差別原則の実効性喪失

無差別原則は、WTO 体制を貫く最も基本的な規範原理であり、GATS 第 2 条の最恵国待遇（Most-Favoured-Nation Treatment: MFN）および GATS 第 17 条の内国民待遇（National Treatment: NT）を中核として、各加盟国に対し他国のサービス提供者を自国事業者と平等に扱うことを求めるものである[124]。実際に EC – Bananas III 事件[125]および Canada – Autos 事件[126]において、WTO 紛争処理機関（パネルおよび上級委員会）は、特定国を優遇したサービス供給が GATS 第 2 条違反に当たると認定している。

越境的データ移転の文脈においても、特定国との間でのみデータ移転を認める制度や、一部の国との間で限定的にデータ移転を行う制度的運用は、他国に対する不利益な差別として MFN 義務に抵触し得る。たとえば特定国のソーシャル・ネットワーキング・サービス（SNS）の利用を禁止する措置は、MFN 義務に違反する可能性がある。加盟国が特定国に属する SNS 事業者（中国の TikTok や米国の Facebook など）の利用や提供を禁止しつつ、他国の SNS（EU 企業のプラットフォームなど）の利用を認める場合、その措置は特定国の事業者に対して不利な待遇を与える差別的措置と評価され得る。当該措置の目的がいかに公共的であっても、その運用が特定国を標的とする形で行われる場合には、同種のサービス供給に対して国籍を理由とする差別的取扱いを行ったとみなされ、MFN 違反に該当する可能性が高い[127]。

さらに、GDPR 第 45 条に基づく十分性認定制度[128]も、EU 域外へのデータ移転を包括的に制御する手段として設計されているが、認定を受けた国の事業者に比して、認定を受けていない国の事業者に対しより厳格な移転条件（標準契約条項や拘束的企業準則など）を課す結果を招く。これは実質的には加盟国間で異なる取引コスト構造を生み出すことで、サービス供給条件に差異を生じさせるおそれがある。十分性認定は、その判断基準に政治的・制度的要素を含むため、すべての第三国に対して透明かつ非差別的に適用されるとは限らず、このような差別的取扱いは MFN 義務に抵触し得る[129]。

しかしながら、越境的データガバナンスの領域においては、この無差別原則はその根拠となる前提条件を失いつつある。

---

[124] 清水章雄（2019）104–125 頁.

[125] WTO (1997) European Communities – Regime for the Importation, Sale and Distribution of Bananas (EC – Bananas III). Report of the Appellate Body, WT/DS27/AB/R, adopted 25 September 1997, paras. 231–234, 246–249. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/27ABR.pdf

[126] WTO (2000) Canada – Certain Measures Affecting the Automotive Industry (Canada – Autos). Report of the Appellate Body, WT/DS139/AB/R and WT/DS142/AB/R, adopted 19 June 2000, paras. 84–100, 162–171. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/139ABR.pdf

[127] Aaronson (2018), pp. 4–16; Willemyns (2018), pp. 4–9; Meltzer and Lovelock (2018), pp. 1–5, 13–25.

[128] GDPR arts. 45–47.

[129] Velli (2019), pp. 884–891; Yakovleva (2024), pp. 65–66, 142–154, 166–174; Saluste (2025), pp. 596–607.

第一に、GATS が想定していたのは、同質的なサービス取引を対象とした経済的待遇の平等であり、データの移転や処理のように、各国の法的・倫理的・技術的条件に左右される領域を規律するための制度ではなかった。越境的データ移転に関しては、各国のプライバシー保護水準、国家安全保障政策、監督体制の整合性など、制度的要素が根本的に非対称である。したがって、同様の状況にある加盟国を同様に扱うという MFN の前提が成り立たない。この構造的不均衡は、無差別原則が実質的に機能しない最大の要因である[130]。

第二に、無差別原則の形式的運用は、むしろ制度間の信頼格差を拡大させる結果をもたらしている。その典型例が、GDPR に基づく十分性認定制度である。EU は、第三国のデータ保護法制が GDPR と「実質的に同等」であると認定された場合に限り個人データの移転を許容するが、この仕組みは実質的には国別の差異的取扱いを制度的に導入するものであり、MFN 原則の理念とは整合しない[131]。ただし、この差異化は恣意的差別ではなく、各国の制度的信頼性に応じた比例的差別化として構成されている。すなわち、越境的データガバナンスにおいては、形式的平等ではなく比例的平等を基準とする新たな平等概念が求められる[132] 。

第三に、データの性質そのものが無差別原則の適用を著しく困難にしている。データは物理的国境を越えて瞬時に移転され、クラウド上で断片化・再構成されながら分散的に処理される。このような構造の下では、取引の供給主体や取引地を特定することが技術的に不可能であり、どの国の事業者がどの国の規制下で活動しているのかを明確に区別できない。したがって、GATS 第 2 条及び第 17 条が前提とする特定の事業者に対する待遇の比較や、その差異を差別として特定するための基盤そのものが失われている。さらに、異なる暗号化基準やデータ処理プロトコルの採用により、各国の技術的互換性が欠如しているため、結果として特定国の事業者が不利益を被っても、それが制度的差別によるものなのか、技術的非互換性の結果なのかを判別することができない。このように、データの非物質的・分散的性質は、無差別原則を実質的に適用不能にしている[133]。

以上のように、越境的データガバナンスとの関係で GATS の無差別原則は、法的にも政策的にも実効性を失っている。他方で、特定国のデータ保護主義的施策が、MFN 義務を含む GATS の関係規定に違反しないと解される場合、それは当該措置の正当化根拠を与えるのみならず、他国が同様の措置を拡大適用する契機となり得る。このように、GATS の無差別原則の適用は越境的データ移転に関して重大な制度的課題を内包しており、その再解釈を通じた新たな制度設計の必要性を示唆している。信頼・同等性・透明性といった価値を無差別原則とどのように整合的に制度化するかが、今後の越境的データガバナンス規範再構成における核心的課題となる[134]。国際経済秩序の公正性と予見可能性を担保するうえで、無差別の理念そのものを放棄することはできない。むしろ、その再構成こそが重要である。すなわち、無差別原則を形式的平等ではなく、リスクおよび信頼水準に応じた比例的平等として再定義する必要がある。各国が法的・技術的整合性を高め、信頼水準を均衡させることによって、データ移転の自由と平等を保障

[130] Aaronson and Leblond (2018), pp. 248–256; Willemyns (2018), pp. 4–9.
[131] Bradford (2020), pp. 25–48; Yakovleva (2024), pp. 111–120.
[132] Kuner (2017a), pp. 888–909; OECD (2023a), pp. 7–9, 19–25.
[133] 川瀬剛志（2015）10–15 頁; Aaronson (2018), pp. 4–16; 東條吉純（2020a）35–55 頁.
[134] Burri (2017), pp. 87–99, 126–129; Aaronson (2018), pp. 4–16; Saluste (2025), pp. 596–607, 611–615.

する構造である。この再構成により、無差別原則は貿易法的義務を超え、制度的信頼に基づく新たな越境的データガバナンス規範として機能し得る[135]。

【参照条文】

GATS（サービスの貿易に関する一般協定）

第 2 条（最恵国待遇）

1. 加盟国は、この協定の対象となる措置に関し、他の加盟国のサービス及びサービス提供者に対し、他の国の同種のサービス及びサービス提供者に与える待遇よりも不利でない待遇を即時かつ無条件に与える。
2. 加盟国は、1 の規定に合致しない措置であっても、「第二条の免除に関する附属書」に掲げられ、かつ、同附属書に定める要件を満たす場合においては、当該措置を維持することができる。
3. この協定の規定は、特定の地域で生産され、かつ、消費されるサービスを国境に隣接する地域に限定して交換することを容易にするため、加盟国が隣接国に対して有利な待遇を与えることを妨げるものと解してはならない。

第 17 条（内国民待遇）

1. 加盟国は、その約束表に記載した分野において、かつ、当該約束表に定める条件及び制限に従い、サービスの提供に影響を及ぼすすべての措置に関し、他の加盟国のサービス及びサービス提供者に対し、自国の同種のサービス及びサービス提供者に与える待遇よりも不利でない待遇を与える（注）。（注：省略）
2. 加盟国は、他の加盟国のサービス及びサービス提供者に対し自国の同種のサービス及びサービス提供者に与える待遇と形式的に同一の待遇を与えるか形式的に異なる待遇を与えるかを問わず、1 の義務を履行することができる。
3. 加盟国が他の加盟国のサービス又はサービス提供者に対して与える形式的に同一の又は形式的に異なる待遇により競争条件が当該他の加盟国の同種のサービス又はサービス提供者と比較して当該加盟国のサービス又はサービス提供者にとって有利となる場合には、当該待遇は、当該加盟国のサービス又はサービス提供者に与える待遇よりも不利であると認める。

第 3 項　自由化原則（および「Free Flow of Data（データの自由な流通）」）の実効性喪失

WTO 体制の根幹をなす自由化原則は、関税その他の貿易障壁を削減し、各国が相互に市場アクセスを拡大することを目的とする国際経済法上の基本理念である。この原則は、GATT および GATS において、モノやサービスの自由な流通を促進する仕組みとして制度化されており、GATS では特に第 16 条（市場アクセス）および第 17 条（内国民待遇）を通じて自由化の制度的枠組みが構築されている。これらの規定は、無差別原則や予見可能性原則と並んで、第二次世界大戦後の国際経済秩序の安定を支えてきた。この場合の自由化とは、国家による貿易制限

[135] 川瀬剛志（2015）10–15 頁; Burri (2017), pp. 87–99, 126–129; Aaronson and Leblond (2018), pp. 245–261; OECD (2023a), pp. 7–9, 11–25, 31.

の形式的な撤廃を意味するものではなく、制度的蓄積と国際協調を通じて、国際市場の開放性と法的安定性を確保する動的なプロセスを意味する[136]。

この自由化原則の理念は、21 世紀のデジタル経済において「Free Flow of Data（データの自由な流通）」として新たに展開された。データを国際取引の主要資源と捉え、モノやサービスと同様に国境を越えて自由に移転されるべきものと位置づける考え方である。米国は巨大 IT 企業の成長を背景に、この理念を自国の通商政策の中核に据え、地域貿易協定において越境的データ移転制限の禁止条項およびデータ国内保存義務の禁止条項を導入するなど（後記第 8 章第 1 節参照）、自由化原則のデジタル版として「Free Flow of Data」の制度化を主導した[137]。この理念は G7 や OECD を通じて国際的共通目標として共有され、デジタル経済における自由貿易の基本原則として一定の実効性を有していた[138]。

GATS 第 16 条に定める市場アクセス義務は、加盟国が約束表において自由化を約した分野について、数量的制限や事業形態の制限など、外国サービス供給を妨げる措置を導入してはならないとするものである。これにより、越境的データ移転を含む国際的なサービス提供の自由化が制度的に保障される。たとえば、データローカライゼーション措置や越境的データ移転制限は、サービス提供のインフラやデータ処理を国内に限定する構造を強制するため、実質的に外国事業者の越境的サービス供給を不可能または著しく困難にする。その結果、第 16 条第 2 項(a)にいう外国サービス供給者の数量的制限に該当し得ると解される[139]。

また、GATS 第 17 条に定める内国民待遇義務は、加盟国が自由化を約束したサービス分野において、外国サービス供給者を自国供給者より不利に取り扱うことを禁止するものであり、差別的取扱いを排除し、公平な競争条件を確保することを目的としている。たとえば、EU が GDPR の運用において域内ではリスクベースアプローチを採用している一方で、個人データの域外移転には同様のアプローチを適用していない点について、GATS 第 17 条の趣旨との整合性の観点から問題を指摘する見解も存在する[140]。さらに、データローカライゼーション措置との関係では、外国企業に対して国内サーバーの設置、現地法人の設立、または特定の技術的基準への適合を義務づけることが多く、これにより国内事業者には生じない追加的コストや制度的負担を課す。このような差別的効果は、たとえ形式的に中立的に適用し得る規制であっても、実質的には外国供給者に対して不利益を与え、第 17 条第 3 項に違反する可能性があると考えられる[141]。

この GATS 第 17 条の適用に関しては、措置の「効果」を重視する WTO パネルおよび上級委員会の判断傾向がある。たとえば、Argentina – Measures Relating to Trade in Goods and Services 事件において、WTO の上級委員会は、措置が外国事業者に不利な競争条件を生じさせる場合には、形式的な平等性が維持されていても内国民待遇義務違反が成立し得ると判示している[142]。この基準を援用すれば、データローカライゼーション措置が国内事業者には実質的

---

[136] Aaronson (2018), pp. 2–5; 清水章雄（2019）104–125 頁; 東條吉純（2020a）35–55 頁.
[137] Aaronson and Leblond (2018), pp. 248–254; OECD (2020), pp. 27–28, 135–139, 163–168; 藤井康次郎・根本拓・福島惇央（2024）112–136 頁.
[138] G7 (2017), pp. 7–9; OECD (2017), pp. 11–15, 144–145.
[139] Willemyns (2018), pp. 8–12; Mitchell and Mishra (2019), pp. 399–403.
[140] Yakovleva (2024), pp. 316–328, 333–337, 350–352.
[141] Burri (2017), pp. 87–99, 126–132.
[142] WTO (2015) Argentina – Measures Relating to Trade in Goods and Services. Report of the Appellate Body, WT/DS453/AB/R, adopted 9 April 2015, paras. 6.161–6.167, 6.177–6.180.
https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/453ABR.pdf

優位を与え、外国事業者にはコスト的・技術的制約を課す限り、内国民待遇義務の違反として認定される余地がある。

総じて、データローカライゼーション措置は、外国供給者による越境的サービス供給を実質的に阻害する構造的効果を有するため、GATS 第 16 条および第 17 条に基づく自由化義務に抵触し得る。特に、目的がプライバシー保護や安全保障であっても、比例性・必要性・無差別性を欠く運用がなされれば、これらの条項の趣旨に反すると評価される可能性が高い。

以上のように、第 16 条と第 17 条は、サービス貿易の自由化を支える GATS の基本原則であり、デジタル貿易やデータ移転規制の国際的整合性を判断するうえで重要な基準となっている。各国が導入する越境的データ移転制限などの国内措置は、GATS 第 16 条および第 17 条に照らして、実質的な市場アクセス制限または差別的取扱いに該当し得る[143]。もっとも、この点については、GATS 第 16 条および第 17 条の適用が各国の約束表に限定されるため、各国のデータ移転規制がこれらの規定に直接抵触するか否かは、約束の範囲およびその解釈に依存する[144]。

越境的データガバナンスの文脈では、近年の地政学的変化や国家主権の再強化、プライバシー保護および安全保障政策の拡張により、この自由化理念（「Free Flow of Data」）はその普遍的機能を失いつつある。

第一に、米中対立の激化により、米国自身が国家安全保障の観点から自由化原則の例外を拡張し、中国製通信機器の排除や外国クラウドサービスへの制限などを通じて、自由なデータ流通を推進する立場から安全保障的規制の主体へと転換した[145]。他方、中国は「サイバー主権」原則の下、国家主導のデータ管理と移転制限を強化しており、両大国による制度的分断が進行している[146]。

第二に、EU の GDPR は、個人データの越境移転を原則として禁止し、十分性認定や適切な保護措置を条件に例外を認める構造を採用している。これにより、「自由な流通」は制度的に例外化され、自由化よりも基本権保護を優先する枠組みが確立された[147] 。

第三に、AI 技術の急速な発展と政府による民間データへのアクセス拡大は、越境的データ移転に新たなリスクをもたらし、各国が安全保障・人権・倫理の観点から自国データの統制を強化する契機となっている[148]。

第四に、米国自身が WTO 体制からの離脱的姿勢を強め、自由化原則の国際的基盤を動揺させている[149]。特に 2025 年に再登場したトランプ政権は、主要貿易相手国に対する追加関税の復活・拡大を通じて通商政策を再び政治化し[150]、WTO 紛争処理制度を事実上機能不全に追い込んで放置したまま、国際通商秩序の予見可能性と法的安定性を大きく損なっている[151]。

---

143 Burri (2017), pp. 87–93, 126–132; Willemyns (2018), pp. 4–18; Mitchell and Mishra (2019), pp. 396–413.

144 Velli (2019), pp. 884–891; Mitchell and Mishra (2019), pp. 398–407; Yakovleva (2024), pp. 65–66.

145 Congressional Research Service (2022) U.S. Restrictions on Huawei Technologies: National Security and Foreign Policy Considerations, R47012, 5 January 2022. https://www.congress.gov/crs-product/R47012

146 横大道聡（2024）2–35 頁; Hung (2025), pp. 3–10, 18–26.

147 Kuner (2017b), pp. 83–102; 石井夏生利（2025）232–245 頁.

148 UNESCO (2022), pp. 24–27, 43–53, 67–70.

149 Horn H, Mavroidis PC (2025) Why the U.S. and the WTO should part ways. VoxEU (Centre for Economic Policy Research), June 25. https://cepr.org/voxeu/columns/why-us-and-wto-should-part-ways

150 WTO (2025); United States (2025).

151 阿部克則（2019）285–308 頁; Office of the United States Trade Representative (USTR) (2020), pp. 1–3; AFP (2025) Trump tariffs leave WTO adrift in eye of the storm. France 24, February 21. https://www.france24.com/en/live-news/20250221-trump-tariffs-leave-wto-adrift-in-eye-of-the-storm

このように、「Free Flow of Data」は、もともと WTO 的自由化原則をサイバー空間に拡張する試みとして国際的に共有されていたが、地政学的緊張、制度的多様化、規範的価値の分岐を経て、もはや普遍的原理としての機能を喪失している。結果として、各国は自国の制度的自律性と価値秩序に基づいてデータ流通を規律する方向へと分岐しており、越境的データガバナンスは、自由化原則を中核とする秩序から、信頼・比例性・リスクベースを基軸とする新たな規範構造への再編の必要性に直面している[152]。

【参照条文】

GATS（サービスの貿易に関する一般協定）

第 16 条（市場アクセス）

1. 加盟国は、第 1 条に規定するサービスの提供の態様による市場アクセスに関し、他の加盟国のサービス及びサービス提供者に対し、自国の約束表において合意し、特定した制限及び条件に基づく待遇よりも不利でない待遇を与える（注）。

（注：省略）

2. 加盟国は、市場アクセスに係る約束を行った分野において、自国の約束表において別段の定めをしない限り、小地域を単位とするか自国の全領域を単位とするかを問わず次の措置を維持し又はとってはならない。

(a) サービス提供者の数の制限（数量割当て、経済上の需要を考慮するとの要件、独占又は排他的なサービス提供者のいずれによるものであるかを問わない。）

(b) サービスの取引総額又は資産総額の制限（数量割当てによるもの又は経済上の需要を考慮するとの要件によるもの）

(c) サービスの事業の総数又は指定された数量単位によって表示されたサービスの総産出量の制限（数量割当てによるもの又は経済上の需要を考慮するとの要件によるもの）（注）

注：この（c）の規定には、サービスの提供のための投入を制限する加盟国の措置を含まない。

(d) 特定のサービスの分野において雇用され又はサービス提供者が雇用する自然人であって、特定のサービスの提供に必要であり、かつ、その提供に直接関係するものの総数の制限（数量割当てによるもの又は経済上の需要を考慮するとの要件によるもの）

(e) サービスが合弁企業等の法定の事業体を通じサービス提供者によって提供される場合において、当該法定の事業体について特定の形態を制限し又は要求する措置

(f) 外国資本の参加の制限（外国の株式保有比率又は個別の若しくは全体の外国投資の総額の比率の上限を定めるもの）

（第 17 条は前記第 2 項末尾に掲載）

第 4 項　予見可能性原則の実効性喪失

予見可能性原則は、WTO 体制の制度的安定性を支える中核的理念であり、各加盟国が採用する貿易関連措置を合理的かつ一貫した基準に基づいて運用し、企業や取引主体に対して一

[152] Burri (2017), pp. 87–99, 126–132; Dimitropoulos et al. (2025), pp. 2–11, 19–25.

定の予測可能な法的環境を提供することを目的とする[153]。GATS 第 3 条および第 4 条は、この理念を具体化する規定として、加盟国に対し、貿易に影響を及ぼす法令・規則・行政決定の公表義務と、一般適用的措置を合理的・公平に運用する義務を課している。さらに、第 6 条は、専門資格や技術基準などの分野で各国の行政措置を「合理的、客観的かつ公平な態様で」実施することを求めており、制度的予見可能性を実体的に担保するものである。これらの規定は、法的安定性と説明責任を制度的に支える基盤として、無差別原則および自由化原則を実質的に補完してきた。

この GATS 第 6 条の枠組みは、近年の電子商取引およびデジタル貿易交渉の展開において、規範的基盤としての重要性を高めている。クラウドサービスやデジタルプラットフォームの普及に伴い、データの越境移転を含むサービス供給は国境を超えて日常的に行われるようになった。しかし、各国が導入する越境的データ移転制限措置は、しばしばサービス提供者に過大な遵守コストを課し、国際的なデジタル取引の自由な展開を阻害する要因となっている。こうした措置は、GATS 第 6 条との整合性が問われる領域であり、国内規制と国際規範との衝突が最も顕在化する論点の一つである[154]。たとえば、データローカライゼーション措置は、自国領域内でデータの保存や処理を義務づけるものであり、国外へのデータ移転を制限する措置と併用されることが多い（後記第 4 章参照）。このような措置は、表面的には国家主権の行使としての国内政策であるが、実際にはクラウド、AI、電子商取引など、データを基盤とする越境的サービス供給に直接的な障害をもたらす。このため、データローカライゼーション措置は、GATS 第 6 条が定める「合理的、客観的かつ公正な態様」（第 1 項）および「サービスの貿易に対する不必要な障害」（第 4 項）との関係で問題となり得る。ここでは、データの域内保管を一律に義務づけるような措置は、その目的（プライバシー保護、国家安全保障など）に照らして必要最小限であるかが厳格に問われる。目的達成のために、より制限的でない他の手段が存在する場合には、当該措置は比例原則に反し、同条第 4 項に定められた「不必要な障害」として違反に問われ得る。この点に関し、Burri（2017）は、データローカライゼーション措置が形式上は「国内規制」であっても、実質的に国外供給者の市場参入を阻害する効果を持つ場合、GATS 第 6 条の適用対象になると指摘する[155]。また、Willemyns（2018）は、データ保護や安全保障を理由とする国内規制であっても、恣意的運用が行われる場合には、GATS 第 6 条の「公平な態様」に抵触するおそれがあるとしている[156]。さらに、Mitchell and Mishra（2019）は、こうした措置が正当化されるためには、比例性・透明性・予見可能性を備えたリスク評価に基づく運用が不可欠であると論じる[157]。

しかしながら、越境的データガバナンスの領域においては、各国の規制政策が急速に多様化・重層化し、国内外の制度的整合性を確保することが困難となっている。その結果、予見可能性原則は法的にも実務的にも深刻な機能不全に陥っている[158]。越境的データガバナンスにおける予見可能性の喪失は、各国の制度的多様化、クラウドや AI 基盤に起因する技術的非対称性、そしてプライバシー・安全保障・産業政策といった規制目的の多層化が重層的に作用し、構造的に生じているものである。これらの要因は相互に関連し、予見可能性が依拠してきた安定性・透

[153] 清水章雄（2019）104–114 頁; WTO (2025), section “Predictability: through binding and transparency.”
[154] Aaronson and Leblond (2018), pp. 245–254, 257–261; 東條吉純（2020b）20–24 頁; WTO (2024), pp. 2–12.
[155] Burri（2017）, pp. 87–99, 126–132
[156] Willemyns (2018), pp. 6–8.
[157] Mitchell and Mishra (2019), pp. 396–407.
[158] Mitchell and Mishra (2019), pp. 396–407; Kaya and Shahid (2025), pp. 222–229.

明性・一貫性を制度内部から掘り崩している。この構造的変化は、以下のような具体的態様として現れている。

第一に、データ関連規制の多くが国家安全保障や法執行を理由として不透明に運用されている点である。米国の CLOUD 法（前記第 1 章第 3 節参照）は、国外所在のデータへのアクセス権限を当局に付与しているが、その具体的運用や協定内容は非公開であり、企業が適用範囲を把握することは困難である[159]。中国の国家情報法およびデータセキュリティ法（前記第 1 章第 3 節参照）に基づくデータ提供義務も同様に、行政指針や口頭通知を通じて非公開的に実施される場合が多い[160]。これらの措置は、形式上は透明性義務の適用対象外とされてはいるものの、実質的には越境的データ流通を著しく阻害する要因となっている[161]。

第二に、各国の制度的非対称性がデータ利用の不均衡を拡大させ、透明性を形式的概念に変えている。たとえば EU の GDPR は十分性認定制度などを通じて規制の内容を公示しているものの、加盟国内のデータ保護当局による判断や執行基準は統一されておらず、第三国事業者がその運用を予測することはほぼ不可能である[162]。OECD の DFFT や APEC の CBPR といった国際的枠組みも、加盟国間で基準や評価方法の共有が十分に進んでいない[163]。

第三に、技術的発展そのものが制度的可視性を失わせている。AI やクラウドをはじめ、ブロックチェーンやフェデレーテッド・ラーニングに代表される分散処理技術は、データの所在・処理経路・再利用過程を自動化・断片化させる結果、規制当局自身が実際のデータ処理フローを把握できない場合がある。これにより、GATS 第 3 条が想定した行政手続の透明化という規範構造が根底から揺らいでいる[164]。

第四に、地政学的要因も予見可能性を制度的に無力化している。安全保障例外（GATS 第 14 条の 2）が各国の裁量的運用を許容していることにより（後記第 5 項参照）、越境的データ移転制限が安全保障上の必要性として容易に正当化される。米中対立や主要国によるサイバー防衛政策の強化は、透明性よりも防御的閉鎖性を優先させ、国際交渉におけるデータ共有を断片化させている。結果として、企業は政治的・地政学的リスクを予見できず、越境的データ流通における法的安定性が失われている[165]。

以上のように、GATS の予見可能性原則は、越境的データガバナンスとの関係では、法制度の流動化、データ利用の非対称性、技術的分散構造、そして安全保障政策の政治化という複合的要因によって実質的に機能を喪失している。もはや GATS が前提としてきた安定的かつ一貫したルール環境は維持されておらず、制度的信頼は大きく損なわれている[166]。今後の国際的制度設計においては、法令の公表や形式的公平性を中心とする従来型の透明性に依拠するのではなく、相互検証可能性と説明責任の共有を基軸とする予見可能性原理への転換が求められ

---

159 Rojszczak (2020), pp. 1–14; Eurojust (2022), pp. 1–3.

160 Creemers (2017), pp. 89–97; China Law Translate (2024), sections “The placement of article 7 suggests it was not intended as a major innovation,” “Article 7 has no enforcement mechanism,” and concluding analysis (“Ultimately, no matter what the laws say…”).

161 OECD (2022c), pp. 27–30; Kaya and Shahid (2025), pp. 222–231; WTO (2025), section “Predictability: through binding and transparency.”

162 Juliussen et al. (2023), pp. 227–230.

163 Robinson et al. (2021), pp. 9–13, 22–26; Vásquez Callo-Müller (2024), sections II–III.

164 OECD (2024), pp. 19–25, 42–45.

165 Mishra (2024), pp. 98–102, 110–120, 143–151.

166 Mishra (2024), pp. 184–187; OECD (2024), pp. 19–29, 42–45; Kaya and Shahid (2025), pp. 228–231.

る。この意味での予見可能性原理は、各国の規制目的、リスク評価、運用基準について相互に検証可能な説明が共有され、その合理性が継続的に確認され得る制度的関係性を基礎とする点に特徴がある。これにより、越境的データ移転における正当性判断とリスク評価が共通理解のもとで行われ、信頼に裏づけられた国際的制度協働が実現可能となる[167]。

【参照条文】

GATS（サービスの貿易に関する一般協定）

第 3 条（透明性）

1. 加盟国は、一般に適用されるすべての措置であってこの協定の運用に関連を有し又は影響を及ぼすものを速やかに、かつ、緊急の場合を除くほか遅くとも当該措置が効力を生ずる時までに公表する。サービスの貿易に関連を有し又は影響を及ぼす国際協定であって加盟国が締約国であるものも公表する。
2. 1 に規定する情報の公表が実行可能でない場合には、当該情報は、他の方法により公に利用可能なものとする。
3. 加盟国は、この協定に基づく自国の特定の約束の対象となるサービスの貿易に対して著しい影響を及ぼす法令又は行政上の指針の導入又は変更を速やかに、かつ、少なくとも毎年、サービスの貿易に関する理事会に通報する。
4. 加盟国は、1 に規定する一般に適用される自国の措置又は国際協定に関する特定の情報についての他の加盟国の要請に対し速やかに応ずる。加盟国は、また、これらのすべての事項及び 3 に規定する通報の義務の対象となる事項に関する特定の情報を要請に応じて他の加盟国に提供するための一又は二以上の照会所を設置する。当該照会所は、世界貿易機関を設立する協定（この協定において「世界貿易機関協定」という。）が効力を生ずる日から二年以内に設置する。個々の開発途上加盟国について、当該照会所を設置する期限に関し適当と認める猶予について合意することができる。当該照会所は、法令の寄託所であることを要しない。
5. いずれの加盟国も、この協定の運用に影響を及ぼすと認める他の加盟国の措置をサービスの貿易に関する理事会に通報することができる。

第 3 条の 2（秘密の情報の開示）

この協定のいかなる規定も、加盟国に対し、その開示が法令の実施を妨げる等公共の利益に反することとなり又は公私の特定の企業の正当な商業上の利益を害することとなる秘密の情報の提供を要求するものではない。

第 4 条（開発途上国の参加の増大）

1. 世界貿易における開発途上加盟国の参加の増大については、第三部及び第四部の規定に従い加盟国が行う交渉に基づく次の事項に関連する特定の約束を通じて促進する。
   (a) 特に商業的な原則に基づく技術の利用による開発途上加盟国の国内のサービスに関する能力並びにその効率性及び競争力の強化
   (b) 開発途上加盟国による流通経路及び情報網の利用の改善
   (c) 開発途上加盟国が輸出について関心を有する分野及び提供の態様における市場アクセスの自由化

[167] Robinson et al. (2021), pp. 9–12, 26–27; Mishra (2024), pp. 187–195; Vásquez Callo-Müller (2024), sections II–III.

2. 先進加盟国及び可能な限り他の加盟国は、自国の市場に関連した次の事項に関する情報の開発途上加盟国のサービス提供者による利用を容易にするため、世界貿易機関協定が効力を生ずる日から二年以内に連絡所を設置する。

(a) サービスの提供の商業的及び技術的側面

(b) 職業上の資格の登録、承認及び取得

(c) サービスに係る技術の利用可能性

3. 本条 1 及び 2 の規定の実施に当たっては、後発開発途上加盟国を特に優先する。後発開発途上国の特別な経済的事情並びにこれらの国の開発上、貿易上及び資金上のニーズにかんがみ、交渉に基づく特定の約束を受け入れるに際して後発開発途上国が重大な困難を有することを特に考慮する。

第 6 条(国内規制)

1. 加盟国は、特定の約束を行った分野において、一般に適用されるすべての措置であってサービスの貿易に影響を及ぼすものが合理的、客観的かつ公平な態様で実施されることを確保する。

2.

(a) 加盟国は、影響を受けたサービス提供者の要請に応じサービスの貿易に影響を及ぼす行政上の決定について速やかに審査し及び正当とされる場合には適当な救済を与える司法裁判所、仲裁裁判所若しくは行政裁判所又はそれらの訴訟手続を維持し、又は実行可能な限り速やかに設定する。加盟国は、当該訴訟手続が当該行政上の決定を行う機関から独立していない場合には、当該訴訟手続が客観的かつ公平な審査を実際に認めるものであることを確保する。

(b) (a)の規定は、加盟国に対し、その憲法上の構造又は法制の性質に反するような裁判所又は訴訟手続の設定を要求するものと解してはならない。

3. 特定の約束が行われたサービスの提供のために許可が必要な場合には、加盟国の権限のある当局は、国内法令に基づき完全であると認められる申請が提出された後合理的な期間内に、当該申請に関する決定を申請者に通知する。加盟国の権限のある当局は、申請者の要請に応じ、当該申請の処理状況に関する情報を不当に遅滞することなく提供する。

4. サービスの貿易に関する理事会は、資格要件、資格の審査に係る手続、技術上の基準及び免許要件に関連する措置がサービスの貿易に対する不必要な障害とならないことを確保するため、同理事会が設置する適当な機関を通じて必要な規律を作成する。当該規律は、これらの要件、手続及び基準が特に次の基準に適合することを確保することを目的とする。

(a) 客観的な、かつ、透明性を有する基準(例えば、サービスを提供する能力)に基づくこと。

(b) サービスの質を確保するために必要である以上に大きな負担とならないこと。

(c) 免許の手続については、それ自体がサービスの提供に対する制限とならないこと。

5.

(a) 加盟国は、特定の約束を行った分野において、当該分野に関し 4 の規定に従って作成される規律が効力を生ずるまでの間、次のいずれかの態様により当該特定の約束を無効にし又は侵害する免許要件、資格要件及び技術上の基準を適用してはならない。

(i) 4 の(a)、(b)又は(c)に規定する基準に適合しない態様

(ii) 当該分野において特定の約束が行われた時に、当該加盟国について合理的に予想され得なかった態様

(b) 加盟国が(a)に基づく義務を遵守しているかいないかを決定するに当たり、当該加盟国が適用する関係国際機関(注)の国際的基準を考慮する。

注:「関係国際機関」とは、少なくとも世界貿易機関のすべての加盟国の関係機関が参加することのできる国際機関をいう。

6. 加盟国は、自由職業サービスに関して特定の約束を行った分野において、他の加盟国の自由職業家の能力を確認するための適当な手続を定める。

(第 14 条の 2 は後記第 5 項末尾に掲載)

第 5 項　GATS の例外規定

GATS 第 14 条および第 14 条の 2 はいずれも GATS の基本原則に対する例外を規定するものである。第 14 条は、加盟国が一定の公共政策目的のために貿易制限的措置を講じることを認める例外(一般的例外)を、第 14 条の 2 は、国家安全保障上の理由に基づく特別の例外(安全保障例外)を定めている。

(1)　GATS第 14 条(一般的例外)

GATS 第 14 条は、「一般的例外」を定め、加盟国が一定の正当な公共目的のために GATS 上の義務から逸脱することを許容している。その中でも第 14 条(c)(ii)は、個人情報やプライバシーの保護といった目的のために加盟国がとる措置を正当化する根拠規定である。この規定は、加盟国が正当な公共目的の達成のために必要な措置を講じることを認め、そのような措置として「個人の情報を処理し及び公表することに関連する私生活の保護」や「個人の記録及び勘定の秘密の保護」などが明示されている。したがって、個人情報保護法や記録管理制度など、データの適正な取扱いを目的とする国内制度が結果として GATS 上の義務と競合する場合であっても、当該措置が第 14 条の要件を満たす限り、例外としての適用が認められる。ただし、第 14 条冒頭の柱書(chapeau)は、これらの例外措置が「恣意的若しくは不当な差別の手段」や「サービスの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てはならないと規定し、例外の濫用を防ぐための制約を設けている。さらに、この例外を適用するためには、当該措置が「必要(necessary)」と評価されることが前提となる。WTO 法における「必要性」には厳格な審査基準が存在し、より制限的でない他の手段によって同一の目的を達成できるか否かが検討される[168]。これまでの GATS または GATT の紛争処理手続における判断としては、プライバシー保護を目的とするデータ移転制限についても、より制限的でない他の手段によって同一の目的を達成できる場合には正当化されないとされている[169]。

[168] Appellate Body Report (2001) Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef, WTO Docs. WT/DS161/AB/R and WT/DS169/AB/R, adopted 10 January 2001, paras. 161–166. https://www.wto.org/ENGLISH/tratop_e/dispu_e/161-169abr_e.pdf

[169] Appellate Body Report (2005), United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WTO Doc. WT/DS285/AB/R, adopted 20 April 2005, paras. 306–308. https://www.wto.org/english/tratop_e/dispu_e/285abr_e.pdf

この点について、Burri（2017）は、GDPR が GATS 第 14 条(c)(ii)の要件には合致するものの、「必要性テスト」と「chapeau テスト」の双方で違反認定の可能性が高いと論じている。すなわち、GDPR は、国際貿易法の観点からみると域外的適用において過剰に制限的であり、WTO 法の「一般的例外」の範囲を超えるおそれがあるとしている[170]。また、Yakovleva（2024）は、GDPR の十分性認定制度が一貫性を欠き、政治的・地政学的判断に左右される可能性を論じるとともに、十分性認定を得ていない国に属する企業にとっては、標準契約条項（SCCs）や拘束的企業準則（BCRs）といった代替手段を利用することが制度上は可能であるものの、その導入には手続的・費用的な負担が大きく、実質的には越境的データ移転の障壁となり得ると指摘し、こうした措置は形式的には中立であるように見えても、実質的には域外事業者に不均衡な制約を課すものであり、GATS 第 14 条柱書に定める「恣意的若しくは不当な差別の手段」または「サービスの貿易に対する偽装した制限」と評価し得ると論じている[171]。

(2)　GATS第 14 条の 2（安全保障例外）

GATS 第 14 条の 2（安全保障例外）は、加盟国が国家安全保障上の理由から GATS 上の義務を一定範囲で履行しないことを認める規定であり、GATT 第 21 条の構造をほぼ踏襲している。条文は三つの要素から構成される。第一に、国家が自国の「安全保障上の重大な利益」に反する情報を提供する義務を負わないとする規定である（第 1 項(a)）。第二に、国家が「自国の安全保障上の重大な利益の保護のために必要であると認める」措置をとることを妨げないとする規定であり、これには軍事供給、核関連物質、戦争または国際関係上の緊急事態という三つの限定的状況が列挙されている（第 1 項(b)）。第三に、国連憲章上の義務の履行を妨げないとする規定であり（第 1 項(c)）、国連安全保障理事会による制裁措置など、国際平和維持活動との整合性を確保する目的を有している。このように、GATS 第 14 条の 2 は、国家安全保障の名の下に一定の裁量を認めつつも、対象を軍事・核・国際危機に限定することで、例外の濫用を防ぐ構造を備えている。また、条文上の「この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。」という第 1 項柱書の文言は、他の規定に優越する性格を示し、GATS の基本原則に対する限定的な優先を明文化している。

ここで重要な点は、加盟国が講じた例外措置については、WTO の紛争処理制度の審査対象になり得るとされていることである。すなわち、これまでの GATS または GATT の紛争処理手続における判断では、安全保障例外については、国家の裁量が比較的広く認められる一方で、その行使には誠実性（good faith）が求められ、濫用は許されないとされている（後記(3)参照）。したがって、越境的データ移転に関する国家措置が GATS の例外規定によって正当化され得るかどうかは、その目的の正当性と手段の必要性・均衡性を、WTO 紛争処理制度において判断し得ることになる。

以上のとおり、第 14 条の 2 は、国家の安全保障上の必要性を考慮しつつも、例外の適用範囲を明確に限定し、多国間貿易体制の均衡を維持しようとする制度的仕組みと位置づけられる。

[170] Burri (2017), pp. 87–93.
[171] Yakovleva (2024), pp. 82–90.

(3)　紛争処理手続における審査可能性と自己判断性

GATS 第 14 条（一般的例外）および第 14 条の 2（安全保障例外）は、加盟国が GATS の基本的義務の履行を免れるための正当化根拠を提供している。特に、第 14 条(c)(ii)は個人情報・プライバシーの保護、第 14 条の 2 は国家安全保障上の利益を理由とする措置を容認しており、この構造はデータ保護やサイバーセキュリティなどの本来の貿易以外の分野にも拡張的に適用される余地を有している。

問題は、これらの例外が本来は限定的に解釈されるべきものであるにもかかわらず、各国が実務上、広範かつ自己判断的に運用している点にある。米国は、GATT 第 21 条および GATS 第 14 条の 2 に規定される安全保障例外について、国家が自国の安全保障上の利益を理由としてとる措置は WTO 紛争処理制度の審査対象外であるとする自己判断的解釈を一貫して主張してきた[172]。これに対し、Russia – Traffic in Transit 事件において、WTO パネルは、GATT 第 21 条に基づく安全保障例外の適用について、加盟国に一定の裁量を認めつつも、当該措置が同条の文言（客観的適用要件の限定列挙）および誠実履行義務（good faith）に照らして正当化されるかをパネルが審査し得ると判断した[173]。すなわち、GATT 第 21 条の安全保障例外は完全な自己判断的条項ではないとの解釈を示したもので、この解釈は GATS 第 14 条の 2 にも準用し得ると解される[174]。

以上のように、第 14 条および第 14 条の 2 は、越境的データ移転に対する規制を一定の条件下で正当化し得るが、いずれも無制限な例外を認めるものではない。プライバシーや安全保障といった正当目的を追求しつつも、恣意的差別の回避と比例原則の遵守が求められる点で、データガバナンスにおける制度的均衡を維持するための中核的な規範枠組みを構成している[175]。

しかし、米国の自己判断性の主張は、後に「米国モデル」と位置づけられる地域貿易協定（日米デジタル貿易協定[176]、USMCA[177]など）の条文設計に影響を与え、安全保障例外の適用について各締約国の自己判断を認める趣旨を取り込む条文構造が形成された（後記第 8 章第 2 節参照）。さらに、GATS の運用実務においては、安全保障やサイバー政策を根拠に、越境的データ移転やデータの流入を規制する国内措置が多くの国で導入されているが、GATS の基本的義務との関係で十分に検証されていない。これらの措置は、将来的に紛争処理の場において GATS 第 14 条の 2 の例外措置と位置づけられるおそれがあり、実質的には自由化原則の適用範囲を狭める効果を有している。結果として、GATS の基本原則は法的には維持されつつも、実務上は加盟国の政策的裁量に大きく依存する構造へと変容していると言わざるを得ない。例外

---

[172] GATT Panel (1986) United States – Trade Measures Affecting Nicaragua, BISD 34S/136. Panel report. https://www.wto.org/gatt_docs/English/SULPDF/91240118.pdf; United States (2017) Third-Party Submission, Russia – Measures Concerning Traffic in Transit, WT/DS512, para. 18 (Sept. 2017). WTO dispute case page. https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm; United States (2018) First Written Submission, United States – Certain Measures on Steel and Aluminium Products, WT/DS544 et al., paras. 230–234. WTO dispute case page. https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds544_e.htm

[173] Panel Report (2019), Russia – Measures Concerning Traffic in Transit, WTO Doc. WT/DS512/R, adopted 26 April 2019, paras. 7.100–7.102. https://www.wto.org/english/tratop_e/dispu_e/512r_e.pdf

[174] Mitchell and Mishra (2019), pp. 401–405.

[175] Mitchell and Mishra (2019), pp. 399–406.

[176] 「デジタル貿易に関する日本国とアメリカ合衆国との間の協定」（Agreement between the United States of America and Japan concerning Digital Trade）（2019 年 10 月 7 日署名、2020 年 1 月 1 日発効）.

[177] 「米国・メキシコ・カナダ協定」（United States–Mexico–Canada Agreement: USMCA）（2018 年 11 月 30 日署名、2020 年 7 月 1 日発効）.

規定は本来の補完的機能を超えて、国家による裁量的政策運用を正当化する装置として機能し、GATS の制度的均衡を損なっている[178]。この傾向は、国家間の信頼関係を前提とする多国間ルールの根幹を揺るがし、越境的データ移転やデジタルサービスに関する統一的規律の確立を一層困難にしている。

【参照条文】

GATS（サービスの貿易に関する一般協定）

第 14 条（一般的例外）

この協定のいかなる規定も、加盟国が次のいずれかの措置を採用すること又は実施することを妨げるものと解してはならない。ただし、それらの措置を、同様の条件の下にある国の間において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サービスの貿易に対する偽装した制限となるような態様で適用しないことを条件とする

(a) 公衆の道徳の保護又は公の秩序（注）の維持のために必要な措置

注：公の秩序を理由とする例外は、社会のいずれかの基本的な利益に対し真正かつ重大な脅威がもたらされる場合に限り、適用する。

(b) 人、動物又は植物の生命又は健康の保護のために必要な措置

(c) この協定の規定に反しない法令の遵守を確保するために必要な措置。この措置には、次の事項に関する措置を含む。

(i) 欺まん的若しくは詐欺的な行為の防止又はサービスの契約の不履行がもたらす結果の処理

(ii) 個人の情報を処理し及び公表することに関連する私生活の保護又は個人の記録及び勘定の秘密の保護

(iii) 安全

((d)および(e)省略)

第 14 条の 2（安全保障のための例外）

1. この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。

(a) 加盟国に対し、その開示が自国の安全保障上の重大な利益に反すると当該加盟国が認める情報の提供を要求すること。

(b) 加盟国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを妨げること。

(i) 軍事施設のため直接又は間接に行われるサービスの提供に関する措置

(ii) 核分裂性物質若しくは核融合性物質又はこれらの生産原料である物質に関する措置

(iii) 戦時その他の国際関係の緊急時にとる措置

(c) 加盟国が国際の平和及び安全の維持のため国際連合憲章に基づく義務に従って措置をとることを妨げること。

（2 省略）

GATT（関税及び貿易に関する一般協定）

第 21 条（安全保障例外）

この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。

[178] Mitchell and Mishra (2019), pp. 399–406; Mishra (2024), pp. 184–193.

(a) 締約国に対し、発表すれば自国の安全保障上の重大な利益に反するとその締約国が認める情報の提供を要求すること。

(b) 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを妨げること。

(i) 核分裂性物質又はその生産原料である物質に関する措置

(ii) 武器、弾薬及び軍需品の取引並びに軍事施設に供給するため直接又は間接に行なわれるその他の貨物及び原料の取引に関する措置

(iii) 戦時その他の国際関係の緊急時にとる措置

(c) 締約国が国際の平和及び安全の維持のため国際連合憲章に基く義務に従う措置をとることを妨げること。

第 2 節　WTO その他の多国間フォーラムにおける統一規範策定の限界

WTO をはじめとする多国間フォーラムでは、越境的データガバナンスに関する国際的統一規範の策定に向けた議論が継続的に行われてきた。しかし、関係国の立場の相違やフォーラム自体の制度的・組織的制約などから、拘束力を有する規範の形成には至っておらず、コンセンサスの確立は依然として困難な状況にある。

本節では、まず第 1 項で GATS による統制の限界を分析し、次いで第 2 項で WTO における交渉の停滞の状況を検討し、さらに第 3 項でその他の多国間フォーラムにおける規範策定の限界を確認する。

第 1 項　GATS による統制の限界

GATS は、サービス貿易の自由化を目的とする多国間協定として、各国が越境的サービス取引に関して共通の基準を確立することを企図していた。しかし、越境的データガバナンスに関する国際的統一規範としては十分に機能していない。その理由は、GATS が制度構造および政策目的の面で現代のデータ取引の性質に適合していないためである。

第一に、GATS は、越境的データ移転を通じたサービス供給にも形式上適用されるが、その規律はデジタル経済の現実を十分に捉えているとは言い難い。すなわち、GATS は 1995 年の WTO 発足時に策定された協定であり、インターネットやクラウド技術が本格的に普及する以前の経済構造を前提としている。そのため、当初からデジタル取引やデータ流通を直接的に規律することを想定しておらず、この枠組み自体に本質的な限界がある[179]。

第二に、越境的データガバナンスにおける中心的課題は、プライバシー保護、サイバーセキュリティ、国家安全保障といった公共目的に基づく制度的制約であり、貿易制限的であっても、その目的が非経済的であることが多い。これらは経済的自由化を前提とする GATS の制度的ロジックと根本的に異なることから、GATS が本来的に想定する市場アクセス義務や無差別義務の枠組みでは十分に処理できない[180]。結果として、加盟国は GATS の下で形式的には自由化義務を負いながらも、実際には例外規定を援用して国内法に基づく規制を優先させている[181]。加えて、第 14 条および第 14 条の 2 が定める例外規定は加盟国に広範な裁量を認める一方、誠実な行使（good faith）などの制限的要素に形式的に言及されるにとどまり、実質的な審査基準は確立していない[182]。

第三に、デジタルサービスやデータ関連分野の自由化約束を行っている国は、米国やシンガポールなど極めて限られており、大多数の国ではこの分野の約束が依然として限定的である。このため、GATS 上の義務は各国の約束表に基づいて適用されるにとどまり、その実効性は大きく限定されている[183]。その結果、第 1 モード（越境取引）に「非拘束（Unbound）」との記載が多く

[179] Aaronson and Leblond (2018), pp. 268–271; Willemyns (2018), pp. 4–6; Mitchell and Mishra (2019), pp. 390–395; 東條吉純（2020a）42–46 頁.
[180] 東條吉純（2020b）10–18, 27–30 頁.
[181] Willemyns (2018), pp. 6–12; Mitchell and Mishra (2019), pp. 397–401; Elsig and Klotz (2021), pp. 42–62.
[182] Willemyns (2018), pp. 10–12.
[183] 東條吉純（2020b）5–9, 18–21 頁.

残り[184]、加盟国がデータ移転を自由化義務の外に置く余地を温存している。すなわち、越境的データ移転規制やサーバー設置義務などの措置が GATS 上の義務違反とみなされにくく、実質的に各国が独自のデジタル主権や安全保障を理由に制限措置を維持できる構造が生じており、デジタル時代に適合した越境的データガバナンスの国際的整合性は確立されていない。

第四に、加盟国間のデータガバナンス体制の多様性が、統一的規範の形成を妨げている。米国は市場競争を基調とする市場支配モデル（Market dominant model）、EU は基本権としてのデータ保護を強調する規範統制モデル（Normative control model）、中国は国家安全保障を重視するサイバー主権モデル（Cyber sovereignty model）を展開している（前記第 1 章第 3 節参照）。このような規範的分断のもとでは、GATS の無差別的自由化原理を各国に一律に適用することは現実的でなく、むしろ対立を深める結果となりかねない[185]。GATS の自由化義務をそのまま越境的データ移転規制に適用すると、公共目的による正当な規制が市場アクセス制限とされるおそれがある一方、各国の主権的裁量や信頼に基づく制度差を十分に反映できないという制度的不整合が生じる。

近年では、こうした制度的制約に加え、地政学的変動が越境的データガバナンスの構造を一層複雑化させている。米中対立の激化や EU による域外規範的統制の強化を背景に、データ流通は経済問題のみならず、国家安全保障、技術覇権、さらには価値や規範の主導権をめぐる争いと密接に結びついている。このような状況の下で、データ移転の自由化原理を基礎とする GATS の理念は、現実の国際政治的力学の中で相対化されつつある。加えて、国家間の信頼の欠如や規範的価値の分断は、WTO の協調的統治モデルの構造的限界を明らかにしている[186]。

以上のとおり、GATS は越境的データ移転に関する一定の法的基盤を提供しているものの、デジタル経済における技術的複雑性やリスクの多様化、さらには地政学的分断の深化に対応するには限界がある。この問題は WTO においても繰り返し議論されてきたが、GATS の制度的枠組みの下で越境的データガバナンスを包括的に扱うことには、加盟国間で依然として大きな見解の隔たりがある。

とはいえ GATS の基本原則は、越境的データガバナンス規範再構成に資するものであり、今後の国際的制度設計に一定の示唆を与えるものである。また、GATS は、非個人データをも国際経済活動の基盤的資源として位置づけ、サービス供給の自由化を促進するための規範を定めている[187]。このことは、越境的データ移転の問題が個人データの領域に限定されるものではなく、より広範な越境的データ移転全般に関わる制度的課題であることを示している[188]。したがって、GATS の基本原則に内在する理念を尊重しつつ、各国の主権的統制と国際的相互運用性を両立し得る規範を再構成することにより、地政学的緊張を超えて均衡的な国際枠組みを形成することが求められる[189]。

184　“Unbound”とは、加盟国が特定の分野または供給形態について約束を行っていないことを意味する。WTO (2001) Guidelines for the Scheduling of Specific Commitments under the General Agreement on Trade in Services (GATS). Doc. S/L/92, 28 March 2001, para. 15. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/L/92.pdf

185　Aaronson and Leblond (2018), pp. 268–271; Willemyns (2018), pp. 13–16; Elsig and Klotz (2021), pp. 42–62.

186　Musoni et al. (2023), pp. 1–10, 18, 21–33, 39–44; Zhang (2024), pp. 1–13.

187　Abe (2021), pp. 3–10, 17–23.

188　OECD (2022b), pp. 4–6, 14–17.

189　Lateef (2025), pp. 879–883, 888–899.

第 2 項　WTO における交渉の停滞

WTO における多国間交渉は、2001 年に開始されたドーハ・ラウンド以降、加盟国間の利害対立や交渉手続の複雑性などを背景に、長期にわたって停滞している[190]。特に、先進国と新興国との間で関税削減や農業補助金の扱いをめぐる意見の乖離が埋まらず、全会一致を原則とする WTO の意思決定方式が合意形成を困難にしている[191]。その結果、電子商取引や環境関連措置などの新たな分野の課題に関して、包括的なルール策定が進まない状況が続いている[192]。このような制度的限界の下で、WTO は国際貿易の統一的なルール策定機関としての機能を十分に果たせなくなっており、加盟国は地域的または分野別の貿易協定、あるいは有志国連携（plurilateral partnerships）を通じて、現実的かつ機動的なルール形成を進める傾向を強めている[193]。

越境的データ移転に対する規制の在り方は、国際的な電子商取引の拡大とともに、WTO において重要な検討課題となってきた。その端緒は、1998 年に採択された「電子商取引に関する作業計画」[194]にある。その後、デジタル技術の発展とともに、データが国際経済における中核的資産としての地位を確立するに至り、越境的データ移転に関する国際的ルール整備の必要性が急速に高まった。こうした情勢を受け、2017 年に開催された第 11 回 WTO 閣僚会議において、加盟国の有志による電子商取引に関する共同声明イニシアティブ（Joint Statement Initiative: JSI）が発足し、電子商取引に関する包括的な貿易ルールの構築を目指す動きが本格化した[195]。

JSI には、2024 年 7 月時点で 91 の国・地域が参加しており、日本はオーストラリアおよびシンガポールとともに共同議長国を務めている[196]。同月には、JSI の「安定化テキスト（Stabilized Text on Electronic Commerce）」が発表され、電子商取引に関する 38 条文が提示された。内容としては、①貿易書類の電子化や規制の透明化等を通じた電子決済の促進による電子商取引の貿易円滑化、②政府データの公開やインターネットのアクセス・使用を通じた開かれた電子商取引の推進、③サイバーセキュリティ、オンライン消費者保護や個人情報保護による電子商取引の信頼性向上に関する規律などの分野において一定の進展が見られた[197]。しかし、越境的データ移転制限の禁止やデータローカライゼーションの禁止といった中核的論点については、各国の意見の隔たりから、同テキストには盛り込まれなかった[198]。特に、米国は安全保障例外に関する自国の主張が反映されていないことなどを理由に同テキストへの支持を表明せず[199]、

---

190 WTO (2023), pp. 26–28.
191 Evenett and Baldwin (2020), pp. 9–15.
192 Mitchell and Mishra (2019), pp. 399–406.
193 Evenett and Baldwin (2020), pp. 9–15.
194 WTO (1998) Work programme on electronic commerce (WT/L/274, 30 September 1998). WTO, Geneva. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/274.pdf
195 WTO (2017) Joint statement on electronic commerce (WT/MIN(17)/60, 13 December 2017). WTO, Geneva. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/60.pdf
196 WTO (n.d.a), para. 1–3.
197 Ministry of Economy, Trade and Industry, Japan (2024) Stabilised text achieved in WTO Joint Statement Initiative on electronic commerce (26 July 2024). https://www.meti.go.jp/english/press/2024/0726_001.html
198 Digital Trade Tracker (2024), paras. 3–5.
199 U.S. Mission to the International Organizations in Geneva (2024) Statement by Ambassador María L. Pagán on the WTO e-commerce Joint Statement Initiative (26 July 2024), para. 4. https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative/

中国も越境的データ移転制限やデータローカライゼーション禁止条項の導入について消極的な立場を示したとされている[200]。

このように、越境的データガバナンスに関する国際的統一規範の策定は WTO において議論が進められてきたものの、安全保障および個人情報保護をめぐる政策優先度の違いなどから各国の立場の隔たりが大きく、コンセンサスの形成は依然として困難である。

第 3 項　その他の多国間フォーラムにおける規範策定の限界

その他の多国間フォーラムで示されている越境的データ移転に関する枠組みや見解も、制度的および実効性の観点から十分とはいえない。たとえば、APEC CBPR[201]および PRP[202]は、参加企業の任意認証制度にすぎず、国際法上の拘束的義務を創設しないものとされている。Global CBPR[203]は枠組みを拡張し、紛争解決や是正手続を制度文書上に位置づけてはいるものの、その実効性は各国当局や認証機関の裁量に委ねられており、国際仲裁や制裁を伴う強制力ある執行メカニズムを欠いている。制度全体は企業行動を一定程度規律し得るものの、国家間の法的整合性を担保する拘束的規範としては機能していない。また、OECD が主導する DFFT の枠組み[204]や、G7 が 2023 年に採択した IAP[205]も、信頼に基づくデータ流通の理念を提示し、政策協調や相互理解を促すうえで重要な意義を有するが、その多くはソフトローにとどまり、法的拘束力や強制的紛争処理制度を備えていない。さらに、WEF[206]や WSIS[207]といったマルチステークホルダー・フォーラムも、対話とガイドライン形成を通じて規範的基盤を提供しているものの、合意内容は勧告的性格にとどまり、遵守確保や違反時の救済を担保する制度的裏付けを欠く。こうした非拘束的な制度設計のもとでは、各国の裁量や国内法制への依存が強まり、国際的な一貫性や予見可能性の確保が困難となっている。さらに近年ではデータの越境移転をめぐる大国間の意見の対立が一層顕在化しており、この規範的対立が国際的な合意形成を阻害し、国際的データガバナンスの制度的分極を深めている。

---

[200] Kang (2024), pp. 119–123.

[201] APEC (2015) Cross-Border Privacy Rules system: Program requirements (APEC ECSG 2015). https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-ProgramRequirements.pdf

[202] APEC (2020) Privacy recognition for processors (PRP) system: Policies, rules and guidelines (Revised 3-16). https://cbprs.org/wp-content/uploads/2020/08/PRP-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-1.pdf

[203] Global CBPR Forum (2024) Global cross-border privacy rules (CBPR) and global privacy recognition for processors (PRP) systems: policies, rules and guidelines (Final, April 2024). https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Policies-Rules-and-Guidelines_Final-as-of-April-11-2024.pdf; U.S. Department of Commerce (2022) Global Cross-Border Privacy Rules declaration (April 2022). https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[204] OECD (2023a), pp. 7–30.

[205] Government of Japan, Digital Agency (2023) Institutional arrangement for partnership (IAP) under the DFFT framework (May 2023), Government of Japan, Tokyo, paras. 1–4. https://www.digital.go.jp/en/policies/dfft/dfft-iap/

[206] World Economic Forum (2021) Advancing data flow governance in the Indo-Pacific: four country analyses and dialogues (White Paper, April 2021), pp. 4–5. https://www3.weforum.org/docs/WEF_Data_Flow_Governance_2021.pdf

[207] United Nations (2005) World Summit on the Information Society (WSIS) outcome documents: Tunis Agenda for the Information Society, December 2005. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html; United Nations (2021) Internet Governance Forum (IGF) mandate renewal report. https://www.intgovforum.org/en

このような現状では、従来の多国間フォーラムの取組だけでは、国際的なデータガバナンスの制度的不整合と価値的分断を是正するには不十分である。各国の制度的多様性を尊重しながら、透明性と相互運用性を制度的に担保するメカニズムを設計する必要がある。実効的な規範再構成のためには、データの性質および利用文脈に応じた階層的な越境移転条件を明確に規定し、第三者的紛争処理手続と連動する拘束的枠組みを構築することが不可欠である[208]。これにより、理念的合意にとどまらず、実効的かつ中立的な国際規範形成への転換が期待される。

[208] Bacchus (2018), pp. 15–28; OECD (2023a), pp. 7–30.

第 3 節　越境的データガバナンス規範再構成に向けた課題

本章では、GATS を含む WTO 体制およびその他の多国間フォーラムにおける越境的データガバナンスの国際的規律の現状と限界を検討した。GATS は、サービス貿易の自由化を目的とする多国間協定として、各国が越境的サービス取引に関して共通の基準を確立することを企図していたが、その適用範囲に関する約束表の制約、デジタル経済への制度的対応の遅れにより、現代のデータ流通構造を十分に包摂することができていない[209]。データの越境移転のように、従来のサービス供給形態では捉えられない新領域においては、既存の GATS の規律構造では整合的かつ一貫した運用を確保することが困難である。また、WTO における多国間交渉はドーハ・ラウンド以降停滞し、電子商取引に関する JSI の取組も限定的な進展にとどまっている[210]。OECD や APEC、G7 などの政府間フォーラムにおいても、理念的合意やソフトローを通じた協調に依拠しており、実効的な拘束力や紛争処理機能を欠いている[211]。その結果、各国が自国法制に基づく政策裁量を拡大し、国際的整合性と予見可能性の確保は一層困難となっている。したがって、GATS および WTO を中心とする既存の多国間体制は、越境的データガバナンスに内在する制度的非対称性を是正する枠組みとして限界を露呈している。

GATS の基本原則は、無差別、自由化、予見可能性、透明性を基礎として構築されており、市場アクセスや競争条件を各国が一定の基準で共有できることを前提にしている。しかし、越境的データ移転の領域では、移転先の法制度、ガバメントアクセスの運用、監督機関の独立性など、相手国ごとに異なる制度環境の評価が不可欠となるため、GATS の諸原則が想定する横並びの前提が成立しない[212]。

最恵国待遇が要求する一律の待遇拡張は、制度構造やリスク水準が大きく異なる国に対して同一の判断を適用することを意味するが、越境的データ移転ではこうした扱いが制度的合理性を持たない[213]。

自由化原則についても、従来の貿易法学が前提とする障壁削減や市場参入拡大の枠組みは、データの保護、公共政策、ガバメントアクセスの制度化など、経済価値と公共的価値が重層的に交差する越境的データ移転には整合しない。国家は、相手国制度の状況に応じて移転を制限したり、追加措置を要求したりするため、自由化の方向に規制を均質化することが妥当とは言えない[214]。移転に関する判断は、市場競争の条件ではなく、制度の信頼性とリスク評価に基づいて行われる。

内国民待遇についても、国内事業者と外国事業者を同一基準で比較できることが前提となるが、越境的データ移転の可否の判断では相手国の法制度や実務運用をも考慮することから、国内と外国の事業者を同質に扱うことが必ずしも合理的ではない。制度環境の違いが移転の許容性に直結するため、国内と外国の行為主体を対照する枠組みでは判断の本質を捉えきれ

[209] Burri (2017), pp. 80–99.
[210] Burri (2017), pp. 80–99; Mitchell and Mishra (2019), pp. 393–394, 407–408.
[211] Jovan (2009), pp. 79–86, 153–162; OECD (2020), pp. 140–150.
[212] Burri (2017), pp. 129–132; Aaronson and Leblond (2018), pp. 267–272.
[213] Burri (2017), pp. 129–132; Willemyns (2018), pp. 6–8, 12–13.
[214] Velli (2019), pp. 884–891.

ない。制度差を踏まえた調整が不可避である以上、内国民待遇の形式的適用は現実の判断構造と乖離する[215]。

予見可能性や透明性原則についても、形式的には適用可能に見えるものの、越境的データ移転の領域では、制度内部の運用やガバメントアクセスの実態が判断の核心を占めており、公開された条文や一般的指針のみをもって判断の全体像を把握することは困難である。判断基準を公表すること自体は可能であり、また不可欠であるが、実際の判断に影響を及ぼす要素の多くが、相手国の監督体制や執行慣行など、形式的な法令公表では十分に可視化されない領域に依存している。そのため、規則の公表を中心とする従来型の透明性原則のみでは、越境的データ移転に求められる実質的な明確性や予見可能性を十分に確保することは難しい[216]。もっとも、このことは予見可能性原則そのものが無効であることを意味するものではなく、判断に用いられるリスク評価の枠組みや運用基準を段階的かつ体系的に明示し、相互に検証可能な形で共有する制度設計を通じて、その実効性を補完・再構成する余地がある。透明性の要請が、形式的公表にとどまらず、運用水準における説明可能性と結びつく場合には、公開されたルールと実際の判断との間に生じてきた乖離は、制度的に管理され得るものとなる[217]。

このように、越境的データ移転は、相手国制度の信頼性やリスク構造を個別に検証する領域であり、市場アクセス中心の貿易原則が前提とする共通の比較基盤を確保することが難しい。結果として、最恵国待遇、自由化原則、内国民待遇といった GATS の基本原則を越境的データ移転にそのまま適用することは、その性質の違いに照らして、制度構造上も規範目的の観点からも困難である。越境的データ移転に GATS の基本原則が適合しないということは、従来の貿易法モデルを基礎とした国際的規律では、データ流通の構造的特質を十分に包摂できないことを示している。データ移転は、市場アクセスや競争条件の調整に還元できる領域ではなく、相手国の法制度、ガバメントアクセスの運用、監督体制の整備状況といった、国家内部の統治構造と密接に結びついた領域である[218]。そのため、国家間の制度差を前提としつつ、相互の制度的信頼性を評価する仕組みを組み込んだ新たな規範構造が求められる。

今後は、各国の制度的多様性を前提に、リスクの程度と利用文脈に応じた比例的かつ柔軟な制度設計を通じて、透明性と相互運用性を制度的に担保する新たな国際枠組みを構築することが求められる[219]。そのような越境的データガバナンス規範再構成にあたっては、規範的対立を先鋭化させている大国主導の枠組みへの依存を可能な限り回避し、中堅国や新興国の主導により、各国の主権的統制を尊重しつつ国際的相互運用性を確保し得る新たな国際規範を策定する方策を探求することが必要となる[220]。

---

[215] Burri (2017), pp. 129–132; Willemyns (2018), pp. 6–8, 12–13.
[216] Christakis (2024b), pp. 99–109.
[217] Burri (2017), pp. 87–99, 129–132; Breitbarth (2021), pp. 541–547; OECD (2022d), pp. 22–34, 44–48; Christakis (2024b), pp. 99–109.
[218] Christakis (2024b), pp. 99–105.
[219] Aaronson and Leblond (2018), pp. 245–251; OECD (2023a), pp. 19–22.
[220] Dimitropoulos et al. (2025), pp. 7–19.

第 4 節　先行研究の潮流と本稿の位置づけ

越境的データガバナンスをめぐる学術的議論は、近年、国際経済法・情報法・政策研究の領域において急速に深化している。最近の先行研究は、WTO 体制が依拠してきた自由化・無差別・予見可能性といった原則が、データを対象とする新たな経済秩序において制度的限界を露呈しつつある点を共通して指摘している。

Burri（2017）は、既存の貿易法的枠組みがデジタル経済の構造変化に適応できていない点を批判し、WTO や FTA（Free Trade Agreement: 自由貿易協定）におけるデータ流通条項を「法的適応の陥穽（pitfalls of legal adaptation）」として分析している。自由化と保護という二項対立を前提とする従来型の規律を超えて、各国の制度的信頼とリスク水準を考慮した柔軟な規範設計の必要性を提起している。さらに、多国間交渉の停滞を踏まえ、FTA やプルリラテラル協定を基盤とする段階的制度構築を提言し、比例性と信頼を基軸とする新たなルール形成プロセスの方向性を提示している[221]。

Aaronson and Leblond (2018)は、EU・米国・中国がそれぞれ固有の規制理念と政策目的に基づく「データ大国（data realms）」を形成していることを指摘し、こうした制度的分断が無差別・自由化を基礎とする WTO 型の普遍主義の機能を著しく損なっていると論じる。すなわち、データを単なる貿易対象ではなく、個人の権利保護や社会的信頼を支える基盤として捉え、各国の規制理念の相違を踏まえつつ、透明性・説明責任・信頼を基軸とするガバナンス枠組みの構築が不可欠であると主張する[222]。この問題意識は、越境的データ流通の秩序を再構築するためには、各国に形式的に同一ルールを押しつけることよりも、データの取扱いに関する制度的信頼を相互に確立することこそが基盤となるとする点で、Burri の提言とも共通する。

Christakis (2024a)は、EU のデータ保護当局が、国外政府によるアクセス可能性の存在それ自体を理由として越境的データ移転を機械的に否定しようとする規範的傾向を、「ゼロリスク前提」という誤謬（the “zero risk” fallacy）として批判している。外国当局に監視権限が付与されているという事実のみをもって移転の違法性を導くべきではなく、当該アクセスの実効的リスク、制度的保障、手続的統制、ならびに国際協力の枠組みを総合的に評価するリスクベースアプローチへの移行が不可欠であると論じている[223]。

Saluste (2025)は、EU の十分性認定制度を差異的取扱いと相互承認の制度的接続として再解釈し、GATS 第 7 条に定められた相互承認枠組みの「機能的同等物」と位置づけ、これを最恵国待遇義務の例外としてではなく、むしろ制度的信頼を前提とした差異的取扱いを通じて同義務を実質的に補完するメカニズムとして理解する。すなわち、無差別の理念は形式的均一性の維持に尽きるものではなく、各国の監督制度・執行能力・規制哲学の差異を適切に評価したうえで、相互に受容可能な水準の保護・執行を確保する協調的整合性（cooperative coherence）を実現することにより、より実質的に達成され得るとする[224]。十分性認定を相互承認の文脈に接続するこの解釈は、比例原則に基づく差異的取扱いと相互信頼の制度化を通じ、従来の形式的無差別義務と各国の自主的規制権限との間の構造的緊張を調整する試みとして評価できる。

---

[221] Burri (2017), pp. 80–99, 126–132.
[222] Aaronson and Leblond (2018), pp. 245–272.
[223] Christakis (2024a), Introduction, Part I.1–1.5, Part III.1–4, Conclusions.
[224] Saluste (2025), pp. 596–615.

Dimitropoulos et al.（2025）は、近年のプルリラテラル協定の動向を検討し、その展開には二つの側面があると指摘している。すなわち、プルリラテラル協定は、WTO を含む国際経済秩序に対し、一方では制度の断片化や先進国と途上国との格差拡大というリスクをもたらし得るものの、他方では既存の多国間制度を補完し、その柔軟性や実効性を高める機能を持ち得るとする。そのうえで、政府調達協定（GPA）、共同声明イニシアティブ（JSI）、地域的自由貿易協定におけるプルリラテラルな章構成、さらには WTO の枠外で形成されつつあるハイブリッド型の取決めを、プルリラテラル主義の具体的形態として整理している。そして、これらの枠組みは、多国間主義を現実的に補完する制度的選択肢として再評価され得ると論じている[225]。このような分析は、越境的データガバナンスの分野において、有志国によるプルリラテラルな枠組みを通じて段階的に制度を構築し、それに基づき規範の再構成を図ろうとする本稿の立場とも整合的である。

また、OECD や World Economic Forum などの国際機関が公表する政策文書も、同様の問題意識を共有している。World Economic Forum（2020）は、各国制度の断片化が国際的予見可能性を低下させているとの認識を示し、越境的データ流通の信頼性を高めるためには、各国の規制体系間の相違を可視化し、共通の政策目標に基づいて調整可能性を確保するための枠組みが必要であると指摘する。同報告書は、データガバナンスの基盤要素を体系化し、国・地域間の制度差を分析するための政策評価ツールや、協働の優先領域を段階的に設定するためのアプローチを提示し、制度的断片化を緩和するための実務的協調メカニズムの整備を提案している[226]。さらに、OECD（2023a）は、DFFT を実質化するためには、形式的な制度整合性の確保のみでは不十分であり、各国が相互に制度的信頼を担保し得る仕組みとして、制度運用の透明性・監督体制・手続的保証を相互に確認し合う「mutual assurance」の概念を中心に据える必要があると指摘する[227]。これらの政策文書は、共通評価指標、モジュール化された制度構造、制度的信頼の可視化といった手法を通じて、断片化した各国制度を実務的に接続する枠組みの構築を目指している点で軌を一にする。

以上の先行研究はいずれも、WTO 体制を支えてきた基本原則がデータガバナンス領域では十分に機能せず、制度的・技術的・地政学的要因の複合のもとで空洞化しつつあるとの認識を共有している。そして、各研究に共通するのは、もはや形式的自由化や画一的無差別といった従来型の枠組みだけでは持続的な秩序形成を維持できないという指摘であり、その克服に向けて「信頼」「比例性」「リスクベース」の各原理を取り込む必要性である。

本稿は、こうした先行研究の潮流を踏まえ、越境的データガバナンスにおける既存諸原則の機能不全を認めつつ、それらを否定するのではなく、リスクベースアプローチに基づいて規範を再構成し、その具体的実装の方策を探求する点に独自性がある。本稿は、先行研究の方向性を理論的に継承しつつ、法技術的レベルでの規範再構成を具体化する試みである。

本稿では、続いて第Ⅱ部において国際的データガバナンスの分断をもたらす五つの国家施策を分析したのち、サイバー空間の分裂回避という観点から、第Ⅲ部において越境的データガバナンス規範再構成の在り方を論じる。

---

225 Dimitropoulos et al. (2025), pp. 1–30.
226 World Economic Forum (2020), pp. 7–10, 16–31.
227 OECD (2023a), pp. 7–9, 15–18, 23–25.

参考文献（はじめに・第Ⅰ部）（本文との対応関係は各頁に脚注番号で表示）

Aaronson SA (2018) Data is different: Why the world needs a new approach to governing cross-border data flows. CIGI Papers No. 197, Centre for International Governance Innovation, Waterloo, ON, Canada, November 2018, 1–22. https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows/

Aaronson SA (2019) What are we talking about when we talk about digital protectionism? World Trade Review, 18(4): 541–577. https://doi.org/10.1017/S1474745618000198

Aaronson SA, Leblond P (2018) Another digital divide: The rise of data realms and its implications for the WTO. Journal of International Economic Law 21(2): 245–272. https://doi.org/10.1093/jiel/jgy019

Abe Y (2021) Data localization measures and international economic law. Public Policy Review 16(5): 1–29. Policy Research Institute, Ministry of Finance, Japan. https://www.mof.go.jp/english/pri/publication/pp_review/ppr16_05_02.pdf

Arcesati R, von Carnap K, Groenewegen-Lau J, Hmaidi A (2023) Fragmenting cyberspace: The future of the internet in China. MERICS Report, November 30 2023, 1–38. MERICS, Berlin. https://merics.org/sites/default/files/2023-11/MERICS%20Report_Future%20of%20the%20internet_final%20(1).pdf

Archick K (2021) U.S.-EU Privacy Shield and transatlantic data flows. Congressional Research Service, R46917, 1–24. https://www.everycrsreport.com/reports/R46917.html

Bacchus J (2018) Might unmakes right: the American assault on the rule of law in world trade. CIGI Paper No. 173. Centre for International Governance Innovation, 1–40. https://www.cigionline.org/publications/might-unmakes-right-american-assault-rule-law-world-trade/

Bradford A (2020) The Brussels effect: how the European Union rules the world. Oxford University Press, Oxford.

Bradford A (2023) Digital empires: The global battle to regulate technology. Oxford University Press, Oxford.

Breitbarth P (2021) A risk-based approach to international data transfers. Eur Data Prot L Rev 7: 539–549. https://edpl.lexxion.eu/data/article/17963/pdf/edpl_2021_04-010.pdf

Burri M (2017) The governance of data and data flows in trade agreements: The pitfalls of legal adaptation. UC Davis Law Rev 51: 65–132. https://lawreview.law.ucdavis.edu/archives/51/1/governance-data-and-data-flows-trade-agreements-pitfalls-legal-adaptation

Castro D (2022) Policymakers should distinguish between data protection and data protectionism. Information Technology and Innovation Foundation (ITIF), May 31. https://datainnovation.org/2022/05/policymakers-should-distinguish-between-data-protection-and-data-protectionism/

Chander A, Lê UP (2015) Data nationalism. Emory Law J. 64: 677–735. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

Chander A (2020) The electronic silk road: how the web binds the world together in commerce. Yale Journal of International Law 45(3): 647–701. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662605

China Law Translate (2024) What China's national intelligence law says, and why it doesn't matter. https://www.chinalawtranslate.com/en/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/ (accessed 22 February 2026).

Christakis T (2024a) The "zero risk" fallacy: International data transfers, foreign governments' access to data, and the need for a risk-based approach. Centre for Information Policy Leadership & Cross-Border Data Forum, 1–95. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_zero_risk_fallacy_-_t.christakis_feb24.pdf

Christakis T (2024b) Data free flow with trust: current landscape, challenges and opportunities. Journal of Cyber Policy 9(1): 95–120. https://doi.org/10.1080/23738871.2024.2421838

Cory N, Dascoli E (2021) How barriers to cross-border data flows are spreading globally, what they cost, and how to address them. Information Technology and Innovation Foundation, Washington D.C.

https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

Creemers R (2017) Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. Journal of Contemporary China 25: 85-100. https://doi.org/10.1080/10670564.2016.1206281

Daskal JC (2018) Borders and bits. Vanderbilt Law Review 71(1): 179-238. https://scholarship.law.vanderbilt.edu/vlr/vol71/iss1/3

Del Giovane C, Ferencz J, López-González J (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

Digital Trade Tracker (2024) What's in the WTO JSI "stabilised" text? (30 August 2024). https://digitaltradetracker.org/2024/08/30/whats-in-the-wto-jsi-stabilised-text/

Dimitropoulos G, Chen RC, Chaisse J (2025) Plurilateralism: A new form of international economic ordering? The Journal of World Investment & Trade 26(1-2): 1-30. https://doi.org/10.1163/22119000-12340355

Drake WJ, Cerf VG, Kleinwächter W (2016) Internet fragmentation: an overview. World Economic Forum, Geneva, 1-76. https://www.weforum.org/publications/internet-fragmentation-an-overview/

EDPB (2020a) Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, adopted 10 November 2020. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

EDPB (2020b) Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, adopted 10 November 2020. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en

EDPB (2020c) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, adopted 20 October 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

EDPB (2020d) Guidelines 05/2020 on consent under Regulation 2016/679, adopted 4 May 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Elsig M, Klotz S (2021) Data flow-related provisions in preferential trade agreements: trends and patterns of diffusion. In: Burri M (ed) Big data and global trade law. Cambridge University Press, Cambridge, 42-62. https://doi.org/10.1017/9781108919234.004

Eurojust (2022) The CLOUD Act. https://www.eurojust.europa.eu/publication/cloud-act (accessed 22 February 2026).

Evenett SJ, Baldwin RE (eds) (2020) Revitalising multilateralism: Pragmatic ideas for the new WTO Director-General. CEPR Press, London. https://cepr.org/system/files/publication-files/60033-revitalising_multilateralism_pragmatic_ideas_for_the_new_wto_director_general.pdf

Ferracane MF (2021) The costs of data protectionism. In: Burri M (ed) Big data and global trade law. Cambridge University Press, Cambridge, 63-82. https://www.cambridge.org/core/books/big-data-and-global-trade-law/costs-of-data-protectionism/A97AC3D1E4EAD2A8B90F33EEF605D672

Ferracane MF, van der Marel E, Lee-Makiyama H (2018) Digital trade restrictiveness index. ECIPE Working Paper, European Centre for International Political Economy, Brussels, 1-137. https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

Fratini S, Hine E, Novelli C, Roberts H, Floridi L (2024) Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society 3:59, 1-27. https://doi.org/10.1007/s44206-024-00146-7

Gao HS (2021) Data regulation with Chinese characteristics. In: Burri M (ed) Big data and global trade law. Cambridge University Press, Cambridge, 245-267. https://www.cambridge.org/core/books/big-data-and-global-trade-law/data-regulation-with-chinese-characteristics/2539ECBA4499D555BD8206948AD8F4BB

G7 (2017) Taormina leaders' communiqué. Taormina, Italy, 26-27 May 2017. https://www.mofa.go.jp/files/000260041.pdf

Gu H (2024) Data, big tech, and the new concept of sovereignty. Journal of Chinese Political Science 29: 591–612. https://doi.org/10.1007/s11366-023-09855-1

Heeks R (2021) From digital divide to digital justice in the Global South: conceptualising adverse digital incorporation. Digital Development Working Paper No. 90, The University of Manchester, pp. 1–13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3907633

Hung HT (2025) Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach. Journal of Computational Social Science 8, Article 24, 1–31. https://doi.org/10.1007/s42001-024-00346-8

Jiang M (2024) Models of state digital sovereignty from the Global South: diverging experiences from China, India and South Africa. Policy Internet 16: 727–738. https://doi.org/10.1002/poi3.427

Jovan K (2009) An introduction to internet governance. https://www.diplomacy.edu/wp-content/uploads/2023/03/IGF_English_2009_FINAL2009.pdf

Juliussen BA, Kozyri E, Johansen D, Rui JP (2023) The third country problem under the GDPR: enhancing protection of data transfers with technology. International Data Privacy Law 13(3): 225–244. https://doi.org/10.1093/idpl/ipad013

Kang S (2024) WTO e-commerce negotiations: a path to the multilateral digital trade rules. Advances in Economics, Management and Political Sciences 71: 119–124. https://doi.org/10.54254/2754-1169/71/20241449

Kaya M, Shahid H (2025) Cross-border data flows and digital sovereignty: legal dilemmas in transnational governance. Interdisciplinary Studies in Society, Law, and Politics 4(2): 219–233. https://www.journalisslp.com/index.php/isslp/article/download/309/516/1730

Kuner C (2017a) Reality and illusion in EU data transfer regulation post Schrems. German Law Journal 18(4), 881–918. https://www.cambridge.org/core/journals/german-law-journal/article/reality-and-illusion-in-eu-data-transfer-regulation-post-schrems/0341A0D14DC345730F9B48A496A968D3

Kuner C (2017b) The Internet and the global reach of EU law. In: Cremona M, Scott J (eds) EU law beyond EU borders: The extraterritorial reach of EU law. Oxford University Press, Oxford, pp. 83–102. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930

Lalova-Spinks T, Valcke P, Ioannidis J P A, Huys I (2024) EU-US data transfers: an enduring challenge for health research collaborations. NPJ Digital Medicine 7(1): 215, 1–5. https://doi.org/10.1038/s41746-024-01205-6

Lateef MA (2025) Digital sovereignty in global trade: Analysing WTO governance of data flows. Beijing Law Review 16(2): 875–910. https://doi.org/10.4236/blr.2025.162044

Lemley MA (2021) The splinternet. Duke Law Journal 70(6), 1397–1427. https://scholarship.law.duke.edu/dlj/vol70/iss6/3

Madison MJ (2020) Tools for data governance. University of Pittsburgh Legal Studies Research Paper No. 2020–10, pp. 29–43. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3653209

Mayer M, Nock PJ (2025) Digital fragmentations, technological sovereignty and new geoeconomics. Global Policy 4(1), 2–13. https://bristoluniversitypressdigital.com/view/journals/gpe/4/1/article-p2.xml

McMahan HB, Moore E, Ramakrishnan S, Hampson S, Arcas BA (2017) Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS 2017), PMLR 54, 1273–1282. https://proceedings.mlr.press/v54/mcmahan17a.html

Meltzer JP (2014) The internet, cross-border data flows and international trade. Asia & the Pacific Policy Studies 1(3), 90–102. https://doi.org/10.1002/app5.60

Meltzer JP, Lovelock P (2018) Regulating for a digital economy: understanding the importance of cross-border data flows in Asia. Brookings Institution, Global Economy & Development Working Paper 113. https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_working-paper.pdf

Mishra N (2024) International trade law and global data governance. Hart Publishing, Oxford. https://library.oapen.org/bitstream/handle/20.500.12657/88173/9781509961719.pdf

Mitchell AD, Mishra N (2019) Regulating cross-border data flows in a data-driven world: How WTO law can contribute. Journal of International Economic Law, 22(3), 389–416. https://doi.org/10.1093/jiel/jgz016

Musoni M, Karkare P, Teevan C, Domingo E (2023) Global approaches to digital sovereignty: Competing definitions and contrasting policy. ECDPM Discussion Paper No 344, May 2023, Maastricht: ECDPM.

https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf
Naef T (2021) Data protection without data protectionism. Springer, Cham.
Nocetti J (2024) A splintered internet? Internet fragmentation and the strategies of China, Russia, India and the European Union. IFRI Studies, 27 February 2024. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_internet_fragmentation_february_2024.pdf
OECD (2015) Data-driven innovation: Big data for growth and well-being. OECD Publishing, Paris. https://doi.org/10.1787/9789264229358-en
OECD (2017) Key issues for digital transformation in the G20. OECD Digital Economy Policy Papers No. 251. OECD Publishing, Paris. https://web-archive.oecd.org/2017-01-12/424822-key-issues-for-digital-transformation-in-the-g20.pdf
OECD (2019a) Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies. OECD Publishing, Paris. https://doi.org/10.1787/276aaca8-en
OECD (2020) OECD Digital Economy Outlook 2020, OECD Publishing, Paris. https://doi.org/10.1787/bb167041-en
OECD (2022a) Going digital to advance data governance for growth and well-being. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/going-digital-to-advance-data-governance-for-growth-and-well-being_246d8cab/e3d783b0-en.pdf
OECD (2022b) Cross-border data flows: Regulatory barriers and the need for proportionality. OECD Publishing, Paris. https://doi.org/10.1787/5031dd97-en
OECD (2022c) Fostering cross-border data flows with trust. OECD Digital Economy Papers No. 343. OECD Publishing, Paris. https://doi.org/10.1787/139b32ad-en
OECD (2022d) Going digital: Guide to data governance policy making. OECD Publishing, Paris. https://doi.org/10.1787/40d53904-en
OECD (2023a) Moving forward on Data Free Flow with Trust: New evidence and analysis of business experiences. OECD Digital Economy Papers, No. 353. OECD Publishing, Paris. https://doi.org/10.1787/1afab147-en
OECD (2023b) The nature, evolution and potential implications of data localisation measures. OECD Trade Policy Papers No. 278. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf
OECD (2024) AI, data governance and privacy: Synergies and areas of international co-operation. OECD Artificial Intelligence Papers No. 22, Paris: OECD Publishing. https://doi.org/10.1787/2476b1a4-en
Office of the United States Trade Representative (USTR) (2020) Report on the appellate body of the World Trade Organization, 28 February 2020. https://ustr.gov/sites/default/files/Report_on_the_Appellate_Body_of_the_World_Trade_Organization.pdf
Pierucci F (2025) Sovereignty in the digital era: rethinking territoriality and governance in cyberspace. Digital Society 4, 1-19. https://doi.org/10.1007/s44206-025-00189-4
Robinson L, Kizawa K, Ronchi E (2021) Interoperability of privacy and data protection frameworks. OECD Going Digital Toolkit Notes No. 21, Paris: OECD Publishing. https://doi.org/10.1787/64923d53-en
Rojszczak M (2020) CLOUD Act agreements from an EU perspective, Computer Law & Security Review 38: 105442, 1-14. https://www.sciencedirect.com/science/article/pii/S0267364920300479
Saluste M (2025) Cross-border 'data adequacy' frameworks under GATS Article VII: aligning WTO members' rights to protect personal data with their international commitments. World Trade Review 24: 593-617. https://doi.org/10.1017/S1474745625000047
Schwartz PM (2018) Legal access to the global cloud. Columbia Law Review 118: 1681-1762. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3008392
Stürmer M, Nussbaumer J, Stöckli P (2021) Security implications of digitalization: the dangers of data colonialism and the way towards sustainable and sovereign management of environmental data. University of Bern, Working Paper, June 2021. https://doi.org/10.13140/RG.2.2.24791.80807

Tenopir C, Allard S, Douglass K, Aydinoglu AU, Wu L, Read E, Manoff M, Frame M (2020) Data sharing, management, use, and reuse: Practices and perceptions of scientists worldwide. PLoS ONE 15(3): e0229003. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0229003

UNCTAD (2021) Digital economy report 2021: Cross-border data flows and development – For whom the data flow. United Nations Conference on Trade and Development. https://unctad.org/system/files/official-document/der2021_en.pdf

UNESCO (2022) Steering AI and advanced ICTs for knowledge societies: a rights, openness, access and multi-stakeholder perspective. UNESCO, Paris. https://unesdoc.unesco.org/ark:/48223/pf0000372132

United States (2025) Executive Order 14257: Regulating Imports With a Reciprocal Tariff To Rectify Trade Practices That Contribute to Large and Persistent Annual United States Goods Trade Deficits. Federal Register, Vol. 90, 7 April 2025. https://www.govinfo.gov/content/pkg/FR-2025-04-07/pdf/2025-06063.pdf

Vásquez Callo-Müller M (2024) From APEC to global: the establishment of the Global CBPR Forum. https://doi.org/10.2139/ssrn.5122314

Velli F (2019) The issue of data protection in EU trade commitments: cross-border data transfers in GATS and bilateral free trade agreements. European Papers 4(3): 881-894. https://www.europeanpapers.eu/en/system/files/pdf_version/EP_EF_2019_I_022_Federica_Velli_00325.pdf

Verhulst S, Young A (2022) Identifying and addressing data asymmetries so as to enable (better) science. Frontiers in Big Data 5: 888384. https://doi.org/10.3389/fdata.2022.888384

Viljoen S (2021) A relational theory of data governance. The Yale Law Journal 131(2), 573-654. https://www.yalelawjournal.org/pdf/131.2_Viljoen_1n12myx5.pdf

von Scherenberg F, Hellmeier M, Otto B (2024) Data sovereignty in information systems. Electronic Markets 34, Article 15, 1-11. https://doi.org/10.1007/s12525-024-00693-4

Weber R H (2014) Legal interoperability as a tool for combatting fragmentation. Global Commission on Internet Governance Paper Series No 4, 2014, 1-50. https://www.cigionline.org/static/documents/gcig_paper_no4.pdf

Willemyns I (2018) The GATS (in)consistency of barriers to digital services trade. Leuven Centre for Global Governance Studies Working Paper No 207: 1-19. https://ghum.kuleuven.be/ggs/publications/working_papers/2018/wp207-willemyns.pdf

World Economic Forum (2020) A roadmap for cross-border data flows: future-proofing readiness and cooperation in the new data economy. World Economic Forum, Geneva. http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf

WTO (1994) Understanding on rules and procedures governing the settlement of disputes (DSU), Annex 2 to the Marrakesh Agreement Establishing the World Trade Organization, adopted 15 April 1994. https://www.wto.org/english/docs_e/legal_e/28-dsu_e.htm

WTO (2023) World trade report 2023: Re-globalization for a secure inclusive and sustainable future. WTO, Geneva. https://www.wto.org/english/res_e/booksp_e/wtr23_e/wtr23_e.pdf

WTO (2024) Information on the agreement on e-commerce. WTO, Geneva. https://www.wto.org/english/tratop_e/ecom_e/information_on_agreement_ecom.pdf

WTO (2025) China initiates WTO dispute regarding US "reciprocal tariffs". 8 April 2025. https://www.wto.org/english/news_e/news25_e/dsrfc_08apr25_e.htm

WTO (n.d.a) Information on the agreement on e-commerce. WTO, Geneva. https://www.wto.org/english/tratop_e/ecom_e/information_on_agreement_ecom.pdf (accessed 22 February 2026).

WTO (n.d.b) Principles of the trading system. WTO, Geneva. https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm (accessed 22 February 2026).

WTO Secretariat (2025) Understanding the WTO. WTO, Geneva. https://www.wto.org/english/thewto_e/whatis_e/tif_e/utw_chap1_e.pdf (accessed 22 February 2026).

Yakovleva S (2024) Governing cross-border data flows: reconciling EU data protection and international trade law. Oxford University Press, Oxford.

Zhang C (2024) China's privacy protection strategy and its geopolitical implications. Asian Review of Political Economy 3(6), 1-13. https://doi.org/10.1007/s44216-024-00028-2

阿部克則（2019）「第 9 章 WTO 上級委員会検討手続第 15 項をめぐる諸問題」阿部克則・関根豪政（編）『国際貿易紛争処理の法的課題』信山社 285–308 頁.
有本真由（2019）「域外リモートアクセスによる証拠収集にかかる米国 CLOUD 法に基づく行政協定に関する一考察」『情報ネットワーク・ローレビュー』第 18 巻 24–34 頁.
https://www.jstage.jst.go.jp/article/inlaw/18/0/18_180002/_pdf/-char/ja
石井夏生利（2025）「各国のプライバシー・データ保護法の理解と国際協調の可能性」音無知展・山本龍彦編『講座 情報法の未来をひらく：AI 時代の新論点 第 3 巻 プライバシー』法律文化社 229–59 頁.
石本茂彦（2022）「第 2 章 国家安全と情報法」石本茂彦・松尾剛行・森脇章編『中国のデジタル戦略と法―中国情報法の現在地とデジタル社会のゆくえ―』弘文堂 37–68 頁.
小野寺良文（2022）「第 6 章 データローカライゼーション」石本茂彦・松尾剛行・森脇章編『中国のデジタル戦略と法―中国情報法の現在地とデジタル社会のゆくえ―』弘文堂 171–193 頁.
加藤紫帆（2024）「経済規制の域外適用とグローバル・ガバナンス」『日本国際経済法学会年報』第 33 号 145–154 頁.
川瀬剛志（2015）「WTO 協定における無差別原則の明確化と変容」RIETI ディスカッション・ペーパー・シリーズ 15–J–004; 10–15 頁. https://www.rieti.go.jp/jp/publications/dp/15j004.pdf
清水章雄（2019）「第 5 章 WTO 体制の基本的規律」『国際経済法〔第 3 版〕』有斐閣 104–125 頁.
東條吉純（2020a）「越境データ移転規制に対する WTO/GATS の適用と限界」『日本国際経済法学会年報』第 29 号 35–55 頁.
東條吉純 （2020b） 「WTO 協定による越境データ流通の規律と限界」RIETI ディスカッション・ペーパー・シリーズ 20–J–011; 1–30 頁. https://www.rieti.go.jp/jp/publications/dp/20j011.pdf
中川淳司（2019）「第 8 章 WTO 体制におけるサービス貿易と知的財産保護」『国際経済法〔第 3 版〕』有斐閣 207–217 頁.
福山章子（2021）「欧州・中国を中心とするデータ保護主義の現状と通商ルールの展望」『世界経済評論』2019 年 1–2 月号（改訂版）; 1–10 頁. https://www.owls-cg.com/wp-content/uploads/2021/02/欧州中国を中心とするデータ保護主義の現状と通商ルールの展望_Owls 福山章子.pdf
藤井康次郎（2020）「Data Free Flow With Trust 構想とクラウド法―近時の経済連携協定デジタル貿易規律の概観と『クラウド法報告書』の紹介―」『日本国際経済法学会年報』第 2 有本 9 号 56–74 頁.
藤井康次郎・根本拓・福島惇央（2024）「越境データ移転規制における透明性の確保―国際的な制度構築に向けて―」石井由梨佳（編）『講座 情報法の未来をひらく：AI 時代の新論点 第 7 巻 安全保障』法律文化社 112–136 頁.
松尾剛行・胡悦（2022）「第 3 章 個人情報の保護と国家のデータ利用」石本茂彦・松尾剛行・森脇章編『中国のデジタル戦略と法―中国情報法の現在地とデジタル社会のゆくえ―』弘文堂 69–107 頁.
三浦秀之（2022）「データをめぐる経済安全保障」『アジア研究シリーズ』第 114 号一般財団法人アジア太平洋研究所 33–40 頁. https://www.asia-u.ac.jp/albums/abm.php?d=448&f=abm00006451.pdf&n=07–プロジェクト報告書 114 号__三浦秀之.pdf
横大道聡（2024）「安全保障の構造変容と情報法―米国の中国プラットフォーム事業者の規制を手がかりに―」石井由梨佳（編）『講座 情報法の未来をひらく：AI 時代の新論点 第 7 巻 安全保障』法律文化社 2–35 頁.

第Ⅱ部

国際的データガバナンスの分断をもたらす五つの国家施策

第Ⅱ部　国際的データガバナンスの分断をもたらす五つの国家施策

第Ⅱ部では、国際的データガバナンスの分断をもたらす五つの国家施策―大国による規範輸出、データローカライゼーション、ガバメントアクセス、越境的ディスカバリ、国家によるデータ流入規制―に焦点を当て（第 3 章～第 7 章）、それぞれの形成背景と制度的影響を分析することにより、越境的データガバナンス規範再構成の方向性を検討する。

国際的データガバナンスの分断は、各国の国内制度差に由来するだけでなく、国家が追求する統治権限、安全保障上の利害、規範的価値が相互に競合し合うことによって引き起こされる複層的現象である。そのなかでも、上記の五つの国家施策は、国家主権の行使と国際的相互接続性との緊張が最も先鋭的に表出する領域であり、越境的データガバナンス規範再構成の在り方を検討するうえで中心的な分析対象となる。これら五施策は、国家がサイバー空間における主権を拡張し、または自国の規範領域を防衛する過程で生じる制度的表現形態として理解することができ、いずれも単独で作用するのではなく、相互に影響を及ぼし合いながら累積的に作用している。これらの相互作用を通じて国際的データガバナンスの分断は深化し、その累積効果として世界のデータ流通が断片化することで、各国が相異なる制度原理と価値観に基づき併存・競合する多極化したデータ秩序が形成されている。このような規範的非対称性の是正は、今後の越境的データガバナンス規範再構成における最重要課題である。

(1) 大国による規範輸出（第 3 章）

大国が自国の法制度や政策原理を国際規範として外部に投射し、他国の制度設計や意思決定に影響を及ぼす現象、いわゆる規範輸出（normative export）は、越境的データガバナンスにおける非対称性を一層深化させる。現在、米国、中国、EU といった大国は、市場アクセス条件、技術標準の設定、域外適用規制、デジタルインフラの支配などを通じて、それぞれ異なる形態の規範輸出を実践している。これらの規範は並立しながら競合し、「ヨコの非対称性」を形成するだけでなく、各ブロック内部にも制度的適応能力や経済力の差に応じて「タテの非対称性」を生じさせる（前記第 1 章第 3 節参照）。その結果、国際社会は複数の価値的・制度的ブロックに分断され、中小国や発展途上国は大国の規範モデルへの適応を迫られるという構造的従属関係に置かれる。大国による規範輸出の競合は、国際的データガバナンスの分断を構造的に深化させる主要因であり、この構造的分断を緩和するためには、既存の規範配置を前提としない越境的データガバナンス規範の再構成が不可欠となる。

(2) データローカライゼーション（第 4 章）

データローカライゼーションは、国家が自国領域内で生成されたデータを自国の監督権限の下に置くことを目的とする政策的手段であり、国際的データガバナンスの分断を最も直接的に顕在化させる現象である。各国は、安全保障や個人情報保護を名目としてデータの国外移転を制限するが、その背後にはデジタル主権の確立や自国産業の競争優位を確保しようとする政策的動機が潜在している。これらの措置が相次いで導入され累積的に作用すると、越境的デー

タ流通が阻害され、国際的相互接続性が低下する。すなわち、データローカライゼーションは、越境的データガバナンスを国家単位で閉塞させる主要因として機能する。

(3) ガバメントアクセス（第 5 章）

ガバメントアクセス（政府機関による民間データへのアクセス制度）は、国家安全保障と個人の権利保障の境界に位置する最もセンシティブな領域であり、各国の制度的理念の相違が顕著に現れる分野である。国家がテロ対策や犯罪捜査などを根拠として、自国域外に所在するデータへのアクセス権限を主張する場合、その行為は他国の主権的管轄権と潜在的に衝突し得る。各国が異なる基準でアクセス権限を設計・運用する結果、相互の制度的信頼は低下し、越境的データ移転の前提条件も不透明化する。このようなガバメントアクセスの制度的不整合は、国際的データガバナンスの分断を助長する重要な要因となっている。

(4) 越境的ディスカバリ（第 6 章）

ディスカバリの越境的適用は、越境的データガバナンスにおける法的衝突の典型例である。米国ディスカバリについては、米国外の訴訟等のためにも利用することができる手続が設けられていることから、米国外の訴訟当事者等が米国外に所在するデータの入手を目的としてディスカバリの越境的適用を利用する事例が増えている。米国の裁判所が他国に所在するデータの開示・提出を命じる場合、それは相手国のデータ保護法や主権原則と直接衝突する。特に電子的保存情報（Electronically Stored Information: ESI）を対象とするディスカバリ（e ディスカバリ）は、企業の国際的なデータ運用に重大な影響を及ぼし、各国が自国民や企業のデータの国外流出を防ぐため国内法制を強化する動きを促している。こうした相互反発の蓄積は、法制度間の相互承認や協力を困難にし、越境的データガバナンスをより複雑かつ不安定な状態へと導いている。

(5) 国家によるデータ流入規制（第 7 章）

国家によるデータ流入規制は、国外からの情報やコンテンツの流入を制限することで、国内の情報空間を統制しようとする政策である。中国のグレート・ファイアウォールやロシアのソブリン・インターネット法などに見られるように、国外情報の制限は政治的統制やデジタル主権の確立を目的としており、その結果として国際的データガバナンスの分断を深刻化させている。これは、データの自由な流通を基礎とする国際秩序に対し、国家単位で閉鎖的な情報環境を形成する動きとして機能し、地政学的境界線に沿った越境的データガバナンス規範のブロック化を招く要因となっている。

第 3 章

大国による規範輸出

第 3 章　大国による規範輸出

国際的なデータガバナンスの規範的分断を生じさせる主な要因の一つは、大国による規範輸出（normative export）である。規範輸出とは、特定の国家または地域が、自国の法制度・価値観・政策基準を国際的規範として外部に拡張し、他国の制度設計や意思決定に影響を及ぼす現象をいう[1]。本章では、越境的データガバナンスの領域において、大国が自国法制度の域外適用や市場支配力を通じて自国規範を他国に拡張する過程に焦点を当てる。

現在、EU、中国、米国はいずれも異なる形態の規範輸出を実践している。EU は、GDPR を中核とする規範統制モデル（Normative control model）に基づき、域外の企業や政府に対して高度なデータ保護水準を事実上強制している[2]。中国は、国家主導で「サイバー主権」を掲げ、国家安全保障を最優先とするサイバー主権モデル（Cyber sovereignty model）に基づき、「中国データ三法」（前記第 1 章第 3 節参照）をはじめとする法体系を通じて越境的データ移転を厳格に制限し、その効力を域外にも及ぼしている[3]。米国は、国家戦略として規範を直接的に輸出するわけではないものの、市場支配モデル（Market dominant model）に基づき、グローバル IT 企業の市場支配力と貿易協定の電子商取引章を通じて、国際的な規範形成に実質的な影響を及ぼしている[4]。

規範輸出は、多くの場合、大国が自国の国内規範を他国に一方的に押しつける一国主義的な措置として現れる[5]。この場合、輸出側は自国法を調整する必要が乏しく、制度的負担も小さい。他方、受け入れ側の企業や行政当局は、複数の法制度への適合を強いられ、コンプライアンス・コストの増大、政策裁量の制約、制度的自律性の喪失といった課題に直面する。こうした過程を通じて、規範形成力が一部の大国に集中するという構造的非対称性が生じている。しかも現状では、大国間で異なる規範体系が併存・対立しており、非大国は制度面および技術面の双方において従属的立場に置かれている。その結果、非大国は、いずれか一方の大国の規範に従うか、あるいは事例ごとに異なる大国の規範を用いるかという制約的選択を迫られている[6]。

このように、大国による一国主義的な規範輸出は、越境的データガバナンスにおける「ヨコの非対称性」と「タテの非対称性」の双方を深化させることにより、国際的データガバナンスの規範的分断を一層顕在化させ、国際的制度秩序の均衡と正統性を損なうものである。規範輸出により大国の規範が域外に及ぶことは、一見すると国際的データガバナンスの基準を収斂させ、制度的な調和に向かうようにも見える。しかし、これは実質的な調和ではなく、一国主義的な規範の投射にすぎず、相互承認や対等な制度調整に基づく協調的統一とは本質的に異なる。EU、中国、米国が採用するデータ保護・監督・越境移転の基準は、価値基盤や制度目的の段階から相互に整合しがたい構造を抱えており、規範輸出が進むほど、むしろ制度的断片化が強化される。すなわち、各大国が独自の規範体系を周辺国へと波及させるほど、複数の制度的ブロック

---

[1] Manners (2002), pp. 238–242.
[2] Bradford (2020), pp. 7–15.
[3] Creemers (2021), pp. 2–10.
[4] Aaronson and Leblond (2018), pp. 252–254.
[5] Bradford (2020), Introduction (p. xiv) (Bradford は、EU による規範輸出について「一国主義的な規範の国際化（unilateral regulatory globalization）」という表現を用いている).
[6] Aaronson and Leblond (2018), pp. 258–264.

が併存する構造が固定化され、非大国は相互に矛盾する規律の板挟みとなり、制度的自律性や選択の余地を失うことになる。このような状況は、国際的な共通基盤の形成を阻み、制度的非対称性を深めるのみならず、サイバー空間全体を複数の排他的ブロックへと分割する方向に作用する。その意味で、規範輸出は分断の解消ではなく、サイバー空間の分裂を促す構造的要因として機能している。

なお、この点に関しては、大国による歩み寄りの努力として、EU は GDPR の十分性認定[7]や標準契約条項（Standard Contractual Clauses: SCCs）[8]などの枠組みによりデータ移転の全面禁止を回避しつつ一定の保護水準を担保する手段を整備しており、米国も EU との枠組協定を通じて法的整合性の確保を図っている[9]。しかし、これらはいずれも、大国の制度モデルを基準とした秩序形成を前提としており、非大国を含む多様な法制度や価値観との対等な相互承認に基づくものとは言いがたい。したがって、こうした動向を参考とすること自体に一定の意義は認められるものの、それだけでガバナンス格差の是正に資するとは限らない。真に求められるのは、制度的整合性および相互運用性を前提としつつ、多元的かつ公平なルール形成を進めることであり、それは、一国主義的な規範輸出ではなく、非大国を含む多様な制度間の相互理解と信頼に基づく協調的枠組みによって実現されるべきである[10]。

本章ではこのような視座に立ち、まず第 1 節から第 3 節において EU、中国、米国による規範輸出の実情を概観し、それぞれのアプローチが越境的データガバナンスに及ぼす影響を検討する。それらの検討を踏まえ、第 4 節では大国による規範輸出の弊害を論じたうえで、越境的データガバナンス規範再構成の方向性を提示する。

[7] European Commission (2023a); 加藤尚徳（2023）260–72 頁.
[8] European Commission (2021).
[9] European Commission (2023b), recitals 13–18; arts 1 and 3.
[10] Arner et al. (2022), pp. 683–696.

第 1 節　EU による規範輸出

EU による規範輸出は、越境的データガバナンスにおける最も顕著な現象の一つであり、特に「ブリュッセル効果（Brussels Effect）」として理論化されてきた。この概念は、EU が域内市場における高度かつ厳格な規制を制定・施行することにより、その規範が市場アクセスを求める多国籍企業や第三国政府に事実上適用されるという現象をいう[11]。特徴的なのは、軍事力や外交的圧力といった強制力を伴わず、EU 市場の経済的魅力と法制度の精緻性、さらに監督当局の執行力を背景に、市場メカニズムを通じた規範拡張が実現される点にある[12]。

第1項　GDPR による規範輸出

ブリュッセル効果を制度的に支える代表例が、GDPR である。GDPR 第 3 条第 1 項は、EU 域内に所在する管理者または取扱者の事業所の活動に関連して行われる個人データの取扱いについて、たとえ処理自体が EU 域外で行われる場合であっても、GDPR を適用する旨を定めている。さらに、第 2 項は、EU 域内に拠点を有しない管理者または取扱者の活動であっても、EU 域内のデータ主体に対して商品またはサービスを提供する場合、あるいはその行動を EU 域内でモニタリングする場合には、GDPR の適用対象となることを明示している（以下、参照条文は各項末尾に掲載する。）。

すなわち、管理者または取扱者の事業所所在地ではなく、データ主体の所在地を基準として適用範囲を定めることにより、EU の個人情報保護規範が、法的に国境を越えて適用される制度構造が確立されている。この法技術は、従来の国際私法的な管轄権や準拠法の決定の枠組みを超え、規範の適用範囲を事実上、地理的制約なく拡張するものである。その結果、EU は域外の法主体に対しても自らの価値体系と規律を実質的に適用し得るようになり、GDPR は EU の規範輸出を支える最も強力な法的基盤となっている。

したがって、EU 市場にアクセスしようとする企業は、本社所在地にかかわらず GDPR への実質的な準拠を求められる。特に、データ処理の適法性（第 6 条）、データ主体の権利（第 12 条～第 23 条）、越境的移転の制限（第 44 条以下）、および高額な制裁金（第 83 条）といった厳格な規定の適用により、企業は自国法と EU 法との整合を図らざるを得ない。このように、GDPR は域内規制を超えて国際的な企業行動を直接的に制御し得る制度として機能しており、EU の規範輸出を最も端的に体現しているといえる。

【参照条文】

GDPR（General Data Protection Regulation）

第 3 条（適用範囲）

1. 本規則は、EU 域内の管理者又は取扱者の事業所の活動に関連してなされる個人データの取扱いに適用される。この場合、その取扱いが EU 域内又は域外でなされるか否かは問わない。

[11] Bradford (2020), pp. 1–6.
[12] Bradford (2020), pp. 25–65.

2. 本規則は、EU 域内に拠点を有しない管理者又は取扱者による EU 在住のデータ主体の個人データの取扱いに適用される。ただし、取扱活動が次に掲げる項目に関連する場合に限る。
(a) EU 在住のデータ主体に対する商品又はサービスの提供。この場合、データ主体に支払が要求されるか否かは問わない。
(b) EU 域内で行われるデータ主体の行動の監視に関する取扱い。
3. 本規則は、EU 域内に拠点を持たない管理者による個人データの取扱いにも適用されるが、国際公法により加盟国の国内法が適用される場所にある管理者による取扱いの場合に限られる。

第 6 条（処理の適法性）
1. 個人データの処理は、次のいずれかに該当する場合に限り適法とする。
(a) データ主体が、1 つ又は複数の特定の目的に関して、自らの個人データの処理に同意した場合。
(b) データ主体が当事者となる契約の履行のため、又は契約締結前にデータ主体の要請に基づき措置を講ずるために処理が必要である場合。
(c) 管理者が法的義務を履行するために処理が必要である場合。
(d) データ主体又は他の自然人の生命に関わる重要な利益を保護するために処理が必要である場合。
(e) 公共の利益のために行われる任務の遂行、又は管理者に付与された公的権限の行使のために処理が必要である場合。
(f) 管理者又は第三者が追求する正当な利益のために処理が必要である場合。ただし、当該利益よりも、データ主体の利益又は基本的権利及び自由が優先する場合を除く。特に、データ主体が児童である場合にはこの限りではない。

（以下略）

第 44 条（データ移転の一般原則）
個人データの第三国又は国際機関への移転は、本規則においてその他の規定がある場合を除き、本規則の他の条項の遵守が確保され、当該第三国、地域又は国際機関が第 45 条に基づき十分なレベルの保護を提供していると認められる場合にのみ行うことができる。すべての個人データの移転は、データ主体の権利と自由を引き続き保護することを確保しなければならない。

第 45 条（十分性認定に基づくデータ移転）
1. 欧州委員会は、特定の第三国、地域若しくは一つ以上の指定部門又は国際機関が十分なレベルの個人データ保護を提供していると判断した場合、当該第三国等への個人データの移転は、追加の認可なく許可される。
2. 欧州委員会は、以下の要素を考慮して十分性の判断を行う:
・ 法の支配、基本的人権の尊重、効果的なデータ保護法の存在（データ主体の権利、監督機関の独立性、救済措置等）
・ 第三国又は国際機関が締結している国際協定
・ データ保護機関の活動及び執行能力
3. 十分性認定が行われた場合、欧州委員会はそれを EU 官報で公示し、定期的に再評価する。

（以下略）

第 83 条
（第 1 項～第 4 項省略）

5. 次に掲げる規定の違反は、第 2 項に従って、最大 2 千万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 4%までの、どちらか高い方を制裁金として科されるものとする。

((a)・(b)省略)

(c) 第 44 条から第 49 条による第三国又は国際機関の取得者への個人データ移転。

(以下略)

第 2 項　他国との摩擦

EUによる一方的な規範輸出は、第三国(域外国)の事業者や法制度に対し、構造的な不均衡をもたらし、摩擦を生じさせている。

(1)　米国との摩擦

EU が GDPR を通じて国際的なデータ保護の標準化を推し進める一方で、米国は、プライバシー保護を主として契約上の自由および消費者保護の枠組みの中で捉える、まったく異なる制度的パラダイムに基づいてデータ規制を構築してきた。EU における個人データ保護が憲法上の人格権と不可分に結びついているのに対し、米国ではプライバシーが連邦憲法上の明文の権利として保障されておらず、個別法によるセクター別・州別の保護が中心である[13]。このような構造的差異は、EU 域外への個人データ移転を規制する GDPR の十分性認定制度において顕在化してきた。2000 年に導入されたセーフハーバー(Safe Harbor)は、EU と米国の間でデータ移転を可能にする一時的な制度的妥協であった。しかし、2015 年の CJEU(欧州司法裁判所)による Schrems I 判決[14]は、NSA など米国当局による監視活動が EU の基本権に反するとしてセーフハーバーを無効とした。これを受けて策定されたプライバシーシールド(Privacy Shield)も、2020 年の Schrems II 判決[15]で再び無効とされた。

このような制度的不整合を受け、両地域は再調整の試みを続けており、2023 年 7 月には新たに EU-U.S. Data Privacy Framework(DPF)が発効した[16]。この枠組では、2022 年の米国大統領令 14086 号によって新たに設置されたデータ保護審査裁判所(Data Protection Review Court)などを通じて、米国当局による監視対象の限定と、EU データ主体に対する救済手続の強化が試みられている[17]。しかし、DPF に対しても市民団体や法学者からは、欧州連合基本権憲章(EU 憲章)第 7 条・第 8 条が保障する権利に対する実効的担保としては依然不十分であるとの批判が根強く、将来的な訴訟リスク、いわゆる Schrems III のリスクが依然として存在する[18]。

---

[13] de Bruin (2022), pp. 128–139.

[14] Schrems v Data Protection Commissioner (Case C-362/14, 6 Oct 2015) ECLI:EU:C:2015:650. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362

[15] Data Protection Commissioner v Facebook Ireland Ltd and Schrems (Case C-311/18, 16 Jul 2020) ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

[16] European Commission (2023b), recital 2.

[17] Executive Order 14086 (2022) Enhancing safeguards for US signals intelligence activities, 87 Fed Reg 62283, 7 Oct 2022. https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf

[18] NOYB – European Center for Digital Rights (2023) European Commission gives EU-US data transfers third round at CJEU. 10 July 2023. https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

このように、GDPR と米国の制度的枠組みとの関係は、データ移転手段や技術的問題にとどまらず、民主主義国家における情報統治と個人の自由をめぐる価値観の対立を背景とする制度的摩擦である。信頼・相互承認・法的対称性に基づく持続可能な枠組みの構築が、越境的データガバナンス全体の持続可能性を左右する課題である。

(2)　その他の国との摩擦

EU による一方的な規範輸出は、他国の事業者や法制度に対し、制度的対応能力や執行体制の格差を十分に考慮しないまま、構造的な不均衡をもたらしている。その典型例が、EU との経済的接点を有しながらも、制度的・技術的インフラが十分に整備されていない国々における GDPR 準拠の困難性である。たとえば、多くのアフリカ諸国では、独立したデータ保護機関の設置や執行力の確保が依然として不十分であり、GDPR と同等の制度的要件を満たすことは極めて困難である[19]。それにもかかわらず、現地企業が EU 市民の個人データを処理する場合には GDPR の適用が及び、事実上その準拠を求められることになる。こうした状況は、EU の規範が域外に及ぶ一方で受入国の制度的選択の自由や政策的余地を狭めるという点で、越境的な規範適用における非対称性の深刻な一例といえる。

また、文化的・法的価値観の相違も、GDPR の一律的な適用に対する抵抗感を生む要因となっている。たとえば、アジアの多くの国では、個人データの保護やプライバシー権の保障が憲法上の明文規定に基づいて制度的に確立されているとは限らず、その保障内容も EU と比較すれば一般に限定的である。多くの法制度では、個人情報保護は主に行政法や取引法の一部として扱われており、人権的次元での体系的保護が制度の中心に据えられているわけではない。このような法的枠組みの相違は、アジア諸国が人格権を中核とする包括的規制モデルである GDPR をそのまま導入・運用することに対する制度的な適合困難性を顕在化させ、GDPR 型規制の受容には制度的摩擦が不可避的に発生する[20]。

GDPR の国際的普及は、一見するとグローバルなデータ保護水準の向上に寄与するものと評価されがちである。しかしその実態は、各国間における制度対応能力の格差や法的価値観の相違が十分に考慮されておらず、各国の制度的・文化的多様性を十分に尊重しないまま単一の規範が国際的に拡張されている状況にほかならない。特に、グローバルサウス諸国や中小規模の事業者にとっては、こうした規範の拡張が制度的・経済的な不利益を構造的に内包するものとなっている。この点は、ブリュッセル効果の負の側面として、国際的な規制的正義（regulatory justice）をめぐる制度的課題を顕在化させている[21]。

【参照条文】

EU 憲章（Charter of Fundamental Rights of the European Union）

第 7 条（私的及び家族生活の尊重）

すべての人は、その私的生活、家族生活、住居及び通信に対する尊重を受ける権利を有する。

第 8 条（個人データの保護）

[19] UNCTAD (2021), pp. 81–91, 114–115, 189–190.

[20] Zhang (2025), pp. 2–14.

[21] Bradford A (2020), pp. 1–6, 25–65; Ryngaert and Taylor (2020), pp. 5–9; UNCTAD (2021), pp. 81–85, 90–91, 114–115, 189–190.

1. すべての人は、自己に関する個人データの保護を受ける権利を有する。
2. 当該データは、特定された目的のために、公正に、かつ、本人の同意又は法により定められた他の正当な根拠に基づいて処理されなければならない。すべての人は、自身に関して収集されたデータへのアクセス権及びその訂正を求める権利を有する。
3. これらの規則の遵守は、独立した当局による監督の対象となる。

第 3 項　EU による規範輸出拡大の動きと課題

EU による規範輸出は、個別法制の普及にとどまらず、国際的な規範形成の枠組みに対しても構造的な影響を及ぼしている。たとえば、EU は OECD、国連、APEC などの多国間フォーラムに積極的に関与し、自らの法制度を参照基準とするモデル規範や契約条項の策定を推進してきた[22]。この結果、EU 法の直接適用が及ばない国においても、GDPR などを参照した国内法制化が進み、EU 型の規範が国際標準として制度的に拡散して、事実上の拘束力を生み出している[23]。この現象は、法制度間の相互運用性を一定程度高める一方で、発展途上国や中小企業にとっては過剰なコンプライアンス負担を課し、国際的な制度的非対称性を拡大させる要因となっている[24]。

また、EU は、非個人データについても、その利活用に関する一連の法整備を通じて、国際的なデータガバナンスの規範形成に影響を及ぼす制度的基盤を築きつつある。2018 年に制定された非個人データの自由流通規則[25]は、加盟国によるデータの国内保存義務を原則禁止し、EU 域内での産業データや機械生成データの自由な移転を保障した。これは、データの保存場所に基づく制限ではなく、相互運用性と透明性を重視した制度モデルを提示するものである。これに続くデータガバナンス法[26]およびデータ法[27]は、いずれも GDPR のような明示的な域外適用条項を有してはいないものの、EU 域外の事業者や第三国政府に対しても事実上の拘束的効果を及ぼし得る規律構造となっている。

データガバナンス法第 5 条は、EU 公共機関が保有するデータの再利用に関し、EU 法上の条件を遵守することを域外の再利用者にも求めており、また第 11 条は、EU 域外のデータ仲介サービス提供者に対して EU 域内代表者の設置を義務づけている。これらの条文は、形式上は EU 域内適用に限定されながらも、EU 市場へのアクセスを媒介として EU 域外の事業者にも制度的遵守を事実上要請する構造を備えている。

---

[22] Aaronson and Leblond (2018), pp. 245–248, 257–259.
[23] Luisi (2022), Introduction, chapters two and three.
[24] Birnhack and Mundlak (2025), pp. 138–139.
[25] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, Official Journal of the European Union L 303/59 of 28 November 2018.
[26] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act), Official Journal of the European Union L 152/1 of 3 June 2022.
[27] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), Official Journal of the European Union L 2023/2854 of 22 December 2023.

さらに、2023 年に制定されたデータ法は、IoT 機器等によって生成される産業データの利用およびアクセスを包括的に規律し、第 4 条および第 5 条において、EU 市場で製品またはサービスを提供するすべての事業者に対し、EU 域内の利用者が当該データにアクセスする権利を保障する義務を課している。この構造は、EU 域外の製造者やサービス提供者に対しても、EU 市場への参入を通じて事実上の遵守義務を生じさせるものである。また、第 32 条は、第三国政府によるデータへのアクセスまたは移転要求に関し、事業者に対し契約上または法的救済手段を含む合理的な保護措置を講じる義務を課しており、EU または加盟国と当該第三国との間に有効な国際協定が存在しない場合には、開示に応じないことを原則としている。この条文は、EU 域内の事業者を第三国の法執行当局から保護するのみならず、他国の主権的行為に対しても実質的な制約を及ぼす準域外適用条項として機能する。

このように、データガバナンス法およびデータ法は、形式的には EU 域内の法秩序を対象としながらも、実質的には EU 市場へのアクセスや国際的データ取引を媒介として、EU の制度原理を域外に波及させる仕組みを有している。

こうした制度的展開と並行して、AI に関する包括的法制として 2024 年に採択された AI 法[28]も、EU によるガバナンスモデルの確立と規範輸出を支える重要な要素である。AI 法は、リスクベースアプローチに基づく包括的規制枠組みを採用し、AI システムをその利用目的や影響の程度に応じて分類している。特に附属書Ⅲ（Annex Ⅲ）に列挙された高リスク用途については、透明性、説明可能性、安全性などの確保を義務づけることにより、AI の社会的受容性と信頼性を制度的に担保する構造を構築している。そして、AI 法第 2 条第 1 項(a)～(c)は、EU 市場における AI システムおよび汎用 AI モデルの提供・利用に関する規制の適用範囲を定め、EU 域内の事業者のみならず、EU 域外に所在する提供者や運用者であっても、その AI システムの出力が EU 域内で使用される場合には本規則の適用対象となることを明示している。すなわち、この条項は、事業者の所在地ではなく AI システムの市場的影響圏（EU 域内での利用）を基準とすることにより、EU 法の実質的な域外適用を制度的に可能とし、EU 市場へのアクセスを媒介として域外主体の行動を規律する構造を明確に示している。したがって、AI 法は形式的には域内適用法であるものの、EU 市場へのアクセスを媒介として EU 域外事業者にも事実上の拘束力を及ぼす構造を備えており、規範的波及効果を有する法制として位置づけられる。さらに、AI 法は、リスク評価・適合性評価・認証制度を通じて、AI システムの設計・運用・監査に関する詳細な基準を国際標準化の文脈にまで拡張しており、EU 域外の開発事業者に対しても制度的同調圧力を生み出している[29]。このような構造は、EU 市場アクセスを通じて域外主体の行動を間接的に規律するという点で、データ法やデータガバナンス法と共通して、GDPR と同じ規範統制モデル（Normative control model）を体現している。したがって、AI 法は域内規制だけではなく、AI システムの設計段階から国際的な規範形成を主導するための制度的基盤として機能している。その目的は、技術革新と基本権保護を両立させる EU 型の統治モデルをグローバル・スタンダードとして定着させることであり、これにより EU は AI 開発と倫理的統治の双方において制度的主導権を確立しつつある。

---

[28] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Official Journal of the European Union L 2024/1689 of 12 July 2024.

[29] Artificial Intelligence Act, arts. 9–10, 16–17, 43.

以上のように、最近における EU の立法は、個人データに限定されない広範な情報資源を対象とし、欧州独自の制度モデルを構築しようとするものである。その特徴は、形式的な域外適用条項を設けるのではなく、EU 市場へのアクセスや国際的取引関係を媒介として、EU 法の制度原理を域外に波及させる点にある。この EU のアプローチは、域内統合の枠を超え、越境的な制度調和や国際的ルール形成の領域において、明確に国際的規範主導権の確立を志向するものである。

本節で述べたとおり、EU の規範輸出は、データ・AI・デジタル市場といった横断的領域を貫く統合的な制度設計のもとで展開されている。総じて EU による規範輸出は、経済的規模、法制度の高度性、監督執行力を基盤とする規範統制モデル（Normative control model）によって支えられた国際規範形成メカニズムである。このメカニズムは、GDPR から、データガバナンス法・データ法・AI 法へと拡大しており、EU 法秩序の国際的拡張を制度的に持続させる仕組みを有する。その結果、国際社会全体におけるデータ保護および AI 倫理の水準は一定の底上げを見せている一方で、各国の主権的自律性や政策裁量は相対的に制約を受ける傾向が強まっている。特に、発展途上国や中小規模事業者にとっては、EU 規範への準拠が過大な遵守コストを伴うことから、越境的データガバナンスにおける制度的非対称性を一層深化させ、各国間の規範競争を激化させる要因となっている。

【参照条文】

データガバナンス法（Data Governance Act）

第 5 条（公共部門機関が保有する保護対象データの再利用に適用される条件）

1. 加盟国は、公共部門機関が保有する本規則の対象となるデータの再利用を許可する場合には、当該再利用が、本規則および適用される EU 法および国内法に定められた条件を遵守して行われることを確保しなければならない。
2. 前項の条件は、再利用者が EU 域内に所在するか否かを問わず適用される。

（以下省略）

第 11 条（EU 域内に設立されていないデータ仲介サービス提供者の代表者）

1. EU 域内に設立されていないデータ仲介サービス提供者であって、EU 域内においてデータ仲介サービスを提供するものは、EU 域内に代表者を指定しなければならない。
2. 当該代表者は、EU 域内に設立された自然人または法人でなければならず、本規則に基づく当該データ仲介サービス提供者の義務に関して、監督当局および関係者からの連絡先として機能するものとする。
3. 代表者の指定は、当該データ仲介サービス提供者が本規則に基づく責任を免れるものではない。

（以下省略）

データ法（Data Act）

第 4 条（製品データ及び関連サービスデータへのアクセス、利用及び提供に関する利用者及びデータ保有者の権利と義務）

1. 利用者が接続製品又は関連サービスからデータに直接アクセスすることができない場合、データ保有者は、当該データ並びにその解釈及び利用に必要な関連メタデータを、不当な遅延なく、利用者が容易に利用できるよう提供しなければならない。

この場合、当該データは、データ保有者が利用できるものと同等の品質で、容易かつ安全に、無償で、包括的かつ構造化され、一般的に利用される機械可読形式で提供されなければならない。また、関連性があり、かつ技術的に可能な場合には、継続的かつリアルタイムで提供されるものとする。

当該提供は、技術的に可能な範囲において、電子的手段による簡易な請求に基づき行われるものとする。

2. 利用者及びデータ保有者は、当該処理が連合法又は加盟国法に定める接続製品の安全要件を損なうおそれがあり、その結果として自然人の健康、安全又はセキュリティに重大な悪影響を及ぼす場合には、契約によってデータへのアクセス、利用若しくはさらなる共有を制限し、又は禁止することができる。

この場合、所管分野の当局は、必要に応じて利用者及びデータ保有者に対し、技術的専門知識を提供することができる。

データ保有者が本条に基づきデータの共有を拒否する場合には、第 37 条に基づき指定された主管当局にその旨を通知しなければならない。

（以下省略）

第 5 条（利用者による第三者とのデータ共有の権利）

1. 利用者又は利用者の代理として行動する者の要請があった場合、データ保有者は、当該データ及びその解釈並びに利用に必要な関連メタデータを、不当な遅延なく、第三者に提供しなければならない。この場合、当該データは、データ保有者が利用できるものと同等の品質で、容易かつ安全に、利用者に対して無償で、包括的かつ構造化され、一般的に利用される機械可読形式で提供されなければならない。また、関連性があり、かつ技術的に可能な場合には、継続的かつリアルタイムで提供されるものとする。データ保有者は、当該データを第三者に提供するにあたって、第 8 条及び第 9 条に従わなければならない。
2. 第 1 項は、まだ市場に投入されていない新しい接続製品、物質又はプロセスの試験の文脈における利用可能なデータには適用されない。ただし、その利用が第三者によって契約上認められている場合を除く。

（以下省略）

第 32 条（国際的なガバメントアクセス及び移転）

1. データ処理サービス提供者は、EU 域内に保有される非個人データについて、その移転又はアクセスが EU 法又は当該加盟国の国内法と抵触するおそれがある場合には、国際的又は第三国の政府当局による当該データへのアクセス又は移転を防止するために、契約上の措置を含む、十分な技術的、組織的及び法的措置を講じなければならない。ただし、第 2 項又は第 3 項に定める場合を妨げるものではない。
2. 第三国の裁判所若しくは裁判機関の判決、又は第三国の行政当局の決定により、EU 域内に保有され、本規則の適用範囲に属する非個人データの移転又はアクセスをデータ処理サービス提供者に対して要求する場合には、当該決定又は判決は、当該第三国と EU との間、又は当該第三国と加盟国との間において効力を有する国際協定（たとえば、司法共助条約）に基づく場合にのみ、承認又は執行されるものとする。
3. 第 2 項にいう国際協定が存在しない場合において、データ処理サービス提供者が、第三国の裁判所若しくは裁判機関の判決、又は第三国の行政当局の決定の宛先とされ、かつ当該決定に従うこ

とが EU 法又は当該加盟国の国内法との抵触を招くおそれがあるときは、当該第三国当局によるデータの移転又はアクセスは、次のいずれかの条件を満たす場合にのみ行うことができる。

（以下省略）

AI 法（Artificial Intelligence Act）

第 2 条（適用範囲）

（1） 本規則は、次の者に適用される。

（a） 欧州連合域内で AI システムを市場に出し、若しくは使用に供し、又は汎用 AI モデルを市場に出す提供者。その提供者が欧州連合内か又は第三国に設立・所在しているかを問わない。

（b） AI システムを運用する者であって、その設立地又は所在地が欧州連合内にある者。

（c） AI システムの提供者及び運用者。その設立地又は所在地が第三国にある者のうち、その AI システムによって生成された出力が欧州連合内で利用される場合。

（以下省略）

第 2 節　中国による規範輸出

中国による規範輸出の特徴は、「サイバー主権」の理念を掲げつつ、ICT インフラや技術基盤の国家主導型供与を通じて間接的かつ構造的に影響力を行使する点にある。すなわち、中国は自国の法制度を国際的標準として直接提示するのではなく、経済支援や技術協力を媒介とし、受入国のデジタル統治基盤そのものを自国モデルに近づける戦略を採用している。このアプローチは、自国の統治モデルを国際的に正当化し、国際デジタル秩序の形成において主導的地位を確立しようとする動きとして位置づけられ、「北京効果（Beijing Effect）」とも称されている[30]。

第 1 項　中国による規範輸出の構造と特徴

制度形成の手法において、中国は多国間ルール形成を経るよりも、二国間の経済協力や技術供与を重視している[31]。代表的な例が、「デジタル・シルクロード（Digital Silk Road）」構想である。これは一帯一路（Belt and Road Initiative）の中核的要素とされ、アフリカ、中東、東南アジアなどの途上国に対し、通信ネットワーク、監視機器、クラウドサービスなどの ICT インフラを包括的に提供するものである[32]。このような枠組みを通じて、中国は受入国におけるデータ管理の仕組みや監視体制の設計に影響を及ぼし、事実上、自国型のデジタルガバナンスの制度的土台を浸透させている。これは、国家主導で経済支援と規範輸出を一体化させ、自国のデジタル統治モデルを間接的に国際展開する試みと位置づけられる[33]。

理念的側面において、中国の規範輸出モデルは、EU のモデルとは根本的に異なる。EU のアプローチが人格権や情報自己決定権といった個人の権利保護を中心に据えるのに対し、中国のモデルは、国家の安全および主権的管理を制度設計の中心に置いている。たとえば、中国の個人情報保護法（PIPL）[34]においても、個人の権利保障は社会的秩序の維持や国家の安全確保といった公共目的に従属する位置づけにある[35]。この価値観の相違は、国際的データガバナンスにおける規範的対立を深刻化させる要因となっている。

さらに、中国の規範輸出の対象は個人データに限定されない。むしろ中心的関心は、経済活動、通信、物流、エネルギーなどの分野における非個人データにある。中国はこれらのデータを国家安全保障および社会統制の観点から重視し、制度的に一体化して管理している。実際、「中国データ三法」は越境的データ移転に対して厳格な制限を課しており、国家安全審査や事前許可を義務づける制度設計を採用している。たとえば、中国国内で収集されたデータの国外提供については、データセキュリティ法（DSL）第 31 条[36]およびデータ越境安全評価弁法第 4 条[37]に基づき、国家安全審査の実施が義務づけられており、企業活動に対しても国家主導の監督権限を及ぼしている。この枠組みの下では、非個人データを含む広範な情報資源全体が「国家安

[30] Erie and Streinz (2021), pp. 14–24, 35–47; 周（2021）71–82 頁; 五十嵐（2024）151–171 頁.
[31] Cheney (2021), pp. 88–99.
[32] Dekker et al. (2020), pp. 3–9.
[33] Cheney (2021), pp. 88–99; Baark (2024), pp. 27–36.
[34] 中華人民共和国個人情報保護法（2021 年 8 月 20 日採択、2021 年 11 月 1 日施行）.
[35] Li and Chen (2024), pp. 6–10.
[36] 中華人民共和国データセキュリティ法（2021 年 6 月 10 日採択、2021 年 9 月 1 日施行）第 31 条.
[37] データ越境安全評価弁法（2022 年 7 月 7 日公布、2022 年 9 月 1 日施行）第 4 条.

全」の名の下に統制されており、経済的・社会的活動のあらゆる局面が安全保障政策の延長線上で管理される体制が形成されつつある[38]。

以上のように、中国の規範輸出は、法制度の模倣や理念の拡散にとどまらず、経済協力・技術供与・制度運用を一体化した国家主導の包括的戦略として展開されている。その目的は、「サイバー主権」の理念を国際的に定着させ、自国の統治モデルを正統化することであり、この戦略的構造が「北京効果」の核心をなしている。結果として、中国は法的規範よりも先に制度的慣行と技術インフラを通じて国際秩序に影響を及ぼす新しい形の構造的な規範輸出を実現している。

【参照条文】

データセキュリティ法（DSL）

第 2 条（適用範囲）

この法律は、中華人民共和国の領域内で行われるデータ処理活動及びその安全保護に適用される。また、中国国外で行われるデータ処理活動であっても、中国の国家安全、公共利益、公民・組織の合法的権益を損なう可能性がある場合には、この法律に基づいて法的責任を追及することができる。

第 24 条（国家安全審査）

国家は、データ安全審査制度を確立し、国家の安全に影響を及ぼし、又はその可能性があるデータ処理活動に対して国家安全審査を実施する。

第 31 条（重要データの越境移転に関する規定）

重要情報インフラ運営者が中華人民共和国国内で運営する過程で収集・生成した重要データの国外移転については、サイバーセキュリティ法の規定に従う。その他のデータ処理者が中国国内で運営する過程で収集・生成した重要データの国外移転については、国家インターネット情報部門及び関連部門が定める管理措置に従う。

データ越境安全評価弁法

第 4 条（越境移転に対する安全評価の申告要件）

データ処理者が国外にデータを提供する場合、以下のいずれかに該当するときは、所在地の省級インターネット情報部門を通じて、国家インターネット情報部門に安全評価を申告しなければならない。

1. 中華人民共和国の領域内に所在するデータ処理者が、重要データを国外に移転する場合。
2. 中華人民共和国の領域内に所在する重要情報インフラ運営者又は 100 万人以上の個人情報を取り扱うデータ処理者が、自ら取り扱う個人情報を国外に移転する場合。
3. 前年 1 月 1 日から累計で 10 万人以上の個人情報又は 1 万人以上の機微個人情報を国外に提供する場合
4. 国家インターネット情報部門が定めるその他の国外移転に該当する場合。

第 2 項　中国による規範輸出の具体例

中国による ICT インフラや技術基盤の国家主導型供与は、技術供与やインフラ整備にとどまらず、受入国の法制度やデジタル統治構造そのものに制度的影響を及ぼしている。中国政府お

[38] Su and Zhang (2025), pp. 3–10.

よび Huawei、ZTE、Alibaba Cloud などの国有・準国有企業は、アフリカ、中東、東南アジア諸国などに対して通信インフラ、監視システム、データセンター、クラウドサービス、電子政府ソリューションを包括的に提供している。これらは、受入国の制度的・技術的枠組みを中国型デジタル統治モデルへと漸次的に接近させる役割を果たしている[39]。

アフリカでは、エチオピア、ケニア、タンザニア、ナイジェリアが主要な受入国である。エチオピアでは、中国政府と Huawei の協力により国家通信網および監視システムが整備され、公共空間における映像監視が行政の一部として制度化された。タンザニアでは、2022 年の電子取引法改正により、国内で生成・取得されたデータの国外移転に政府の事前許可を義務づける制度が導入され、中国モデルの法制度的影響が明確に確認される[40]。このような制度設計は、国家安全保障を最上位の法益として位置づけ、データを統治資源とみなす中国の規範的アプローチを反映している。

中東地域においても、サウジアラビア、アラブ首長国連邦（UAE）、エジプトなどがデジタル・シルクロードの重点パートナーとして位置づけられている。特に UAE の「スマート・ドバイ」構想やサウジアラビアの「NEOM」計画では、中国企業が AI 監視・顔認識技術、ビッグデータ解析基盤を提供し、都市レベルでの統治データインフラを形成している[41]。これらの協力は、経済開発を名目としつつ、データの集中管理や監視技術の行政利用を制度的に正当化する役割を果たしており、中国の技術的・規範的影響力が制度的枠組みを通じて浸透・拡大する構造を示している。

アジア地域においても、中国はデジタル・シルクロード構想の下で、自国型デジタル統治モデルの輸出を積極的に進めている。パキスタン、ラオス、カンボジア、ミャンマーなどがその主要な受入国であり、これらの国々では、中国の技術的支援と経済協力を通じて、政府のデータ管理基盤や電子行政制度の整備が進められている。特にパキスタンでは、中国・パキスタン経済回廊（China-Pakistan Economic Corridor: CPEC）の一環として「安全都市（Safe City）」プロジェクトが展開され、Huawei などの中国企業によって監視カメラ網、交通監視システム、顔認識 AI を備えた都市監視インフラが構築された。このプロジェクトは、治安維持を名目に行政監視体制を技術的に強化するものであり、中国の安全保障優先型のサイバー主権モデル（Cyber sovereignty model）の制度的影響を直接的に示す事例と評価されている[42]。さらに、ラオスやカンボジアにおいても、中国のクラウド基盤およびデータセンター整備支援が進められ、政府のデータ管理や電子行政の運用が中国的な集中型データ統治構造に接近しつつあると指摘されている。これらの国々では、経済発展や行政効率化を掲げた技術支援を通じて、結果的に国家によるデータ集中管理を正当化する制度的枠組みが浸透しており、中国の規範輸出が技術供与と制度運用の双方を媒介に展開されていることが明らかである[43]。これらの事例はいずれも、中国が多国間

[39] Dekker et al. (2020), pp. 5–13; Erie and Streinz (2021), pp. 14–24, 42–65.
[40] Dekker et al. (2020), pp. 5–13; Cheney (2021), pp. 88–99; Erie and Streinz (2021), pp. 42–65; Dike and Owusu (2024), pp. 488–493.
[41] ITP Staff (2016) (reporting that Dubai's Roads and Transport Authority (RTA) and Huawei signed a Memorandum of Understanding at GITEX Technology Week to cooperate on the development of smart road and transport infrastructure); Dekker et al. (2020), pp. 14–17.
[42] Erie and Streinz (2021), pp. 42–47, 50–89.
[43] Erie and Streinz (2021), pp. 42–47, 48–65, 83–92.

ルール形成ではなく、二国間の技術協力や融資、契約ベースの政策連携を通じて、制度的影響力を拡大する国家戦略を体系的に推進していることを示している。

中国モデルの規範輸出は、インフラ提供にとどまらず、受入国側の法制度やデジタル統治アーキテクチャに対して、制度的・理念的双方の側面から波及的影響を及ぼしている。監視・認証技術の導入とそれに伴う制度整備が相互に作用することで、中国モデルの制度的波及が加速し、越境的データガバナンスにおける民主的基盤の脆弱化が懸念される。こうした体制は、国家がテクノロジーを用いて個人の行動を監視・制限し、政治的統制を強化する特徴を有する権威主義体制（authoritarian regimes）として位置づけられる[44]。このように、中国の規範輸出は、国家主導・技術媒介型の規範輸出モデルとして、法的拘束よりも制度的・構造的影響を通じて他国のデジタル統治体制を再編するものであり、EU や米国のモデルとは対照的な構造を形成し国際的データガバナンスの分極化を構造的に一層深化させる要因となっている。

[44] Gunitsky (2015), pp. 42–49.

第 3 節　米国による規範輸出

米国による規範輸出は、EU や中国とは異なる独自の特徴を有し、市場支配力を基盤とする間接的影響力によって、越境的データガバナンスにおける事実上の国際標準形成を推進するものである。すなわち、EU が GDPR を中心とする法的手法を用いて域外適用を制度的に強制し、中国が国家安全保障を最優先とする統制モデルを輸出しているのに対し、米国は主としてグローバル企業の市場支配力、貿易協定の電子商取引章、そして選択的な域外適用法を組み合わせることによって、事実上の国際標準を形成している。

第 1 項　米国の市場支配モデル

米国は市場支配モデル（Market dominant model）に基づき、グローバル IT 企業の市場影響力と貿易協定の電子商取引章を通じて、国際的な規範形成に実質的な影響を及ぼしている。米国の主要プラットフォーマーは、世界的な市場支配力を背景に、利用規約、プライバシーポリシー、データ取扱基準を一律に適用することで、各国企業や個人に対して事実上の国際的規範を設定している[45]。これらの企業は、米国法に基づくデータ開示義務を自社のサービス規約に組み込み、国外の顧客にも同様の条件を課しており、結果として、他国の企業であっても米国政府によるデータアクセス請求への対応を余儀なくされる状況が生じている[46]。この構造は、他国の国内法制やデータ保護規制との間で法的リスクを顕在化させる要因となっている。

また、アプリ配信市場においては、米国企業が運営する主要な配信プラットフォームが、データプライバシーやセキュリティに関する独自基準を提供条件として設定しており、開発者はこれに従わなければ市場への参入が制限される。こうしたガイドラインは、ユーザーデータの収集や広告トラッキングの方法について詳細な規定を含み、しばしば GDPR や現地法とは異なるコンプライアンス構造を持ち、各国法の要件と不整合を生じ得る[47]。こうしたグローバル・プラットフォーマーの自己規制的ルールは、各国の法制度を迂回しつつ、実務的拘束力を持つ準公共的規範として作用している。その結果、各国の開発者は現地法よりも企業内部のルールへの適合を優先せざるを得ず、米国企業の内部基準が事実上の国際標準として機能している[48]。

さらに、デジタル広告分野においても、米国発の主要広告プラットフォームが市場の大半を支配し、データ収集やターゲティング広告に関する標準仕様を事実上設定している[49]。このような

---

[45] Bloch-Wehba (2019), pp. 33–56, 66–79; Javed and Sajid (2024), pp. 17–26.

[46] Apple Inc. (2024) Transparency Report. Available at: https://www.apple.com/legal/transparency/ (accessed 22 February 2026); Google LLC (2024) Transparency Report: Government requests for user information. https://transparencyreport.google.com/government-requests (accessed 22 February 2026); Meta Platforms Inc. (2024) Transparency Center: Government requests for user data. https://transparency.fb.com/data/government-data-requests/ (accessed 22 February 2026); Microsoft (2024) Law enforcement requests report. https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (accessed 22 February 2026).

[47] Apple Inc. (2026) App Review Guidelines. Available at: https://developer.apple.com/app-store/review/guidelines/ (accessed 22 February 2026); Google LLC (2026) Provide Information for Google Play's Data safety section. Available at: https://support.google.com/googleplay/android-developer/answer/10787469 (accessed 22 February 2026); EDPB (2020d), paras. 13–15.

[48] loch-Wehba (2019), pp. 33–42, 57–63, 66–79; Javed and Sajid (2024), pp. 17–26.

[49] Bloch-Wehba (2019), pp. 33–42, 57–60; Javed and Sajid (2024), pp. 23–26; Google (2025) About personalized ads. https://support.google.com/adspolicy/answer/143465 (accessed 22 February 2026).

標準は、国際的に広く導入される一方で、各国の法制度や価値観と必ずしも整合的ではないことが指摘されてきた[50]。

総じて、米国のプラットフォーマー企業は、法的強制力を伴わないにもかかわらず、市場支配力を背景に自社の技術仕様や利用条件を各国企業に受け入れさせることで、越境的データガバナンスにおける事実上の国際標準を形成している[51]。この企業主導の規範輸出は、各国の法制度に対する間接的影響を強めると同時に、国内規制との整合性をめぐる摩擦を増大させることにより、国際的な制度的非対称性をさらに深刻化させる要因となっている[52]。

第 2 項　国内法の越境的適用による規範輸出効果

米国は国内法の限定的な越境的適用によっても、国外データに対する制度的影響力を強化してきた。代表的なものが、2018 年に制定された CLOUD 法[53]である。この法律は、米国内企業が保管するデータについて、データの物理的所在を問わず米国当局の開示請求に応じる義務を課すものである。これにより、米国企業が提供するクラウドサービスを利用する EU 企業やアジア諸国の企業も、米国法の適用下に置かれる構造が生まれた。さらに、FISA 第 702 条[54]も同様に、米国企業が収集・管理するデータへの米国当局によるアクセスを認める仕組みを持ち、国外の個人・企業に対しても事実上の影響力を及ぼしている。これらの国内法は、越境的データ移転の自由化を促進する国際協定と並行して運用され、米国型規範の制度的浸透を一層強化している。

これらの法律では、米国企業またはその支配下の事業体が管理するデータは、データの所在国にかかわらず米国法の開示義務の対象となるため、各国企業は契約設計やデータガバナンス方針を米国法制に合わせる必要が生じる。この結果、他国の制度設計や企業行動は、法的強制よりも市場アクセスの必要性によって米国型の規範に従属する傾向を強めている。

以上のように、米国の規範輸出は、直接的な法的拘束ではなく、市場支配力と企業エコシステムを媒介とする間接的制度支配を通じて進展しており、越境的データガバナンスにおける事実上の国際標準を形成している。このモデルは、形式的には各国企業の自主的適応の結果として現れるが、実質的には米国法秩序への制度的従属を生み出し、グローバルな規範的非対称性を深化させる効果を有している[55]。

---

[50] たとえば、IAB Europe が策定した「Transparency and Consent Framework（TCF）」は、Google が主導する形で広く導入されたが、2022 年にはベルギーのデータ保護当局（DPA）が GDPR との適合性をめぐって法的問題を指摘した。Belgian Data Protection Authority, Decision 01/2022 (Feb. 2, 2022), https://www.dataprotectionauthority.be/publications/decision-quant-au-fond-n-01-2022.pdf

[51] Bloch-Wehba (2019), pp. 33–42, 57–79; Javed and Sajid (2024), pp. 17–26.

[52] Aaronson and Leblond (2018), pp. 245–248, 254–261; Bradford (2020), pp. 3–9, 65–67; Cory and Dascoli (2021), pp. 6–14, 20–26.

[53] Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115–141, div. V, 132 Stat. 1214 (2018).

[54] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a (Section 702).

[55] Aaronson and Leblond (2018), pp. 245–248; Cory and Dascoli (2021), pp. 6–14.

第 3 項　貿易協定による米国型規範の拡大

米国は、貿易協定を通じて、越境的データ移転制限禁止およびデータローカライゼーション禁止の原則を国際ルールとして定着させてきた。米国は、1998 年の WTO 電子商取引作業計画[56]の採択以降、電子商取引を GATS 第1条に規定された「サービスの貿易」に位置づけ、デジタル製品およびデータの越境移転の自由化を推進してきた[57]。しかし、2000 年代初頭の WTO 交渉は、各国の意見の相違・対立によって停滞した[58]。そのため、米国は二国間および地域協定を通じた規範拡散戦略へと転換し、2012 年 3 月発効の米・韓国自由貿易協定（KORUS）[59]において、越境的データ移転制限の禁止に関する条項を導入した。

その後、2020 年 1 月発効の日米デジタル貿易協定[60]および同年 7 月発効の米国・メキシコ・カナダ協定（USMCA）[61]において、基本原則を定めた三原則条項（後記第 8 章第 1 節参照）が採用され、米国の TPP 離脱後における二国間・地域交渉の枠組みを通じて、米国の主導によるデジタル貿易自由化の国際規範形成のための中核的政策手段として機能した[62]。加えて、デジタル経済パートナーシップ協定（DEPA）[63]などの新たな地域的枠組みにおいても、同様の条項を拡散させることで、米国の市場支配モデル（Market dominant model）を国際的に定着させる動きが進められてきた。

総じて、米国は、WTO 多国間交渉の停滞を背景として、二国間・地域協定において自国市場へのアクセスを交渉上の優位として活用し、その見返りとして相手国にデータ移転自由化やデータローカライゼーション措置の禁止を受け入れさせることで、市場支配モデル（Market dominant model）を確立するに至った[64]。他方で、CLOUD 法や FISA 第 702 条に象徴される米国政府の広範なデータアクセス権限は、EU の GDPR や中国のデータ法制との制度的齟齬を顕在化させ、越境的データガバナンスの断片化を深刻化させている[65]。

---

[56] WTO (1998) Work Programme on Electronic Commerce, WT/L/274, adopted by the General Council on 25 September 1998. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/274.pdf

[57] Yakovleva (2024), pp. 154–157.

[58] Malkawi (2006), pp. 5–6.

[59] 米韓自由貿易協定（KORUS）（2007 年 6 月 30 日署名、2012 年 3 月 15 日発効）.

[60] 日米デジタル貿易協定（2019 年 10 月 7 日署名、2020 年 1 月 1 日発効）.

[61] 米国・メキシコ・カナダ協定（USMCA）（2018 年 11 月 30 日署名、2020 年 7 月 1 日発効）.

[62] Miura (2023) paras. 1–3; Dale and Aizawa (2024), pp. 2–7.

[63] デジタル経済パートナーシップ協定（Digital Economy Partnership Agreement; DEPA）（2020 年 6 月 11 日署名、2021 年 1 月 7 日発効）〔加盟国：ニュージーランド、シンガポール、チリ〕.

[64] Aaronson and Leblond (2018), pp. 245–248, 254–261; Yakovleva (2024), pp. 154–157.

[65] Aaronson and Leblond (2018), pp. 251–261; Cory and Dascoli (2021), pp. 6–14, 20–26; Zhou and Jiang (2024), pp. 214–215.

第 4 節　大国による規範輸出とデータガバナンス規範再構成の方向性

大国による規範輸出は、多くの場合、一国主義的な規範の投射であり、相互承認や対等な制度調整に基づく国際的統一規範の策定とは本質的に異なる。各大国が独自の規範体系を周辺国へと波及させるほど、複数の制度的ブロックが併存する構造が固定化され、非大国は相互に矛盾する規律の板挟みとなり、制度的自律性や選択の余地を失うことになる。このような状況は、国際的な共通基盤の形成を阻み、制度的非対称性を深めるのみならず、サイバー空間全体を複数の排他的ブロックへと分割する方向に作用し、サイバー空間の分裂を促す構造的要因として機能する。このような国際的データガバナンスの分断を回避するためには、各国の主権的統制を尊重しつつ国際的相互運用性を確保し得る越境的データガバナンス規範の再構成が不可欠となる。それは、大国の一国主義的な規範輸出で達成し得るものではなく、非大国を含む多様な制度間の相互理解と信頼に基づく協調的枠組みによってのみ実現できる。

第 1 項　大国による規範輸出の弊害

大国による規範輸出は、越境的データガバナンスに深刻な非対称性をもたらす構造的要因として機能している。このプロセスは、形式上は国際協調を通じたルール形成として現れるが、実質的には規範形成権の偏在と制度的従属関係の生成を伴うものである。現在の国際環境においては、EU の GDPR に代表される規範統制モデル（Normative control model）、中国の国家安全法およびいわゆる「データ三法」に基づくサイバー主権モデル（Cyber sovereignty model）、さらに米国のグローバル企業による市場支配力や貿易協定を通じた制度拡張に依拠する市場支配モデル（Market dominant model）が並存している。これら三つのモデルは制度的根拠や政策理念を異にしつつも、域外的影響力の拡張を通じて規範形成権の集中をもたらす点で共通している。そして各国企業および行政当局に対し多重的な適合義務を課すことで、制度的複雑性と経済的負担を同時に増幅させている。

このような規範輸出は、少なくとも三つの深刻な帰結をもたらす。

第一に、受入国の制度的自律性を著しく制約する。域外適用を伴う規制は、国内法体系と整合しない義務を第三国に課す場合が多く、各国は自国の憲法秩序や政策優先順位の再調整を余儀なくされる。たとえば GDPR は、域外事業者にも高水準のデータ保護義務を課すことにより、事実上、第三国の立法過程や規制設計に影響を及ぼしている[66]。また米国の CLOUD 法や FISA 第 702 条は、米国企業のサービスを利用する国外主体に対して米国法上の開示義務を間接的に及ぼし得るため、他国の主権的統制権限との制度的緊張を生み出している[67]。このように規範輸出は、受入国の制度的自律性を外部から制約する作用を持つ。

第二に、発展途上国および中小企業に過大なコンプライアンス・コストを課す。複数の異なる法体系への同時適合が求められる場合、制度適応能力や資源に制約のある主体ほど不利な影響を受けやすい。こうした負担の累積は、制度対応能力の格差を拡大させるだけでなく、政策選択の実質的自由度を縮減させる方向に働く。その結果、データガバナンスにおける格差はさ

[66] Gstrein and Zwitter (2021), pp. 7–11, 18–20.
[67] Bilgic (2018), pp. 333–344, 347–351.

らに拡大し、越境的データガバナンスにおける「タテの非対称性」が構造的に固定化される。また、発展途上国の政策形成能力は外部規範への適応に優先的に動員されることとなり、国内産業政策やデジタル主権確保の余地が縮減する可能性が高まる[68]。

第三に、国際的相互運用性が損なわれ、制度的断片化が加速する。各大国が異なる制度モデルを域外に投射することにより、相互に整合しない複数の規範体系が重層的に併存する状況が形成される。この結果、国家間におけるデータ移転の摩擦が増大し、相互接続性を欠く規範ブロックが並立する「ヨコの非対称性」が生じ、国際的なデジタル協力の制度的基盤が分断される危険が高まる[69]。

以上のとおり、大国による規範輸出は、主権的自律性の制約、制度的非対称性の固定化、国際的相互運用性の阻害など、越境的データガバナンスに深刻な歪みをもたらしている。これらの弊害は、一部大国による一方的な規範投射を前提とする現行の規範形成構造そのものに起因するものであり、大国による規範の延長線上での調整によって解消することは困難である。したがって、越境的データガバナンスの安定的構築のためには、大国主導型モデルに代わる、新たな評価原理と協調枠組みの構想が不可欠となる。

第 2 項　越境的データガバナンス規範再構成の方向性

大国による規範輸出がもたらした制度的非対称性を克服するためには、特定の国家モデルに依拠しない中立的かつ包摂的な越境的データガバナンス規範の確立が求められる。越境的データガバナンスにおける根本的課題は、主権・市場・人権といった相互に競合する価値の調整にあり、そのいずれかに偏した制度設計は、必然的に他の価値を侵害し、国際的信頼の基盤を損なう危険を伴う。したがって、規範再構成にあたっては、価値間の均衡と制度間の相互運用性を両立させることを中心課題として位置づける必要がある[70]。

このような規範再構成にあたっては、次のような方向性が重要となる。

第一に、柔軟かつ公平なガバナンス枠組みの構築である。従来の大国主導型交渉は、特定の法制度や経済圏の論理を他国に投射する構造を内包しており、結果として一方的な規範移転を正当化してきた。これに代えて、各国が自国の法文化や制度的成熟度に応じて段階的に参画し得る柔軟で公平な枠組みを構築することが不可欠である。このような枠組みは、各国の制度的多様性を尊重しつつ、共通の原理に基づく協調的ルール形成を可能にするものであり、越境的データガバナンスの公正性と実効性を担保する基盤となる[71]。

第二に、規範再構成においては、データの性質・利用目的によるリスクの程度に応じて、保護や管理の水準を段階的に設計することが重要である。すべてのデータ移転に対して同一の法的・技術的要件を適用する一律的なモデルは、過剰な規制を生み出す一方で、実効的な保護を損なうリスクを伴う。これに対し、第Ⅲ部で検討するリスクベースアプローチに基づく運用規範の再構成は、各状況の文脈的特性を踏まえ、リスクに比例した柔軟かつ適合的な制度設計を可能

[68] Cory and Dascoli (2021), pp. 6–10, 12–14; UNCTAD (2022), pp. 39–45, 60–67.
[69] Aaronson and Leblond (2018), pp. 245–248, 257–261.
[70] Aaronson and Leblond (2018), pp. 245–248, 257–261; UNCTAD (2022), pp. 39–45, 60–67, 71–74, 94–95.
[71] Aaronson and Leblond (2018), pp. 245–248, 257–261; Aaronson (2018), pp. 4–16.

にする視座を提供するものである。この方向性は、国家間の多様性を前提としつつ、共通の原理に基づく国際的整合性を確保するための理論的基盤となり得る[72]。

第三に、規範再構成は、ルールの調和化にとどまらず、制度的相互依存の再構築を通じて、信頼を媒介とする相互主義的枠組みを確立することが重要である。すなわち、各国が相互に他国の制度を尊重しつつ、リスク評価や監督体制に関するデータ共有・相互承認を制度的に担保することが求められる。こうした信頼に基づく相互主義的枠組みの形成が、断片化した現行秩序を再接続し、持続可能な国際的データ流通の枠組みを整備する鍵となる[73]。

以上のように、越境的データガバナンス規範再構成は、大国主導の一方的な規範投射を超えて、透明性・柔軟性・比例性・信頼性を基軸とする新たな多国間協調の枠組みを志向するものである[74]。その観点から、第Ⅲ部で検討するリスクベースアプローチは、今後の制度的均衡を導く中核的設計原理となる。今後の越境的データガバナンスにおいては、深刻な規範的対立が続く大国の影響を可能な限り回避し、中堅国や新興国が構築した有志国連携の主導により、各国の主権的統制を尊重しつつ国際的な相互運用性を確保し得る規範を再構成することが求められる[75]。

[72] Cory and Dascoli (2021), pp. 6–10, 12–14; Moerel (2022) Introduction and section 3 (Summary Conclusions); Christakis (2024a), pp. 15–27, 57–62, 68–85.
[73] Aaronson (2018), pp. 7–16; Dale and Aizawa (2024), pp. 2–7.
[74] Centre for International Trade and Policy (CITP) (2024), pp. 1–10.
[75] Aaronson and Leblond (2018), pp. 267–272; UNCTAD (2021), pp. 97–116; 141–167; 169–177; OECD (2023a), pp. 19–28; Christakis (2024b), pp. 101–113; Dimitropoulos et al. (2025), pp. 7–19.

第 4 章

データローカライゼーション

第 4 章　データローカライゼーション

近年、各国は国内データの保護を目的として、データの収集・処理・移転に関する規制を強化する動きを加速させており、その代表的な政策手段がデータローカライゼーション措置である。データローカライゼーションとは、ある国の領域内で生成されたデータについて、その保存、処理または管理を当該国の領域内にとどめることを義務づける政策的枠組みであり、国家安全保障の確保、個人データ保護の強化、経済的主権の維持などを根拠として導入が進められている。データローカライゼーション措置は、一部の国において過度な規制を伴うデータ保護主義へと転化しつつあることが国際的にも問題視されている[76]。

過去約 10 年間において、データローカライゼーション措置を導入した国・地域の数は急速に増加している。2023 年の OECD 報告書（以下「OECD 報告書（2023）」という。）によれば、「明示的な（explicit）」データローカライゼーション措置[77]は 2023 年初頭までに 40 か国で 96 件確認され、そのうち約半数は 2015 年以降に新たに導入されたものである[78]。また、2021 年の ITIF 報告書（以下「ITIF 報告書（2021）」という。）によると、「明示的な」措置に加え「事実上の（de facto）」データローカライゼーション措置も含めた場合、これらの措置を導入している国（措置数）は、2017 年の 35 か国（67 件）から 2021 年初頭には 62 か国（144 件）へと拡大しており、特に中国（29 件）、インド（12 件）、ロシア（9 件）、トルコ（7 件）が多いとされている[79]。

各国がデータローカライゼーション措置を導入する主たる目的について、OECD 報告書（2023）は、①個人データの保護、②法執行の実効性の確保、③国家安全保障の維持、④データの安全性向上、⑤国内産業政策の推進の五つを主要目的として挙げている[80]。データローカライゼーション措置の内容や規制の強度は、その目的や対象分野によって異なり得るが、データの国内保存義務に加えて越境移転の原則禁止を定め、個別の許可によってのみ越境移転を認める類型が最も規制の強いものとされている。最近では、「明示的な」措置の 3 分の 2 以上がこの類型に該当すると報告されている[81]。以上のように、近年のデータローカライゼーション措置は、自国データの国内保存義務と越境移転制限を組み合わせる形が主流となっている。

データローカライゼーションをめぐっては、全面的に否定されるべき措置か、それとも一定の範囲で正当性を有し得る措置として理解すべきかが重要な論点となる。本稿では国際的なデータガバナンスの現状を踏まえて、後者の視点に立ち、リスクベースアプローチの導入によってデータローカライゼーションを限定的に許容しながら実効的に統制するための越境的データガバナンス規範再構成の在り方を検討する。

この方針に沿って、本章では、第 1 節で中国におけるデータローカライゼーション、第 2 節で GDPR による事実上のデータローカライゼーション、第 3 節でその他の国におけるデータローカライゼーション措置を取り上げ、その実情と法制上の特徴を整理する。それらを踏まえ、第 4 節

---

[76] Ferracane (2021), pp. 63–65, 69–78.
[77] Del Giovane et al. (2023), pp.5–13（「明示的な（explicit）」データローカライゼーション措置とは、法律または規則によりデータの国内保存または処理を義務づけることを意味する）.
[78] Del Giovane et al. (2023), pp. 12–13.
[79] Cory and Dascoli (2021), p. 3.
[80] Del Giovane et al. (2023), pp. 6–7.
[81] Del Giovane et al. (2023), p. 12.

では、データローカライゼーションの正当性と弊害を分析したうえで、越境的データガバナンス規範再構成の方向性を提示する。

第 1 節　中国におけるデータローカライゼーション

中国のデータローカライゼーションの特徴は、法令や規則において規定された「明示的な」措置を中心とする点にある。1989 年施行の国家秘密法[82]における国家機密データの国外移転禁止を始め、国家機密・地理情報、電気通信、銀行・金融、信用調査、保健・生命情報、オンライン経済・消費者関連、証券など幅広い分野において、法令や規則に基づく措置が段階的に拡大してきた。また、近年では「中国データ三法」と称される包括的データガバナンス関連法令が制度の基盤を形成し、その下位規範の整備も進められている（表 1 参照）。

【表 1：中国における主なデータローカライゼーション措置】

中国における主なデータローカライゼーション措置（「明示的な」法令に限定[83]）

国家機密・地理情報関連

（1989 年）国家秘密法（国家機密の国外移転禁止・国家安全保障）

（2016 年）地図管理条例（地理情報の国家主権保護）

（2016 年）測絵地理情報局による自動車運転支援地図（高精度地図）管理に関する通知（高精度地図データの越境移転制限）

電気通信関連

（2000 年）電気通信条例（通信インフラ及びデータ保護）

銀行・金融関連

（2006 年）電子銀行業務管理弁法（金融データの国内保存要求）

（2011 年）商業銀行における個人金融情報保護通知（個人金融情報の国内管理指針）

（2019 年）金融消費者権益保護実施弁法（第 34 条）（金融消費者のデータ保護義務化）

（2019 年）銀行カード決済機関管理弁法（第 3・20 条）（決済データの国内処理要求）

（2019 年）AML/CTF 管理弁法（不正送金対策とデータ保存義務）

（2020 年）個人金融情報保護技術仕様（情報管理に関する技術的要件）

（2020 年）個人金融情報分類管理技術仕様（データ分類に基づく制御基準）

信用調査関連

（2013 年）信用調査業管理条例（第 24 条）（調査データの越境移転制限）

（2019 年）信用格付業管理暫定弁法（格付情報の規制と保存義務）

（2021 年）信用調査機関管理規則（データ越境の事前審査強化）

保健・生命情報関連

（2014 年）人口健康情報管理弁法（健康情報の国内管理）

（2018 年）科学データ管理弁法（政府資金研究成果の保護）

（2019 年）ヒト遺伝資源管理条例（生命情報の国家的統制強化）

オンライン経済・消費者関連

（2016 年）非銀行系決済業務管理弁法（オンライン決済のデータ規制）

---

[82] 中華人民共和国国家秘密法（1988 年 9 月 5 日制定、1989 年 5 月 1 日施行、2010 年 4 月 29 日改正）.

[83] 各法令の制定文および国家互聯網信息弁公室（CAC）による関連通達・部門規範文書; Cory and Dascoli (2021), pp. 49–54; Dai (2022), pp. 13–15, 91–97; Zhou and Jiang (2024), pp. 213–215.

（2016 年）オンライン出版サービス管理規程（メディア関連データの国内制御）
（2016 年）ネット配車サービス運営暫定規程（利用者情報の国内保存要求）
証券関連
（2019 年）中華人民共和国証券法（第 117 条）（証券データの越境移転制限）
包括的データガバナンス関連（「中国データ三法」及び関連規則）
（2017 年）サイバーセキュリティ法（CSL）（インフラ防護及びデータ国内保存の原則化）
（2021 年）データセキュリティ法（DSL）（国家データの分類・分級及び越境移転制限）
（2021 年）個人情報保護法（PIPL）（個人データの越境移転制限）
（2021 年）重要情報インフラ安全保護条例（CII オペレータの国内保存義務化）
（2022 年）越境データ移転安全評価弁法（審査・承認制度の実施細則）
（2023 年）データ越境提供標準契約弁法（標準契約方式による越境移転管理）
（2026 年）個人情報越境移転認証弁法（個人データの越境移転のための適法化手続）

中国の法制では、多くの法律が抽象的かつ高位の規定にとどまる一方、行政規則や国家標準を通じて具体的義務が導かれ、形式上は「推奨基準」とされる規範であっても、事実上の拘束力を有することで制度全体の実効性を確保している[84]。こうした広範囲なデータローカライゼーション措置は、規制や貿易障壁のみならず、国家主権と国家安全保障を基軸とする「サイバー主権」の具現化として正当化されている。すなわち、国家安全、公共の利益、国民のプライバシー保護といった現代国家の責務を体現するとともに、国際的データガバナンス秩序における国家主導型モデルの一形態として位置づけられる[85]。

「中国データ三法」は、世界における「明示的な」データローカライゼーション措置の代表例とされている[86]。2017 年施行のサイバーセキュリティ法（CSL）[87]、2021 年施行のデータセキュリティ法（DSL）[88]、同年施行の個人情報保護法（PIPL）[89]は、それぞれ重要情報インフラ保護、データ分類管理、個人情報保護を柱とし、分野横断的な制度化を支える基盤を形成している。CSL は重要情報インフラ運営者に対し、国内保存義務と国外移転時の安全評価を課し（第 37 条）、DSL はデータの分類・分級管理を導入して国外移転のための当局審査を規定する（第 31 条）。さらに PIPL は包括的な個人情報保護制度を構築し、大量データ処理者に国内保存義務を課すとともに、国外移転について安全評価や標準契約などの要件を設けている（第 38 条～第 40 条）[90]。また、DSL 第 36 条および PIPL 第 41 条後段は、中国国内に保存されたデータの外国司法機関・法執行機関への提供を原則禁止し、主管当局の事前許可を義務づけている。この仕組みは米国ディスカバリ制度の越境的適用と実際に衝突し、米国の裁判例においても争点となっている（後記第 6 章第 3 節参照）。

[84] Dai (2022), pp. 13–15.
[85] Zhou and Jiang (2024), pp. 213–215.
[86] Cory et al. (2020), p. 19; Cory and Dascoli (2021), pp. 3–4. 49–54; Del Giovane et al. (2023), pp. 5–12.
[87] 中華人民共和国サイバーセキュリティ法（Cybersecurity Law: CSL）（2016 年 11 月 7 日制定、2017 年 6 月 1 日施行）.
[88] 中華人民共和国データセキュリティ法（Data Security Law: DSL）（2021 年 6 月 10 日制定、2021 年 9 月 1 日施行）.
[89] 中華人民共和国個人情報保護法（Personal Information Protection Law: PIPL）（2021 年 8 月 20 日制定、2021 年 11 月 1 日施行）.
[90] これに加え、PIPL 第 38 条の枠組みを具体化する下位規範として、個人情報越境移転認証弁法が制定され、2026 年 1 月に施行された。劉新宇・崔文英（2025）28–33 頁.

中国におけるデータローカライゼーションは、国家機密、金融、生命情報など多岐にわたる分野の規制を基盤としつつ、近年は「中国データ三法」を中心とする包括的な法体系へと集約されてきた。その根底にはサイバー主権を軸とする国家統制の論理が貫徹されており、形式的には安全保障やプライバシー保護を掲げながらも、実質的には越境的データ流通を国家戦略の一環として管理・統制しようとする構造が明確化している。この体系は、国際的データガバナンス秩序における国家主導型サイバー主権モデル（Cyber sovereignty model）の典型的実践として位置づけられる[91]。

【参照条文】

サイバーセキュリティ法（CSL）

第 37 条

重要情報インフラ運営者は、中華人民共和国国内で収集し又は生成した個人情報及び重要データを、国内に保存しなければならない。業務上の必要により、これらのデータを国外に提供する必要がある場合には、国家インターネット情報部門が関連部門とともに規定する安全評価を経なければならない。法律、行政法規に別段の定めがある場合は、その規定に従う。

データセキュリティ法（DSL）

第 31 条

重要情報インフラ運営者は、中国国内での業務において収集又は生成した重要データの国外への移転に関し、サイバーセキュリティ法の規定に従うものとする。その他のデータ処理者は、中国国内での業務において収集又は生成した重要データの国外への移転に関し、国家網信弁公室が国務院の関係部門と共同で制定する規則に従わなければならない。

第 36 条

中華人民共和国の組織又は個人は、主管当局の許可を得ないで、中華人民共和国国内に保存されているデータを外国の司法機関又は法執行機関に提供してはならない。

個人情報保護法（PIPL）

第 38 条

個人情報処理者が個人情報を国外に提供する場合には、以下のいずれかの条件を満たす必要がある：

1. 国家インターネット情報部門による安全評価に合格していること。
2. 国家インターネット情報部門が定めた専門機関による個人情報保護認証を受けていること。
3. 国家インターネット情報部門が公表した標準契約書に基づいて受領者と契約を締結し、その契約内容が同法に従って個人情報の保護責任を明確にしていること。
4. 法律、行政法規その他国家インターネット情報部門の規定により、国外移転が認められているその他の条件に適合していること。

また、国外提供にあたっては、個人に対して明示的に通知し、同意を得ることが必要である。

第 39 条

[91] Zhou and Jiang (2024), pp. 213–215; Hung (2025), pp. 3–7, 21–26.

個人情報を受け取る国外の組織又は個人は、本法に基づく個人情報保護基準を満たさなければならず、個人の合法的権益を確実に保護しなければならない。国家インターネット情報部門は、必要に応じて国外の受領者に対して個人情報保護状況の報告を要求することができる。

第 40 条

重要情報インフラ運営者及び法律・行政法規の定めるところにより処理する個人情報の数量が国家網信部門の定める基準を超える個人情報取扱者が、中華人民共和国国内で生成又は収集した個人情報は、原則として国内に保存しなければならない。国外に提供することが真に必要である場合には、国家網信部門が組織して行う安全評価に合格しなければならない。

第 41 条（後段）

個人情報取扱者は、主管当局の許可を得ないで、中華人民共和国国内に保存されている個人情報を他国の司法機関又は法執行機関に提供してはならない。

第 2 節　GDPR による事実上のデータローカライゼーション

各国のデータローカライゼーション措置のうち、「事実上の」措置の代表が GDPR であるとされている[92]。すなわち、GDPR は、個人データの域外移転に厳格な条件を課すことにより、事実上のローカライゼーション効果を生み出すと同時に、EU 独自の規範統制モデル（Normative control model）を国際的に投射する制度として機能している。

GDPR は、第 44 条において、欧州経済領域（EEA）の域内で取得した個人データを第三国に移転するための一般原則を定め、第 45 条の「十分性認定（adequacy decision）」を受けていない場合には、域外への移転を原則として禁止している。さらに、第 46 条ないし第 49 条において、第三国が十分性認定を受けていない場合の個人データの域外移転について、適切な保護措置（appropriate safeguards）が講じられていることを条件に、その移転を認めている。具体的には、標準契約条項（Standard Contractual Clauses: SCCs）、拘束的企業準則（Binding Corporate Rules: BCRs）、行政機関または監督当局によって承認された契約条項等を通じて、受け手側が EU と実質的に同等のデータ保護を担保できる体制を整えている場合に限り、個人データの域外移転が可能となる。また、これらの措置が存在しない場合であっても、特定の例外的状況（本人の明示的同意、契約履行のための必要性、重大な公共の利益など）に該当する場合には、個人データの移転が例外的に認められることがある（第 49 条）。

そして、第 83 条第 5 項では、これらの規定に違反して域外に個人データを移転した場合には、重い制裁金（最大 2 千万ユーロ又は全世界年間売上高の 4%までのいずれか高い方）を科すものと規定している。この制裁規定は、域外移転のリスクを重く評価し、その発生自体を抑制するための実効的な制裁手段として設計されている点に特徴がある。実際に、GDPR に基づく制裁実務においては、域外移転を含む違反行為に対し、極めて高額な制裁金が科されている。たとえば、ルクセンブルク当局は 2021 年、ターゲティング広告に関する個人データ処理の違法性を理由として、Amazon Europe Core に対し 7 億 4,600 万ユーロの制裁金を課した[93]。また、アイルランドデータ保護委員会は 2023 年、EU 域内から米国への個人データ移転について、Schrems II 判決後も十分な保護措置が確保されていなかったとして、Meta Platforms Ireland に対し 12 億ユーロの制裁金を科した[94]。これらはいずれも、GDPR 第 83 条第 5 項に基づく上限規模に近い制裁であり、GDPR の制裁規定が理論上の威嚇にとどまらず、実務上も現実に機能していることを示す例である。

ITIF 報告書（2021）は、個人データの域外移転手続の厳格さや罰則の重さを踏まえ、GDPR について、「世界で最も重要な事実上のデータローカライゼーションの枠組みになりつつある」と指

---

[92] Cory and Dascoli (2021), p. 7.

[93] Commission nationale pour la protection des données (CNPD, Luxembourg), Decision regarding Amazon Europe Core S.à r.l., 15 July 2021; https://cnpd.public.lu/en/actualites/national/2025/03/amazon-decision.html; CNPD press confirmation of 2021 fine, https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html

[94] Data Protection Commission (Ireland), Data Protection Commission announces conclusion of inquiry into Meta Ireland, 22 May 2023 (final decision adopted 12 May 2023; administrative fine €1.2 billion; transfers from EU/EEA to the US found to infringe Article 46(1) GDPR), https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland; European Data Protection Board, Decision (final decision on transfers, 12 May 2023, PDF), https://www.edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf

摘している[95]。このように、EU が域内法として制定した厳格な規制が、国際企業による自発的な準拠やグローバルな事業設計の見直しを通じて、域外にも事実上の規制影響力を及ぼす現象は、「ブリュッセル効果（Brussels Effect）」と称されている[96]。なお、日本も個人情報保護法により第三国への個人データ提供に一定の制約を課しているものの、その制度設計は本人同意を中心とする柔軟な許容構造を採用しており、域外移転それ自体を原則禁止としたうえで高度な制度的説明責任や継続的評価義務を課す GDPR とは規範の重心を異にするため、国際企業の事業構造を広範に再編させるほどの抑止効果や域外への規範的影響力を有しているとは評価し難く、日本の個人情報保護法をもって、日本を EU と同列に「事実上のデータローカライゼーション実施国」と位置づけることはできない[97]。

GDPR による個人データの域外移転規制についても、米国ディスカバリ制度の越境的適用との間で実際に「衝突」が生じており、この点が争点となった米国の裁判例も存在する（後記第 6 章第 3 節参照）。

このように EU は、GDPR により域外移転に厳格な条件を課すことで域外に自らの規範を投射し、基本権保障を基盤とする規範統制モデル（Normative control model）を国際的に具現化している。その結果、「ブリュッセル効果」を通じて他国のデータ保護政策にも波及し、越境的な個人データおよびプライバシー保護の制度的基盤を形成することで、EU はグローバルなデータガバナンスにおいて権利保護を中心とする独自の方向性を示している。もっとも、そのような制度設計が国際経済秩序や技術協力に与える影響は決して小さくなく、GDPR のもたらす規範的意義とともに、その正当性や潜在的弊害について検討することが不可欠である。

【参照条文】

GDPR（EU 一般データ保護規則）

第 44 条（データ移転の一般原則）

個人データの第三国又は国際機関への移転は、本規則においてその他の規定がある場合を除き、本規則の他の条項の遵守が確保され、当該第三国、地域又は国際機関が第 45 条に基づき十分なレベルの保護を提供していると認められる場合にのみ行うことができる。すべての個人データの移転は、データ主体の権利と自由を引き続き保護することを確保しなければならない。

第 45 条（十分性認定に基づくデータ移転）

1. 欧州委員会は、特定の第三国、地域若しくは一つ以上の指定部門又は国際機関が十分なレベルの個人データ保護を提供していると判断した場合、当該第三国等への個人データの移転は、追加の認可なく許可される。
2. 欧州委員会は、以下の要素を考慮して十分性の判断を行う:
   - 法の支配、基本的人権の尊重、効果的なデータ保護法の存在（データ主体の権利、監督機関の独立性、救済措置等）
   - 第三国又は国際機関が締結している国際協定

[95] Cory and Dascoli (2021), p. 7.
[96] Bradford (2020), pp. 1–6.
[97] Bradford (2020), pp. 25–32; Cory and Dascoli (2021), pp. 6–8; Igaya and Sudoh (2025), pp. 173–178; 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（令和7年 12 月一部改正）. https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore

・ データ保護機関の活動及び執行能力

3. 十分性認定が行われた場合、欧州委員会はそれを EU 官報で公示し、定期的に再評価する。

第 46 条（適切な保護措置に従った移転）

1. 第 45 条第 3 項による決定がない場合は、管理者又は取扱者が適切な保護措置を提供し、執行力あるデータ主体の権利及びデータ主体に関する効果的な法的救済が利用可能な状態である場合に限り、管理者又は取扱者は第三国又は国際機関に個人データを移転することができる。
2. 第 1 項で定める適切な保護措置は、監督機関からの特定の認可を必要とせず、次に掲げるものによって講じられてもよい。

(a) 公的機関又は団体間の法的拘束力又は執行力のある法律文書。

(b) 第 47 条に従った拘束的企業準則。

(c) 第 93 条第 2 項で定める審査手続に従って欧州委員会によって採択された標準データ保護条項。

（以下略）

第 49 条（特定の状況における例外）

1. 第 45 条第 3 項に準拠した十分性の決定がない場合、又は第 46 条による適切な安全対策（拘束的企業準則を含む。）がない場合、第三国又は国際機関への個人データの移転又は個人データ移転の集合は、次に掲げるいずれかを満たしている場合においてのみ、行われるものとする。

(a) 十分性の決定及び適切な安全対策がないことによってデータ主体に関する当該移転から生じ得るリスクについての情報が提供された後、データ主体がその提案された移転に明示的に同意した場合。

(b) データ主体と管理者との間における契約の履行のため、又はデータ主体の要求により取られる契約前措置の実施のため、移転が必要な場合。

(c) 管理者及びその他自然人又は法人との間におけるデータ主体の利益に帰する契約の締結又は履行のために移転が必要な場合。

(d) 公共の利益の重大な事由のために移転が必要な場合。

(e) 法的主張時の立証、行使又は抗弁に移転が必要な場合。

（以下略）

第 83 条（制裁金の一般条件）

（1～4 略）

5. 次に掲げる規定の違反は、第 2 項に従って、最大 2 千万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 4%までの、どちらか高い方を制裁として科されるものとする。

((a)･(b)省略)

(c) 第 44 条から第 49 条による第三国又は国際機関の取得者への個人データ移転。

（以下略）

第 3 節　その他の国におけるデータローカライゼーション

近年では、その他の国においてもデータローカライゼーション措置や越境的データ移転制限措置が拡大しつつある。以下では、データローカライゼーション措置を講じている主要国の現状を概観する。これらの国における制度の中には、表向きはデータ主権やプライバシー保護の強化を掲げつつも、実態としては国家による情報統制や戦略的資産管理の手段として機能している場合も見られる。そのような場合には、国際的な相互運用性や信頼に基づく越境的データガバナンスへの障壁となり得る。

第 1 項　米国

米国にはデータローカライゼーションの実施を義務づける一般的な法律は存在しないとされてきたが、2011 年以降、特定の連邦政府機関（主に国防・情報分野）は、米国内で運用され、アクセス主体を原則として米国市民に限定したクラウドサービスの利用を、調達契約上の要件として義務づけており、関連データを米国内に保存することが求められている。これは法令による直接的な義務ではなく、契約上の要件として実施されており、国際武器取引規則（ITAR）[98]、連邦リスク管理プログラム（FedRAMP High）[99]、国防総省のクラウド・セキュリティ要件（DoD SRG Level 4/5）[100]、刑事司法情報サービス（CJIS）[101]などの規制遵守に基づく制度的要請として運用されている。これらの基準においては、機密性の高い業務に対応するクラウド環境が、論理的に、また必要に応じて物理的にも米国外の環境と隔離され、運用・管理に関与する者が米国市民に限定されることが明示されている。

さらに、2024 年には PADFA（Protecting Americans' Data from Foreign Adversaries Act of 2024）が制定され[102]、米国市民のセンシティブな個人データが中国等の「敵対的外国勢力（foreign adversaries）」に取得されることを防止するための包括的制度が導入された。PADFA は、データの国外移転に対する事前審査権限や、外国所有のデジタルプラットフォームに対する強制的売却命令（divestment）措置を可能にするなど、対外的なデジタル主権の行使を制度的に支えるものとなっている。いわゆる「敵対的外国勢力」と認定された国家又はその支配下にある法人に対し、米国市民の個人識別可能なセンシティブ情報の譲渡、販売、提供を全面的に禁止することをその中核としている。従来は自由貿易の一部とみなされてきた越境的データ移転を、国家的脅威の観点から制限対象とし得ることを明確化したもので、「中国データ三法」と同様に安全保障を基軸とする規制強化の潮流に属する。

---

[98] United States (2026) International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120–130. https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M (accessed 22 February 2026).

[99] U.S. General Services Administration. Federal Risk and Authorization Management Program (FedRAMP) High Baseline. https://www.fedramp.gov/understanding-baselines-and-impact-levels/ (accessed 22 February 2026).

[100] U.S. Department of Defense / Defense Information Systems Agency, Cloud Computing Security Requirements Guide (SRG) (including Impact Levels 4/5), DoD Cyber Exchange document library. https://public.cyber.mil/dccs/dccs-documents/ (accessed 22 February 2026).

[101] U.S. Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Security Policy (latest version; e.g., v5.9.2 June 2023), CJIS Security Policy Resource Center. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center (accessed 22 February 2026).

[102] United States (2024) Protecting Americans' Data from Foreign Adversaries Act of 2024, Public Law 118–50. https://www.congress.gov/118/plaws/publ50/PLAW-118publ50.pdf

このように、PADFA は、米国の対外的個人データ保護政策における転換点を示すものである。PADFA は、越境的データガバナンスにおける米国の戦略的対応として位置づけられ、国家安全保障とプライバシー保護の交錯する領域において、新たな制度的枠組みを形成した立法である。このような立法措置の背景には、近年中国等の国家が関与する越境的なデータ取得行為に対する米国内の懸念が強く影響しており、特に第三者を介して流通する商業データが国家安全保障に与える潜在的リスクが問題視されてきた。PADFA は、従来の国家情報法（FISA）や外国投資リスク審査委員会（CFIUS）の手法とは異なり、民間部門における自発的な情報取引そのものを制度的に制限することを通じて、「デジタル主権」の概念を再定義する試みであるといえる[103]。

PADFA の制定は国際的議論を呼び起こし、特に GDPR に基づく十分性認定や越境移転規制との整合性が問題視されている[104]。PADFA によるデータ遮断や強制的売却命令は契約的・制度的安定性を損なうおそれが指摘され、国家安全保障を名目とする過剰規制がデータ保護主義へと転化し、自由なデータ流通を萎縮させると批判されている[105]。

以上のとおり、米国のデータローカライゼーションは、当初は特定機関の契約上の要請として実施されてきたが、PADFA の制定を契機に、国家安全保障と個人データ保護を統合する立法的枠組みへと質的に転換した。これにより米国は、対外的に「デジタル主権」の概念を再定義し、自由市場型データ政策を安全保障と接合する制度的枠組みへと転換したと評価できる。

【参照条文】

PADFA（米国人のデータを敵対的外国勢力から保護する法律）

第 2 条(a)

(a) いかなるデータブローカーも、米国に居住する個人に関する個人識別可能な機微データを、以下の者に対して販売、譲渡、提供、ライセンス、リース、配布、開示、又はその他の方法により利用可能とすることを行ってはならない。

1. 「敵対的外国勢力（foreign adversary）」に該当する国家。

2. かかる敵対的外国勢力が所有、支配、又は指揮する法人、組織、その他の団体。

（以下省略）

第 2 項　インド

インドにおけるデータローカライゼーション措置は、1993 年の公文書法（Public Records Act）に端を発し、通信、金融、保険、エネルギーなどの分野に段階的に拡張してきた。その展開は、特定分野ごとの規制導入から、包括的なデータ保護法制の確立へと移行しつつ、国家に広範な裁量権を付与する統治構造を特徴としている（表 2 参照）。

金融分野では、インド準備銀行（RBI）が 2018 年に決済データの国内保存を義務づけ、国外移転を制限する規制を導入した。この措置は、金融安定性および監督当局のアクセス確保を目

[103] Aaronson (2025), pp. 11–17.

[104] European Data Protection Board (2024), pp. 20–22（paras. 57–63）; Aaronson (2025), pp. 11–17.

[105] Swire (2024), pp. 4–6.

的とし、国外の大手決済事業者にも例外なく適用された点が国際的注目を集めた[106]。その後も証券、保険、電力などの分野において、規制当局が通達やガイドラインを通じて国内保存義務を明文化し、制度的拘束力を高めている。

さらに 2023 年に成立したデジタル個人データ保護法（DPDP 法）[107]は、分野別規制を統合し、個人データの処理に関する包括的枠組みを提供する法律である。同法は、国外移転について、中央政府が「通知により指定する国」以外への移転を禁止可能とする規定を有し（第 16 条）、事実上、いわゆる「許容国リスト方式」に基づく制限的移転モデルを採用している。これは、国外移転を原則として禁止し、例外的に許容する構造をとるものである[108]。

このようにインドの制度は、国家安全保障や監督権限の確保にとどまらず、データを国家戦略資源とみなし[109]、戦略産業の保護および国際交渉上の影響力の確保をも意図する点に特徴がある[110]。したがって、インドのアプローチは、表面的にはプライバシー保護を標榜しながらも、実質的にはデジタル主権の強化と国家統制の拡張を基盤とする「管理型モデル」の典型として評価し得る。

【表 2：インドにおける主なデータローカライゼーション措置】

インドにおける主なデータローカライゼーション措置（「明示的な」法令に限定）[111]
（1993 年）公文書法第 4 条：公的記録の国外移転を原則禁止
（2007 年）統一通信ライセンス契約：通信サービス提供者による加入者情報の国外移転の禁止
（2012 年）国家データ共有・利用政策：政府データの国内保存
（2013–2014 年）会社法に基づく会計規則：財務情報のバックアップの国内保存
（2017 年）外国直接投資（FDI）統合方針通達第 1.3(ix)項：放送分野における加入者データベースの国内保管
（2017 年）保険規制開発庁（IRDAI）指針：保険契約者の原本記録の国内保存
（2017 年）電子情報技術省（MeitY）「政府機関向けクラウド契約に関する指針」：政府関連のクラウド契約について政府データの国内サーバー保存を義務づけ

[106] Bailey and Parsheera (2018), pp. 9–13.

[107] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India), Ministry of Electronics and Information Technology (MeitY), The Digital Personal Data Protection Act, 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[108] DPDP Act 2023, Section 16: Cross-border transfer of personal data. DPDP Act 2023 – Section-wise Explanation. https://dpdpa.com/dpdpa2023/chapter-4/section16.html (accessed 22 February 2026); Securiti (2024),

[109] Vila Seoane (2021), pp. 1735–1739.

[110] Jiang (2024), pp. 732–734.

[111] 各法令の制定文および Cory and Dascoli (2021), pp. 42–45; Bailey and Parsheera (2018), pp. 9–13; Vila Seoane (2021), pp. 1735–1739; Jiang (2024), pp. 732–734; Ministry of Electronics & Information Technology (MeitY), Digital Personal Data Protection Act, 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf; Reserve Bank of India, Circular on Storage of Payment System Data, DPSS.CO.OD.No.2785/06.08.005/2017–18, 6 April 2018. https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995; Insurance Regulatory and Development Authority of India (IRDAI), Guidelines on Information and Cyber Security for Insurers, 7 April 2017. https://irdai.gov.in/document-detail?documentId=1354286; Securities and Exchange Board of India (SEBI), Cyber Security and Cyber Resilience Framework, 6 November 2020. https://www.sebi.gov.in/legal/circulars/nov-2020/outsourcing-of-activities-business-continuity-plan-and-disaster-recovery-and-cyber-security-and-cyber-resilience-framework-limited-purpose-clearing-corporation_48106.html

（2018 年）インド準備銀行（RBI）決済データ保存規則：決済データの国内保存
（2020 年）証券取引委員会（SEBI）サイバーセキュリティ通達：重要データの国内保持
（2021 年）RBI 電子 KYC 規制の改正：電子的本人確認の技術インフラの自社施設保管
（2022 年）インド電力省「サイバーセキュリティ指針」：クラウドサービスの国内サーバー使用
（2023 年）デジタル個人データ保護法（2023 年公布、段階的に施行予定）

第 3 項　ロシア

ロシアにおけるデータローカライゼーション措置は、2013 年の信用機関向け顧客データの国内保存規則に始まり、2014 年の個人データ法改正で、ロシア国民の個人データを国内に保存することが義務づけられたことを契機に本格化した。その後、決済データ、通信・インターネット事業者によるトラフィックデータ、さらには政府機関によるクラウド利用に至るまで、データの国内保存義務は領域横断的に拡張されてきた（表 3 参照）。これらの規制は、表向きには市民のプライバシー保護や国家インフラの安全確保を根拠とするが、実際には国家による情報統制と監視体制の制度化を実質的に可能にする制度基盤として機能している[112]。

監督当局である Roskomnadzor（個人データ保護監督庁）は、個人データ法に基づく違反に対し、行政罰に加えてウェブサイトやドメインの遮断措置を発動する権限を持ち、制度の執行能力を実質的に担保している[113]。さらに、ヤロヴァヤ法改正（2016 年以降）は通信事業者に広範な通信記録の国内保存義務を課し、ロシア連邦保安庁（FSB）によるアクセス権限を制度的に保障するものであった[114]。また、2019 年の公共調達制限により政府機関の外国製クラウド利用が禁止され、国家による情報インフラ統制が一層強化された[115]。こうした規制群は、国家安全保障、サイバー主権、市民権益保護といった理念によって正当化されているが、同時に国家の監視的権限を拡張する仕組みとして機能している点が重要である[116]。

このようにロシアのデータローカライゼーション制度は、形式的にはプライバシー保護を標榜しつつ、実質的には国家安全保障の名の下で情報流通を国家インフラに囲い込む仕組みを構築したものである。その結果、ロシアのモデルは安全保障的統制を中核とするサイバー主権モデル（Cyber sovereignty model）として、制度類型上、越境的データガバナンスにおける最も硬直的かつ権威主義的なアプローチの典型に位置づけられる[117]。

[112] Freedom House (2020), pp. 5–7, 10.
[113] DLA Piper (2025a), section “Enforcement.”
[114] Human Rights Watch (2016), para. beginning “The legislation requires telecommunications and Internet companies to retain copies of all contents of communications …”; Human Rights Watch (2020), paras. beginning “Forced Data Retention and the ‘Yarovaya’ Amendments,” and “The Russian government has long been criticized for excessive blocking of internet access and for using internet regulations for censorship ….”
[115] Human Rights Watch (2020), para. beginning “In May 2019, the government ordered internet service providers to store data, as prescribed by the Yarovaya amendments, using only Russia-manufactured technical means ….”
[116] Freedom House (2020), pp. 5–7, 10.
[117] Freedom House (2020), pp. 5–7, 10, 13; Human Rights Watch (2020), para. beginning “The Russian government has long been criticized for excessive blocking of internet access ….”

【表 3:ロシアにおける主なデータローカライゼーション措置】

ロシアにおける主なデータローカライゼーション措置(「明示的な」法令に限定)[118]
(2013 年)信用機関向けデータ保存規則:銀行・信用機関の全ての顧客データの国内保存
(2014 年)個人データ法改正(連邦法第 242 号):個人データの国内での収集・保存
(2014 年)国家決済システム法(連邦法第 161 号):国際ブランドの決済カードの国内での処理
(2016 年)ヤロヴァヤ法改正(第 1 次):通信・インターネット事業者はテキスト・音声・画像などすべての通信内容を最大 3 年間ロシア国内で保存する義務、及び FSB による無令状アクセスを許容
(2018 年)ヤロヴァヤ法の追加改正:通信・クラウド事業者による通信記録の 6 か月保存義務と国内保存義務、及び暗号鍵の提出義務の強化
(2019 年)公共調達制限(大統領令):政府機関による外国製クラウドサービスの利用を原則禁止し、政府機関のデータを国内インフラで保存
(2019 年)FSB 設備設置義務(FSB 命令):通信・IT 企業が情報システムに FSB 指定機器を設置し、自動的に当局がアクセス可能とする措置を義務化
(2021 年)外国 IT 企業規制法:ロシア国内ユーザーが 50 万人を超える外国企業に、①現地事務所の設置、②データの国内保存、③削除要請への対応を義務化
(2023 年)個人データ法改正:クラウド事業者・通信プラットフォーム個人データの処理においてロシア国外の関連法人との共有を制限し、明示的な同意と越境移転条件の厳格化を導入

第 4 項　トルコ

トルコにおけるデータローカライゼーション措置は、国家のデジタル主権および経済安全保障を確保することを目的として、2010 年代半ば以降に急速に制度化された。2013 年の「決済及び電子マネー法」により、インターネット決済サービスに係るデータを 10 年間国内に保存することが義務づけられたのを皮切りに[119]、2018 年には上場企業および金融機関に対し情報システムの国内保有義務が導入された[120]。さらに、2019 年の規制により公的機関による外国クラウド利用が禁止され[121]、2020 年には銀行・金融機関に対して国内インフラ保有義務が再確認されるなど[122]、分野別に制度が段階的に拡張されてきた(表 4 参照)。

2020 年のソーシャルネットワーク規制法改正は、一定規模以上のソーシャルメディア事業者に対し、国内代表者の設置、苦情処理義務、裁判所命令への対応、個人データの国内保存を

[118] 各法令の制定文および Roskomnadzor official statements (various years); Cory and Dascoli (2021), pp. 35–36; OECD (2023a), pp. 11–18.
[119] Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, Official Gazette No. 28690 (27 June 2013).
[120] Capital Markets Board (CMB), Communiqué on Management of Information Systems (No. VII–128.9), Official Gazette No. 30356 (5 January 2018).
[121] Presidential Circular No. 2019/12 on Information and Communication Security Measures, Official Gazette No. 30823 (6 July 2019).
[122] Regulation on Banks' Information Systems and Electronic Banking Services, Banking Regulation and Supervision Agency (BRSA), Official Gazette No. 31069 (15 March 2020).

含む包括的な規制を課し、国外プラットフォームに対する統制を大幅に強化した[123]。また、2016 年施行の個人データ保護法（KVKK）は、当初から越境移転について本人の明示的同意または「十分な保護水準」を有する国への移転に限定していたが[124]、2024 年に枠組みが拡充され、標準契約条項（SCCs）や監督当局による承認を含む多様な移転メカニズムが制度的に導入された[125]。さらに、同年 7 月に施行された「越境データ移転規則」によって、これらの移転に関する申請手続や保障措置の要件が具体化され[126]、形式的には移転の余地を残しつつも、実態としては広範なローカライゼーション効果をもたらす制度が整備されている。

銀行システムの国内保持義務は、銀行内部システム規則第 11 条により主要システムとバックアップを国内に設置することが義務づけられており、2022 年以降の制度強化により実効性が高まっている[127]。また、生体・遺伝情報を含む特別カテゴリーデータの処理についても、KVKK 法および関連決定により厳格な管理措置が要求されており[128]、これらの分野における越境移転については、前記の越境データ移転規則に基づく厳格な手続および安全措置が適用される。加えて、2025 年のサイバーセキュリティ法は、クラウドサービス事業者やデジタルプラットフォームに対する国家の監督・統制権限を制度的に明確化し、データ管理をめぐる国家介入の法的基盤を一層強化した[129]。

こうした一連の措置は、トルコ政府が「国家デジタル主権」や「経済独立」の理念を前面に掲げる一方で、GDPR との整合性確保に課題を残し、国際的な相互運用性との摩擦を不可避的に内包する点に特徴づけられる。実際、個人データ保護法は、越境移転を原則として本人の明示的同意または十分な保護水準を有する国への移転に限定し、標準契約条項や当局承認を必要とする制度を整備しているが、実務上は厳格な適用が多国籍企業の運用や国際データ流通に大きな制約を与えている[130] 。

【表 4:トルコにおける主なデータローカライゼーション措置】

トルコにおける主なデータローカライゼーション措置（「明示的な」法令に限定）[131]
（2013 年）決済及び電子マネー法：インターネット決済サービスのデータを国内に 10 年間保存

[123] Law No. 7253 amending the Law on the Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications, Official Gazette No. 31199 (31 July 2020); Information and Communication Technologies Authority (BTK), Procedures and Principles Regarding Social Network Providers, Official Gazette No. 31427 (2 April 2021).

[124] Law No. 6698 on the Protection of Personal Data, Official Gazette No. 29677 (7 April 2016), Art. 9.

[125] Law No. 7499 amending Law No. 6698 on the Protection of Personal Data, Official Gazette No. 32487 (12 March 2024), amending Art. 9.

[126] Regulation on the Procedures and Principles Regarding Cross-Border Personal Data Transfers, Official Gazette No. 32598 (10 July 2024), Arts. 5–12.

[127] Banking Regulation and Supervision Agency (BRSA), Regulation on Banks' Information Systems and Electronic Banking Services, Official Gazette No. 31069 (15 March 2020), art. 11.

[128] Law No. 6698 on the Protection of Personal Data, Official Gazette No. 29677 (7 April 2016), Art. 6; Turkish Personal Data Protection Authority (KVKK), Decision No. 2018/10 on Processing of Special Categories of Personal Data.

[129] Law No. 7545 on Cybersecurity, Official Gazette No. 32690 (15 July 2025).

[130] DLA Piper (2025b), sections "Transfer of personal data," and "Enforcement."

[131] 各法令の制定文および KVKK Board Decisions No. 2020/915, 2021/238, 2023/134; Cory and Dascoli (2021), pp. 37–38; OECD (2023a), pp. 11–18; DLA Piper (2025b), sections "Transfer of personal data," and "Enforcement."

(2016 年)個人データ保護法(KVKK, Law No. 6698):個人データの越境移転を、本人の明示的同意又は「十分な保護水準」を有する国への移転に限定(制定当初の基本構造)
(2018 年)資本市場委員会(CMB)情報システム管理通達:上場企業・資本市場関係機関に情報システムの国内保有・運用を義務づけ
(2019 年)大統領通達 2019/12 号(情報通信セキュリティ)第 3 条;公的機関のデータを外国クラウドに保存することを禁止し、重要情報・機微情報の国内保存を義務化
(2020 年)銀行情報システム規則(BRSA Regulation):銀行・金融機関に全情報システムの国内保有を再確認させる措置
(2020 年)インターネット出版規制法改正(SNS 規制法):月間ユーザー100 万人超の SNS 事業者に対し、①国内代表者の設置、②苦情処理義務、③裁判所の削除命令への迅速対応、④個人データの国内保存の義務づけ
(2022 年)銀行内部システム規則改正(art. 11):金融機関の全情報システムの国内保持義務
(2023 年)個人データ保護法改正ガイドライン(KVKK):生体・遺伝情報の取扱いに関する規制強化、越境的移転の同意要件と管理強化
(2024 年)越境データ移転規則(KVKK 下位規範):標準契約条項(SCCs)、監督当局承認等の移転メカニズムを制度化しつつ、詳細な申請手続・安全措置要件を設定
(2025 年)サイバーセキュリティ法(公布):クラウドサービスやプラットフォームに対する国家的制御・監督権限を法定化

第 5 項　インドネシア

インドネシアにおけるデータローカライゼーション措置は、2010 年代初頭以降、国家主権およびサイバー空間における統制確立を目的として制度化されてきた(表 5 参照)。2012 年の政府規則第 82 号は、すべての電子システム運用者に国内データセンターおよび災害復旧センターの設置を義務づける包括的規制であり、インドネシアにおけるデータローカライゼーション政策の起点となった[132]。しかし、国際的クラウド事業者や多国籍企業からの強い反発を受け、2019 年の政府規則第 71 号により改正され、民間主体については国外保存・処理を条件付きで許容する一方、政府機関に対しては依然として国内保存義務が維持された[133]。この改正は、主権的統制と国際的整合性の間で調和を図ろうとするものである。

分野別のローカライゼーション義務も継続的に強化されている。2016 年には保険業界に国内データセンター設置を義務づけ[134]、2021 年には政府機関が利用するクラウドサービスに関して可用性ゾーンの地理的分散や暗号鍵の国内保管を義務づける基準が導入された[135]。さらに

[132] Government Regulation of the Republic of Indonesia No. 82/2012 on the Implementation of Electronic Systems and Transactions, State Gazette No. 190, Oct. 15, 2012.
[133] Republic of Indonesia, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, State Gazette No. 185 of 2019; Innis and Wiyoso (2018), pp. 1–2, 4–6; Information Technology & Innovation Foundation (ITIF) (2025), p. 1.
[134] Otoritas Jasa Keuangan (OJK), Regulation No. 38/POJK.05/2016 on the Implementation of Risk Management in the Use of Information Technology by Non-Bank Financial Institutions, Official Gazette of Indonesia, 2016.
[135] Ministry of Communication and Informatics (Kominfo), Circular Letter No. 3/2021 on Governance of Cloud Computing Services for Government Agencies, Jakarta, 2021.

2022 年に制定された個人データ保護法（PDP 法）は、インドネシアにおける初の包括的データ保護法であり、越境移転について①十分な保護水準を備えた国への移転、②標準契約条項の締結、③データ主体の明示的同意という三層的要件を定めた[136]。2022 年に発出された規制が 2023 年以降に本格的に適用されることにより、金融サービス分野における準拠義務が明確化され、越境的移転規制の実効性が高められた[137]。

このようにインドネシアの制度は、国家主導の統制を維持しつつも国際的相互運用性との調和を模索する点に特徴があり、全面的ローカライゼーションから条件付き越境移転の許容へと転換した事例として位置づけられる[138]。

【表 5：インドネシアにおける主なデータローカライゼーション措置】

インドネシアにおける主なデータローカライゼーション措置（「明示的な」法令に限定）[139]
（2012 年）政府規則第 82 号（GR 82/2012）：すべての電子システム運用者に対し、国内データセンターおよび災害復旧センターの設置を義務づける包括的ローカライゼーション規制
（2016 年）金融サービス庁（OJK）規則第 69/POJK.05/2016 号：保険会社及び再保険会社に対し、国内にデータセンター及び災害復旧センターを設置する義務を課す
（2019 年）政府規則第 71 号（GR 71/2019）：GR 82/2012 を改正し、民間電子システム運用者については国外保存・処理を条件付きで許容する一方、政府機関に対しては国内保存義務を維持
（2021 年）通信・情報技術省通達第 3 号（第 3/2021 号）：中央政府機関による第三者クラウドサービスの利用に関し、①インドネシア国内の異なる場所に少なくとも 2 つの可用性ゾーンを有すること、②暗号鍵は国内で保存することなどのセキュリティ基準を提示
（2022 年）個人データ保護法（PDP Law）成立（2024 年施行）：越境的データ移転に関する包括的枠組を初めて明記し、①十分な保護水準のある国への移転、②標準契約条項の締結、③データ主体の明示的同意といった段階的要件を導入
（2023 年）OJK 規則 No. 22/2023：金融サービス事業者に対し、越境移転に際して PDP 法への準拠を義務づけ

第 6 項　小結

以上の検討から明らかなように、各国のデータローカライゼーション措置は、それぞれの歴史的背景と政策目的に応じて多様な展開を示している。米国は当初、契約ベースの制度運用に依拠していたが、PADFA の制定により安全保障を基軸とする立法的枠組みへと転換した。インドは分野別規制から包括的制度へと漸進的に移行しつつ、国家裁量を広く維持する管理型アプロ

[136] Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, State Gazette No. 165 of 2022 (enacted October 17, 2022).
[137] Otoritas Jasa Keuangan (OJK), Circular Letter No. 29/SEOJK.03/2022 on the Implementation of Risk Management in the Use of Information Technology by Commercial Banks, applied from 2023 in alignment with Law No. 27 of 2022 on Personal Data Protection.
[138] Han (2024), pp. 277–280.
[139] 各法令の制定文および Innis and Wiyoso (2018), pp. 1–2, 4–6; Cory and Dascoli (2021), pp. 45–47; OECD (2023a), pp. 11–18; Han (2024), pp. 277–280; Information Technology & Innovation Foundation (ITIF) (2025), p. 1.

ーチを採用している。ロシアは名目上プライバシー保護を掲げつつ、実質的には統制的なサイバー主権モデル（Cyber sovereignty model）を制度化しており、トルコは段階的な制度的拡張の中でデジタル主権の確立を前面化している。インドネシアは包括的義務から条件付き越境移転への修正を経て、主権と開放性の均衡を模索する調整的枠組みを採用した。これらの事例は、データローカライゼーションが個人データおよびプライバシーの保護措置としてのみ理解されるものではなく、各国のデジタル主権の行使、国家安全保障上の要請、さらには経済戦略と密接に結びついて展開されていることを示している。その中には、防衛、刑事司法、金融インフラなど、特定の高リスク分野に限定され、政策目的との対応関係が比較的明確な措置も含まれており、国家主権の行使として一定の正当性が認められる余地がある。他方で、規制の対象や範囲が過度に拡張された場合には、越境的なデータ流通や国際的な技術協力、事業活動に深刻な制約をもたらし、国際的な相互運用性や信頼の基盤を損なう危険性を内包している。

近年の各国の政策動向を踏まえると、データローカライゼーションは例外的な措置にとどまらず、今後も多くの国において、分野別又は制度的に拡大していくことが見込まれる。各国で導入が進むこれらの措置は、形式上は国内法制の選択として位置づけられているものの、その影響は国内にとどまらない。データの保存場所や移転条件が国ごとに異なる形で定められることにより、越境的なデータ流通は制度ごとに制約を受け、法制度、技術基盤、事業運営の前提が乖離しやすくなる。このような状況が進行すれば、サイバー空間は本来備えてきた相互接続性を損ない、制度的ブロック別に区切られた秩序へと変質するおそれがある。

以上を踏まえると、データローカライゼーションへの対応は、各国の国内規制の問題として個別に処理されるべきものではなく、各国に共通する越境的データガバナンスの課題として捉える必要がある。越境的データガバナンス規範の構築にあたっては、国家主権の行使として一定の正当性を有する分野別・限定的措置を包摂しつつも、比例性や必要性を欠く過度なデータローカライゼーション措置を抑制するための共通原理と評価基準を国際的に整備することが、今後の中心的課題となる。

第 4 節　データローカライゼーションとデータガバナンス規範再構成の方向性

各国におけるデータローカライゼーション措置の実情を踏まえると、一定の範囲ではその正当性を認め得る一方で、深刻な弊害が存在することが明らかとなる。越境的データガバナンス規範再構成については、こうした正当性および弊害の両面を踏まえて方向性を検討する必要がある。

第 1 項　データローカライゼーションの正当性

データローカライゼーションは、国家による公共目的の実現および国際法上の例外規定に基づく制度的措置として、一定の範囲において正当化され得る。

第一に、安全保障の観点から、データは軍事、エネルギー、インフラといった基幹領域に直結する戦略的資源である。国外移転はサイバー攻撃や諜報活動の脆弱性を高めるおそれがあるため、国家が自国領域内でデータを保管・処理させることによって統制を確保しようとする措置は、安全保障上の正当な目的に基づく政策判断として理解し得る。この場合、国際的相互運用性およびデータ流通の安定性を確保するための方策を講じつつ、目的と手段の均衡性が維持される限りにおいて、その合理性が認められる[140]。この論理は、GATT 第 21 条および GATS 第 14 条の 2 に規定される安全保障例外の趣旨と整合する。

第二に、個人データおよびプライバシー保護の観点では、データが第三国に移転される場合、当該国の法制度や執行力の差異により保護水準が変動し、データ主体が実効的な救済を得られないリスクが生じる。国家が自国法の下での監督および救済を確保するために、一定の範囲で国内処理を求めることは、制度的信頼性の維持という観点から合理性を有するものであり、国際的相互運用性および越境的データ移転の円滑化を確保するための方策を講じつつ、目的と手段の均衡性が担保される限りにおいて、その正当性を認めることができる[141]。この点は、GATT 第 20 条および GATS 第 14 条における公共政策例外の趣旨と整合する。

第三に、経済政策および産業振興の観点から、データは AI やクラウドを含むデジタル産業の基盤資源であり、その集積は研究開発能力と国際競争力の向上に資するものである。国家が一定の範囲でデータの国内管理を促進することは、産業基盤の強化や技術自立性の確保を目的とする政策的判断として理解し得るものであり、市場アクセスや国際的相互運用性の確保のための方策を講じつつ、目的と手段の均衡性が確保される限りにおいて、その合理性が認められる[142]。

以上を踏まえると、データローカライゼーションは、安全保障、個人情報保護、経済振興といった多元的目的の下で、一定の範囲内においては国際経済秩序との整合性を保ちつつ正当化され得る。主権国家の基本的責務として承認されるとともに、国際的ルールに照らしても、公共政策例外および安全保障例外の適用を通じてその正当性を法制的に根拠づけることができる。

---

[140] Aaronson and Leblond (2018), pp. 267–272; OECD (2023a), pp. 11–25; Pierucci (2025), section 5.
[141] EDPB (2020b), paras. 31–49; OECD (2023a), pp. 11–25.
[142] Cory and Dascoli (2021), pp. 9–15; OECD (2023a), pp. 10–14, 19–22; Han (2024), pp. 265–270.

第 2 項 データローカライゼーションの弊害

他方、データローカライゼーションは、経済的・技術的・制度的観点から深刻な弊害を伴う。これらの弊害は、データ保護主義による弊害（前記第 1 章第 2 節参照）と本質的に共通するものである。

第一に、経済的側面では、国内保存義務や越境移転制限により、企業は各国でサーバーやシステムを個別に設置する必要が生じ、そのコスト負担は甚大となる。特に中小企業や新興国企業にとっては重大な参入障壁となり、国際市場へのアクセス機会を奪う。このような負担の偏在は、国際的な経済効率性を損ない、競争環境の均衡を崩す要因となる[143]。

第二に、技術的側面では、データの囲い込みが越境的な技術協働や研究開発を阻害する。AI の高度化や疫学研究など、多国間データ共有を前提とする領域では、ローカライゼーション措置が研究速度や技術革新を著しく低下させる[144]。また、データの断片化は国際的なサイバーセキュリティ体制の構築を困難にし、全体の脆弱性を高める危険性を内包する[145]。

第三に、制度的側面では、越境的な協力体制や国際的サービス提供が機能不全に陥り、医療や金融、クラウドや AI など多領域の連携が阻害される[146]。さらに各国が独自のデータ移転規制を強化すれば、制度調和や相互運用性が損なわれ、規制の断片化が加速する。クラウド基盤や監督制度が国家ごとに閉じた体系として構築されれば、インターネット空間は複数の制度的ブロックに分裂し、相互運用性は長期的に失われる[147]。特に制度的対応能力の低い国々では、国際経済秩序における不平等が固定化され、国際的なデータガバナンスの分断を一層深める要因となり得る[148]。

総じて、データローカライゼーションは、経済効率性、技術革新、制度的調和のいずれにも阻害的に作用し、長期的にはサイバー空間の分裂を誘発する。こうした負の影響を抑制しつつ公共目的と国際的整合性を両立させる協調的枠組みを構築することが、持続可能な国際的データガバナンスの確立に不可欠である[149]。

第 3 項　データガバナンス規範再構成の方向性

本章では、国家のデータローカライゼーション措置によるデータ保護の強化が国際的に進展するなかで、越境的データガバナンス規範再構成に向けた課題を検討した。国家は個人データおよびプライバシーの保護や国家安全保障といった目的を追求する責務を負っており、一定の範囲でデータの国内管理を要求する措置は直ちに否定されるべきものではない。しかし、各国が自国領域内へのデータ囲い込みを拡大する方向へ向かえば、制度的・技術的基盤は国境ごとに区画化され、相互運用性の低下、国際的連携の機能不全、研究開発の停滞、制度的非対

---

143 Cory and Dascoli (2021), pp. 9–17; OECD (2023a), pp. 15–22; Pierucci (2025), section 3.
144 Cory and Dascoli (2021), pp. 9–17; OECD (2023a), pp. 13–14, 17–18, 21; Han (2024), pp. 265–270.
145 Cory and Dascoli (2021), pp. 6–14; OECD (2023a), pp. 13–17, 19–20; Han (2024), pp. 265–270; Lalova-Spinks et al. (2024), pp. 1–3.
146 OECD (2023a), pp. 13–18, 21–22; Lalova-Spinks et al. (2024), pp. 1–3; Han (2024), pp. 265–270.
147 Nocetti (2024), pp. 8–16, 28–30.
148 Aaronson and Leblond (2018), pp. 267–272; Cory and Dascoli (2021), pp. 6–14; OECD (2022c), pp. 13–18, 27–32; Han (2024), pp. 265–270.
149 Aaronson (2018), pp. 5–11, 13–17; OECD (2022c), pp. 27–32; Han (2024), pp. 265–270; Pierucci (2025), section 3.

称性の固定化といった深刻な影響が生じ得る。本章の分析が示すとおり、データローカライゼーションの拡大は、経済効率や技術革新を阻害するだけでなく、サイバー空間の分裂を通じて国際秩序の安定に長期的な影響を及ぼす構造的問題である。

以上を踏まえると、越境的データガバナンス規範の再構成に向けては、国家主権の正当な行使を前提としつつも、制度的公平性および予見可能性を確保し、国際的相互運用性を維持する枠組みが不可欠となる。その際、第Ⅲ部で論じるように、DFFT を指導理念として位置づけ、リスクベースアプローチに基づき移転条件を段階的に評価する制度設計が現実的な方策となる。データの性質のみに基づいてデータローカライゼーションの可否を一律的に判断するのではなく、当該データの利用文脈に基づくリスク評価を判断の要素とすべきである。データの性質と利用文脈を交差的に考慮したリスク評価に基づく仕組みは、国家の正当な統制権限と国際的信頼形成との両立を可能とし、サイバー空間の分裂を抑止するうえで有効である。特にデータローカライゼーション措置の可否の判断にあたっては、講じられる措置が目的に必要な最小限度の措置でなければならず、より制限的でない代替手段が存在する場合にはデータローカライゼーションは許容されないというデータ最小化原則を中核的な基準とすべきである。

このような方向性は、制度的断片化が進む現状において、持続可能で包摂的な越境的データガバナンス秩序を確立するための理論的基盤を提供し、国際社会における制度的相互運用性の回復に資するものである[150]。

[150] Aaronson and Leblond (2018), pp. 267–272; OECD (2022c), pp. 8–9, 13–22, 31–32; Han (2024), pp. 265–270; Pierucci (2025), section 3.

第 5 章

ガバメントアクセス

第 5 章　ガバメントアクセス

ガバメントアクセスとは、政府機関（捜査機関・規制機関・情報機関を含む。）が民間主体の保有するデータを法的または事実上の手段によって取得する行為をいう[151]。犯罪捜査、行政規制その他の公的目的に基づく取得が典型であるが、秘密裡の諜報活動によるデータ取得も広義には含まれる。越境的データガバナンスの文脈では、ガバメントアクセスは国家主権の行使と、個人のプライバシー権・データ保護権などの基本権、さらには国際的相互運用性との間に緊張関係を生じさせる[152]。自国企業が越境的に取得した外国発データについても、自国法の適用を通じて政府当局がアクセスを求め得る制度構造を備えている点は、国際的な議論において看過できない争点となる。

ガバメントアクセスは、その制度的形態において二つに大別される。第一は、政府当局が他国の企業や個人に対してデータの提供（開示）を要求するパターンであり、裁判所命令や行政権限に基づき外国の民間主体に直接的にデータを求める類型である。第二は、自国の民間主体を媒介として外国のデータに間接的にアクセスするパターンである。この場合、表面的には民間契約に基づくデータ移転にすぎないが、当該データが政府当局への協力義務の対象とされる制度構造の下では、自国政府による間接的取得が制度的に担保され得る。

ガバメントアクセスの正当性については、全面的に否定すべきか、あるいは一定の範囲で認めつつ統制すべきかが重要論点となる。本稿では、国際的なデータガバナンスの現状を踏まえ、後者の視点に立つ。すなわち、ガバメントアクセスを例外なく排除するのではなく、リスクベースアプローチなどの手法を用いて、一定の範囲で許容しつつ実効的な統制を実現する越境的データガバナンス規範再構成の在り方を検討する。

この方針に沿って、本章ではまず、中国、米国、EU その他の法域におけるガバメントアクセス制度を概観し、それらが越境的データガバナンスに与える影響を分析する（第 1 節～第 4 節）。これらの比較検討を踏まえ、第 5 節で、ガバメントアクセスと越境的データガバナンス規範再構成の方向性を提示する。

[151] 渡辺翔太 (2019) 2 頁; OECD (2022e), scope paragraph preceding the “Principles for government access to personal data held by private sector entities,” defining “government access.”
[152] Kuner (2017a), pp. 882–910.

第 1 節　中国のガバメントアクセス

中国におけるガバメントアクセスは、国家によるサイバー空間の統治と安全保障政策の一環として制度的に展開されてきた。本節では、その歴史的経緯を概観したうえで、近年における展開とそれに対する国際的批判を整理する。

第 1 項　歴史的経緯

中国におけるガバメントアクセスの展開は、1978 年の改革開放以降に加速した情報流通の拡大と軌を一にしつつ、1980 年代から 1990 年代にかけて、党および政府機関が社会的安定と政治秩序の維持を目的として監視技術や情報管理制度の導入に着手したことに端を発する[153]。特に、1989 年施行の国家秘密法[154]は、国家機密を広範に定義し、通信の検閲や出版物の流通制限など具体的監督行為への法的根拠を与えるものであった。

1999 年の江沢民による「情報化による工業化の牽引」戦略は、その後 2006 年の「国家情報化発展戦略綱要」において制度的に位置づけられた[155]。この方針の下で、情報通信インフラ整備が推進されるとともに、政府による情報へのアクセス・管理体制の強化が国家政策として進められた。2000 年代に入ると、インターネットの普及を背景に、インターネット空間を統治する必要性が高まり、2009 年の新疆ウイグル自治区における暴動を契機に、政府はインターネット空間を「イデオロギー的闘争の主戦場」と位置づけた[156]。広域的通信遮断や SNS 閉鎖、微博（Weibo）を含む監視・検閲体制の導入は、情報統制型プラットフォームを制度的に活用する転換点となった[157]。

さらに、2015 年には、李克強首相による政府活動報告で「インターネット・プラス」政策が打ち出され、モバイルインターネット、ビッグデータ、クラウドコンピューティング、IoT 等の先端技術が社会経済統治に組み込まれた[158]。同年に施行された国家安全法[159]は、国家安全保障を、経済発展・社会秩序・国民福祉をも包含する広範な概念として定義し、個人や法人に国家安全への協力義務を課すことで、政府による包括的なデータアクセス権限を法的に裏付けた。

そして、2017 年に施行されたサイバーセキュリティ法（CSL）[160]により、実名登録制度やアプリ審査義務を根拠づけるとともに、重要情報インフラ事業者に対するデータ国内保存義務を導入した（同法第 37 条）。これにより、個人情報や企業データが継続的に国家による監督の下に置かれる体制が形成された。その後、2021 年施行のデータセキュリティ法（DSL）[161]および個人情

---

153 Harwit and Clark (2001), pp. 378–392.
154 中華人民共和国国家秘密法（1988 年 9 月 5 日制定、1989 年 5 月 1 日施行、2010 年改正）.
155 中華人民共和国国務院『国家情報化発展戦略綱要（2006–2020 年）』第 I 章第 2 節（2006 年 3 月）. https://www.gov.cn/gongbao/content/2006/content_315999.htm
156 Xu et al. (2022), pp. 387–397.
157 Creemers (2017), pp. 85–100.
158 State Council of the People's Republic of China (2015) Report on the work of the government. Delivered by Li Keqiang at the Third Session of the 12th National People's Congress, 5 March 2015. https://english.www.gov.cn/archive/publications/2015/03/05/content_281475066179954.htm; Creemers (2017), pp. 89–95.
159 中華人民共和国国家安全法（2015 年 7 月 1 日制定・施行）.
160 中華人民共和国サイバーセキュリティ法（2016 年 11 月 7 日制定、2017 年 6 月 1 日施行）.
161 中華人民共和国データ安全法（2021 年 6 月 10 日制定、2021 年 9 月 1 日施行）.

報保護法（PIPL）[162]は、データ越境移転に際し安全評価、政府事前承認、第三者監査等を義務化し、外国企業による中国発データの移転を事実上厳格に制限した。

これら一連の法制度は、国家安全保障の名の下でデータを戦略的資源と位置づけ、国内外のデータを国家統制体系に組み込む枠組みを制度的に確立している。その結果、越境的データガバナンスにおいては、国際的相互運用性が阻害され、外国企業にとって法令遵守リスクが恒常的に生じる構造を形成している。こうした中国モデルは、「サイバー主権」を掲げた統治アプローチの典型であり、他国との間に制度的非対称性を拡大させ、国際的データガバナンスにおけるルール形成過程にも大きな影響を及ぼしている[163]。

第 2 項　国家安全法および国家情報法による制度的正当化

2015 年に施行された国家安全法および 2017 年に施行された国家情報法[164]は、中国における包括的な国家安全保障戦略の法的基盤として機能しており、ガバメントアクセスを制度的に正当化する上位法として位置づけられる。

国家安全法第 2 条及び第 15 条では、国家安全の概念を、軍事や治安に限定せず、人民の福祉、経済社会の持続可能な発展、国家の「重大な利益」など非常に広範な領域に拡張して定義しており、中国政府が「全面的国家安全観」に基づいて包括的な安全保障政策を正当化する根拠条文となっている。また、第 25 条では、国家による「サイバー空間の安全」の維持、「インターネット及び情報技術分野における国家の主権」の擁護等が明記されており、いわゆる「サイバー主権」の法的根拠が与えられている。この規定により、中国政府は、国内のインターネット空間における通信、データ、コンテンツに対するアクセス・監視・遮断を、国家安全保障の名の下に遂行する包括的な権限を獲得している。

さらに、第 77 条および第 78 条は、すべての個人、法人その他の組織に対して国家安全保障への協力義務を明示し、国家安全を名目とする情報提供および技術支援の要求に対して、法的根拠を与えている。これらの条文からは、企業を含むあらゆる主体が政府からの協力要請に応じる法的義務を負うものと解釈できる。特に、通信事業者やインターネットプラットフォームを含む IT 関連企業においては、ネットワークインフラやユーザーデータを管理する立場にあるため、政府のアクセス要求を受けてその内容を提供する構造が制度的に組み込まれている[165]。これは、ガバメントアクセスが法制度だけでなく、実務レベルでも規範化・常態化されていることを意味し、その枠組みは、契約的または任意的協力の範囲を超えている。

加えて、国家情報法は、第 7 条においてすべての組織および個人に国家情報活動への協力義務を課し、国家安全法の理念を具体的な執行義務へと転化している。

このように、国家安全法および国家情報法は、ガバメントアクセスに関する一般原則を定めた上位法として機能しており、「全面的国家安全観」という包括的理念に基づき、制度化された国家によるデータアクセスの法的枠組みを支えている。その統治構造は、欧米諸国に見られるような司法的監督を前提とする限定的な監視制度とは本質的に異なり、越境的データガバナンス

[162] 中華人民共和国個人情報保護法（2021 年 8 月 20 日制定、2021 年 11 月 1 日施行）.
[163] Chen and Gao (2024), pp. 2424–2439.
[164] 中華人民共和国国家情報法（2017 年 6 月 27 日制定、2017 年 6 月 28 日施行）.
[165] European Union Institute for Security Studies (2021).

における制度的非対称性を拡大させ、国際的な相互信頼や制度的相互運用性の確立を阻害する根本的障壁となっている[166]。

【参照条文】

国家安全法

第 2 条（国家安全の定義）

この法律において「国家安全」とは、国家政権、主権、統一、領土の完全性、人民の福祉、経済社会の持続可能な発展、国家の他の重大な利益が比較的安全な状態にあり、内外からの脅威が効果的に予防・制御され、国家の持続的な安全保障能力が確保されていることをいう。

第 15 条（国家安全政策の策定）

国家は、国家安全戦略と関連する政策を策定し、全面的な国家安全観に基づき、国家安全の取組を計画的に推進し、国家安全制度の整備及び能力建設を強化し、国家安全を確保する。

第 25 条（サイバー空間の安全と主権）

国家は、サイバー空間の安全を維持し、インターネット及び情報技術分野における国家の主権、安全、発展利益を擁護する。

第 77 条（国家安全維持への協力義務）

いかなる個人及び組織も、国家の安全を損なう行為をしてはならず、国家の安全を維持する責任と義務を有する。

国家安全機関及び公安機関は、法により、関連する個人及び組織に対して支援及び協力を求めることができる。関係個人及び組織は、法律及び行政法規の規定に従って、真実を提供し、支援及び協力の義務を履行し、国家の秘密を守らなければならない。

第 78 条（協力拒否への責任追及）

いかなる個人又は組織も、国家安全機関及び公安機関が法により行う国家安全の作業に干渉してはならない。

個人又は組織が国家安全機関や公安機関による協力・支援の要請を拒否したり、妨害した場合には、法に基づき責任を追及される。

国家情報法

第 7 条

いかなる組織及び市民も、国家情報活動に協力する義務を負う。

第 3 項　「中国データ三法」による具体的実装

中国におけるガバメントアクセスは、20 世紀後半から行政規則や業界ガイドラインの形で段階的に導入されていたが、CSL により初めて法的根拠を伴う包括的な義務として確立された。これにより、利用者の身元を、そのオンライン上の言論・活動と直接的に結びつけることが可能となり[167]、モバイルアプリの提供には事前登録および内容審査が義務づけられ、アプリストアの運

[166] Creemers (2017), pp. 89–100.
[167] Lee and Liu (2016), pp. 4–15, 23–29.

営事業者には、掲載アプリに含まれる違法情報を監視・報告する責任が課された[168]。加えて、特定業種における集中データ処理体制の導入によって、個人データや企業データが国家の継続的な監督下に置かれる構造が形成された[169]。こうした制度の積み重ねは、国家によるデータアクセスを日常的かつ体系的な統治手段へと制度化した。

そして、「中国データ三法」による一連の制度整備は、中国国内におけるデータ統制の強化にとどまらず、越境的データガバナンスにも深刻な影響を与えた。特に、2021 年に施行された DSL および PIPL において、データの越境移転に対して安全評価、政府の事前承認、第三者監査等の複雑な手続が義務化され、外国企業による中国発データの移転は事実上厳格に制限された。このような制度的枠組みは、「サイバー主権」を根拠として国家が国境を越えるデータ流通を自国の管轄下に置く統制の一形態と理解されており[170]、国際企業にとって制度的・法的リスクを恒常的に内包する体制を形成している。

【参照条文】

サイバーセキュリティ法（CSL）

第 37 条

重要情報インフラ運営者は、中華人民共和国国内で収集し又は生成した個人情報及び重要データを、国内に保存しなければならない。業務上の必要により、これらのデータを国外に提供する必要がある場合には、国家インターネット情報部門が関連部門とともに規定する安全評価を経なければならない。法律、行政法規に別段の定めがある場合は、その規定に従う。

データセキュリティ法（DSL）

第 31 条（重要データの越境移転に関する安全管理）

重要情報インフラ運営者は、中国国内での業務において収集又は生成した重要データの国外への移転に関し、サイバーセキュリティ法の規定に従うものとする。その他のデータ処理者は、中国国内での業務において収集又は生成した重要データの国外への移転に関し、国家網信弁公室が国務院の関係部門と共同で制定する規則に従わなければならない。

個人情報保護法（PIPL）

第 38 条（越境移転の一般要件）

個人情報処理者が個人情報を国外に提供する場合には、以下のいずれかの条件を満たす必要がある：

1. 国家インターネット情報部門による安全評価に合格していること。
2. 国家インターネット情報部門が定めた専門機関による個人情報保護認証を受けていること。
3. 国家インターネット情報部門が公表した標準契約書に基づいて受領者と契約を締結し、その契約内容が同法に従って個人情報の保護責任を明確にしていること。
4. 法律、行政法規その他国家インターネット情報部門の規定により、国外移転が認められているその他の条件に適合していること。

また、国外提供にあたっては、個人に対して明示的に通知し、同意を得ることが必要である。

---

[168] British Chamber of Commerce in China (2023), para. beginning “The Notice also requires that network access service providers ….”

[169] Creemers (2017), pp. 91–97.

[170] Chen and Gao (2024), pp. 2426–2439.

第 40 条（重要情報インフラ運営者及び大量データ取扱者の国内保存義務）

重要情報インフラ運営者及び法律・行政法規の定めるところにより処理する個人情報の数量が国家網信部門の定める基準を超える個人情報取扱者が、中華人民共和国国内で生成又は収集した個人情報は、原則として国内に保存しなければならない。国外に提供することが真に必要である場合には、国家網信部門が組織して行う安全評価に合格しなければならない。

第 4 項　国際的批判

中国におけるガバメントアクセスの実際の運用は、法制度上の根拠に基づきながらも、党主導の政治体制と一体化した極めて不透明な実務慣行によって支えられており[171]、その構造は公式法令よりも実務上の裁量に依存している[172]。国家安全や公共利益の名の下に、公安・国家安全当局からのデータアクセス要求に対しては、正式な司法手続を経ることなく、外国企業に応答が求められることが常態化している[173]。また、営業許可の維持や市場参入の継続を条件として、外資系企業が現地法人や合弁会社を通じてアクセスに協力する構造も広く見られる。こうした慣行は、企業内に設置される共産党委員会の影響力や、「行政指導」と称される非公開かつ拘束力を持たない政府の要請によって制度的に補強されている。さらに、国家安全法および国家情報法に基づく包括的な協力義務や監督体制の強化により、企業はデータ提供義務の有無や範囲を自己判断する余地がほとんどなく、監視に対する異議申立ての制度的保障も極めて限定的である。こうした制度的・実務的特徴が、中国政府によるガバメントアクセスを恣意的かつ制度化された形で実行可能にしており、越境的データ移転における相互信頼性や法的予見可能性を損なう要因となっている[174]。

このように、中国におけるガバメントアクセス制度の展開は、国家安全保障の観点に基づく情報統制として実施されてきたが、国際的には、外国企業に対する実質的な技術移転圧力を構成するとの批判が強まっている[175]。特に、クラウドサービスやビッグデータ領域において、外国企業が中国市場に参入するためには、現地法人の設立や中国企業とのパートナーシップを通じて、自社の運用情報やプラットフォーム構造を政府機関の監督下に置かざるを得ない構造が制度化されている。2017 年以降に制定された「中国データ三法」（前記第 1 章第 3 項参照）によって、こうした構造は法的にも根拠づけられた。これらの法制度のもとでは、外国企業が収集・処理する個人・非個人データも中国国内で保持・審査される義務が課され、国家が技術的知見・データ資産にアクセスする実質的権限を有するに至っている。制度の透明性や正当手続の保障が乏しい状況においては、実質的に強制的な技術移転要求に等しい構造を形成している[176]。

中国におけるガバメントアクセスは、外国企業に対する技術移転を目的とする制度的手段として国際的に問題視されてきた。たとえば、米国は 2018 年、WTO に提訴し、中国が外国企業に対して合弁事業の設立や技術・ノウハウの開示を事実上義務づけ、知的財産の移転を強いて

[171] Creemers (2017), pp. 91–100.
[172] Zhang (2024), pp. 6–13.
[173] Creemers (2017), pp. 93–100.
[174] Creemers (2017), pp. 94–100, Xu (2024), pp. 290–294.
[175] USTR (2018), pp. 19–47, 177–182.
[176] Chen and Gao (2024), pp. 2426–2439.

いると主張した[177]。この申立てでは、国家安全や監督審査を名目とした制度が、外国企業の機密情報へのアクセス手段として機能している点が争点とされたが[178]、WTO パネルの手続はその後停止されたままとなっている。国際機関レベルでは、OECD が 2022 年に「民間部門が保有する個人データへのガバメントアクセスに関する原則」[179]（以下「OECD ガバメントアクセス原則」という。）を策定し、政府による個人データへのアクセスは、法的明確性、正当目的、比例性、監督および救済の確保を伴うべきであるとした。この宣言は、国家安全や法執行を理由とするアクセス権限の濫用が国際的なデータ流通と制度的信頼を損なうおそれがあることを明示し、OECD 加盟国を含む 38 の参加国に対し、透明性と説明責任を備えた制度設計を求めている。また、非個人データを含むデーター般に対する政府アクセスについても、信頼確保の観点から、G7 などの国際フォーラムにおいて重要な論点として認識されている[180]。

さらに米国は、中国などのガバメントアクセスに対抗するため、2024 年、米国人の機微な個人データを「敵対的外国勢力（foreign adversaries）」へ提供することをデータブローカーに禁じる PADFA[181]を制定した。これに続いて司法省は 2024 年 12 月、バルクの機微データや政府関連データが中国などに渡ることを抑止するための規則を段階的に発効させる枠組みを整えた[182]。

中国のガバメントアクセス制度は、国家主権の問題にとどまらず、企業間の競争条件、技術的優位性の維持、国際通商ルールの正当性に深刻な影響を与えている。特に、クラウドインフラや AI 学習データ、IoT プラットフォームを介した情報流通において、中国側の制度的アクセスが一方的な情報取得構造として機能しており、越境的データガバナンスの非対称性拡大の要因となっている[183]。ガバメントアクセスに対する国際的規律の整備と制度的歯止めの導入は、グローバルな制度的信頼と相互運用性を確立するための最重要課題である[184]。

【参照条文等】

OECD：民間部門が保有する個人データへのガバメントアクセスに関する原則（抄）

Ⅳ. 比例性

ガバメントアクセスは、正当な公共目的を追求するために必要な範囲に限定されなければならず、当該目的との関係において不均衡なものであってはならない。

そのようなアクセスは、追求される正当な公共目的の性質および重要性に照らして適切なものでなければならず、当該目的を達成するために合理的に利用可能な、より制約の少ない代替手段が存在しない場合に限り実施されるべきである。

---

177 USTR (2018), pp. 19–45.

178 WTO (2018) Request for Consultations by the United States, China—Certain Measures Concerning the Protection of Intellectual Property Rights, WT/DS542/1, 26 March 2018.
https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/542-1.pdf

179 OECD (2022e).

180 OECD (2019a), pp. 17–19, 24–34; G7 Digital and Technology Ministers (2021). pp. 2–3, section A "G7 Roadmap for Cooperation on Data Free Flow with Trust."

181 Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA), Pub. L. No. 118–45 (Apr 24, 2024).

182 U.S. Department of Justice (DOJ) (2024) Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern: Final Rule (27 Dec 2024), 90 days after publication (effective 8 Apr 2025).
https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern

183 USTR (2023), pp. 66–68, 86–87; OECD (2023b), pp. 6–15, 17–21.

184 OECD (2019a), pp. 78–99; Raslan RAA (2024), pp. 20–43.

ガバメントアクセスは、無差別的、包括的又は過度に広範なものであってはならず、アクセスの範囲、対象となる個人データの種類、アクセスの期間および方法は、当該正当な公共目的を達成するために必要な最小限のものに限定されなければならない。

比例性の評価にあたっては、ガバメントアクセスが個人のプライバシーおよび個人データの保護に及ぼす影響の重大性、影響を受ける個人の範囲、ならびに当該アクセスに対して設けられている手続的保障および効果的な救済手段の有無が考慮されなければならない。

V. 透明性

ガバメントアクセスに関する一般的な法枠組みは明確で、かつ広く公衆が利用できなければならない。そうすることで、個人はガバメントアクセスが自身のプライバシーやその他の人権・自由に与える潜在的影響を考慮可能となる。

ガバメントアクセスに関する透明性を確保する仕組みが存在しなければならない。ただし、これらの仕組みは、国家安全保障や法執行活動に対し有害となる情報の開示を防ぐ必要性とのバランスをとる必要がある。

こうした仕組みには、監督機関による政府の法的要件順守状況の公表、政府記録へのアクセスを求める手続、定期報告、場合によっては個別通知などが含まれる。私企業も、ガバメントアクセス要請に関する集計的統計報告を許され得る。

VI. 監督

ガバメントアクセスが法的枠組みに適合するよう、効果的で公平な監督メカニズムが存在しなければならない。

監督機関とは、社内部門のコンプライアンス、裁判所、立法委員会、独立行政機関などを含むことができる。これら監督機関は、アクセス要求に関する情報の取得・審査、調査、監査、政府機関との対応、違反への対処を行う能力を有すべきである。

監督機関はその職務行使の際、干渉を受けず、十分な財政・人員・技術的資源をもって活動でき、調査結果を文書化し報告を作成、可能な限り公表すべきである。

VII. 救済

法的枠組みは、国民がガバメントアクセスによる個人データの扱いの違反を特定し是正できる、有効な司法及び非司法上の救済手段を提供すべきである。

米国：PADFA（Protecting Americans’ Data from Foreign Adversaries Act of 2024）

第 2 条

（a）禁止事項

データブローカーは、合衆国の個人に関する個人識別可能な機微データを、以下のいずれかに対して販売、ライセンス供与、賃貸、取引、移転、開示、提供、アクセス許可、又はその他の方法により利用可能とすることを行ってはならない。

1. 敵対国（foreign adversary country）
2. 敵対国が支配する法人又は団体（entity controlled by a foreign adversary）

（以下省略）

第 2 節　米国のガバメントアクセス

米国におけるガバメントアクセス制度は、国家安全保障の確保と適正手続保障との均衡をめぐる緊張関係のなかで発展してきた。その形成過程は、冷戦期の情報収集体制に端を発し、テロ対策やサイバーセキュリティ政策の拡張とともに、監視権限の拡大と司法的統制の制度化が並行して進められてきた点に特徴がある。本節では、冷戦期から現代に至るまでの制度的展開を概観し、米国型ガバメントアクセスの構造的特徴を明らかにする。

第 1 項　歴史的経緯（～2001 年）

米国におけるガバメントアクセスは、冷戦期の国家安全保障体制に端を発する。1947 年に創設された中央情報局（CIA）および 1952 年に設立された国家安全保障局（NSA）は、外国勢力に対する通信傍受を含む広範な情報収集活動を遂行してきた[185]。1970 年代にはウォーターゲート事件やチャーチ委員会の調査を契機に、政府による監視の行き過ぎに対する批判が高まり、1978 年には外国情報監視法（FISA）が制定された。同法は、国家安全保障上の脅威とされる外国政府や外国人に対する電子的監視を可能にするもので、従来の法執行目的とは異なる独立の監視手続を創設するとともに、監視活動に司法的監督の枠組みを制度化した[186]。具体的には、監視の実施に先立ち、外国情報監視裁判所（Foreign Intelligence Surveillance Court: FISC）に対し政府機関が申請を行い、その正当性と必要性について審査を受ける制度が整備された。

第 2 項　同時多発テロ事件（2001 年）～スノーデン事件（2013 年）

2001 年の同時多発テロ事件以降、米国政府は国家安全保障対策を強化し、2001 年制定の USA PATRIOT 法により FISA の監視権限が大幅に拡張されることとなった[187]。その後、2008 年の FISA Amendment Act により導入された第 702 条は、外国に所在する外国人を対象とする通信の収集を可能にし、通信事業者に対する命令を通じて大規模なデータ取得を制度化した[188]。

2013 年、NSA の元契約職員エドワード・スノーデンによる暴露は、NSA が「PRISM」や「XKeyscore」などのプログラムを通じて国内外のデータに広範なアクセスを行っていた実態を世界的に明らかにした[189]。さらに、英国政府通信本部（GCHQ）との連携による「MUSCULAR」プログラムでは、Google や Yahoo の海外データセンター間の通信リンクを秘密裏に傍受し、司法的承認を経ることなく、数億件規模の通信データにアクセスしていた事実が判明した[190]。こうした包括的かつ不透明な監視体制は、EU 諸国において個人データの域外移転に係る法的正当性へ

---

[185] Central Intelligence Agency (2026) About CIA https://www.cia.gov/about/ (accessed 22 February 2026); National Security Agency (2026) Sharing Our Storied Past https://www.nsa.gov/History/ (accessed 22 February 2026).
[186] Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. § § 1801-1885c).
[187] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[188] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended at 50 U.S.C. § 1881a).
[189] Snowden (2019), pp. 229-257.
[190] Amnesty International and Privacy International (2015), pp. 8-9.

の疑義を生じさせ、2020 年の CJEU による Schrems Ⅱ判決[191]で米国の監視制度は GDPR に基づく十分性を満たさないとの判断に至る一因となった。

第 3 項　CLOUD 法（2018 年～）

2018 年には CLOUD 法[192]が成立し、米国当局が米国企業に対し、国外に保管されたデータの提供を命じる法的権限が明文化された（合衆国法典第 2713 条）。この法律は、Microsoft Ireland 事件[193]において、国外サーバー上のデータに対する米国法の適用が問題となり（表 6 参照）、その際に明らかとなった法的曖昧性に対処するものであった。

CLOUD 法は、連邦貯蔵通信法（Stored Communications Act; SCA）を改正する形で、米国の通信サービスプロバイダに対し、データの保存場所にかかわらず、ユーザーのデータを提供する義務を課している。これにより、たとえそのデータが外国に保管されていても、米国内に拠点を置く企業であれば、米国政府の令状又は召喚状に従ってデータを開示しなければならない。

【表 6：Microsoft Ireland 事件の概要】

Microsoft Ireland 事件の概要

In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), cert. granted, 138 S. Ct. 356 (2017), vacated as moot, 138 S. Ct. 1186 (2018)

このケースは、米国連邦政府が、米国外に保存された電子メールデータに対して、米国の刑事訴訟手続に基づきアクセスを求めることが可能か否かをめぐって争われた事案である。2013 年、米国連邦捜査局（FBI）は、麻薬捜査に関連して Microsoft 社に対し、SCA（改正前）の下で発付された令状に基づき、同社が保有する電子メールデータの開示を命じた。問題となったデータは、同社のアイルランド・ダブリン所在のサーバーに保存されていたため、Microsoft 社は、SCA の令状は域外適用を予定しておらず、国外サーバーに保存されたデータには及ばないと主張し、当該データの提供を拒否した。

連邦地裁は政府の主張を認め、国外に保存されているデータであっても米国企業が管理する以上、SCA の令状に基づく開示義務は及ぶと判断した。これに対し、第二巡回区控訴裁判所は 2016 年、SCA は域外適用を予定しておらず、米国当局が国外サーバーに保存されたデータに直接アクセスを求めることはできないとする判断を下した。この判断は、米国法の域外適用に関する原則や、他国の主権との衝突との関係で注目された。

もっとも、当該判断は最終的に最高裁判所に上告され、2017 年には審理に付されたものの、2018 年に CLOUD 法が制定され、米国企業が管理するデータについては、その保管場所が国外であっても米国当局の令状に基づく開示義務が生じることを明確に規定したため、本件は「moot（訴えの利益を喪失した）」として最高裁において却下された。

---

[191] Schrems II, Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (CJEU).
[192] Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, div. V, 132 Stat. 1214 (2018).
[193] In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), cert. granted, 138 S. Ct. 356 (2017), vacated as moot, 138 S. Ct. 1186 (2018).

CLOUD 法は、特定国との間でデータアクセスに関する「実行協定（executive agreements）」を締結する制度も導入しており（合衆国法典第 18 篇第 2523 条）、2019 年に米国と英国との間で初の協定が署名されたことはその代表例である[194]。この制度により、信頼関係にある外国政府は、自国の法律に基づき米国通信事業者に対して特定の条件の下でデータ開示を要請できる一方、米国当局による越権的な取得を抑制する調整メカニズムも整備されている[195]。もっとも、CLOUD 法は他国のプライバシー法やデータ保護法との抵触リスクを内包しており、GDPR との関係では、企業が米国の要請と EU のデータ移転規制の板挟みになる可能性が指摘されている[196]。このため、同法は、米国の捜査権限の拡張と越境的データアクセスをめぐる国際的な法的対立の象徴ともなっている[197]。

以上のように、米国のガバメントアクセス制度は、冷戦期の対外情報収集から始まり、テロ対策、越境的な法執行へと発展してきた。CLOUD 法は、他国に保存されているデータに一方的に米国の主権を及ぼす形でガバメントアクセスを拡張しており、その結果、国家間のデジタル主権行使に非対称性を生じさせ、越境的データガバナンスの制度的均衡に構造的な歪みをもたらしている。この非対称性は、EU や他国の反発を招き、越境的データ移転の国際ルール形成において米国の主導的立場を困難にするものである[198]。

【参考条文（以下は、抜粋・要約）】

FISA (Foreign Intelligence Surveillance Act)

第 702 条（外国にいる非米国人に対する電子通信の取得）

（a）許可された監視活動

司法長官及び国家情報長官は、外国に所在する非米国人からの情報収集を目的として、外国の諜報活動を行うことを合理的に信じるに足る場合に、電子通信事業者を通じて、その通信内容や関連情報の取得を承認することができる。

（b）対象の制限

この情報収集は、外国にいる非米国人に限定されており、米国市民や米国内の人を対象とすることはできない。

（c）裁判所による監督

このような活動は、FISA 裁判所（FISC）の承認を必要とし、実施にあたっては収集対象の選定、最小化措置（米国人に関する情報の削除や秘匿）などの手続が定められる。

（d）通信事業者への協力命令

---

[194] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, signed 3 Oct. 2019. https://assets.publishing.service.gov.uk/media/5d9b01dfe5274a5a243406e7/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

[195] U.S. Department of Justice, Criminal Division, CLOUD Act Resources. https://www.justice.gov/criminal/cloud-act-resources

[196] European Data Protection Board and European Data Protection Supervisor (2019); Cleary Gottlieb (2019), paras. beginning "As a result, the EDPS and EDPB strongly recommended that an international agreement be concluded …," and "Absent such an agreement, the lawfulness of complying with a U.S. warrant cannot be ascertained …."

[197] Cochrane (2021), pp. 24–79.

[198] Cochrane (2022), pp. 169–210; Zalnieriute (2022), pp. 28–45.

通信事業者は、政府の要請に応じて、必要な情報の提供や技術的支援を行うことが求められる。これに応じることを拒否した場合、裁判所の命令に従うことが義務づけられる。

CLOUD 法関係（18 U.S.C. § 2713（2018）; 18 U.S.C. § 2523（2018））

第 2713 条（通信及び記録の保存・開示義務）

電子通信サービス又はリモート・コンピューティングサービスの提供者は、加入者又は顧客に関する通信の内容並びに記録その他の情報を保存、バックアップ又は開示する義務を負う。この義務は、当該通信、記録又は情報が米国内に所在するか国外に所在するかを問わず、当該提供者の占有、保管又は管理下にある限り適用される。

第 2523 条（外国政府によるデータアクセスに関する実行協定）

(a) 権限

司法長官は国務長官の同意を得て、外国政府との間で実行協定（executive agreement）を締結することができる。この協定により、当該外国政府は米国の電子通信サービス事業者やリモート・コンピューティングサービス事業者に対し、直接的にデータアクセスの要請を行うことが可能となる。

（以下略）

第 3 節　EU のガバメントアクセス

EU におけるガバメントアクセス制度は、米国や中国と比較して、伝統的に厳格な制約の下に置かれ、基本権保護と公共政策目的との間の緊張関係を調整しつつ、漸進的かつ原則重視の制度設計によって進展してきた。しかしながら、近年において、EU は行政分野におけるデータアクセス制度への整備を進める方向へと転換しつつある。

第 1 項　歴史的経緯

EU のガバメントアクセスに関する制度的基盤には、EU 法秩序の核心に位置づけられた基本権保護がある。すなわち、プライバシー権および個人データ保護権は EU 基本権憲章に明示され[199]、欧州人権裁判所（ECHR）および欧州司法裁判所（CJEU）の判例法が、国家によるデータアクセスの憲法的限界を明確にする上で中心的な役割を果たしてきた。たとえば、S. and Marper v. United Kingdom（2008）[200]では、犯罪に関与していない市民の DNA や指紋の無期限保存が欧州人権条約第 8 条に違反すると判断され、比例原則と目的限定性の遵守が強調された。また、Digital Rights Ireland 事件（2014）[201]では、EU のデータ保持指令に基づく無差別なメタデータの長期保存義務が、EU 基本権憲章の下で違憲とされ、国家による情報取得に対する憲法的コントロールが一層厳格化された。そして、2018 年に施行された GDPR は、その第 48 条で第三国政府の要請に対するデータ移転の原則的禁止を定め、域外国によるガバメントアクセスに対する防御的構えを示した[202]。

他方で、テロ対策や国家安全保障の領域においては、CJEU においても加盟国による通信データの保持やアクセスが比例原則の枠内で限定的に承認されてきた。たとえば、Privacy International 事件[203]および La Quadrature du Net 事件[204]において、CJEU は、一般的かつ無差別なデータ保持は原則として EU 法に反するとしつつも、国家安全保障および重大犯罪防止を目的とする場合に限り、通信データの保持・アクセスを比例原則の下で限定的に認め得ると判示し、国家安全保障の脅威に対処するための厳格に限定された措置については、例外的に認容され得る余地を示した。これらの判決では、保持措置が「厳格に必要」であることを要件としている。このことは、通常の刑事捜査や行政監督に比して、テロ対策が別扱いされ、広範なアクセスを可能とする規範的正当化を与えられてきたことを示している。ただし、かかるアクセスが容認される場合であっても、限定的範囲、監督手続、透明性確保といった条件を欠くことは許されず、比例原則の拘束力は維持されてきた。

---

[199] European Union, Charter of Fundamental Rights of the European Union, 2012/C 326/02, OJ C 326, 26.10.2012, Arts. 7–8.
[200] S. and Marper v. United Kingdom, App. Nos. 30562/04 & 30566/04, Eur. Ct. H.R. (2008).
[201] Case C-293/12, Digital Rights Ireland Ltd v Minister for Communications [2014], EU:C:2014:238.
[202] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 48, 2016 OJ L 119/1.
[203] Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2020], EU:C:2020:790.
[204] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others [2020], EU:C:2020:791.

【参照条文】

EU 基本権憲章

第 7 条（私生活及び家族生活の尊重）

すべての人は、その私的及び家庭生活、住居並びに通信に対して尊重を受ける権利を有する。

第 8 条（個人データの保護）

1. すべての人は、自らに関する個人データの保護を受ける権利を有する。
2. 当該データは、あらかじめ定められた目的のために適正に処理されるものとし、当該本人の同意又は法令により定められた他の正当な根拠に基づかなければならない。すべての人は、自らに関して収集されたデータにアクセスする権利を有し、それを訂正させる権利を有する。
3. これらの規則への準拠は、独立した機関による監督を受けるものとする。

GDPR

第 48 条（第三国当局又は裁判所による開示要求）

第三国又は国際機関の裁判所若しくは行政当局から、個人データの移転又は開示を要求する判断、決定若しくは命令は、国際協定、例えば当該第三国又は国際機関と欧州連合との間で締結された相互の法的援助条約等に基づく場合でなければ、認められない。

第 2 項　近年における EU のスタンスの変化

近年、EU は各種データの行政領域におけるガバメントアクセスの制度化へと踏み出しており、そのスタンスを大きく変容させつつある。2023 年制定のデータ法および 2024 年制定の AI 法は、市場監督や公共目的の遂行を根拠として、公的機関にソースコードや産業データへのアクセス権限を明確に制度化した点で、EU のガバメントアクセス政策における重要な転換を示している。

データ法は、EU 法体系において初めて、公的機関が民間企業保有データへのアクセスを要求し得る制度を明文で設けた法令である。同法第 15 条から第 17 条は、緊急時および特定の公共利益目的の遂行を理由として、公共部門機関が企業保有のデータ（個人データおよび非個人データを含む。ただし、個人データについては GDPR との関係で一定の条件が付される。）にアクセスするための根拠を示している[205]。緊急時アクセスは、自然災害、感染症の急速な拡大、重要インフラ障害など、公衆に重大な危害が現に生じている場合に、政府機関が必要なデータ提供を求め得る制度である。この場合、対象データの範囲、利用目的、保存期間は厳格に限定され、危機対応と無関係な二次利用は禁止される。

公共目的アクセスは、人命保護、安全確保、重要公共サービスの維持など、特定の公益目的に密接に関連する場合に認められる制度であり、公的機関は他に実効的な入手手段が存在しないことを示さなければならない。また、当該データへのアクセスが企業の競争上の地位、知的財産、営業秘密を不当に侵害しないよう、適切な保護措置を講じることが求められる。さらに、アクセス要求の手続には、理由提示、要求内容の文書化、保護措置の明示、利用目的の限定、アクセス期間の管理、独立監督機関による検証といった手続要件を通じ、多層的な手続保障が制

[205] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 Dec. 2023 (EU Data Act), arts. 15–17, 2023 O.J. (L 2023/2854).

度的に組み込まれている。企業側には、要求が不必要または過剰であると判断した場合に異議申立てや司法審査を求める途が確保されている。これらの制度設計により、データ法は、緊急時や公益目的に限定した公的アクセスを認めつつ、比例原則・透明性・独立監督および企業の権利保護を通じて、公的権限の過度な拡張を防ぐ統制的枠組みを構築している。

さらに、AI 法第 74 条第 12 項および第 13 項は、市場監督当局に対して、高リスク AI システムの適合性評価に必要な文書および訓練・検証・試験データセットに関し、適合性評価の実施に必要な範囲での完全なアクセス権限、ならびに条件付きで当該システムのソースコードへのアクセス権限を付与する規定を設けた[206]。この規定は、アルゴリズム、データセット、技術仕様に関する詳細な検証を行うための制度的手段を市場監督当局に付与することを意味する。これにより行政領域におけるガバメントアクセスの射程は、従来の規制枠組みを超える水準へと拡張された。

EU におけるガバメントアクセスは、従来、刑事捜査および国家安全保障領域に限定されてきた。特に GDPR 第 23 条や関連 CJEU 判例は、目的限定性、比例原則、代替手段の不存在、独立監督、透明性確保といった厳格な要件を満たす場合に例外的に公的アクセスを認める構造を維持してきた。しかし、近年のデータ法および AI 法に見られる立法動向は、行政監督および公共目的を根拠とするアクセス権限を制度として明確に承認するものであり、EU が国際的に米国の CLOUD 法や中国の国家情報法・サイバーセキュリティ法に基づくアクセス制度を批判してきた従前の立場との整合性に根本的な疑問を生じさせる[207]。このような立法動向は、EU 規範の一貫性に対する疑問を招くのみならず、国際的規範形成における EU の主張の規範的正当性を再検証することを不可避とする課題を提示する。

【参照条文】

<u>データ法</u>

第 15 条（データ利用に関する例外的必要性）

1 本章の意味における特定のデータ利用に関する例外的必要性は、時間的及び対象的に限定され、以下の場合にのみ存在するとみなされる。

(a) 要請されたデータが、公的緊急事態に対応するために必要であり、公共部門機関、欧州委員会、欧州中央銀行又は連合機関が、同等の条件の下で当該データを適時かつ効果的に入手する他の手段を有しない場合。

(b) 上記(a)に該当しない状況において、かつ非個人データに限り、以下の条件を満たす場合。

(i) 公共部門機関、欧州委員会、欧州中央銀行又は連合機関が、欧州連合法又は国内法に基づき活動し、かつ法律で明示的に規定された特定の任務（公式統計の作成、公的緊急事態からの被害軽減又は復旧など）の遂行を妨げる特定のデータの欠如を確認した場合。

(ii) 公共部門機関、欧州委員会、欧州中央銀行又は連合機関が、当該データを入手するために利用可能な他の手段をすべて尽くした場合。これには、市場価格での非個人データの購入、既存

[206] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), art. 74(12)–(13), 2024 O.J. (L 2024/1689).

[207] Nanni (2024), Discussion section (GDPR、Data Act、Data Governance Act 等の EU データ関連立法および国際的言説に内在する規範的緊張関係とその限界を批判的に検討している).

のデータ提供義務の活用、又は当該データの適時の入手を保証し得る新たな立法措置の採用が含まれる。

2 第 1 項(b)は、マイクロ企業及び小規模企業には適用されない。

3 公共部門機関が市場で非個人データを購入することができなかったことを証明する義務は、公共の利益に基づく特定の任務が公式統計の作成である場合、かつ当該データの購入が国内法により認められていない場合には適用されない。

第 17 条（データ提供要求の手続）

1 公共部門機関、欧州委員会、欧州中央銀行又は連合機関が、第 15 条に基づく例外的必要性によりデータの提供を要請する場合、その要求は書面で行われなければならない。

2 当該要求には、少なくとも以下の事項を含めるものとする。

(a) 要請されるデータ及びメタデータの明確な特定

(b) データ利用の目的及びその法的根拠

(c) データが利用される具体的な用途

(d) 利用が許容される期間

(e) データの保護及びセキュリティを確保するために講じられる技術的・組織的措置

3 個人データが要請される場合には、要請者は適切な技術的及び組織的保護措置（擬似匿名化やその他のデータ保護措置を含む）を明示しなければならない。

4 要請者は、第 15 条に定められた条件が満たされていることを証明する責任を負う。

AI 法

第 64 条（市場監督当局の権限）

1 市場監督当局は、規制遵守を評価するために必要とされる場合、高リスク AI システムに関する次の情報又は資源へのアクセスを要請できる。

(a) 技術文書及び EU 適合宣言書、ならびに当該システムのトレーニング、検証及び試験に用いられたデータセットに関する記録。

(b) 高リスク AI システムのログ、仕様、アルゴリズムに関する記録。

(c) 遠隔アクセスを含む、システムの利用可能なインターフェース（API 等）を通じた実際の挙動の確認。

2 市場監督当局は、必要と認められる場合、理由を付した正式な要請に基づき、高リスク AI システムのソースコードへのアクセスを要求できる。

3 当該アクセスにより得られたすべての情報は、本規則第 78 条に定める機密保持義務に従って取り扱われなければならない。

第 4 節　その他の国のガバメントアクセス

その他の国におけるガバメントアクセス制度は、法制度設計や運用形態の点で大きく異なっており、これらの差異は、ガバメントアクセスの正当性、透明性、監督可能性に直接的な影響を及ぼしている。その結果、制度間の信頼性格差が国際的なデータガバナンスの不均衡を助長している。

インドでは、2000 年情報技術法およびその下位規則に基づき、法執行機関がプラットフォーム事業者に対してユーザーデータの提供を要請することが認められているが、当該手続に明確な司法審査が付随しない場合が多く、恣意的な運用を許すおそれがあると指摘されている[208]。

ロシアにおいては、2006 年施行の「情報・情報技術・情報保護に関する法律」および「通信法」に基づき、外国 IT 企業に対してロシア国内にサーバーを設置し、ロシア市民の個人データを国内で保存・提供することを義務づけており、国家によるデータアクセスを正当化する制度的枠組みが構築されている[209]。

エジプトでは、2015 年に制定された反テロ法に基づき、国家安全保障を理由とする電子通信データの収集・分析が広範に認められており、外国企業に対しても当該アクセスへの協力義務が課される可能性がある[210]。

インドネシアでは、2022 年に個人データ保護法が施行され、包括的な保護枠組みが導入されたものの、通信・情報省によるアクセス命令の手続的透明性および司法的統制の欠如については、依然として国際的な懸念が残されている[211]。

トルコでは、2016 年の国家非常事態宣言以降、情報通信技術庁（BTK）に対し、裁判所の関与を要しない広範な監視権限が付与され、実際に司法命令を経ることなく通信データへのアクセスが行われた事例も報告されている[212]。

ブラジルでは、2018 年に制定された一般データ保護法（LGPD）により、データ主体の権利保護が制度的に整備された一方、刑事手続におけるガバメントアクセスについては、司法命令に基づくデータ開示が引き続き広く認められており、その実際の運用は捜査機関の裁量に大きく依存している[213]。

以上のように、各国のガバメントアクセス制度には制度的・運用的な格差が存在し、こうした制度間の信頼性格差が、越境的データガバナンスにおける非対称性を一層深刻化させている。米国や EU のように一定の法的保障が制度化されている国々と比較すると、ガバメントアクセス

---

[208] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Feb. 25, 2021 (India), issued under the Information Technology Act, 2000; Internet Freedom Foundation (2021), paras. beginning under the headings "Contracted timelines for assistance to law enforcement agencies," "Grievance redressal mechanism," and "Emergency blocking powers."

[209] Federal Law No. 149-FZ on Information, Information Technologies and Information Protection (27 July 2006) (Russia); Federal Law No. 126-FZ on Communications (7 July 2003) (Russia); Gurkov (2020), sections 6.3 Localization requirement and 6.4 Yarovaya law.

[210] Egypt, Law No. 94 of 2015 on Combating Terrorism (Anti-Terrorism Law); Freedom House (2023a), section C6, para. beginning "The government can obtain user information from companies without due process."

[211] Indonesia, Law No. 27 of 2022 on Personal Data Protection; Freedom House (2023b), sections B3, C5 and C6.

[212] Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication (2007) (Turkey), as amended by Decree Laws under the State of Emergency, 2016-2018; Freedom House (2023c), sections C5 and C6.

[213] Brazil, Law No. 13.709 of August 14, 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD); Federal Law No. 12.965 of April 23, 2014 (Marco Civil da Internet); Freedom House (2023d), sections C5 and C6.

の正当性や透明性に課題を抱える多くの新興国は、国際的事業者からデータ移転先やクラウド拠点としての信頼を得ることが難しい[214]。その結果、多国籍企業は法的リスクや不透明な介入の可能性を回避するため、当該国におけるデータ処理やビジネス展開を控えるなど、移転先国を慎重に選別する傾向を強めている。こうした対応の差異は、各国の法制度に起因する構造的な不平等を反映しており、国際的なデータ流通の公平性を損なう要因となっている[215]。

ガバメントアクセスに関する国際的制度の整備に際しては、合法性（legality）、必要性（necessity）、比例性（proportionality）の各原則を満たす枠組みの構築が不可欠である。既存の OECD 原則や G7 声明は一定の方向性を示しているものの、多くのアジア諸国やグローバルサウスの十分な参加を欠いており、その正当性と包摂性には限界がある。したがって、今後の国際制度設計においては、グローバルサウスを含む多様な国々が参加する包摂的な対話の場を確保し、透明性・相互性・監督可能性といった共通原理を共有することによって、国際的信頼を基礎とする制度的均衡をいかに具体的に構築するかが、中心的な課題となる[216]。

[214] UNCTAD (2021), pp. 81–91, 115–116.
[215] Aaronson (2018), pp. 7–16.
[216] UNCTAD (2021), pp. 81–91, 115–116; Aaronson (2018), pp. 7–16; Cate et al. (2012), pp. 195–199.

第 5 節　ガバメントアクセスとデータガバナンス規範再構成の方向性

各国におけるガバメントアクセスの実情を踏まえると、以下のとおり、一定の範囲で正当性が認められる一方で、深刻な弊害が存在することが明らかとなる。

第 1 項　ガバメントアクセスの正当性

ガバメントアクセスは、国家による公共目的の実現および国際法上の例外規定に基づく制度的措置として、一定の範囲で正当性を認めることができる。犯罪捜査やテロ対策、経済安全保障、公共衛生の維持などの公益目的において、国家当局が民間部門に蓄積されたデータにアクセスできなければ、効果的な法執行やリスク管理は著しく制約される。現代社会において、データは社会基盤として機能しており、その適切な利用は、国家および市民社会双方にとって不可欠である。

このようにガバメントアクセスの必要性が国際的に認識されるなかで、その制度を一律に否定することは、国家が果たすべき公共目的の実現や法執行上の責務を軽視するおそれがある。適正な法的根拠および手続的統制の下で行われるアクセスは、国家主権の正当な行使として制度的正当性を有するものであり、これを全面的に否定することは、現実的な統治要請を軽視する結果となりかねない。この観点からすれば、一定範囲でのガバメントアクセスは制度的正当性を有する[217]。OECD ガバメントアクセス原則や EU の GDPR 第 48 条にも見られるように、透明性・比例性・監督を条件として、ガバメントアクセスの正当性の範囲を画定する制度設計が求められる[218]。

この点に関し、2024 年に国連総会で採択された新サイバー犯罪条約[219]は、ガバメントアクセスの国際的制度化に新たな次元を付与するものである。同条約は、国境を越えた電子証拠の収集および保存を迅速化し、加盟国当局による国際的な電子証拠アクセスの制度的仕組みを整備することを目的としている。従来のブダペスト条約が欧州機関主導の枠組みに依拠していたのに対し、新条約は普遍的な国連枠組みにおいてガバメントアクセスの正当性を承認した初の国際的合意であり、アクセス権限の国際的調和を推進する契機となり得る[220]。

今日では、ガバメントアクセスは国家主権の行使という根拠のみで正当化されるものではなく、公共目的と基本権保護の均衡をいかに制度的に確保するかによって、その正当性の可否が規定される[221]。したがって、越境的データガバナンス規範の再構成においても、ガバメントアクセスを全面的に否定するのではなく、リスクベースアプローチに基づき、限定的かつ条件付きの承認を前提とすることが、正当性の担保に不可欠である。

---

217 Cate et al. (2012), pp. 195–199; Bannelier (2025), pp. 140–155.
218 OECD (2022e), Preamble; Principles I, II, V and VI.
219 United Nations (2024) United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. UN General Assembly Resolution 79/243, adopted 24 December 2024. https://docs.un.org/en/a/res/79/243
220 Bannelier (2025), pp. 140–144.
221 Kuner (2017a), pp. 892–906.

第 2 項　ガバメントアクセスの弊害

他方、ガバメントアクセス制度の拡張は、越境的データガバナンスに以下のような深刻な弊害をもたらしている。

第一に、各国の制度間でアクセス権限や手続的保障に関する基準が大きく異なるため、同一データに対し複数の法域から相反する法的要求が課される「法の衝突（conflict of laws）」が生じやすい[222]。たとえば、米国のクラウド法は国外サーバー上のデータについても開示を義務づける一方、EU の GDPR は域外移転に厳格な制限を課しており、Schrems Ⅱ判決（2020 年）は米国当局による監視権限の過剰さを理由に、米国へのデータ移転の法的基盤を否定した[223]。このように相反する規制は、企業にとっていずれかの法令に違反するリスクに直面する状況を生み出している[224]。

第二に、ガバメントアクセスの強化は、個人のプライバシー権や企業秘密の保護を脅かすものである。政府当局が裁判所令状や事前通知を伴わずに、広範な権限でデータへアクセスできる制度設計は、基本的人権の侵害および国際的信頼の低下を招く危険がある。実際、米国国家安全保障局（NSA）による PRISM プログラムの存在が暴露された際、国際的なデータ移転制度全体に対する信頼が著しく損なわれ、これにより、EU と米国の間では Safe Harbor および Privacy Shield といった協定が相次いで破綻した[225]。

第三に、各国が自国のガバメントアクセス権限を拡張する動きは、データを国境内に囲い込むデータ保護主義を助長し、グローバルなデジタル経済の断片化を加速させる。企業はデータを法域ごとに分散保管せざるを得ず、コストの増大と国際競争力の低下を招くとともに、研究開発や AI 技術の進展を阻害する可能性がある[226]。

これらの弊害を克服するためには、各国が独自の監視権限拡張を優先する現状を超え、国際的な協調枠組みの構築が不可欠である。具体的には、①ガバメントアクセスの法的根拠、範囲、救済手段に関する透明性の確保、②アクセス要求における比例性原則の遵守、③法域をまたぐデータ移転時のリスク評価基準の国際的整合が求められる[227]。ガバメントアクセスは国家安全保障のみならず、越境的データガバナンスの安定性および国際経済秩序の信頼性にも直結する問題である。各国は自国の法制度を優先するだけでなく、国際的な相互運用性を確保する視点から、比例性原則とリスクベースアプローチを軸とした調整メカニズムを整備することが不可欠である。

第 3 項　越境的データガバナンス規範再構成の方向性

近年、クラウドサービスやデータストレージが国境を越えて分散するなか、多くの国の政府当局は、法執行や国家安全保障を理由として、企業やプラットフォーム事業者が保有するデータ

---

222 Kuner (2017a), pp. 892–906.
223 Court of Justice of the European Union (CJEU) (2020) Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems Ⅱ), Case C-311/18, Judgment of 16 July 2020; GDPR, arts. 44–49.
224 Kuner (2017a), pp. 892–906.
225 Greenleaf (2021), pp. 6–11.
226 Docksey and Propp (2023), pp. 6–12.
227 EDPB (2020a), pp. 14–25, Annex 3; OECD (2022e), Preamble, Principles I, Ⅱ, V and Ⅶ.

へのアクセス権限を拡大している。各国が自国の監視権限を拡張する傾向は、プライバシー保護や企業秘密の保持、さらには国際的信頼の確保に深刻な影響を及ぼしている[228]。

こうした状況の下、国家間交渉や二国間協定による対応には限界があり、WTO 電子商取引交渉は停滞し、地域貿易協定もデータ自由流通原則に対して公共政策例外や安全保障例外を広く認めるなど、国際的統一基準を提示するには至っていない。ガバメントアクセスに対抗するためのソースコード移転等要求禁止条項についても、司法機関や行政審査機関による要求を適用除外する旨の規定が設けられている（後記第 8 章第 1 節参照）。現状では、各国が自国の公共政策や安全保障上の利益を優先し、越境的データ移転における透明性と予見可能性が著しく損なわれている。このため、国際企業は法的リスクを回避するため、データを分散管理せざるを得ず、それが国際的データガバナンスの断片化や国際経済秩序への不信感を助長している。このような制度的非対称性は、データ主権の名の下に監視権限を強化する動きを正当化し、グローバルな相互運用性と信頼性の確立を阻む構造的要因となっている。したがって、国際的調和を実現するためには、ガバメントアクセスの権限、範囲、手続的保障に関して、相互運用性を備えた国際基準を策定することが求められる[229]。

ガバメントアクセスが正当性を有するためには、データ最小化原則およびリスクベースアプローチに基づいて、明確な法的制約を設けることが不可欠である。これらの原則は抽象的理念にとどまるものではなく、データの性質および利用文脈に基づくリスク評価に応じた制度的対応として具現化されなければならない。すなわち、ガバメントアクセスは厳格に限定された例外的措置であり、国家による一般的・無差別なデータ取得を正当化する根拠にはなり得ない。データ取得の範囲は目的に照らして必要最小限でなければならず、より制限的でない代替手段が存在する場合には、ガバメントアクセスは許容されない。また、アクセスの根拠は明確に法律に定められ、独立機関による監督を伴わなければならない。この仕組みによって、権限濫用や恣意的介入の危険を抑止し、基本権侵害を最小化することが期待される[230]。そのためには、越境的データ移転に伴うリスクを、データの性質、利用文脈など実効的な複数の要素に基づいて評価し、リスク水準に応じて保護措置を段階的に設定する制度モデルが望ましい[231]。

ガバメントアクセスをめぐっては、他の領域に先行して、越境的データ移転に伴う制度的リスクを体系的に評価・管理する手法として、リスクベースアプローチを導入する考え方が国際的に浸透しつつある。たとえば、OECD ガバメントアクセス原則は、透明性、必要性、比例性、独立監督を中核とする制度的リスク評価モデルを提示し、国際的な合意形成を大きく前進させた[232]。また、DFFT は、リスクに応じた柔軟な移転評価を制度的に支える指導的理念として機能し得る[233]。このような潮流は、従来の形式的な越境的データ移転規制を超え、制度的信頼性と比例原則に基づく新たな越境的データガバナンスの構築に向けた理論的基盤を形成しつつある。他方、EDPB（European Data Protection Board：欧州データ保護理事会）は、第三国における監視権限の行使「可能性」の有無に依拠した柔軟な評価を許容せず、Schrems Ⅱ判決の考え方に基づき、第三国の法制度が実質的同等性（essential equivalence）を制度的に満たすか否かを中心的基

[228] Kuner (2017a), pp. 892–902; OECD (2022e), Preamble, Principles I, II and V.
[229] OECD (2022e), Preamble, Principles I, II and V; Docksey and Propp (2023), pp. 6–9, 15–30.
[230] Kuner (2017a), pp. 892–902; OECD (2022e), Preamble, Principles I, II, V
[231] Docksey and Propp (2023), pp. 10–15, 18–22.
[232] OECD (2022e), Preamble, Principles I, II, V and VI.
[233] World Economic Forum (2022), pp. 4–9.

準とする厳格な立場を維持している[234]。すなわち、EDPB は GDPR の域内適用においては、処理の性質および文脈に応じたリスクベースアプローチを広く認めているが、第三国への越境移転に関しては、Schrems II 判決を踏まえ、受入国法制度の実質的同等性を中心基準とする厳格な枠組みを採用している[235]。このようにデータ移転に対する規範的統制については域内と域外で非対称性が生じており、越境移転をリスクに応じて弾力的に許容するリスクベースアプローチの導入は、現行の EDPB の解釈枠組みの下では、制度的に困難であると言わざるを得ない。

ガバメントアクセスをめぐる国際的議論は、全面禁止や対抗措置としての越境的データ移転の包括的制限といった硬直的対応によっては克服できない。従来のように受入国の法制度のみに依拠して一律に移転を禁止したり、包括的なアクセス制限を設けたりする手法も、柔軟性を欠き、国際的な相互運用性の確保を困難にする。このような課題に対し、第Ⅲ部で検討するリスクベースアプローチおよび CRDM モデルは、データの性質と利用文脈を交差的に評価し、比例性と必要最小限性を確保することにより、柔軟かつ持続可能で、技術的発展との調和も可能にする。したがって、この枠組みは、規制の正当性と信頼性を高めつつ、越境的データガバナンス規範の再構成に理論的基盤を提供し、国際的信頼の再構築に向けた出発点となる。

[234] EDPB (2020a), paras. 42–49, 56–59, 70–75; EDPB (2020b), paras. 18–47.
[235] EDPB (2021a), paras. 42–43.3, 49; EDPB (2021b), paras. 18–22.

第 6 章

ディスカバリの越境的適用

第 6 章　ディスカバリの越境的適用

越境的データガバナンスにおいては、訴訟手続をはじめとする司法手続によるデータの越境移転の在り方も課題となる。近年の情報通信技術の発展によって、社会生活のあらゆる面でデジタル化が進み、訴訟においてもデジタル証拠（デジタルデータで構成された証拠をいう。以下同じ。）が重要な役割を占めるようになっている。また、データ通信の発達により、デジタル証拠が他国に存在することも一般化している。しかし、訴訟手続は各国の国内法によって規定されており、国境を越えて裁判権や捜査権を直接行使することは他国の主権を侵害することになる。そのため、越境的な証拠収集手続の確立が必要とされるようになった。

越境的証拠収集は、ある国における訴訟等のために国境を越えて他国に存在する証拠を収集するものであり、他国の主権との関係から国際協力が不可欠なものとなる。越境的証拠収集の手続的ルートは、①嘱託書（letter rogatory）による証拠調べの共助要請、②国際条約や二国間取決めに基づく請求、③訴訟当事者等による裁判所への直接申立てという三つのルートに大別することができる。このうち、①については、要請に応じるかどうかは受託国の任意であり、手続に時間を要する。また、②については、刑事関係の二国間条約として刑事共助条約（Mutual Legal Assistance Treaty: MLAT）が各国間で締結されているほか、民商事関係の多国間条約として「民事又は商事に関する外国における証拠収集に関するハーグ条約」[236]（以下「ハーグ証拠条約」という。）が締結されており、2025 年 7 月 24 日現在、米国、イギリス、フランス、ドイツ、スイス、スペイン、中国、ロシアなど 69 の国・地域が加盟している（日本はハーグ証拠条約には加盟していない。）[237]。これらの条約については、デジタル証拠の収集には必ずしも適していないことや証拠入手までに時間を要することなどの問題点が指摘されている[238]。③については、フランス、ドイツ、日本などの証拠（文書）提出命令制度なども含まれるが、当事者主導の典型例としては英米法におけるディスカバリ（pre-trial discovery）が挙げられる。

英米法のディスカバリは、正式審理（trial）に先立ち、訴訟当事者が自己の保有する訴訟関連情報を相手方に開示する手続である。なかでも、米国ディスカバリ（米国の法令または規則に基づくディスカバリ手続をいう。以下同じ。）は、その対象範囲の広さゆえに、「リベラルで当事者主導の米国ディスカバリは、世界でも独特なものである」と評されている[239]。米国ディスカバリは、紙媒体の文書のみならず、デジタルデータ等の電子保存情報（Electronically Stored Information: ESI）も対象とする。情報通信技術の発展により、物理的に国境を越えずに、他国に存在するデータにアクセスすることができるようになったことから、そのようなデータにも米国ディスカバリが越境的に適用されるようになった。そして、米国外の企業等も、迅速な証拠収集を求めて米国ディスカバリを利用するようになり、ディスカバリの越境的適用が拡大した。

---

[236] Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (adopted 18 March 1970), Hague Conference on Private International Law. https://www.hcch.net/en/instruments/conventions/full-text/?cid=82

[237] Hague Conference on Private International Law, Status Table — Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters (last updated 24 July 2025). https://www.hcch.net/en/instruments/conventions/status-table/?cid=82

[238] United States Department of Justice, CCIPS (2008), Section II.B.3.b, p. 4; Swire and Hemmings (2017), pp. 696-700, 704-705; New York City Bar Association, E-Discovery Working Group (2020), Introduction and section II (Common Circumstances Triggering Cross-Border Discovery in New York).

[239] Harkness et al. (2015), p. 1.

ディスカバリの越境的適用は、米国裁判所の命令に基づき他国に所在する証拠（データ）の提出（開示）を強制するという点において、国家の法的権限が国外の民間主体に直接及ぶという構造をなす。この特徴は、行政府によるガバメントアクセスと共通し、国外データへの国家権限の行使という制度的性質を備えており、越境的データガバナンスにおける主権衝突や法制度間の矛盾を顕在化させる。米国法が他国に保存されたデータに適用される際、他国のデータ関連規制（データローカライゼーションなど）やデータ越境移転規制における義務との非両立による「衝突（conflict of laws）」が発生し、ディスカバリの越境的適用に関する紛争が頻発することから、米国裁判例が蓄積されている。いずれにせよ、米国外に保存されたデータに対してディスカバリの越境的適用が認められる以上、この制度は越境的データガバナンスに重大な影響を及ぼし得るものである[240]。

本章では、まず第 1 節で米国ディスカバリの越境的適用の二つの類型を概観し、次いで第 2 節でディスカバリの越境的適用の主な問題点を検討する。さらに、第 3 節ではディスカバリの越境的適用と他国法令の衝突に関する米国裁判例を検討し、第 4 節でディスカバリの越境的適用の拡大と比例原則について分析する。その上で、第 5 節でディスカバリの越境的適用とデータガバナンス規範再構成の方向性を提示する。

[240] Zambrano (2016), pp. 167–180, 194–199.

第 1 節　米国ディスカバリの越境的適用の二つの類型

米国ディスカバリは、連邦民事訴訟規則（Federal Rules of Civil Procedure）（以下「FRCP」という。）第 26 条から第 37 条に規定されており[241]、主として民事訴訟手続で用いられるが、連邦政府機関が利用する場合もある[242]。

米国ディスカバリの越境的適用には、大きく二つの類型がある。第一は、米国で提起された民事訴訟におけるディスカバリ（以下「米国訴訟におけるディスカバリ」という。）が、国境を越えて他国に存在する情報に及ぶ場合であり、第二は、米国の訴訟ではなく、米国外で係属する訴訟手続等において、米国ディスカバリの制度が利用される場合である。したがって、ディスカバリの越境的適用には、米国訴訟のみならず、米国外の訴訟等のために米国外に存在するデータを収集する場合も含まれる。

以下、この二つの類型に分けて、制度および重要裁判例を概観する。

第 1 項　米国訴訟におけるディスカバリの越境的適用

米国訴訟におけるディスカバリの越境的適用は、たとえば、米国企業が日本企業に対して米国で提起した訴訟のディスカバリにおいて、日本企業が日本で保有しているデータを米国企業に提供（開示）するという形態である。これにより、米国訴訟におけるディスカバリが国境を越えて日本に存在するデータに及ぶことになる。

FRCP 第 26 条(b)(1)は、ディスカバリの対象について、秘匿特権または開示禁止の対象となる事項を除き、当該訴訟における主張等に関連性を有する全ての情報が対象になり得ると規定している。そして米国裁判所は、その管轄下にある者（法人を含む。以下、管轄関係について同じ。）が他国に存在する情報を保有していると認められる場合には、当該情報について米国ディスカバリを適用することができるとしてきた。たとえば、1968 年の連邦巡回控訴裁判所（第 2 巡回区）の裁判例では、「米国外に存在するドキュメントを保有している者に対して連邦裁判所が人的裁判管轄を有している場合に、当該裁判所が当該ドキュメントの提供を命じる権限を行使し得るということは、もはや疑う余地のないことである。」と判示しており[243]、1960 年代までには、米国訴訟におけるディスカバリの越境的適用を認める考え方が実務において確立していたとされている[244]。

その後、情報通信技術の発展により、米国内に居住または存在する者（対象者）が米国外のデータに米国内からアクセスすることができるようになったが、そのような場合には当該対象者が当該データを保有していると認められて、米国訴訟におけるディスカバリの越境的適用が拡大した[245]。米国訴訟におけるディスカバリについては、ESI に対するディスカバリ（e ディスカバリ）

---

[241] 米国では州法に基づくディスカバリ制度も存在するが、本稿では FRCP に基づく連邦民事訴訟におけるディスカバリを検討の対象とする。

[242] たとえば、米国が当事者となる民事訴訟において、連邦政府機関は FRCP に基づくディスカバリ手続を私人と同様に利用することができる。United States v. Procter & Gamble Co., 356 U.S. 677, 682–683 (1958).

[243] United States v. First Nat'l City Bank, 396 F.2d 897, 900–901 (2d Cir. 1968).

[244] Zambrano (2016), pp. 164–167.

[245] Camden Iron & Metal, Inc. v. Marubeni America Corp., 138 F.R.D. 438 (D.N.J. 1991).

の拡大を不安視する意見も強くなったが[246]、2015 年 FRCP 改正では、FRCP 第 26 条(b)(1)の規定中に「当該事件における必要性との比例（proportional to the needs of the case）」を考慮しなければならないという趣旨の文言が挿入され、ディスカバリに関する一般的要件として比例原則が明示的に加えられた。この改正について、アドバイザリー委員会（Advisory Committee）の注釈（Notes）では、e ディスカバリの拡大に伴うディスカバリの量およびコストの増大を背景として、ディスカバリの範囲を事件の実質的必要性に照らして適切に制限し、その負担と費用を現実的な水準に調整することを目的とするものであると説明された[247]。

【参照条文】

連邦民事訴訟規則（Federal Rules of Civil Procedure: FRCP）

第 26 条(b)(1)（ディスカバリの許容範囲）

当事者は、秘匿特権又は開示禁止の対象とならない限り、当該事件の主張又は抗弁に関連し、かつ当該事件における必要性との比例（proportional to the needs of the case）を踏まえて許容される事項について、ディスカバリを行うことができる。かかる比例の判断に当たっては、事件の重要性、争点の金額的価値、当事者の相対的アクセスの可能性、当事者の資源、争点の解決に対するディスカバリの重要性、ならびに負担又は費用がその利益に優越するか否かを考慮するものとする。関連性のある事項は必ずしも訴訟における証拠能力を有する必要はない。

第 2 項　米国外の訴訟等のためのディスカバリ（1782 条ディスカバリ）

(1)　1782 条ディスカバリの概要

米国外の訴訟等について米国ディスカバリを利用することができるという制度は、合衆国法典 28 編第 1782 条（28 U.S.C. § 1782）（以下「1782 条」という。）に規定されており、一般に「1782 条ディスカバリ」（Section 1782 Discovery）と呼ばれている。

1782 条ディスカバリの原型は、1855 年の立法によって連邦裁判所が他国の裁判所等からの嘱託書（letter rogatory）に応じて証人尋問を実施することが認められたことに始まる[248]。その後、1948 年に 1782 条が制定され、数次の改正を経て、1964 年改正で現在の条文に近い形となった。1782 条の立法目的は、①国際的な訴訟の当事者等に対して米国連邦裁判所による効率的な方法の支援を提供すること、②米国が他国に例を示すことによって当該他国から同様の支援が米国裁判所に提供されることを促すことの二つであるとされている[249]。

1782 条に明示的に規定されている主な要件（以下「1782 条の法定要件」という。）は、①対象者が米国内（連邦地方裁判所の管轄地域内）に居住しまたは存在すること、②他国または国際的な審決機関における手続で使用するためであること、③申立てによる場合には、申立人が利

[246] Advisory Committee on Civil Rules (2006) Report of the Civil Rules Advisory Committee (June 2006). Judicial Conference of the United States. https://www.uscourts.gov/sites/default/files/fr_import/CV06-2006.pdf; The Sedona Conference (2018), pp. 65-69, 93-108.

[247] Supreme Court of the United States (2015) Federal Rules of Civil Procedure, Rule 26, Advisory Committee Notes to 2015 Amendment.

[248] Cavanagh (2021), pp. 86-88.

[249] In re Application of Malev Hungarian Airlines, 964 F.2d 97, 100 (2d Cir. 1992).

害関係者であることの三つである。日本での訴訟の当事者の双方が日本企業であっても 1782 条ディスカバリを利用することができる。たとえば、中国企業の間における中国での訴訟について、米国関連会社に対する 1782 条ディスカバリが認められた裁判例がある[250]。

1782 条ディスカバリの例としては、日本において外国企業が日本企業に対して訴訟を提起し、その訴訟について米国ディスカバリを利用するという形態が考えられる。この場合、日本にはディスカバリ制度が存在しないため、外国企業は日本の訴訟手続では日本企業が保有している情報の提供（開示）を受けることはできない。しかし、最近では、日本企業（親会社）とその米国子会社等との間で業務に関するデータが日常的に送受信され（またはクラウドに保存されたデータにアクセスすることにより）、米国子会社等が親会社のデータ（と同一内容のデータ）を保有していることも少なくない。その場合、米国子会社等に対する 1782 条ディスカバリを実施すれば、米国子会社等が保有している親会社のデータについて提供（開示）を受けることができる[251]。

【参照条文】

合衆国法典 28 編 1782 条（28 U.S.C. § 1782）

連邦地方裁判所は、その管轄地域内に居住し又は存在する者に対し、他国の又は国際的な審決機関（tribunals）の手続（正式な起訴前に実施される刑事事件の捜査を含む。）で用いるため、証言若しくは供述又は文書その他の物の提供を命じることができる。この命令は、他国の若しくは国際的な審決機関による嘱託書（letter rogatory）若しくは請求(request)、又は利害関係者の申立てにより発することができ、証言又は陳述を与えること、あるいは文書その他の物件を提出することを、裁判所が任命した者の前で行うよう指示することができる。

（中略）

裁判所が命令により別段の定めをしない限り、連邦民事訴訟規則に従い、証言又は陳述は取得され、文書その他の物件は提出されるものとする。いかなる者も、法的に適用される特権に違反して証言若しくは陳述を行い、又は文書その他の物件を提出することを強制されない。

(2)　インテル裁判

1782 条ディスカバリに関する米国裁判におけるリーディングケースは、2004 年の連邦最高裁判所のインテル裁判[252]である。インテル裁判は、1782 条の法定要件について広い解釈を示しつつ、それらの要件を満たしている場合でも、1782 条ディスカバリを認めるかどうかについては、連邦地方裁判所が裁量権を有しているとし、その裁量権を行使するに当たっての 4 つの考慮要素を示した（表 7 参照）。

1782 条の法定要件およびインテル裁判を踏まえると、1782 条ディスカバリについては、①訴訟以外の行政審判や準司法手続、さらには刑事事件の捜査についても申立てができること、②訴訟提起前でも申立てができること、③訴訟当事者でなくても利害関係者であれば申立てができることなどの点で、米国訴訟におけるディスカバリよりも広い範囲で申立てをすることができる

[250] In re Application of TPK Touch Solutions (Xiamen), Inc., 2016 U.S. Dist. LEXIS 159681 (N.D. Cal. 2016).
[251] Marubeni Am. Corp. v. LBA Y.K., 335 Fed. Appx. 95, 97-98, 2009 U.S. App. LEXIS 12953 (2d Cir. 2009).
[252] Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241 (2004) [hereinafter cited as Intel].

ことになる。また、1782 条ディスカバリについては、同様の事案で米国訴訟におけるディスカバリが認められることは要件としないとされており[253]、米国訴訟におけるディスカバリが認められないような事案でも1782 条ディスカバリが認められることがある。現に、インテル裁判では、インテル社が、本件は米国訴訟におけるディスカバリが認められない事案であると主張したが、その主張は認められなかった。

なお、1782 条ディスカバリについても、その適用がひとたび認められれば、その後の手続は FRCP の規定が適用され[254]、裁判所の特段の命令がない限り、FRCP 第 26 条その他の FRCP の関係規定が適用される[255]。

【表 7:インテル裁判の概要】

インテル裁判の概要

Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241 (2004)

本件の背景となる米国外手続は、Advanced Micro Devices, Inc.（以下「AMD 社」という。）が、Intel Corp.（以下「インテル社」という。）による欧州競争法違反を主張して、欧州委員会（EC）競争総局（DG-Competition）に提出した Antitrust Complaint である。当該手続は、日本の公正取引委員会の審査手続に類似する行政委員会型の準司法手続に該当する。AMD 社は、インテル社に対して関係資料の提出命令を出すべきであると主張したが、EC 競争総局はこれを認めなかった。そのため、AMD 社は、当該資料の提供を求めて、米国連邦地方裁判所（カリフォルニア北部地区）に 1782 条ディスカバリの申立てを行った。同地方裁判所は、EC 競争総局の Antitrust Complaint の手続には 1782 条は適用されないとの理由で申立てを却下したが、控訴審である連邦巡回控訴裁判所（第 9 巡回区）はこれを差し戻したため、インテル社が連邦最高裁判所に上告した。

連邦最高裁判所はまず、1782 条の法定要件について、以下のとおり広範な解釈を示した。すなわち、①1782 条ディスカバリの前提となる手続には行政審判機関や準司法機関の手続も含まれること、②米国外手続が「係属中(pending)」である必要はなく、合理的に予見可能な手続（within reasonable contemplation）も含むこと、③対象資料が当該外国手続での証拠開示対象となり得ることは要件としないこと、④1782 条ディスカバリの申立てができる「利害関係者（interested person）」は、当該外国手続の当事者に限定されず、当該手続に実質的利害を有する者を含むこと、である。さらに、連邦最高裁判所は、1782 条の法定要件を充足する場合であっても、連邦地方裁判所はディスカバリ命令の発令について裁量を有しているとし、その裁量判断における考慮要素として、①対象者が外国手続の当事者であるか否か（当事者でない場合にはディスカバリを認める方向に働く）、②申立ての基礎となる外国手続の性質（得られた証拠が外国手続で利用可能か）、③外国手続における証拠収集制限を回避しようとする意図の有無、④対象者に課される負担の程度、の四点を挙げた。そのうえで、控訴審判決（差戻しの判断）を是認し、事件を連邦地方裁判所に差し戻す旨を命じた。

[253] Intel, at 263.
[254] 28 U.S.C. § 1782 (a).
[255] Heraeus Kulzer GmbH v. Biomet Inc., 633 F.3d 591, 595, 2011 U.S. App. LEXIS 1389 (7th Cir. 2011).

(3)　1782 条ディスカバリの越境的適用

近年では、1782 条ディスカバリについても、一定の場合には越境的適用が認められるようになった。連邦巡回控訴裁判所のレベルでは、2016 年の第 11 巡回区の裁判例[256]や 2019 年の第 2 巡回区の裁判例[257]において、「対象となるドキュメントや電子保存情報が他国に存在するという事実は、それ自体で(per se)、1782 条ディスカバリの適用を妨げるものではない」と判示され、米国外に存在する情報についても 1782 条ディスカバリの適用が肯定された。これらの裁判例は、米国外で係属する訴訟等のための 1782 条ディスカバリが、米国内に所在する対象者を介して、再度国境を越え、米国外に存在する情報に及び得ることを示している。もっとも、連邦地方裁判所のレベルでは、テキサス州などにおいて同様に越境的適用を認めた裁判例[258]が見られる一方、他の裁判所においては、ディスカバリ対象情報の大部分が米国外に存在すること等を理由として、裁量により越境的適用を認めなかった裁判例[259]も存在する。

[256] Sergeeva v. Tripleton Int'l Ltd., 834 F.3d 1194, 1198-1200 (11th Cir. 2016).
[257] In re del Valle Ruiz, 939 F.3d 520, 532-533 (2d Cir. 2019).
[258] In re Oasis Focus Fund LP, 2023 U.S. Dist. LEXIS 171930 (W.D. Tex. 2023).
[259] In re Judicial Assistance Pursuant to 28 U.S.C. § 1782 by Macquarie Bank Ltd., 2015 U.S. Dist. LEXIS 72544 (D. Nev. 2015).

第 2 節　ディスカバリの越境的適用の主な問題点

米国ディスカバリの越境的適用については、米国訴訟におけるディスカバリの問題点が米国内だけではなく他国の訴訟当事者等にも波及する点が問題となるほか、他国法令との衝突も問題となり得る。

第 1 項　米国訴訟におけるディスカバリの問題点の他国への波及

米国訴訟におけるディスカバリについては、次のような問題点が指摘されてきた。すなわち、①対象範囲が広範で情報入手の手段として利用されるおそれがあること、②重要情報流出のおそれがあること、③厳格な制裁措置によりディスカバリが強制され得ること、などである。そして、これらの問題点は、越境的適用によって米国外の企業や個人にも波及し得る[260]。

また、1782 条ディスカバリは米国外の訴訟等を対象とする制度であるが、1782 条に基づく申立てが認容されてディスカバリの実施が許可された場合、その後の具体的な手続は、米国訴訟におけるディスカバリと同様に FRCP の規定に従って行われる[261]。したがって、①～③のような米国訴訟におけるディスカバリの制度的問題点は、1782 条ディスカバリを通じて他国の企業・個人に波及し得る。

以下では、そのような米国訴訟におけるディスカバリの問題点を整理する。併せて、1782 条ディスカバリには事前の反論の機会が制度的に保障されていないことについても、越境的適用の問題点として指摘する。

(1)　対象範囲が広範で情報入手の手段として利用されるおそれがあること

米国ディスカバリでは、弁護士依頼者間秘匿特権などの秘匿特権の対象となるものを除き、当該訴訟における主張と関連性を有する全ての情報が提供（開示）の対象になり得る（FRCP 第 26 条(b)(1)）。したがって、その対象は広範囲に及び、企業の営業秘密（trade secret）や個人情報等の重要情報も対象になる。たとえば、コカ・コーラの「完全な製法（complete formula）」という極めて機密性の高い企業秘密についてディスカバリが認められた裁判例もある[262]。また、個人情報との関係でも、米国裁判所は、GDPR による規制を理由とするディスカバリの拒否を認めず、EU 居住者の個人情報を対象とするディスカバリを命じてきた（後記第 3 節参照）。このように、米国ディスカバリの対象の範囲は広く、競争関係にある企業間の訴訟において、自社の企業秘密を相手方企業に開示するよう命じられることもあり、ディスカバリの対象とされるだけで業務上の不利益を被るおそれがある。

さらに、米国ディスカバリは、「証拠漁り（fishing expedition）」に利用されるおそれもある。たとえば、相手方を訴える根拠となる証拠を有していないにもかかわらず訴訟を提起し、ディスカバ

---

[260] 片岡弘（2024）94-101 頁.

[261] 1782 条（28 U.S.C. § 1782(a)）は、裁判所が特段の手続を定めない限り、情報の開示等は FRCP に従って行われる旨を定めている。FRCP 第 26 条ないし第 37 条は、米国訴訟におけるディスカバリ手続を規定しており、1782 条ディスカバリにも適用される。

[262] Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 1985 U.S. Dist. LEXIS 16644 (D. Del. 1985).

リを申し立てることで、相手方の保有する情報の中から自分に有利な証拠を入手するといったことが考えられる。企業間の訴訟では、相手方企業の保有する秘密情報をディスカバリで入手することを目的として（名目的に）訴訟を提起するという戦略に用いられる場合もある。したがって、「証拠漁り」は、訴訟上の証拠収集を目的とする場合に限られず、競争関係にある企業の秘密情報を得ること、あるいは和解金の獲得を目的とする場合も含まれる[263]。

米国裁判例においても、ディスカバリが“fishing expedition”に利用されることが問題視されてきた[264]。しかし、どのような場合がそれに該当するのかについては必ずしも明らかではなく、ディスカバリの要否を決定する判断基準として用いることは困難である。Thornburg（2006）は、ディスカバリは“fishing expedition”そのものであると述べ、裁判所が“fishing expedition”という用語を消極的な判断の理由づけのために安易に使用することについて疑問を呈している[265]。いずれにせよ、米国ディスカバリが、相手方当事者等の保有する重要情報（企業秘密等）を入手する手段として利用されるおそれがあることは確かである。

(2)　重要情報流出のおそれがあること

米国ディスカバリの対象が企業秘密等の重要情報に及ぶ場合には、裁判所において、当該情報を保護するための保護命令（protective order）を発することができる[266]。保護命令の具体的内容は、裁判所の裁量によって決められるが、競争関係にある企業間等の訴訟において機密性が極めて高い情報がディスカバリの対象になる場合には、“Attorneys Eyes Only”（弁護士のみ閲覧が可能という扱い。以下「AEO」という。）として相手方当事者には閲覧させない措置が命じられる。他方、保護命令が発せられていない場合には、訴訟当事者がディスカバリで得た情報については、「適切と思われる方法で他へ提供することができる」とされており[267]、ディスカバリの対象となった企業秘密等の重要情報が外部の第三者に提供されて流出するおそれがある。

近年では、保護命令の内容として AEO を用いる事例が増加しており、たとえば、競争関係にある企業間の訴訟において、開示側当事者が企業秘密である自社製品のソースコードを相手方に開示するに当たり、秘密保護のための措置として AEO では不十分であると主張したものの、裁判所が AEO で足りるとした裁判例もある[268]。また、1782 条ディスカバリにおいても、保護命令の内容が問題となり、AEO が命じられた裁判例がある[269]。しかし、保護命令違反行為が第三者による厳しい目で監視されているわけではなく、違反行為があったとしても相手方には容易には分からないことなどを踏まえると、AEO が秘密保護の措置として常に十分であるかについては検討の余地がある。しかも、訴訟への対応方針については、弁護士はクライアントと相談するのが通常であることから、ディスカバリの対象物やデータそのものが相手方当事者に渡されないとしても、その内容が相手方当事者に伝わるおそれを完全に排除することはできない。

さらに、保護命令が発せられても、違反行為に対して科される制裁が主として金銭的制裁しかなく、故意の情報流出行為等を阻止するには十分とはいえない。実際に、訴訟当事者や弁護

[263] Thornburg (2006), pp. 1-11, 27-36.
[264] Hofer v. Mack Trucks, Inc., 981 F.2d 377, 380-381 (8th Cir. 1992).
[265] Thornburg (2006), pp. 1-6.
[266] FRCP26(c).
[267] Jepson Inc v Makita Elec Works, 30 F.3d 854, 857 (7th Cir. 1994).
[268] Superior Edge Inc v Monsanto Co, 2014 US Dist LEXIS 173426 (D. Minn. 2014).
[269] AIS GmbH Aachen Innovative Sols v Thoratec LLC, 2021 US Dist LEXIS 17744 (N.D. Cal. 2021).

士による保護命令違反に関連する裁判例が少なくない。これらの裁判例には、訴訟当事者が保護命令に違反してディスカバリの対象となった秘密情報を流出させた事例[270]や、弁護士がディスカバリで開示を受けた情報を保護命令に違反して知り合いの弁護士に漏らし、その弁護士が当該情報を他の訴訟で使用しようとして発覚した事例[271]などが含まれている。加えて、2022 年には、ニューヨークの大手法律事務所に所属する幹部弁護士らが、国際テロ事件訴訟の関係で保護命令の対象とされていた高度な機密情報（サウジアラビア高官の証言記録など）を、数年間にわたり記者に漏えいしていた事実が発覚し、裁判所は同事務所および関係弁護士に対して制裁措置を課した[272]。

近年において米国ディスカバリの越境的適用が増加していることに加え、明るみに出た事例のほかにも未発覚の情報流出事案が存在すると考えられる状況を踏まえると、米国ディスカバリの越境的適用が拡大するなかで、重要情報（企業秘密等）の流出リスクは相対的に高まっているということができる。

(3)　厳格な制裁措置によりディスカバリが強制され得ること

米国裁判所は、対象者がディスカバリ命令に従わない場合に、厳しい制裁措置を課してきた。制裁措置の内容には、敗訴判決、訴訟の打切り、制裁金の賦課、関連証拠の使用制限、さらには相手方当事者の主張を認めたものとみなす措置などが含まれる（FRCP 第 37 条(b)(2)）。

訴訟外の第三者を対象とするディスカバリにおいても対象者に厳格な制裁が課されることがあり、たとえば、米国訴訟の当事者ではない中国銀行に対し、中国国内で管理する口座情報の開示が命じられ、同行が中国法上の守秘義務を理由に拒否したところ、連邦地方裁判所が民事法廷侮辱を認定し、命令に従うまで1日当たり 5 万ドルの制裁金を課した裁判例がある[273]。

1782 条ディスカバリにおいても厳格な制裁が課されることがあり、たとえば、ロシアでの訴訟に関し、フロリダに所在する企業が米国外に保有する情報のディスカバリ命令に応じなかったため、連邦地方裁判所が民事法廷侮辱を認定し、弁護士費用およびコストの支払を命じ、加えて命令に従うまで 1 日あたり 500 ドルの制裁金を支払うことを命じた裁判例がある[274]。

このように、米国ディスカバリの対象者が命令に従わない場合には厳しい制裁措置が課され得るが、米国外で保有されている情報の開示を制裁によって強制することについては、当該情報が所在する国の主権を侵害するおそれがあると批判されてきた[275]。

(4)　1782 条ディスカバリには事前の反論の機会が制度的に保障されていないこと

1782 条ディスカバリの申立ては、一般的に ex parte で行われる[276]。この ex parte とは、相手方に通知しない申立てを意味し、申立てが行われても、米国外で進行している訴訟等の相手方当事者や当該訴訟が係属する他国裁判所には通知されない。そして、申立てが認められて召

[270] Sciara v. Campbell, 2022 U.S. Dist. LEXIS 204019 (D. Nev. 2022).
[271] SIMO Holdings Inc. v. H.K. uCloudlink Network Tech. Ltd., 2020 U.S. Dist. LEXIS 230317 (S.D.N.Y. 2020).
[272] In re September, 2022 U.S. Dist. LEXIS 182536 (S.D.N.Y. 2022).
[273] Tiffany (NJ) LLC v. China Merchants Bank & Bank of China, 2015 U.S. Dist. LEXIS 128570 (S.D.N.Y. 2015).
[274] Sergeeva v. Tripleton International Ltd., 834 F.3d 1194 (11th Cir. 2016).
[275] Curran (2016), pp. 1141–1149.
[276] Harkness et al. (2015), pp. 38–40.

喚状（subpoena）が発付された段階になって初めて、ディスカバリ対象者がその事実を知り、異議がある場合には異議申立てを行うことになる。

しかも、1782 条ディスカバリを認めるか否かについては連邦地方裁判所に広い裁量が認められているため、異議申立て段階では、対象者は連邦地方裁判所の判断に裁量権の濫用があったことを立証しなければならず、ディスカバリ命令が出された時点では、対象者にとって反証のハードルが極めて高くなっている。さらに、米国外での訴訟等の相手方当事者は、1782 条ディスカバリの申立て手続に当事者として参加することができず、場合によっては、ディスカバリが実施された後に、米国外の訴訟手続の中でその違法性や不当性を主張して争うほかない。このように、1782 条ディスカバリについては、その妥当性等を事前に争う機会が制度的に保障されておらず、事後的に争う仕組みにとどまっているうえ、発出済みのディスカバリ命令について争う際の反証負担も極めて重い。

1782 条ディスカバリで ex parte による申立てが認められる点については、米国の研究者からも批判が示されている。たとえば、Cavanagh（2021）は、1782 条ディスカバリの申立てを ex parte で行うことを認めないこととし、他国裁判所や相手方当事者への通知を義務化することなどを提言している[277]。

第 2 項　他国の主権や法令との衝突

米国ディスカバリの越境的適用は、米国裁判所の開示命令が米国外に所在する情報や文書に及ぶものである。その結果、米国裁判所の命令は、当該情報が所在する国の主権的統制と緊張関係を生じさせ、当該他国の法秩序と衝突する可能性を内包している[278]。米国ディスカバリの越境的適用は、以下のような形で、国家間等の制度的緊張として顕在化しやすい。

第一に、領域主権との衝突が生じる。国外所在データの開示命令は、他国の主権的統治領域に対する法的介入と捉えられ得る。保護対象情報が個人データや安全保障情報である場合、所在国は自国法令の優越性が損なわれると懸念し、制度的摩擦が高まる[279]。

第二に、他国法令との抵触が生じる。GDPR、諸外国のブロッキング法（後記第 3 節参照）、中国のデータ法制など、域外移転やアクセス要件に厳格な規制を課す法体系は、米国ディスカバリの広範な適用と容易に整合しない。企業は米国法と所在国法との相反する法的要求の狭間に置かれ、いずれに違反しても重大なリスクを負うことになる[280]。

第三に、クラウドや分散処理環境の普及により、データの所在地が特定困難となる現代的状況が問題を複雑化させている。複数法域にまたがる保存構造の下では、米国裁判所が国外データを対象とするハードルが一層低下し、越境的開示の機会が増大する[281]。

第四に、多国籍企業に対するコンプライアンス負担と経済的影響の増大である。米国ディスカバリが国外所在データにも及ぶ場合、企業は広範な探索・保全・審査を行うだけでなく、所在国法令との抵触を回避するために追加的な管理体制や技術的措置を講じる必要が生じる。このよ

---

277 Cavanagh (2021), pp. 100–108.
278 Jackson (2003), pp. 782–791; Curran (2016), pp. 1141–1149.
279 Curran (2016), pp. 1141–1149.
280 Kuner (2015), pp. 235–241.
281 Brupbacher (2019), pp. 1–3.

うな重層的対応は運用コストを引き上げ、越境的データ処理の予見可能性を低下させ、国際的データガバナンスの分断を助長する要因となる[282]。

総じて、米国ディスカバリの越境的適用は、他国の主権的統制との衝突、他国法令との整合性、越境的データ移転の安定性、そして制度的信頼性に深刻な摩擦を生じさせる構造を有している[283]。国外所在データへの一方的アクセスが慣行化すれば、米国の手続的要請が他国の規制体系に実質的に優越する状態を生じさせ、主権平等原則との緊張関係を一層高める。この構造は、越境的データガバナンスにおける制度的非対称性を拡大させる要因となる。

[282] Brupbacher (2019), pp. 1–3; Belt (2024), sections “Regulatory Environment,” and “Jurisdictional Issues.”
[283] 片岡弘（2024）94–104 頁.

第 3 節　ディスカバリの越境的適用と他国法令との衝突に関する米国裁判例

米国ディスカバリの越境的適用に対処するための諸外国における立法的対応としては、ハーグ証拠条約による米国ディスカバリの実施拒否の宣言（それに伴う国内法の整備）やブロッキング法の制定などが行われてきた。

ハーグ証拠条約は、大陸法系諸国がコモンロー諸国のディスカバリの越境的適用への不安を抱いていたことなどを考慮し、その第 23 条において、「ドキュメントについてコモンロー諸国のディスカバリ（pre-trial discovery）のために発せられた請求書（Letter of Request）を実施しない旨の宣言をすることができる」と規定している[284]。その結果、国際私法ハーグ会議（Hague Conference on Private International Law: HCCH）の資料によれば、2025 年 11 月時点で、加盟国 69 か国中 51 か国が第 23 条に基づいて何らかの宣言を行っている[285]。なかでも、米国と同じコモンローの国であるイギリスは、1976 年に同条約を批准したが、米国ディスカバリのイギリス国内への越境的適用に対処するため、同条に基づいて、「ドキュメントについてディスカバリのために発せられた請求書を実施しない」旨を宣言している[286]。

また、米国ディスカバリの越境的適用を制限ないし阻止するため、ブロッキング法（blocking statute）やデータ保護法（data protecting law）などを制定した国もある。ブロッキング法とは、自国の領域内で他国の法律が適用されることを阻止する法律の総称であるが、越境的証拠収集の文脈では、米国ディスカバリの自国への適用を阻止する趣旨を定めた法律を意味し、これまでに少なくとも 15 か国で制定されている[287]。また、個人情報など一定の分野の情報が国外に流出することを防止するため、そのような情報を国外に流出させた者に対して刑事罰を科す規定を盛り込んだデータ保護法を制定した国もあり（中国 DSL 第 36 条および PIPL 第 41 条後段：前記第 4 章第 1 節参照）、ディスカバリの越境的適用を制限する効果が見込まれている。

最近では、諸外国において越境的データ移転制限を伴うデータローカライゼーションなどのデータ保護措置が拡大しており（前記第 4 章参照）、そのような措置と米国ディスカバリの越境的適用との「衝突」が問題となる事例も発生している。すなわち、米国外に保存されているデータへの米国ディスカバリの越境的適用に対し、当該データが保存されている国のデータ保護法令を理由に米国ディスカバリに応じることを拒否することができるかという形で争いとなる。そのような事例については、GDPR や「中国データ三法」との関係で米国裁判例が蓄積されつつある。今後は、その他の国の法令との「衝突」も問題となり得る。

---

[284] ハーグ証拠条約第 23 条; Amram (1970), pp. 3-4.

[285] Hague Conference on Private International Law (2024) Table reflecting the applicability of Article 23 (Pre-Trial Discovery of Documents), Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, July 2024. https://assets.hcch.net/docs/3b290a7b-3885-4481-86c5-f8289f4ee759.pdf (accessed 22 February 2026).

[286] United Kingdom of Great Britain and Northern Ireland (2025) Declarations, notifications and reservations under the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters. Hague Conference on Private International Law. https://www.hcch.net/en/instruments/conventions/status-table/notifications/?csid=564&disp=resdn (accessed 22 February 2026).

[287] Hoda（2018）, p. 232-240, 251-254（ブロッキング法を制定した国として、フランス, スペイン, スイス, メキシコ, エクアドル, ウルグアイ, チリ, 南アフリカ, 中国, マレーシア, シンガポール, UAE, ヨルダン, レバノン, イスラエル, ケイマン諸島などが挙げられている）.

第 1 項　米国連邦最高裁判所のリーディングケース（アエロスパシアル裁判）

米国ディスカバリと他国法令との適用関係に関する代表的判例は、1987 年の連邦最高裁判所のアエロスパシアル裁判[288]である。この裁判では、米国ディスカバリの越境的適用とハーグ証拠条約およびフランスのブロッキング法との関係が問題となった（表 8 参照）。欧州の数か国が連邦最高裁判所に意見書（amicus curiae brief）を提出し[289]、フランス、ドイツおよびスイスはハーグ証拠条約の排他性（国内法の適用を排除すること）を主張し、イギリスはハーグ証拠条約の優位性（国内法よりも優先して適用されること）を主張したが、これに対して、米国連邦政府も意見書を提出して反論した（排他性および優位性の両方を否定した。）[290]。連邦最高裁判所は、排他性については全員一致の判断で否定し、優位性については 5 対 4 の僅差で否定した[291]。このように、連邦最高裁判所は、ハーグ証拠条約は米国ディスカバリに優先するものではなく、米国ディスカバリよりも先に同条約による手続を履行しなければならないわけではないとした[292]。

また、この裁判で、連邦最高裁判所は、フランスのブロッキング法との関係について、「米国裁判所は、その管轄下にある者に対して証拠の提供を命じる権限を有しており、たとえ当該提供行為が他国の法令に違反する可能性があるとしても、外国法令は米国裁判所の権限を排除するものではない」旨の考え方（以下、この論旨を「アエロスパシアル裁判の論理」という。）を示し[293]、米国ディスカバリの適用が他国で制定されたブロッキング法などに抵触する場合でも、米国裁判所は当該他国に存在する情報を対象とするディスカバリを命ずることができる旨判示した。ただし、ここでは外国法令の適用を全面的に否定したわけではなく、米国ディスカバリの越境的適用の可否の判断に当たっては、国際礼譲分析（comity analysis）を行うとして、五つの考慮要素（以下「アエロスパシアル・ファクターズ」という。）を示した[294]。なお、米国ディスカバリの越境的適用が認められるためには、アエロスパシアル・ファクターズの全てを満たしていなければならないわけではなく、総合的に判断するものとされている[295]。

【表 8：アエロスパシアル裁判の概要】

アエロスパシアル裁判の概要
Société Nationale Industrielle Aérospatiale v. United States District Court for the S. Dist. of Iowa, 482 U.S. 522 (1987) 米国内で発生した航空機墜落事故をめぐる損害賠償請求訴訟において、フランス国営企業（航空機の製造・販売会社）である被告会社（Société Nationale Industrielle Aérospatiale）が人的裁判管轄について異議を述べることなく連邦地方裁判所（アイオワ南部地区）で応訴したものの、ディスカバリ

[288] Société Nationale Industrielle Aérospatiale v. United States District Court for the S. Dist. of Iowa, 482 U.S. 522 (1987) [hereinafter Aérospatiale].
[289] Brief for the Republic of France as Amicus Curiae; Brief for the Government of the United Kingdom and Northern Ireland as Amicus Curiae; Brief for the Federal Republic of Germany as Amicus Curiae; Brief for the Government of Switzerland as Amicus Curiae.
[290] Brief for the United States and the Securities and Exchange Commission as Amicus Curiae.
[291] Aérospatiale, at 529–544.
[292] Aérospatiale, at 536–540.
[293] Aérospatiale, at 544, n. 29.
[294] Aérospatiale, at 544, n. 28.
[295] In re Rubber Chems. Antitrust Litig., 486 F. Supp. 2d 1078, 1082 (N.D. Cal. 2007).

の対象がフランス国内で同社が保有する情報に及ぶと、当該情報はハーグ証拠条約の手続によってのみ取得されるべきであり、フランスのブロッキング法の規定により米国ディスカバリには応じられないと主張した。地方裁判所が被告会社の異議を退けてディスカバリを命じたため、被告会社が控訴したが、連邦巡回控訴裁判所（第 8 巡回区）が被告会社の控訴を棄却したため、被告会社が連邦最高裁判所に上告した。

連邦最高裁判所は、ハーグ証拠条約は、他国で証拠を収集するための選択的な（optional）手続を定めたものであり、加盟国の国内法を変更したり、特定の手続の採用や国内手続の変更を加盟国に強制したりするものではないとし、米国での訴訟の当事者が FRCP に基づいて国外情報のディスカバリを求める場合にも、同条約の手続を先に履行する義務はないと判示した。

さらに、フランスのブロッキング法との関係について、「米国裁判所は、その管轄下にある訴訟当事者に対して証拠の提出を命じる権限を有しており、たとえその提出行為が他国の法律に違反することになろうとも、当該法律によって米国裁判所の権限が奪われることはない」とした上で、米国対外関係法リステイトメント（Restatement (Revised)）[296]を引用し、米国ディスカバリの越境的適用の可否を判断するために国際礼譲分析（comity analysis）を行うべきであるとして、①対象情報の重要性、②請求の具体性、③情報の米国起源の有無、④代替手段の利用可能性、⑤米国及び他国の利益の比較衡量、という五つの要素を示した。本件法廷意見は 5 対 4 の僅差であったが、連邦最高裁判所は、控訴審判決を破棄し、これらの国際礼譲分析の要素を適切に考慮してディスカバリの可否を再判断させるため、審理を連邦地方裁判所へ差し戻した。

アエロスパシアル・ファクターズの五番目の考慮要素は、米国ディスカバリに応じない場合に米国の重要利益がどの程度害されるかと、米国ディスカバリに応じた場合に対象情報が所在する国の重要利益がどの程度害されるかを比較し、いずれをより重視すべきかを判断するための比較衡量を求めるものであり、五つの要素のなかでも実務上最も重視されてきた要素である[297]。この要素を中心に、アエロスパシアル裁判後の下級審裁判では、アエロスパシアル・ファクターズによる国際礼譲分析（表 9 参照）が広く用いられ、一種の判例法としての役割を果たすに至っている。もっとも、これらの下級審裁判においては、アエロスパシアル・ファクターズの解釈・適用が米国ディスカバリの越境的適用を肯定しやすい方向にバイアスがかかった判断につながっていると指摘され[298]、その結果、米国ディスカバリの越境的適用が実質的に拡大され、現代型「法帝国主義（legal imperialism）」であるとの批判が生じている[299]

【表 9：国際礼譲（international comity）】

国際礼譲（international comity）

米国裁判で用いられてきた国際礼譲（international comity）の概念は、17 世紀のオランダの法学者 Ulrich Huber の記述を起源とし、英国を経て、米国に伝わったとされている[300]。米国連邦最高裁判所

[296] American Law Institute (1987) Restatement of the foreign relations law of the United States (revised), section 442(1)(a). American Law Institute, Philadelphia.
[297] Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1476 (9th Cir. 1992).
[298] Sant (2015), pp. 184–203, 213–227.
[299] Cavanagh (2021), pp. 92–95.
[300] Dodge (2015), pp. 2085–2088.

は、1895 年の Hilton v. Guyot において、「いかなる法律も、その権威が由来する主権の及ぶ範囲を超えては、それ自体の力ではいかなる効果も持たない。」として、厳格な属地主義の考え方を示した上で、国際礼譲について、「法的な意味では、絶対的な義務の問題でもなく、単なる礼儀や善意の問題でもない。しかし、それは、一つの国が、国際的な義務及び利便性、並びに自国民又は自国の法律の保護下にある他の人々の権利を適切に考慮しつつ、その領土内で、他国の立法上、行政上又は司法上の行為を許容するという認識をいう。」と判示した[301]。

当初、国際礼譲の概念は、米国裁判所が他国の法律や裁判を適用する根拠として機能したが、20 世紀前半になると、米国裁判所の裁判管轄（国家裁判権）についての考え方が厳格な属地主義から離れ始めたことにより、国際礼譲の概念は、米国法及び米国裁判権の越境的適用を制限するという新たな役割を与えられることになった[302]。そして、アエロスパシアル裁判では、米国ディスカバリの越境的適用の可否を検討するに当たって、国際礼譲分析（comity analysis）という考え方が用いられた。

第 2 項　GDPR と米国ディスカバリの越境的適用との関係

米国裁判所は、GDPR による規制と米国ディスカバリの越境的適用が問題となった事例の多くにおいて、GDPR による規制を理由とするディスカバリの拒否を認めず、EU 居住者の個人情報についてディスカバリを命じてきた。たとえば、2020 年の連邦地方裁判所（ニュージャージー）の裁判例[303]では、ディーゼル車の排出ガスに関連する消費者クラスアクションにおいて、ドイツ企業が保有する EU 居住者の個人情報の開示が求められた。同企業は、GDPR の規制に抵触するなどとして異議を唱えたが、同裁判所は「アエロスパシアル裁判の論理」を引用したうえで国際礼譲分析を実施し、米国の利益（米国の消費者保護の利益）が EU（ドイツ）の利益（EU 居住者の個人情報保護）を上回っているとして開示を命じた（表 10 参照）。

【表 10：ディスカバリの越境的適用と GDPR に関する裁判例】

ディスカバリの越境的適用と GDPR に関する裁判例

In re Mercedes-Benz Emissions Litig., 2020 U.S. Dist. LEXIS 15967 (D.N.J. 2020)

原告（個人）は、ドイツ企業である D 社（Daimler AG）等が製造・販売する自動車を購入したが、その広告に虚偽があったなどとして、D 社等に対する損害賠償請求訴訟を米国で提起した。そのディスカバリにおいて、原告が D 社に対し、関連情報を保有している可能性のある D 社従業員を特定するための情報（以下「本件従業員情報」という。）の提供（開示）を求めたが、D 社は、本件従業員情報のうち EU 居住者の個人情報に該当する部分を提供（開示）することは、GDPR の規制に抵触することになり、D 社に不当な負担を課すものであるなどとして反論した。

連邦地方裁判所（ニュージャージー）は、米国裁判所がその管轄下にある者に対して有する権限は他国の法律によって奪われることはないとしたうえで、本件従業員情報は本件訴訟において重要なもので、国際礼譲分析（comity analysis）によっても提供（開示）が相当であるとし、秘密保持につい

[301] Hilton v. Guyot, 159 U.S. 113, 163-164 (1895).
[302] Dodge (2015), pp. 2087-2095.
[303] In re Mercedes-Benz Emissions Litig., 2020 U.S. Dist. LEXIS 15967 (D.N.J. 2020).

ては保護命令（protective order）により“Highly Confidential”として取り扱うことができるなどとして、D社に対し、本件従業員情報の提供（開示）を命じた。

また、2022 年の連邦地方裁判所（テキサス東部地区）の裁判例[304]では、同裁判所が、「GDPR49(1)は、法的請求の理由づけ、申立てまたは防御のために必要な情報の提供を（域外移転禁止の）例外として規定している。」「同条についての EU 加盟国向けのガイドライン[305]でも、訴訟手続に関連する情報提供については、一定の場合に同条の例外に該当し得るとされている。」などと指摘し、「GDPR を主張するだけでは FRCP に規定されたディスカバリの義務を免れることはできない。」として、GDPR を理由として情報提供を拒否することは FRCP に基づくディスカバリ義務に反するとし、ドイツ企業がドイツ国内で保有している個人情報に該当するデータの提供（開示）を命じた。

第 3 項　中国データローカライゼーション措置と米国ディスカバリの越境的適用の関係

中国のデータローカライゼーション措置と米国ディスカバリの越境的適用との関係に関する米国裁判例については、二つのパターンに分けて考えることができる。第一は、米国裁判所において関連中国法を解釈し、当該中国法と米国ディスカバリの越境的適用との間に「衝突」は存在しないと認定して国際礼譲分析を回避するもので、この場合には、米国ディスカバリの適用要件を満たしているかという点に基づいて判断されることになる。第二は、関連中国法と米国ディスカバリの越境的適用とが「衝突」していると認定し、国際礼譲分析を実施するというものである。いずれのパターンでも、米国裁判所は、米国ディスカバリの越境的適用を認めている。

(1)　「衝突」は存在しないとされた裁判例

2022 年の連邦地方裁判所（イリノイ北部地区）の裁判例[306]では、中国 DSL 第 36 条後段および PIPL 第 41 条後段の規定（いずれも、中国国内で保存されているデータや個人情報について、「主管当局の許可を得ずに、他国の司法機関又は法執行機関に提供してはならない」旨を定めている。）について、それらの規定で禁止されているのは、他国の司法機関等の求めに応じて情報を提供することであるが、米国ディスカバリは訴訟当事者の間で情報をやり取りするものであり、司法機関等に情報を提供するものではないことから、それらの規定と米国ディスカバリとの「衝突」は存在しないとして、中国国内で保存されているデータや個人情報について米国ディスカバリの越境的適用を認めた。このような米国裁判所の一連の下級審裁判例における解釈によれば、DSL 第 36 条後段や PIPL41 条後段の規定は、米国ディスカバリに応じて提供される情報については適用されないことになる[307]。

[304] Arigna Tech. Ltd. v. Nissan Motor Co., Ltd., 2022 U.S. Dist. LEXIS 135245 (E.D. Tex. 2022).
[305] European Data Protection Board (2018) Guidelines 2/2018 on derogations of Article 49 under Regulation (EU) 2016/679, p. 11.
[306] Philips Med. Sys. (Cleveland), Inc. v. Buan, 2022 U.S. Dist. LEXIS 35635 (N.D. Ill. 2022).
[307] Intex Rec. Corp. v. Bestway (USA), Inc., 2023 U.S. Dist. LEXIS 194563 (C.D. Cal. 2023).

また、2023 年の連邦地方裁判所（ニューヨーク南部地区）の裁判例[308]では、中国 PIPL 第 13 条の規定（中国国内の個人情報について本人の同意を得ないで処理することができるという例外として、「法律」上の義務の履行などが規定されている。）について、同条の「法律」は、中国法に限られず、米国の法律も含むと解されることから、米国ディスカバリに応じることは同条の例外に該当し、PIPL の規定と米国ディスカバリとの「衝突」は存在しないとして、中国国内の個人情報について米国ディスカバリの越境的適用を認めた。このような解釈によれば、他の法律（中国以外の法律を含む。）で同様に規定されている場合にも、同じ結論になり得る。

(2) 「衝突」が存在するとされた裁判例

2023 年の連邦地方裁判所（イリノイ北部地区）の特許権侵害訴訟の裁判例[309]では、ディスカバリの対象であるソースコードは CSL 第 37 条の「重要データ」に該当し、国外移転には中国当局の許可を必要とすることから、同条の規定は米国ディスカバリをブロックする趣旨になるが、国際礼譲分析を実施すれば、米国の利益（米国の特許を保護する利益）が中国の利益（国民を法律に従わせる利益）を上回るとして、中国国内で保存されているデータ（ソースコード等）について米国ディスカバリの越境的適用を命じた。

第 4 項　その他の国のデータ保護措置と米国ディスカバリの越境的適用との関係

その他の国におけるデータの越境移転制限と米国ディスカバリの越境的適用が問題になった事例として、たとえば、2014 年の連邦地方裁判所（ニューヨーク南部地区）の裁判例[310]では、スイス等の銀行秘密保護法制によるデータの越境移転制限との関係が問題となり、スイスについては銀行秘密保護法の罰則を適用した多数の実例があることから、スイスの利益が米国の利益を上回るとして、スイスの銀行口座情報に対する米国ディスカバリの越境的適用を認めなかったが、フランス、ヨルダンおよび UAE の銀行口座情報については、それらの国における罰則適用の実績が乏しいことなどから、米国の利益が上回るとして越境的適用を認めた。このように、米国ディスカバリの越境的適用を阻止するためには、米国裁判所のディスカバリ命令に従った自国民をも処罰するなど、国家としての強い意志を示して現に実行することが必要とされる。

[308] Owen v. Elastos Found., 343 F.R.D. 268 (S.D.N.Y. 2023).
[309] Motorola Sols., Inc. v. Hytera Commc'ns Corp., 2023 U.S. Dist. LEXIS 161194 (N.D. Ill. 2023).
[310] Motorola Credit Corp. v. Uzan, 73 F. Supp. 3d 397 (S.D.N.Y. 2014).

第 4 節　ディスカバリの越境的適用の拡大と比例原則

米国訴訟におけるディスカバリは、かつては紙文書を中心とし、関連性のある情報は広く開示すべきであるという理念に支えられていた。しかし、社会のデジタル化に伴って、電子メール、メタデータ、バックアップデータ、クラウド保存データなどが膨大な量となり、従来の広範なディスカバリのモデルでは、当事者に過大なコストと復元・検索・レビューワークの負担が生じるようになった。こうした負担増大に対応するため、FRCP は 2000 年代以降段階的に改正され、費用対効果や情報取得の必要性を考慮した調整として比例原則の要素が徐々に追加されていった[311]。2015 年改正では、FRCP 第 26 条(b)(1)の文言に比例性が明示的に組み込まれ、「当該事件における必要性との比例」がディスカバリの要件として明文化された（前記第 1 節参照）。

一方、越境的データ流通が高度化・常態化するにつれ、ディスカバリの越境的適用も量的・質的に拡大し、外国企業や第三国に所在する個人に対しても、米国型ディスカバリに固有の広範な提出義務が及ぶ場面が増加している。The Sedona Conference（2024）が指摘するように、こうしたディスカバリの越境的適用の実施は、当事者が依拠する法制度、プライバシー保護水準、情報管理体制、データ移転規制の相違によって、国内訴訟とは比較にならない複雑な負担を生じさせる[312]。相手国の法体系と整合しない提出要求や、データ保護義務との抵触が生じ得る点を踏まえると、米国裁判所の要求が形式的には正当でも、外国当事者にとっては著しい不均衡や遵守困難性を伴う場合がある。このため、FRCP に明文化された比例原則は、国境を越える文脈においては、当該事件における証拠の必要性、相手国法令との衝突可能性、データの所在国への負担、情報へのアクセス可能性などを総合的に調整する基準として位置づけられるべきである[313]。

第 1 項　ディスカバリの越境的適用の拡大

連邦最高裁判所は、アエロスパシアル裁判において、他国の主権に配慮するための考慮要素（アエロスパシアル・ファクターズ）を示して「国際礼譲分析」を行うとしたが（前記第 3 節参照）、その後の下級審裁判におけるアエロスパシアル・ファクターズの運用は、形式上は国際礼譲分析を採用しながらも、圧倒的多数の事例で米国ディスカバリの越境的適用を肯定する方向の判断がなされている。この点に関し、Sant（2015）は、米国ディスカバリの適用を認める方向にバイアスがかかった判断がなされていると指摘している[314]（表 11 参照）。

【表 11：米国ディスカバリの越境的適用の拡大（Sant の研究）】

米国ディスカバリの越境的適用の拡大（Sant の研究）
Sant は、米国ディスカバリの越境的適用に当たって他国の法律に違反することが問題となった 54 の裁判例（以下「対象裁判例」という。）について、アエロスパシアル・ファクターズの五つの考慮要素

311 Allman (2006), pp. 8–12; Gensler and Rosenthal (2013), pp. 855–864.
312 The Sedona Conference (2024), pp. 676–681, 694–699.
313 The Sedona Conference (2024), pp. 676–681, 727–735.
314 Sant (2015), pp. 184–203, 213–230.

ごとに、米国ディスカバリの越境的適用を認める方向（以下「積極方向」という。）に判断されたか、あるいは認めない方向（以下「消極方向」という。）に判断されたかを調査した。各考慮要素についての調査結果は、以下のとおりであった。

① 一番目の考慮要素の「対象となる情報の重要性」については、対象裁判例のうち 91 パーセントで積極方向に判断されており、そのような裁判例では、当該訴訟との「関連性（relevancy）」が認められただけで「重要性」が認定されるなど、低いハードルで積極方向の判断がなされている。

② 二番目の考慮要素の「請求の具体性の程度」については、対象裁判例のうち 92 パーセントで積極方向に判断されており、アエロスパシアル裁判で連邦最高裁判所が「対象となるドキュメントが限定されているか」という意味でこの考慮要素を示したにもかかわらず、下級審裁判例では、「対象となるドキュメントが特定されているか」という観点で判断がなされている。

③ 三番目の考慮要素の「対象となる情報が米国起源であるか」については、五つの考慮要素のうち唯一の客観的要素であり、対象裁判例のうち積極方向に判断されたものはわずか 6 パーセントにとどまり、残りの大半は消極方向に判断されている。他方で、他の四つの主観的要素はいずれも 80 パーセントを超える事案で積極方向に判断されており、それらのなかには、対象となったドキュメントが他国で作成されたものであると認定したにもかかわらず、積極方向に判断したものもある。したがって、三番目の考慮要素が客観的に判断されるものであるとしても、全体の結論に大きな影響力はないということができる。

④ 四番目の考慮要素の「獲得のための代替手段の使用可能性」については、対象裁判例のうち 85 パーセントで積極方向に判断されており、ハーグ証拠条約その他のルートの手続によることが（客観的には）可能であるにもかかわらず、それらは複雑で時間がかかるなどとして、「代替手段」とは認めないとの判断がなされている。

⑤ 五番目の考慮要素の「米国の利益や当該他国の利益を害する程度」は、ディスカバリに応じない場合に米国の重要利益を害する程度とディスカバリに応じた場合に当該情報が存在する国の重要利益を害する程度を比較して、いずれを重視すべきであるかという考慮をするというものであるが、対象裁判例のうち 81 パーセントで積極方向に判断されており、米国裁判所が他国の利益を十分に考慮しているかについては疑義が呈されている。

以上の分析から、Sant は、アエロスパシアル・ファクターズが形式上は中立的な衡量基準として設計されているにもかかわらず、下級審の運用においては実質的に米国ディスカバリの越境的適用を肯定する方向へ作用していると結論づけている。

また、1782 条ディスカバリは、2004 年のインテル裁判の後に急増したとされており、Bento（2020）は、1782 条ディスカバリの申立てが、2010 年代には 1990 年代の 9 倍以上に増加したと指摘している[315]。さらに、Wang（2020）は、インテル裁判の翌年の 2005 年から 2017 年までの間に米国外の民事訴訟のための 1782 条ディスカバリの申立てが約 4 倍に増加したと指摘している[316]。Wang（2020）は、2015 年に申し立てられた 1782 条ディスカバリについて調査し、申立てが認容または一部認容された割合は、全体では 94 パーセント、米国外の審決機関（tribunals）からの申立てに限れば 98.9 パーセント、訴訟当事者等からの申立てについては 90 パーセントで

[315] Bento (2020), p. 20.
[316] Wang (2020), pp. 2106–2120.

あったとしており[317]、1782 条ディスカバリの申立てが極めて高い割合で認容または一部認容されていることが示されている。このように 1782 条ディスカバリの申立てが高い割合で認容されていることも 1782 条ディスカバリの拡大につながっているものと考えられる。

第 2 項　ディスカバリの越境的適用における比例原則の必要性

以上のように米国ディスカバリの越境的適用が拡大していることは、他国の主権および国内法令との衝突を不可避的に増大させ、越境的なデータアクセスをめぐる国際的摩擦を構造的に深刻化させる要因となっている。米国裁判所が自国制度の越境的適用を介して国外に所在する情報へのアクセスを広範に認容する状況は、データの管理・保護をめぐる各国の規制体系と正面から衝突し、企業に対し相反する法的義務を同時に負わせる結果を招いている。特に、欧州における厳格な個人データ移転規制と、米国における広範なディスカバリ制度との制度的衝突は顕著であり、GDPR 域外移転規制との関係では、越境移転の適法性判断が両制度間の根本的な発想の相違を反映して緊張関係を強めている[318]。また、アジア諸国を含む多くの国家が国家安全保障の観点からデータの国外流出を慎重に管理する制度を整備するなかで[319]、米国ディスカバリの強制的性質が併存する状況は、越境的データガバナンスにおける制度的非対称性を一層拡大させている。

ディスカバリの越境的適用における比例原則について、The Sedona Conference（2024）は、FRCP 第 26 条(b)(1)の枠組みを越境事件に適用する際には、米国訴訟と同様の負担・費用・重要性の衡量だけでは不十分であると指摘する。すなわち、外国法令（データ保護規制、移転規制、秘匿義務、刑事罰を伴う規制など）との抵触は、米国訴訟には現れない独自のリスクを伴うため、比例性判断の中心的要素として扱われるべきであり、また、対象データが外国に保管されている場合には、当事者が実際に情報へアクセスできるかという実効的取得可能性が比例性判断に影響を及ぼすとする。これらの要素を踏まえると、ディスカバリの越境的適用における比例原則は、単なる量的調整にとどまらず、複数法域間の法的・実務的制約を調整する基準として機能すべきであるとしている[320]。

データの分散化・クラウド化が進む今日では、情報の物理的所在が国境線と一致しない事例が急増しており、領域主権を基礎とする伝統的な国際私法的調整手法では、各国の法制度間に生じる衝突を円滑に解消することが難しくなっている。こうした状況を踏まえると、越境的データガバナンスをめぐる現行の断片化した規範構造を前提のまま維持することは、制度的摩擦を恒常化させ、国際協力の基盤を著しく損なうおそれがある[321]。

越境的データガバナンス規範の再構成に向けては、各国の主権的規制権限と越境的なデータ取得の必要性との均衡を図りつつ、透明性・比例性・相互運用性を基礎とする新たな評価枠組みを構築することが不可欠である[322]。米国ディスカバリの越境的適用の拡大が示す制度的緊

---

317 Wang (2020), p. 2122.
318 Kuner (2017a), pp. 882–902.
319 Christakis (2024b), pp. 97–107.
320 The Sedona Conference (2024), pp. 727–735, 738–745.
321 OECD (2023b), pp. 5–16, 27–28.
322 Aaronson and Leblond (2018), pp. 245–253, 262–268; UNCTAD (2021), pp. 81–90, 99–116, 171–180; OECD (2023b), pp. 5–16, 27–28; Christakis (2024b), pp. 96–113.

張は、まさに越境的データガバナンス規範の再構成を迫る構造的課題であり、国際的な調和と信頼確保のための制度設計が急務となっている。

第 5 節　ディスカバリの越境的適用とデータガバナンス規範再構成の方向性

本章では、米国ディスカバリの越境的適用が、他国主権の侵害、重要情報流出リスクの増大、事前反論機会の欠如など、複合的な問題を生じさせていることを明らかにした。米国裁判所が自国制度の越境的適用を介して国外に所在する情報へのアクセスを広範に認容する状況は、データの管理・保護をめぐる各国の規制体系と正面から衝突し、企業に対し相反する法的義務を同時に負わせる結果を招いている。下級審裁判例におけるアエロスパシアル・ファクターズの運用が、形式上は中立的な衡量基準であるにもかかわらず、実質的には米国ディスカバリの適用を肯定する方向へ傾斜しているとの指摘は、この構造的問題を象徴している。さらに、GDPR の域外移転規制の強化やアジア各国における安全保障目的の情報統制拡大によって、外国法との抵触は制度的な摩擦を一段と深刻化させている。企業が複数法域間で相反する義務を同時に負わされる事例は増加し、越境的データガバナンスにおける国際的摩擦は制度的にも実務的にも放置できない状況に至っている。

米国ディスカバリの越境的適用は、広範な情報開示義務を前提とする米国民事訴訟制度の特性を背景に、国外所在データについても広く開示を求め得る構造をとってきた。しかし、越境的データ流通の深化と各国におけるデータ保護強化の潮流の下では、従来型の広範な開示要請は、外国法との抵触、企業の二重責務、権利侵害リスクの増大といった問題を顕在化させている。特に、国外データにアクセス可能であることをもって当該データを保有していると認めてディスカバリの越境的適用を拡大するに至って、他国主権との衝突が顕在化してきた。この点について、アエロスパシアル裁判は「国際礼譲分析」を通じた調整の方向性を示したものの、デジタル化に伴う情報侵害リスクの高まりや、法域間の保護基準の多元化に対して、同裁判の枠組みのみでは対応しきれない局面が生じている[323]。

米国民事訴訟制度内部でも、ディスカバリの肥大化に対する制度的自制を求める動きが強まり、2015 年改正により FRCP 第 26 条には比例原則が明示的に組み込まれた。この改正は、ディスカバリに伴う負担と訴訟上の必要性との均衡を図る理念を明確化し、過度な情報要求を抑制する方向へ制度の運用方針を転換したことを意味する[324]。この比例性重視の潮流は、1782 条ディスカバリにも波及し、連邦裁判所は、要求の過大性、第三者負担、情報の重要性などを衡量する運用を明確化し、1782 条においても比例性がディスカバリ付与判断の主要基準として体系的に位置づけられつつある[325]。このような動きは、ディスカバリの越境的適用における国際的文脈に照らしても重要であり、外国法制との調整可能性を広げる契機となる。

以上のとおり、比例原則の適用は、米国制度内部のみならず国際的文脈でも重要性を増している。外国法令との抵触リスク、実効的取得可能性、外国当事者への負担といった越境的適用に固有の要素を評価対象に組み込むことは、従来の米国訴訟における量的・費用的調整を超え、複数法域間の法的・技術的制約を適切に調整するための前提となる[326]。今後は、ディスカバリの越境的適用にあたり、比例原則に基づいて、開示が立証にとって真に必要か、外国法に違反しない取得方法が存在するか、開示後のガバメントアクセスのおそれはないか、より侵害性

[323] Zambrano (2016), pp. 164–180, 201–208.
[324] Federal Judicial Center (2015), pp. 1–7.
[325] Bento (2020), pp. 201–213.
[326] Bento (2020), pp. 201–213; The Sedona Conference (2024), pp. 727–735, 738–745.

の低い手段が確保されているかといった実質的検討が制度的に組み込まれることも期待される。さらに長期的には、米国外に存在する情報（データ）の収集については、米国ディスカバリの越境的適用ではなく、国際的に統一された新たな手続的規範に基づく証拠収集の枠組みへと移行することが望まれる。

したがって、越境的データガバナンス規範再構成に向けては、比例原則に基づき、各国の裁判権を含む主権的統制と越境的証拠収集の相互運用性を調整するための越境的証拠収集に関する共通枠組みを構築することが求められる[327]。ここでの比例原則は、負担と必要性の調整に限定されるものではなく、データの性質および利用文脈に基づくリスク評価、外国法令との衝突のおそれ、データ主体の権利保護を勘案し、越境的証拠収集における過剰干渉を防ぎつつ必要最小限の開示のみを正当化する制度原理として機能しなければならない。この枠組みを導入することにより、データ保護、機微情報の安全性、第三国法との整合性を含む複合的評価が可能となり、主権尊重と国際協力を両立させる調整メカニズムとして機能させることができる。

[327] Zambrano (2016), pp. 174–180, 201–208; Bento (2020), pp. 215–238; The Sedona Conference (2024), pp. 727–735, 738–745.

第 7 章

国家によるデータ流入規制

第 7 章　国家によるデータ流入規制

近年、一部の国において、国家によるデータ流入規制が顕著となっている。ここでいう国家によるデータ流入規制とは、外国で生成または収集されたデータが自国の領域内に移転・導入されることを法制的または技術的手段によって制限または禁止する措置をいう。このような規制は、国外データの受入れが国家の情報秩序や社会的安定に影響を及ぼすことを抑止する目的で設計された制度的措置であり、国家安全保障、公共秩序の維持、社会的価値体系の保全といった観点から正当化されることが多い[328]。典型的には、国外で生成されたニュース、SNS コンテンツ、映像・音声配信データなど、国内に影響力を有する情報の流入によって政治的または社会的安定が損なわれることを防ぐ措置として現れる。また、近年では生成 AI やアルゴリズムの越境利用に関して、バイアス転移や価値体系の侵食など、国外で学習されたモデルやデータセットを自国内で利用することに伴うリスクが顕在化しつつある[329]。国外データを通じて国内の社会構造や価値体系が外部から影響を受ける可能性があることから、国家は言語的・文化的アイデンティティの維持や法的・制度的一貫性の確保を目的として、国外データの導入を制限する傾向を強めている[330]。

こうしたデータ流入規制は、国家主権の観点から一定の政策的根拠を主張し得るものの、他方でデータ流通の自由を制約し、知識や技術の越境的共有を阻害するという構造的な弊害を伴う。国外由来データの受入れを制限することは、学術研究や産業技術の発展に不可欠なデータの相互参照や国際的な協力関係を困難にし、研究や技術開発の国際的な連携体制を分断するリスクを生じさせる。AI、医療、環境などの分野では、異なる制度や文化圏から得られる多様なデータを統合的に分析することが科学的知見の深化に直結しており、流入規制はその前提条件を根本から制約する[331]。

さらに、データ流入統制は、国家間の情報アクセス格差を生じさせるのみならず、イノベーションと人権の双方に深刻な影響を及ぼす。国外データの受入れを制限する国家は、自国の情報空間を保護し得る一方で、外部との知識循環を断ち切ることにより、技術革新や新たな価値創出の基盤を自ら狭める危険を伴う。データの多様性は科学的発見や社会的課題解決の基礎であり、その流入を制限することは、知的探究の自由を制度的に制約することを意味する。また、データの流通が限定される環境では、国民が国外の言論・文化・科学的知見に触れる機会が失われ、思想・表現・学問の自由といった基本的権利が実質的に損なわれる。したがって、デジタル主権の確立を名目とする流入規制は、国家の自立を強化するどころか、社会の創造的潜在力と市民の権利的自由を同時に縮減させるという内在的矛盾を抱える[332]。

以上のように、データ流入規制は主権行使の在り方の問題にとどまらず、国際的相互依存の下で自由と多元性をいかに保障するかという、より根源的な規範的課題に関わるものとなる。国

[328] Chander and Lê (2015), pp. 686–720; Kuner (2015), pp. 236–244; Aaronson (2018), pp. 7–16.
[329] Surbakti (2025), pp. 307–314.
[330] Kaya and Shahid (2025), pp. 219–232.
[331] Chander and Lê (2015), pp. 713–739; McMahan et al. (2017), 1273–1277; Aaronson (2018), pp. 7–16.
[332] Chander and Lê (2015), pp. 721–739; Aaronson and Leblond (2018), pp. 248–253, 259–268; OECD (2019a), pp. 15–19, 59–71, 87–94.

家のデジタル主権を維持しつつ、国際社会における知識・技術・価値の循環を断たないためには、主権の行使と国際協働との均衡を制度的に確保する仕組みが不可欠である。

本章では、まず第 1 節において、国家によるデータ流入規制について、中国、ロシア、イランなどにおける具体的事例を取り上げて各国の規制の実態を整理し、次いで第 2 節で国家によるインターネット遮断の現状を概観する。これらを踏まえ、第 3 節で越境的データガバナンス規範再構成の方向性を検討する。

第 1 節　国家によるデータ流入規制の実情

本節では、データ流入規制を実施している主要国として、中国、ロシア、イランなどの実情を概観する。

第 1 項　中国（グレート・ファイアウォール）

(1) 歴史的経緯

中国では、1990 年代後半のインターネット商用化と電子メール導入に伴い、公安部が主導したゴールデン・シールド計画がその基盤となり、国家によるインターネット空間統制の技術的・制度的枠組みへと発展し、後に「グレート・ファイアウォール」と称されるようになった[333]。

中国政府は 1997 年に「コンピュータ情報ネットワーク国際接続安全保護管理規定（暫定）」を制定し、公安部門がネットワーク上のコンテンツ検閲や利用者監視を行うための基盤を整備した[334]。その後、2000 年代初頭には、国外ニュースサイトや人権団体のウェブサイトなど、国家のイデオロギーや公共秩序に反するとみなされるデータへのアクセスを遮断するシステムが本格的に稼働した[335]。

2009 年には新疆ウイグル自治区で発生した暴動を受け、同地域全体でインターネット接続が数か月にわたり遮断され、「グレート・ファイアウォール」の監視・遮断機能が強化されたことが国際的に注目された[336]。2010 年代に入ると、中国国内の SNS プラットフォームを保護・育成する政策の下、Facebook、Twitter、YouTube など主要な国外サービスが長期的にブロックされ、これに代わる国内サービス（WeChat、Weibo など）が拡大した[337]。

さらに、習近平政権下で国家安全保障の枠組みが強化されるとともに、2017 年施行のサイバーセキュリティ法[338]など関連法制が整備され、「グレート・ファイアウォール」は国家主導のサイバー空間管理装置としてより高度化し、国外サービスの遮断やコンテンツ検閲の強化が進められた。近年では、国外からの VPN 接続や暗号化通信技術に対する監視・制限も強められており、「グレート・ファイアウォール」は中国における「サイバー主権」政策を象徴する制度的装置となっている[339]。

(2) 「グレート・ファイアウォール」の実態

中国の「グレート・ファイアウォール」におけるインターネット検閲は、単一の巨大な「壁」ではなく、複数の技術と主体が段階的に作用する分散的な仕組みで構成されている[340]。技術的には、

---

[333] Quan (2022), pp. 19–23.
[334] Computer Information Network International Interconnection Security Protection and Management Rules, 30 Dec 1997. https://digichina.stanford.edu/work/computer-information-network-international-interconnection-security-protection-management-rules/; Creemers (2017), pp. 89–91.
[335] Ensafi et al. (2015), pp. 63–65; Quan (2022), pp. 20–23.
[336] Stone (2009), p. 1471.
[337] Creemers (2017), pp. 91–95.
[338] 中華人民共和国サイバーセキュリティ法（2016 年 11 月 7 日制定、2017 年 6 月 1 日施行）.
[339] Ensafi et al. (2015), pp. 63–68; Quan (2022), pp. 22–28; Wu et al. (2023), pp. 1–14.
[340] Ensafi et al. (2015), pp. 61–65; Bock et al. (2021), pp. 1–6; Quan (2022), pp. 19–23; Wu et al. (2023), pp. 3–10.

IP レンジ遮断、URL フィルタリング、DNS ポイズニング（偽応答の注入による誤誘導）、ディープ・パケット・インスペクション、中間者攻撃、TCP リセットなどが組み合わされ、国外の主要サービス（Google、Facebook、YouTube、Twitter 等）は中国国内の代替サービスに置き換えられている。DNS ポイズニングは DNS の authoritative response に偽応答を注入する active injection 型遮断を実現し、日次で数十万件規模のドメインを対象とする。こうした検閲は固定的ではなく、地域差、プラットフォーム差、時間的変動を伴うとされる。ウェブ検閲には冗長系が導入され、一次検閲をすり抜けた通信を二次系が補足する。キーワード検閲では、禁止語を含むリクエストの後続通信を一定時間まとめて遮断する「ペナルティボックス」方式が抑止力として機能するほか、利用者属性や意図を推測して対象を拡張する動的な挙動も確認されている[341]。

プラットフォーム側でも検閲が実施されており、微博や微信、オンラインゲームなどでは、政府のガイドラインの下で各社が独自の禁止語リストを運用し、発売時期・出版社・開発者といった要因によって差が生じる。企業には自律規制の誓約書への署名など制度的な自己規律が求められ、さらに数百万規模の人手検閲とアルゴリズムが組み合わされて、投稿の監視・削除や愛国的コンテンツの増幅が行われている。VPN などの回避手段は一部を除いて制度上違法化されている。検閲は時間的にも動的に強弱がつき、党大会などの政治イベント前後には予防的（プロアクティブ）に関連語が広く遮断され、事件・不祥事の発生時には事後的（リアクティブ）に連想語や周辺語まで一斉に拡張される[342]。

対外的な通信遮断に加え、物理的な攻撃機能である「グレート・キャノン」が分散型サービス妨害（DDoS）攻撃などに用いられた事例も確認されている。これらは検閲が受動的な防御にとどまらず、必要に応じて対外的圧力手段として活用され得ることを示す[343]。他方、国内については世論の「ガス抜き」や下級官僚に対する限定的な批判を許容しつつ、重要な争点については、政府が望ましいと判断する視点や解釈が社会的に共有されるような情報環境を誘導する運用が行われている。すなわち、完全なデータ遮断ではなく、特定のデータの到達を困難にしつつ、可視化されるデータを政策的に調整することで、政府が望ましいとする社会的理解の方向性を事実上形成する統治装置として機能している[344]。

総じて、「グレート・ファイアウォール」の実態は、多層・分散・動的という三つの特性を兼ね備え、技術的遮断、企業による自律規制、人手とアルゴリズムの大量運用、そして時間・地域・受け手に応じた可変ロジックを統合した統治技術である。このモデルは、国内統制の中核であると同時に、デジタル・シルクロード等を通じて域外にも波及し得る、輸出可能な制度的・技術的パッケージとしての性格を強めている[345]。

(3)　小括

中国の「グレート・ファイアウォール」は、国外からのデータやコンテンツの流入を技術的かつ制度的に遮断する国家的枠組みとして、各国の越境的データガバナンスに重大な影響を及ぼし

[341] Ensafi et al. (2015), pp. 61–65, 68–72; Bock et al. (2021), pp. 1–6; Wu et al. (2023), pp. 3–14.
[342] Knockel et al. (2015), pp. 2–8; Creemers (2017), pp. 91–99; King et al. (2017), pp. 484–492.
[343] Marczak et al. (2015), pp. 1–6.
[344] Creemers (2017), pp. 91–99; King et al. (2017), pp. 484–492; Quan (2022), pp. 24–28.
[345] Creemers (2017), pp. 91–99; King et al. (2017), pp. 484–492; Quan (2022), pp. 24–29; Wu et al. (2023), pp. 3–14; Jiang (2024), pp. 731–736.

てきた。このシステムは、国外のニュースサイトや SNS、動画共有サービスなどを恒常的にブロックすることにより、国家安全保障や社会秩序維持の名の下で、国内情報空間を国家主導で管理し、データの自由な流通を制限している。

このようなデータ流入規制は、中国が主張する「サイバー主権」の体現であると同時に、越境的データガバナンスにおける規範的非対称性を象徴している。すなわち、中国政府は、自国にとって重要と判断される国外データのみを選択的に流入させる一方で、国家や特定主体による国外データへのアクセスと利用を統制する体制を構築している。これらの施策を講じていない国々と比較すれば、越境的データフローの管理に関するガバナンスの差異は顕著であり、国際的な制度調和に断絶を生じさせていると指摘されている[346]。この状況は、国際的なデータ流通の自由、表現の自由、経済活動の自由といった普遍的価値と、国家安全保障や公共秩序維持といった国家的利益との均衡をいかに確保するかという、越境的データガバナンスに内在する根本的課題を浮き彫りにしている[347]。

第 2 項　ロシアにおけるデータ流入規制

(1)　歴史的経緯

ロシアにおけるデータ流入規制は、旧ソ連期から連続する情報統制の伝統を背景として形成されてきた。ソ連時代には、国外からの情報流入は国家のイデオロギー的安定を脅かす要因とみなされ、通信・出版・放送のいずれも厳格な検閲と管理の対象とされた。このように情報を統治資源と考える発想は、1991 年のソ連崩壊後も根強く残り、ロシア連邦の法制度においても情報保護を国家安全保障の一部として位置づける方向で継承された[348]。

1990 年代には一時的に情報空間の自由化が進んだものの、2000 年代に入るとプーチン政権は国家による統制の再構築を進め、サイバー空間を主権的管理の対象として制度化した。2000 年の「情報安全保障ドクトリン」は国外情報の影響を「国家体制に対する脅威」と明示し、2008 年のグルジア紛争を契機にサイバー防衛と通信監視体制が拡充された。2011 年以降には、通信監視システム SORM の拡張を通じて国外サーバー経由の通信監視が常態化し、国外データの受入れに対する法制度的基盤が整備された[349]。

2010 年代後半には「サイバー主権」の概念が政策上の中心に据えられ、国外由来情報の流入制御が制度化された[350]。2012 年の「有害情報遮断法」[351]によりウェブサイトのブロック権限が拡大され、2016 年の「ヤロヴァヤ法」[352]により通信事業者にデータ保存義務が課された。さらに

---

346 Creemers (2017), pp. 91–99; Arner et al. (2022), pp. 660–683; Jiang (2024), pp. 728–736.

347 Creemers (2017), pp. 91–99; Aaronson and Leblond (2018), pp. 259–266; OECD (2022a), pp. 18–21, 34–41; Quan (2022), pp. 24–29.

348 Asmolov (2024), pp. 33–42.

349 Polyakova and Meserole (2019), pp. 5–11; Asmolov (2024), pp. 36–42.

350 Epifanova (2020), section "The New 'Sovereign Internet Law'"; Litvinenko (2021), pp. 6–12.

351 Federal Law No. 139-FZ of 28 July 2012 on Amendments to the Federal Law on the Protection of Children from Information Harmful to Their Health and Development and Certain Legislative Acts of the Russian Federation.

352 Federal Law No. 374-FZ of 6 July 2016 on Amendments to the Federal Law on Counteracting Terrorism and Certain Legislative Acts of the Russian Federation regarding the Establishment of Additional Measures for Countering Terrorism and Ensuring Public Safety.

2019 年の「ソブリン・インターネット法（Sovereign Internet Law）」[353]では、国内通信事業者に対する深層パケット検査（DPI）機器の設置義務化や国家管理の DNS インフラ整備を通じて、国外インターネットからの物理的・技術的切断を可能とする仕組みが導入され、国家が自律的にトラフィックを制御できる体制が構築された。

(2) 現在の状況

2022 年のウクライナ侵攻以降、情報統制を強化する一連の法制度的・技術的措置が講じられている。この統制は、国外からの批判的言説や多元的情報が国内に流入することを抑制する政策の一環として運用されており、情報環境の閉鎖性と制度的自己完結性の形成に寄与している。政府は、Facebook、Instagram、X（旧 Twitter）など主要な国外ソーシャルメディア・プラットフォームを遮断する一方で[354]、他の事業者にはコンテンツ削除義務およびユーザーデータの国内保存義務（データローカライゼーション）を課している[355]。これらの措置は、デジタル主権の強化を標榜する法政策の一部を構成しており、国外由来の情報流入に対する制度的制限として位置づけられる[356]。

他方で、ロシアの通信インフラは表面的には拡大傾向を示しており、2024 年時点で全国水準において約 9 割の世帯が自宅でインターネット接続を有していると推計されている[357]。しかし、通信容量やネットワーク安定性の確保と並行して、データ遮断機能を備えた技術環境（例：5G 基地局の国産化計画）が制度的に整備されつつあり、インフラの拡張が必ずしもデータの自由化を意味しない点に留意する必要がある[358]。

法制度面では、「外国の代理人」法の定義が拡張され、外国との関係性を根拠に個人・団体が広範に指定されるようになった。この指定に基づき、ロシア司法省は裁判所の判断を経ずにウェブサイトの遮断を行うことが可能となっている[359]。さらに、「好ましくない組織」への指定制度では、国外由来の報道機関や市民団体との関係そのものが刑事罰の対象となり得るとされており[360]、制度的抑圧の対象範囲が情報源との接触段階にまで拡大している。

さらに、2022 年 3 月以降に導入された「軍の信用を損なう行為」や「虚偽情報の流布」に関する法令に基づき、国外情報を引用して批判的言説を行った市民・ジャーナリストの訴追事例が

---

353 Federal Law No. 90-FZ of 1 May 2019 on Amendments to the Federal Law on Communications and the Federal Law on Information, Information Technologies and Information Protection.

354 Freedom House (2024a), sections A "Obstacles to Access," and B "Limits on Content."

355 Federal Law No. 242-FZ of 21 July 2014 amending the Federal Law "On Personal Data" (data localization requirement for personal data of Russian citizens); Freedom House (2024a), section B "Limits on Content."

356 Creemers (2017), pp. 91–99; Epifanova (2020), section "The New 'Sovereign Internet Law'"; Litvinenko (2021), pp. 6–12.

357 International Telecommunication Union (ITU), Datahub "Russia, Individuals Using the Internet." https://datahub.itu.int/data/?e=RUS (accessed 22 February 2026).

358 Epifanova (2020), section "The New 'Sovereign Internet Law'"; Litvinenko (2021), pp. 6–12; Mahon and Walker (2024), pp. 34–49.

359 Krupskiy (2023), paras. beginning with "Over the last eleven years, Russian legislation on 'foreign agents' has become considerably stricter," "Throughout these developments, the main characteristic of Russian legislation on 'foreign agents' has remained unchanged," and "At the start of the war in Ukraine in February 2022," section "The Institution of 'Foreign Agents' as a Repressive Policy Mechanism."; Freedom House (2024a), section B "Limits on Content."

360 Hamlett (2017), pp. 256–267, 275–283.

多数報告されている。これらの規制は、国外との情報接触自体を危険視する法的構造を形成しており、処罰範囲の拡張および量刑の重罰化（最大 15 年の禁錮刑）が進行している[361]。

このような制度的措置は、データの流出規制のみならず、データ流入の遮断を通じて国内情報空間を閉鎖的に構築する手段として機能しており、ロシアの権威主義的統治体制における中核的要素となっている。政府は、選挙操作や体制批判の排除にこれらの制度を体系的に活用しており、国際人権法の観点からも構造的な懸念が提起されている[362]。

第 3 項　イランにおけるデータ流入規制

イラン・イスラム共和国では、2021 年以降、国家情報ネットワーク（National Information Network: NIN）の拡張が急速に進められてきた。その主目的は、国家のデジタル主権を確保するとともに、国民の国際インターネットへの依存度を削減し、国外由来の情報流入を構造的に制限することである。この政策的方向性は、インターネットへの接続基盤の整備と技術的発展を伴いつつ、同時に政府による選択的遮断・規制手段の制度化にもつながっている[363]。

イラン政府は、NIN を通じて独自のサイバー空間構築を目指しており、2024 年初頭には光ファイバー網のカバレッジが 75%に達するとの見通しが示された[364]。しかしながら、NIN に関する統計の正確性や進捗状況は、市民団体やデジタル権利団体から繰り返し疑問視されており、国内インフラの実効性が国際標準に照らして限定的であるといえる[365]。

インフラ整備と並行して、当局は国際インターネットへのアクセス制限策を強化している。具体的には、国外帯域の速度制限、料金引き上げ、国際サービスの価格的非優遇措置を通じて、ユーザーの接続行動を NIN へと誘導している[366]。このような制度的誘導は、国際的情報へのアクセスをコスト構造の面から困難化し、実質的に国外コンテンツの遮断をもたらす構造的規制といえる。

さらに、国外からの衛星インターネット接続手段に対しても厳格な制限が課されている。特に、Starlink 社が 2022 年 9 月以降に抗議活動の支援目的で提供したサービスに対して、イラン政府は国際電気通信連合（ITU）に規制違反の通報を行い、2024 年 3 月には同社インフラの撤去を正式に要求した。この対応は、国家認可を受けない通信手段に対する排除方針を明示するものであり、国外通信網によるデータ流入に対する体系的遮断姿勢の一端を示している[367]。

このように、イランにおけるデータ流入規制は、技術インフラ、料金政策、ライセンス制度、衛星通信遮断など、多層的な手法を通じて実施されており、国内外データへの非対称的なアクセス体制を制度的に形成している。これにより国民は、国内データ網に制限された接続空間に閉じ込められ、政治的・社会的な言説形成の基盤が著しく狭められていると指摘されている[368]。

---

[361] McCarthy et al. (2023), pp. 127–146.
[362] McCarthy et al. (2023), pp. 127–146; Office of the High Commissioner for Human Rights (2023); Freedom House (2024a), section B “Limits on Content.”
[363] Akbarzadeh et al. (2024), pp. 4–8.
[364] Freedom House（2024b）, section A “Obstacles to Access.”
[365] Akbarzadeh et al. (2024), pp. 4–8; Freedom House (2024b), section A “Obstacles to Access.”
[366] Freedom House (2024b), section A “Obstacles to Access.”
[367] Freedom House (2024b), section A “Obstacles to Access.”
[368] Freedom House (2024b), sections A “Obstacles to Access,” and C “Violations of User Rights.”

第 4 項　その他の国々におけるデータ流入規制

その他の国々においても国家安全保障や公共秩序を名目としたデータ流入規制が顕著にみられる。

トルコでは、テロ対策や大規模抗議活動の抑制を理由として、国外 SNS やニュースサイトへの一時的なアクセス遮断が繰り返し実施されてきた。2013 年以降、Twitter や Facebook などの主要プラットフォームに対するブロッキング措置は、国内治安維持を目的とする政策手段として定着しており、さらに国外プラットフォームに対してコンテンツ削除およびデータ保存を義務づける法制度が整備されている。このように、技術的手段と法的規制を併用した情報統制は、制度的に一層強化されつつある[369]。

インドにおいても、国家安全保障や宗教的緊張を理由とした国外情報へのアクセス制限が拡大している。近年、国境紛争や国内治安問題を背景に、TikTok など国外製アプリケーションの禁止、特定ニュースサイトへの接続制限、VPN 利用に対する規制強化などが進展した。これらの政策は、国外情報が社会的安定を脅かす潜在的リスクとして認識され、情報空間における国家主権の確立を目的とするものである[370]。

北朝鮮では、国外からの情報流入が体制の安定を脅かすものとされ、国家による情報統制体制の中核として厳格なデータ流入規制が敷かれている。国民のインターネット利用は原則禁止され、国家管理のイントラネット「光明網」のみが使用可能である。国外ウェブサイトや SNS へのアクセス、外国メディアの所持は刑事罰の対象とされ[371]、放送機器や出版物も国家によって統制されている[372]。こうした制度は、思想統制と安全保障を目的とした技術的・法的遮断構造であり、外国からの情報伝達に対しては外交的・軍事的排除措置を伴う[373]。結果として、表現の自由や情報アクセス権が根本的に制限され、閉鎖的な情報環境が体制維持の手段として固定化されている[374]。

欧州諸国においても、ドイツとフランスを中心に、自由なデータ流通を原則としつつ、国家安全保障や公共秩序を理由とする国外コンテンツへのアクセス制限を制度化している。ドイツでは NetzDG 法により、テロリズムや過激思想を助長する投稿の削除義務が国外プラットフォームにも課され[375]、フランスではテロ関連サイトや偽情報サイトに対して行政当局による遮断命令が可

---

[369] Human Rights Watch (2022); Freedom House (2024c), sections B “Limits on Content,” and C “Violations of User Rights.”

[370] Freedom House (2024d), sections A “Obstacles to Access,” B “Limits on Content,” and C “Violations of User Rights.”

[371] Fisher (2018), pp. 68–72; Freedom House (2024e), sections B “Political Pluralism and Participation,” and D “Freedom of Expression and Belief.”

[372] Center for Strategic and International Studies (CSIS) (2019); Reporters Without Borders (RSF) (2025), sections “Media landscape,” and “Sociocultural context.”

[373] Freedom House (2024e), sections B “Political Pluralism and Participation,” and D “Freedom of Expression and Belief.”

[374] United Nations Human Rights Council (2014), Ⅲ. A. Violations of the freedoms of thought, expression and religion, paras. 26–31.

[375] ARTICLE 19 (2017); Heldt (2019), pp. 2–14.

能となっている[376]。さらに EU も、2022 年に制定したデジタルサービス法（Digital Services Act）[377]において、越境的デジタルプラットフォームに対するコンテンツ削除義務や透明性要件を明記し、データ流通の管理を制度的に進めている[378]。

以上のように、各国におけるデータ流入規制は、その強度や方法こそ異なるものの、国家安全保障、公共秩序の維持、社会的価値観の保護といった政策目的と密接に結びついており、技術的手段と法制度を組み合わせた多層的な統治戦略として展開されている。

[376] Organization for Security and Co-operation in Europe (OSCE) (2015); European Parliament and Council (2022) Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union L 277/1, 27 October 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

[377] European Parliament and Council (2022) Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union L 277/1, 27 October 2022.

[378] Digital Services Act, arts. 14–17, 24–42.

第 2 節　国家によるインターネット遮断

第 1 項　概要

国際 NGO の Access Now が 2025 年に公表したレポートによると、インターネットの遮断は、2016 年には 27 か国で 78 件が確認されていたが、その後増加傾向を示し、2023 年には 39 か国で 283 件、2024 年には 54 か国で 296 件が確認され、過去最高を記録した（表 12 参照）。

【表 12：インターネット遮断の発生件数と発生国数（2016 年～2024 年）】

年	2016	2017	2018	2019	2020	2021	2022	2023	2024
国数	27	23	28	36	34	39	40	39	54
件数	78	111	202	221	168	194	201	283	296

（Access Now (2025), p. 4）

これらの統計は、必ずしも国家によるインターネット遮断に限定されず、国外の攻撃者が特定国の通信網に対して遮断・妨害を行った事例も含んでいる。その前提で、2024 年にインターネット遮断が発生した国（国外からの遮断を含む。）は、ミャンマー（85 件）、インド（84 件）、パキスタン（21 件）、ロシア（19 件）などが主要な例として挙げられる[379]。遮断の背景別では、紛争関連が 11 か国で 103 件、抗議運動関連が 24 か国で 74 件、試験実施関連が 7 か国で 16 件、選挙関連が 8 か国で 12 件にのぼる[380]。

これらのうち、国家が関与して自国へのデータ流入を規制しているケースをピックアップすると、主に政府や治安当局が公権力を行使して国外発のデータ通信を遮断・制限した事例が該当する。具体的には、ミャンマーにおける軍政による全国規模の通信遮断や衛星インターネット端末の押収、インド政府による抗議活動や選挙期間中の通信制限、パキスタンにおける治安上の名目によるモバイル通信遮断、ロシア政府によるウクライナ占領地域の通信統制などが挙げられる[381]。これらはいずれも、国家が制度的・組織的に国外からのデータ流入を抑制し、国民のアクセスを統制することを目的とする国家主導のデータ流入規制として位置づけられる。

また、2024 年には、情報通信プラットフォームのブロックが 35 か国で 71 件発生しており、回数別に見ると、X（旧 Twitter）が 14 か国で 24 回、Facebook が 12 か国で 22 回、WhatsApp が 10 か国で 20 回、YouTube が 10 か国で 15 回、Instagram が 10 か国で 13 回などとなっている。これらのうち、国家の関与によるケースと考えられるものは、政府または治安当局が公権力を行使して通信事業者やプラットフォーム事業者にアクセス遮断を命じた事例であり、具体的には、インド、バングラデシュ、ヨルダン、ミャンマー、パキスタン、ロシア、タンザニア、トルコ、ベネズエラなどの諸国における遮断が該当する。これらは、抗議運動や選挙、治安維持を名目として

[379] Access Now (2025), pp. 4–5.
[380] Access Now (2025), pp. 7–10.
[381] Access Now (2025), pp. 4–10.

国外発のデータ流入を制限し、国民の通信・表現空間を統制する目的で実施された国家主導のデータ流入規制の一形態と位置づけられる[382]。

さらに、越境的なインターネット遮断は、2024 年には 8 か国で 25 件が確認されており、実施件数の多い国はロシア（7 件）、イスラエル（6 件）、タイ（4 件）などであった。これらは、ロシアがウクライナへの侵攻、イスラエルがガザ地区への攻撃、タイがミャンマーに対するサイバー犯罪対策に関連して実施したものであり、いずれも国家が関与したものと考えられる[383]。

このように、国家によるインターネット遮断は、国外から自国へのデータの流入を制限し、国民の通信・表現活動を統制する手段として制度化・常態化しつつある。各国政府は、国家安全保障、治安維持、選挙管理、公共秩序の維持といった名目を掲げながら、実際には批判的言論や市民の動員、国外発の情報伝達を抑制する目的で通信遮断を発動している。こうした措置は、表現の自由や知る権利といった基本的人権を直接的に侵害するのみならず、国際社会におけるデータ流通の自由と透明性を著しく損ない、国家によるデータ流入規制の制度的常態化を促進している[384]。

第 2 項　国家によるインターネット遮断の手法

国家によるインターネット遮断は、近年ますます精緻化し、多様な技術的手法が組み合わせて用いられるようになっている。代表的な手法としては、DNS ブロッキング（DNS blocking）[385]、BGP ルート操作（BGP route manipulation）[386]、ディープ・パケット・インスペクション（Deep Packet Inspection: DPI）[387]、およびモバイル通信停止（mobile network shutdown）[388]が挙げられる（表 13 参照）。これらの手法は、遮断の範囲、精度、実装難易度がそれぞれ異なり、国家の政策目的や情報統制の戦略に応じて選択・併用されている[389]。近年では、複合的な戦術へと進化しつつあり、たとえば DNS ブロッキングと DPI を組み合わせた「選択的遮断」や、BGP ルート操作とモバイル通信停止を併用する「ハイブリッド型遮断」などが用いられ、遮断は全面停止から特定リスクを狙う制御型統治へと移行している[390]。このような技術的手段の高度化は、国家がインターネット基盤層そのものに制度的に介入し得る条件を整えることとなった（後記第 3 項参照）。これらの技術的手法は、国家の統制能力を飛躍的に高めた一方で、人権保障の観点から重大な懸念を招いており、その正当化の限界を検討する必要がある。

---

382 Access Now (2025), pp. 6–21, 24–27.
383 Access Now (2025), pp. 14–15.
384 Access Now (2025), pp. 6–27.
385 Morishita et al. (2023), section 5.1.1 “DNS Interference”; UNIDIR (2023), pp. 1–4, 9–12,
386 Morishita et al. (2023), section 5.3.2 “Adversarial Route Announcement”; UNIDIR (2023), pp. 1–4, 9–12,
387 Morishita et al. (2023), sections 4.2.5 “DPI Identification,” 4.3.1 “Shallow Packet Inspection and Transport Header Identification,” and 5.4.2 “Censorship in Depth”; UNIDIR (2023), pp. 3–5, 9–12.
388 Access Now (2025), pp. 6–10, 14–15; UNIDIR (2023), pp. 3–7, 9–12.
389 Morishita et al. (2023), sections 5.1 “Application Layer,” and 5.4 “Multi-layer and Non-layer”; UNIDIR (2023), pp. 3–7, 9–12; Access Now (2025), pp. 6–10.
390 Morishita et al. (2023), sections 4.2.5 “DPI Identification,” 5.1.1 “DNS Interference,” and 5.3.2 “Adversarial Route Announcement”; UNIDIR (2023), pp. 3–7, 9–12; Access Now (2025), pp. 6–15.

【表 13：国家によるインターネット遮断の技術的手法】

国家によるインターネット遮断の技術的手法
DNS ブロッキング（DNS blocking） 国家によるインターネット遮断で最も広く利用される手法である。政府や ISP が DNS（Domain Name System）の名前解決を拒否したり、誤った IP アドレスを返したりすることで、特定サイトへのアクセスを遮断する。コストが低くサービス単位で制御可能だが、外部パブリック DNS の利用によって比較的容易に回避される。
BGP ルート操作（BGP route manipulation） 国家規模でのインターネット遮断を可能にする強力な方法である。BGP（Border Gateway Protocol）のルート情報を「撤回」又は「誤誘導」することで、国外や特定ネットワークへの接続を物理的に遮断できる。2008 年には、パキスタン政府の操作が世界規模の YouTube 障害を引き起こした事例がある。
ディープ・パケット・インスペクション（Deep Packet Inspection: DPI） 通信データのパケットを解析し、特定サービスやプロトコルを識別して選択的に遮断する技術である。中国の「グレート・ファイアウォール」やイランの抗議デモ対策で広く用いられている。HTTPS の普及により内容解析は難しくなっているが、通信パターンやメタデータの解析を組み合わせることで実効性は維持されている。
モバイル通信停止（mobile network shutdown） 抗議デモや社会不安時に国家がとる即効性の高い手段とされる。通信事業者に命じて、特定地域や全国規模で携帯電話網を停止させる。情報拡散の抑制には一定の効果があるが、金融取引、緊急医療、災害対応など社会活動全般に深刻な影響を及ぼし、国際的批判も強い。

第 3 項　インターネット基盤層に対する国家の制度的統制とサイバー空間分裂の危機

国家がインターネット基盤層に対して制度的統制を及ぼす手法として、通信経路の選別、名前空間の管理、キャッシュ階層への介入が組み合わせて用いられる場合、サイバー空間は形式的な接続性を維持しつつも、実質的には国家による統制的境界に応じて異なる構造と挙動を示す情報空間へと変質する傾向が強まる[391]。

第一に、通信経路に対する統制としてのフィルタリングは、国際ゲートウェイや主要 ISP におけるパケットの検査・分類を通じて、特定の通信を遅延、遮断、選別する仕組みである[392]。この統制は技術的措置にとどまらず、国家が越境的通信の可否を政策目的に照らして決定し得る制度的基盤を形成する点に特徴がある[393]。

[391] Morishita et al. (2023), sections 4.1 “Points of Control,” 5.1.1 “DNS Interference,” 5.3.2 “Adversarial Route Announcement,” 5.4.2 “Censorship in Depth,” and 6.5 “Domain Name Seizures”; UNIDIR (2023), pp. 1–4, 9–12.
[392] Morishita et al. (2023), sections 4.1 “Points of Control,” 4.2.5 “DPI Identification,” 4.3.1 “Shallow Packet Inspection and Transport Header Identification,” 5.2 “Transport Layer,” and 5.3 “Routing Layer”; UNIDIR (2023), pp. 3–7.
[393] Morishita et al. (2023), sections 4.1 “Points of Control,” 4.2.5 “DPI Identification,” 4.3.1 “Shallow Packet Inspection and Transport Header Identification,” 5.2 “Transport Layer,” and 5.3 “Routing Layer”; UNIDIR (2023), pp. 3–7.

第二に、名前解決の書換えは、DNS に対する応答を国家管理層で再解釈し、本来のグローバルルートとは異なる接続結果を強制する仕組みである。これにより、国外サービスへの到達が技術的には可能であっても、名前空間の段階で切断されることが生じる。DNS はインターネットにおける識別体系の根幹を構成するため、この層への介入は、国家ごとに異なる情報体系が生じる基盤的条件を作り出し、国際的に共有されるサイバー空間の一体性を徐々に弱める方向に作用する[394]。

第三に、キャッシュ操作は、DNS キャッシュに保存される応答情報について、国家が更新のタイミングや保持内容に介入することで、国内利用者に古い情報や特定の情報を継続的に返す仕組みである[395]。本来であれば外部インターネット空間で行われた変更や最新の応答が反映されるはずだが、キャッシュが意図的に更新されない場合、利用者は国家が選別したデータに基づいてアクセスする状況が生じる。この手法は、表向きには通信の高速化や安定性向上と説明されることがあるものの、実質的には国家が望ましいと判断したデータのみを恒常的に維持できる制度的手段として機能し、国内の情報空間を外部と異なる方向へと誘導する作用を持つ[396]。

これら三層の統制手法が組み合わされると、通信層、識別層、キャッシュ層がそれぞれ国家の制度的判断に依存する構造が形成され、結果として国家内部には、国際的インターネットと表面上は接続しつつも、政策目的に応じて分岐した実質的閉域空間が成立する[397]。この構造は、越境的データ移転に対する選別的統制を容易にし、越境的データガバナンスにおける非対称性を深層的に支える仕組みとなる。すなわち、国家間でアクセス可能な情報空間が系統的に異質化することにより、相互運用性、透明性、信頼性といった国際的データガバナンスが依拠すべき共通基盤が弱体化し、制度間摩擦と不均衡が構造的に拡大する[398]。これらのインフラ層における介入は、表層的なコンテンツ規制とは次元を異にし、ネットワーク構造そのものの挙動を国家ごとに差異化する点に制度的特徴がある[399]。このように、国家によるインターネット基盤層への制度的介入は、サイバー空間を分裂に導く構造的な非対称性を生み出す主要因となっている。

以上のような現状に照らせば、サイバー空間の分裂は、国家の制度的選好と技術的能力が結合した結果であり、これを全面的に阻止することは困難である。しかし、分裂が不可逆的な断絶へと進展することを回避し、最低限の相互運用性と国際的信頼を維持する余地は残されている[400]。したがって、必要とされるのは、分岐しつつある複数の制度的ブロックを相互接続し、透明性と比例性に基づく越境的データガバナンス規範の再構成である。

---

394 Morishita et al. (2023), sections 4.1 “Points of Control,” and 5.1.1 “DNS Interference”; UNIDIR (2023), pp. 1–4, 9–12.

395 Morishita et al. (2023), section 5.1.1 “DNS Interference”; UNIDIR (2023), pp. 3–7, 9–12.

396 Creemers (2017), pp. 85–95. Morishita et al. (2023), section 5.1.1 “DNS Interference”; UNIDIR (2023), pp. 3–7, 9–12.

397 Aaronson and Leblond (2018), pp. 264–266. Morishita et al. (2023), sections 4.1 “Points of Control,” 5.1.1 “DNS Interference,” 5.3.2 “Adversarial Route Announcement,” and 5.4.2 “Censorship in Depth”; UNIDIR (2023), pp. 1–4, 9–12.

398 Aaronson and Leblond (2018), pp. 245–272; UNIDIR (2023), pp. 1–4, 9–12; Morishita et al. (2023), section 5.4.2 “Censorship in Depth”; Nocetti (2024), pp. 8–16, 31–32; Svanadze et al. (2025), pp. 578–580.

399 Deibert and Rohozinski (2010), pp. 3–12.

400 Deibert and Rohozinski (2010), pp. 3–12; Aaronson and Leblond (2018), pp. 245–272; UNIDIR (2023), pp. 1–4, 9–12; Nocetti (2024), pp. 8–16, 31–32; Svanadze et al. (2025), pp. 578–580.

第 3 節　国家によるデータ流入規制とデータガバナンス規範再構成の方向性

国家によるデータ流入規制は、国家が国外からの情報・コンテンツへのアクセスを制度的・技術的手段によって制限する政策であり、越境的データガバナンスにおける非対称性を構造的に拡大し、規範的分断を深化させる要因となっている[401]。国際社会は、人権、貿易、技術基盤など多様な観点からこれを批判し、厳格な比例原則に基づく運用を求めてきた。越境的データガバナンス規範再構成においても、こうした国際社会の動向を踏まえた検討が不可欠である。

第 1 項　国家によるデータ流入規制が越境的データガバナンスに及ぼす影響

国家によるデータ流入規制は、国際的なサービス貿易やイノベーションの基盤を分断し、国外企業による市場アクセスや研究機関間の情報共有の機会を大きく制限する。中国の「グレート・ファイアウォール」、ロシアによる国外 SNS 遮断、イランの国家情報ネットワーク（NIN）などは、恒常的な情報遮断を通じて自国のサイバー空間を閉鎖的に構築しており、国家が情報資源を選択的に統制することで一国主義的なデジタル主権の主張を強化する基盤となっている[402]。

また、こうした遮断政策は、越境的データガバナンス規範の形成に深刻な分断をもたらす。自由なデータ流通を推進する国々が信頼性と透明性を前提とした制度設計を進める一方、流入規制を強化する国々は安全保障や文化的保護を名目としつつ国外情報の遮断を制度化し、国際的な規範形成において対立軸を形成している[403]。

さらに、このような規範的非対称性は国際的協調の可能性を著しく低下させる。開放性と相互運用性を重視する国々と、情報遮断を恒常化する国々との間では共通のルール形成が困難となり、信頼に基づく越境的データガバナンスモデルの構築が阻害される結果、デジタル主権と自由なデータ流通の間の緊張関係が一層先鋭化する[404]。

以上のように、一部国家で実施される全面的なインターネットの遮断や、中国の「グレート・ファイアウォール」に代表される国外サービス・データベースへの接続ブロックは、自国の情報環境を国家主導で統制することを目的とするものであり[405]、安全保障や公共秩序の維持、さらには宗教・文化的価値観の保護などを理由として正当化される場合が多い。このような国家によるデータ流入規制は、サイバー空間を自国で囲い込み、データ流通を統制するデジタル主権の実践として位置づけられる一方、自由なデータ流通を理念とする国際的なサービス貿易やイノベーション活動に深刻な影響を及ぼす危険性を内包している[406]。その結果、国家によるデータ流入

---

401 Deibert and Rohozinski (2010), pp. 3–7.

402 Deibert R, Rohozinski R (2010), pp. 3–7; Aaronson and Leblond (2018), pp. 267–272; UNCTAD (2021), pp. 86–90, 114–116; UNIDIR (2023), pp. 4–9.

403 Aaronson and Leblond (2018), pp. 267–272; UNCTAD (2021), pp. 86–90, 114–116; OECD (2022a), pp. 40–42; UNIDIR (2023), pp. 4–12.

404 Aaronson and Leblond (2018), pp. 267–272; UNCTAD (2021), pp. 171–174, 183–184; OECD (2022a), pp. 34–35, 40–42; UNIDIR (2023), pp. 3–12.

405 Ensafi et al. (2015), pp. 63–71; Quan (2022), pp. 19–23; U.S. Department of State (2023), section 1(h) “Arbitrary or Unlawful Interference with Privacy, Family, Home, or Correspondence.”

406 Creemers (2017), pp. 86–93; Aaronson and Leblond (2018), pp. 267–272; Arner et al. (2022), pp. 660–676.

規制は、安全保障等の国家的利益と越境的なデータ流通の自由の間でいかに均衡を確保するかという、越境的データガバナンス規範再構成の核心的課題の一つを構成することになる[407]。

第 2 項　国家によるデータ流入規制に対する国際社会の動向

(1) 国家によるデータ流入規制と国際的人権規範

データ流入規制は、表面的には国家の主権的判断に基づく国内的措置として位置づけられる。国際法上、国家は自国領域内の通信や情報空間を統制する権限を有し、国家安全保障や公共秩序の維持を理由として国外からの情報流通を制限することが形式的には主権の範囲に含まれると解されている。しかし、インターネット遮断措置を含むデータ流入規制は、表現の自由や情報へのアクセス権といった国際人権法上の基本的権利に重大な影響を及ぼすため、国家による権限行使が無制約であるわけではなく、国際社会が共有する人権保障や自由な通信の原則との間に固有の緊張関係を生じさせる。

この点について、国際人権規約（ICCPR）第 19 条[408]は、情報を「あらゆる手段により、求め、受け、及び伝える自由」を保障し（同条第 2 項）、その制限を「法律で定められた場合」に限り、かつ「他者の権利又は信用の尊重」または「国家安全保障、公の秩序、公衆衛生又は公衆道徳の保護」を目的とする場合に限定すると規定している（同条第 3 項）。さらに、同条の適用に関し、国連自由権規約委員会「一般的意見第 34 号」（2011 年）で表現の自由に対する制限の要件として、法律に基づくこと（第 22 項）、制定目的に合致すること（第 33 項）に加え、必要性および比例性を明確に挙げている。すなわち、制限は「正当な目的のために必要不可欠」であり、かつ「最も侵襲性の低いもの（最も制限的でない手段）」でなければならないとされている（第 34 項）[409]。したがって、国家が国外からの情報流入を遮断する行為がこれらの要件を満たさない場合、表現の自由や知る権利の不当な制約として国際的に問題視され得る。

以上のように、国家によるインターネット遮断やデータ流入規制は、人権・貿易・通信の自由に関心を持つ他国や国際機関が異議を唱え得る国際的関心事項として扱われ、単なる国内規制の問題を超えて、国際的規範統治の枠組みの中に位置づけられている。

【参照条文等】

国際人権規約（ICCPR）

第 19 条（意見及び表現の自由）

1. すべての者は、干渉されることなく意見を持つ自由を有する。
2. すべての者は、表現の自由を有する。この権利には、国境を越えてあらゆる種類の情報及び思想を、口頭、文字、印刷、芸術、その他あらゆる手段により、求め、受け、及び伝える自由を含む。

---

[407] Aaronson and Leblond (2018), pp. 267–272; OECD (2022c), pp. 13–18, 27–30; Arner et al. (2022), pp. 660–676.

[408] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 19.

[409] 国連自由権規約委員会「一般的意見第 34 号（自由権規約第 19 条：意見及び表現の自由）」（2011 年）第 22 項、第 33 項–第 35 項. United Nations Human Rights Committee (2011), paras. 22, 33–35. https://undocs.org/CCPR/C/GC/34

3. 第 2 項の権利の行使には、特別の義務及び責任が伴う。このため、これらの権利の行使は、法律で定められた場合で、かつ、次に掲げる目的のために必要な限度においてのみ、一定の制限を受けることができる。

(a) 他者の権利又は信用の尊重のため

(b) 国家安全保障、公の秩序、公衆衛生又は公衆道徳の保護のため

国連自由権規約委員会「一般的意見第 34 号」(2011 年)

第 22 項

第 3 項は、表現の自由の制限を特定の条件に明確に限定している。制限は法律によって定められる場合にのみ許され、その法律は必要性及び比例性の要件を満たし、かつ第 3 項に掲げられた目的のために限られなければならない。法律は、個人が自己の行動をそれに従って調整できるよう、十分な明確性をもって規定され、かつ公に利用可能でなければならない。

第 33 項

制限は、その制定目的にのみ適用されるものでなければならず、かつ当該制限の根拠となる特定の必要性と直接に関連していなければならない。

第 34 項

制限は、正当な目的のために必要不可欠であることが求められる。制限措置は、厳格な必要性の基準に適合し、保護目的を達成し得る手段の中で最も侵襲性の低いもの(最も制限的でない手段)でなければならない。さらに、比例原則が遵守される必要がある。すなわち、保護目的を実現するための最も制限的でない手段が選択されるべきであり、制限は特定の目的に限定され、個人の他の権利を不当に侵害してはならない。

第 35 項

締約国が表現の自由の制限について正当な根拠を主張する場合には、脅威の具体的かつ個別的な性質、及び当該措置の必要性と比例性を立証しなければならない。特に、当該表現と主張される脅威との間に直接的かつ即時の関連性が存在することを明確に示す必要がある。

(2) 国家によるデータ流入規制に対する国際的批判

国家によるデータ流入規制やインターネット遮断に対しては、近年、他国や国際機関が様々な観点から批判を表明する例が増加している。これらの国際的批判は、人権侵害、貿易障壁、インターネットの一体性に対する弊害など、それぞれ異なる規範目的に基づいて展開されている。また、これらは、法的拘束力を伴うものに限らず、国連、WTO、地域協定、国際通信制度など複数のフォーラムを通じて外交的・制度的に展開されている。

国際人権法の分野では、国連人権理事会が 2016 年の決議において「オフラインで保障される権利はオンラインにおいても等しく保護されるべきである」と確認し、かつインターネット遮断を「情報へのアクセスおよび表現の自由に対する重大な侵害」として明確に非難した[410]。この決議は、国家による通信遮断を人権侵害行為として明示的に位置づけた点で重要であり、その後の

[410] 国連人権理事会「『オンラインにおける人権の促進、保護及び享有』に関する決議」(A/HRC/32/L.20, 2016 年 7 月 1 日)前文および第 1 項. United Nations Human Rights Council (2016), Resolution A/HRC/32/L.20: The promotion, protection and enjoyment of human rights on the Internet, adopted 1 July 2016, preamble and para. 1. https://undocs.org/A/HRC/32/L.20

国連特別報告者の声明や普遍的定期審査（UPR）において各国の遮断事例が繰り返し問題化される契機となった。たとえば、ミャンマーやイランの大規模遮断に対しては、国連特別報告者が ICCPR 第 19 条違反を指摘し、EU や日本、カナダなどが共同声明を通じて批判した[411]。

さらに、国際経済法・通商法の分野においても、国家によるデータ流入制限は国際的懸念事項として取り扱われている。WTO 電子商取引共同声明イニシアティブ（JSI）においては、日本、EU、米国などが、各国による過度なデータアクセス制限やローカライゼーション措置をデジタル貿易に対する障壁となり得るものとして問題視し、自由で信頼に基づくデータ流通（DFFT）の理念と整合的なルールの構築を主張してきた[412]。また、米国通商代表部（United States Trade Representative: USTR）が毎年公表する外国貿易障壁報告書では、中国のウェブサイト遮断やフィルタリングをはじめとする各国のオンラインアクセス制限が、米国企業の越境的なデジタルサービス提供を妨げる貿易上の障壁として繰り返し指摘されている[413]。

加えて、国際通信制度においても、ITU、ICANN、IETF といった技術ガバナンス機構が、国家による越境通信遮断に対して制度的・技術的な異議を表明してきた。たとえば、2013 年 10 月のモンテヴィデオ声明では、ICANN、IETF、ISOC などが「国家または地域によるインターネット分断を回避すべき」と明記し、インターネットの統一性を損なう国家的遮断政策に対して警鐘を鳴らした[414]。

以上のように、国家によるデータ流入規制はもはや純粋な国内問題にとどまらず、国際人権法、通商法、通信法といった複数の国際的規範体系にまたがる問題として認識されている。各国や国際機関による異議申立ては、国家主権の行使が国際的義務と衝突し得ることを示し、データ流通の自由と人権保障をめぐる新たな国際的規範対立の焦点を形成している。

【参照条文等】

国連人権理事会「『オンラインにおける人権の促進、保護及び享有』に関する決議」

オフラインで保障される権利はオンラインにおいても同様に保護されるべきであることを確認し、表現の自由が世界人権宣言並びに市民的及び政治的権利に関する国際規約第 19 条に基づき、国境を越え、いかなる媒体を通じても適用されることを強調する。

第 3 項　越境的データガバナンス規範再構成の方向性

国家によるデータ流入規制は、一般的には情報へのアクセス権や表現の自由を制約する行為として国際的に批判されるが、一定の条件下ではその正当性が限定的に認められる余地がある。これは、国家が自国の安全や公共秩序を維持する責任を負う以上、越境的な情報流通の自由と安全保障・公共利益との間で一定の調整を図らざるを得ないという現実的要請に基づいている。

---

411 European External Action Service (EEAS) (2023); United Nations Human Rights Council (2023), paras. 53–55.

412 WTO (2021); Burri and Kugler (2024), pp. 400–411.

413 USTR (2024), pp. 49–55.

414 Montevideo Statement on the Future of Internet Cooperation, 7 October 2013, ICANN. https://www.icann.org/en/news/announcements/announcement-07oct13-en.htm

第一に、国家安全保障上の理由が挙げられる。サイバー攻撃や外国勢力による世論操作、偽情報の拡散といった事象は国家の主権や社会的安定を脅かす現実的な脅威となり得るため、国家は国外発の通信や情報流入を制限することがある。たとえば、武力紛争や内戦状態において軍事作戦に関連する通信を遮断する行為は、情報統制としてではなく、防衛上の必要措置として理解される場合がある。このようなケースでは、データ流入規制は国家の自存確保のための安全保障政策の一環として位置づけられる[415]。

第二に、公共目的の達成を理由とするケースである。国外から流入する情報が犯罪行為や社会的混乱を助長する場合、国家はその拡散を防止する義務を負う。たとえば、児童ポルノ、テロ関連情報、ヘイトスピーチ、誤情報などが越境的に流入する際、国家が通信事業者やプラットフォーム事業者に対してブロッキングや削除を命じることは珍しくない。このような措置は公共の安全や人権保護を目的とする限り、国際的にも一定の合理性が認められている[416]。近年では、国際的なサイバー犯罪条約（ブダペスト条約）[417]や EU のデジタルサービス法（DSA）[418]などが、国家による限定的な介入の制度的位置づけを明確化している。

第三に、文化的・倫理的価値の保護という観点からの正当化も存在する。国家は国内の宗教的・文化的価値観を尊重する立場から、特定のコンテンツやプラットフォームへのアクセスを制限する場合がある。イスラム諸国では、宗教的教義に反するとされる表現を防ぐ目的で国外発の情報をブロックする事例が報告されている[419]。このような措置は文化的自決権や社会的調和の維持という観点から一定の理解を得る場合もあり、必ずしも正当化根拠に乏しいわけではない。ただし、政治的抑圧や恣意的検閲に転化する危険性を伴うため、正当化の根拠と限界は慎重に吟味される必要がある。

以上のように、国家によるデータ流入規制は、国家安全保障、公共利益、文化的秩序の保護といった明確な目的に基づき、かつ必要最小限の範囲にとどまる場合に限り、国際的に容認される余地がある。他方で、その範囲を超えた恣意的な情報遮断や政治的動機による規制は国際人権法上の義務に反し、国際社会から強い批判を招く。こうした国際的潮流を踏まえ、国家による包括的通信遮断を抑制し、必要性と比例性に基づくリスクベースアプローチの導入を求める議論が進展している[420]。近年では、全面的な通信停止ではなく、特定地域、特定サービス、あるいは時間的に限定した接続制御を行うことで、権利侵害を最小化しつつ公共目的を達成する方策が模索されつつある[421]。

---

415 Kuner (2011), pp. 22–24; Office of the United Nations High Commissioner for Human Rights (2022), paras. 8, 24, 33–34.

416 Burri (2017), pp. 87–93; United Nations Human Rights Committee (2011), paras. 34–36, 43.

417 Council of Europe (2001) Convention on Cybercrime (Budapest Convention), ETS No. 185, adopted 23 Nov 2001, entered into force 1 July 2004. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

418 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). OJ L 277, 27.10.2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

419 Shishkina and Issaev (2018), pp. 2–7.

420 Breitbarth (2021), pp. 541–546; Office of the United Nations High Commissioner for Human Rights (2022), paras. 8, 24, 59–61.

421 Carnegie Endowment for International Peace (2022); Internet Society (2025).

国連人権理事会や国際 NGO（Access Now など）は、インターネット遮断を人権侵害として一貫して非難しており[422]、その国際的監視の枠組みは拡大している。Cloudflare Radar[423]や NetBlocks[424]といったインターネットトラフィック可視化ツールの発展、Access Now をはじめとする市民社会組織による監視・訴訟活動の強化、そして国際機関による規範形成の動きは、国家による過剰な通信統制を抑制する複層的な対応を形成しつつある。これらの動向は、デジタル時代における人権保障の新たな試金石として、国際法的・制度的な議論の深化を促す契機となっている[425]。

したがって、越境的データガバナンス規範再構成においては、国家によるデータ流入規制を主権的裁量の問題として放置するのではなく、国際人権法・通商法・技術ガバナンスといった複数の規範体系との整合性を確保しつつ、その正当化根拠と限界を透明な手続と明確な評価基準の下で再定義する必要がある[426]。情報遮断が安全保障や公共目的を根拠として一定の合理性を有し得るとしても、その適用は必要最小限にとどめられ、かつ実質的リスクに応じた比例的措置として構築されなければならない。全面的な通信停止のような広範な介入ではなく、対象領域の特定、時間的限定、技術的代替手段の確保といった、権利侵害の最小化を前提とする制度設計が求められる[427]。そして、国家による情報遮断の実態を国際的に可視化し、独立的監視と説明責任を制度化することは、グローバルな信頼形成の基盤を整えるうえで不可欠である[428]。こうした枠組みを整備することによって初めて、各国が安全保障上の懸念を抱えつつも、越境的なデータ流通の自由を維持し、国際的協調を促進することにつながる[429]。

第Ⅲ部で検討する CRDM モデルは、データの性質と利用文脈によって評価されるリスクに応じて、データ移転規制を必要最小限に限定すべきであるとするもので、国家による過剰なデータ流入規制を問題視する最近の国際的潮流と軌を一にする。国家が自国の責務を全うするために極めて限られた範囲のデータ流入規制が国際的に容認される余地があるとしても、権利侵害を最小化しつつ公共目的を達成するための方策が講じられなければならない。CRDM モデルは、この要請に応えるべく、実質的リスクに即した段階的保護措置を提示することで、国家規制と越境的データ流通の調和を図る制度的枠組みを提供するものである。

---

422 United Nations Human Rights Council (2022b), paras. 8, 24, 59–61; Access Now (2025), pp. 7–10, 12–14, 24–27.
423 Cloudflare (2024) Cloudflare Radar. https://radar.cloudflare.com (accessed 22 February 2026).
424 NetBlocks (2026) NetBlocks. https://netblocks.org (accessed 22 February 2026).
425 Carnegie Endowment for International Peace (2022); Access Now (2025), pp. 4–6, 12–14, 24–27
426 WTO (2021); OECD (2022e), Principles I–II, V–VII; Burri and Kugler (2024), pp. 400–407, 411–423.
427 United Nations Human Rights Committee (2011), paras. 34–36, 43; Office of the United Nations High Commissioner for Human Rights (2022), paras. 59–61.
428 Office of the United Nations High Commissioner for Human Rights (2022), paras. 24, 59–61; United Nations Human Rights Council (2023), paras. 20–27, 61–64; Access Now (2025), pp. 22–24.
429 WTO (2021); OECD (2022e), Principles I–II, V–VII; Burri and Kugler (2024), pp. 400–407, 411–423.

参考文献(第Ⅱ部)(本文との対応関係は各頁に脚注番号で表示)

Aaronson SA (2018) Data is different: Why the world needs a new approach to governing cross-border data flows. CIGI Papers No. 197, November 2018, 1–22. https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows/

Aaronson SA (2019) What are we talking about when we talk about digital protectionism? World Trade Review, 18(4): 541–577. https://doi.org/10.1017/S1474745618000198

Aaronson SA (2025) A difficult balance: privacy, national security and the free flow of data. CIGI Paper No. 330, Centre for International Governance Innovation, August 2025, 1–23. https://www.cigionline.org/documents/3472/Susan_Ariel_Aaronson_.pdf

Aaronson SA, Leblond P (2018) Another digital divide: The rise of data realms and its implications for the WTO. Journal of International Economic Law 21(2): 245–272. https://doi.org/10.1093/jiel/jgy019

Access Now (2025) Keep it on 2024: Global internet shutdowns report. Access Now, New York. https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf

Akbarzadeh S, Hoffmann C, Rahim M, Smith B (2024) Cyber surveillance and digital authoritarianism in Iran. Global Policy (March 2024), 1–11. https://www.globalpolicyjournal.com/sites/default/files/pdf/Akbarzadeh%20et%20al.%20-%20Cyber%20Surveillance%20and%20Digital%20Authoritarianism%20in%20Iran.pdf

Allman TY (2006) The impact of the proposed federal e-discovery rules. Richmond Journal of Law and Technology 12(4): 1–25. https://scholarship.richmond.edu/jolt/vol12/iss4/2

Amnesty International and Privacy International (2015) Two years after Snowden: Protecting human rights in an age of mass surveillance. June 2015. https://www.amnesty.nl/content/uploads/2015/06/two_years_after_snowden_final_report_en_a4.pdf

Amram PhW (1970), Explanatory Report on the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters. Hague Conference on Private International Law. https://assets.hcch.net/docs/9983529a-481a-4eae-9900-8f971ec70c11.pdf

Arner DW, Castellano GG, Selga ĒK (2022) The transnational data governance problem. Berkeley Technology Law Journal 37(2): 623–692. https://btlj.org/wp-content/uploads/2023/04/0001-37-2-Arner-web-4-10.pdf

ARTICLE 19 (2017) Germany: The act to improve enforcement of the law in social networks (Network Enforcement Act). ARTICLE 19, London. https://www.article19.org/resources/germany-act-improve-enforcement-law-social-networks/

Asmolov G (2024) The history of Russian media and internet regulation. In: Sloane W, Raspopina A (eds), Kremlin Media Wars: Censorship and Control Since the Invasion of Ukraine. Routledge, London and New York, 33–43. https://library.oapen.org/bitstream/handle/20.500.12657/101135/9781003483908_10.4324_9781003483908-5.pdf

Baark E (2024) China's Digital Silk Road: Innovation in a new geopolitical environment. East Asian Policy 16: 25–38. https://doi.org/10.1142/S1793930524000023

Bailey R, Parsheera S (2018) Data localisation in India: questioning the means and ends. NIPFP Working Paper No. 242, National Institute of Public Finance and Policy, New Delhi, 1–51. https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf

Bannelier K (2025) Risks and opportunities of the UN cybercrime convention for the UNDOC & the fight against transnational organised crime: A first assessment. Transnational Criminal Law Review 4(1): 140–155. https://doi.org/10.22329/tclr.v4i1.9468

Belt WW Jr (2024) Cross-border eDiscovery: complexities of international data sources and data protection laws. CDS Legal, 16 May 2024. https://cdslegal.com/insights/cross-border-ediscovery-complexities-of-international-data-sources-and-data-protection-laws/

Bento LVM (2020) The globalization of discovery. Kluwer Law International, Alphen aan den Rijn.

Bilgic S (2018) Something old, something new, and something moot: the privacy crisis under the CLOUD Act. Harvard Journal of Law & Technology 32(1): 321–356. https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech321.pdf

Birnhack M D, Mundlak G (2025) Brussels effect(s) and the rise of a privacy profession. International Data Privacy Law, 138–156. https://doi.org/10.1093/idpl/ipaf005

Bloch-Wehba H (2019) Global platform governance: Private power in the shadow of the state. SMU Law Review 72(1): 27–83. https://scholar.smu.edu/smulr/vol72/iss1/9/

Bock K, Naval G, Reese K, Levin D (2021) Even censors have a backup: Examining China's double HTTPS censorship middleboxes. FOCI 2021: 1–7. https://doi.org/10.1145/3473604.3474559

Bradford A (2020) The Brussels effect: how the European Union rules the world. Oxford University Press, Oxford.

Breitbarth P (2021) A risk-based approach to international data transfers. European Data Protection Law Review 7(4): 539–549. https://doi.org/10.21552/edpl/2021/4/9

British Chamber of Commerce in China (2023) New regulations on the filing of mobile apps. 2023.09.04. https://britishchamber.cn/en/new-regulations-on-the-filing-of-mobile-apps/

Brupbacher OM (2019) Navigating data privacy in complex cross-border discovery. The Sedona Conference, June 11 2019, 1–6. https://www.thesedonaconference.org/sites/default/files/conference_papers/Required%202.2-%20Navigating%20Data%20Privacy%20in%20Complex%20Cross-Border%20Discovery_Brupbacher%20%5Bupdated%5D.pdf

Burri M (2017) The governance of data and data flows in trade agreements: the pitfalls of legal adaptation. UC Davis Law Review 51(1): 65–132. https://lawreview.law.ucdavis.edu/archives/51/1/governance-data-and-data-flows-trade-agreements-pitfalls-legal-adaptation

Burri M, Kugler R (2024) Regulatory autonomy in digital trade agreements. Journal of International Economic Law 27(3): 397–424. https://academic.oup.com/jiel/article/27/3/397/7718688

Carnegie Endowment for International Peace (2022) Government internet shutdowns are changing: how should citizens and democracies respond? Washington DC. https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en

Cate FH, Dempsey JX, Rubinstein IS (2012) Systematic government access to private sector data. International Data Privacy Law 2: 195–199. https://www.repository.law.indiana.edu/facpub/2615

Cavanagh ED (2021) Discovery in federal courts in support of foreign litigation: lending a helping hand or legal imperialism? Federal Courts Law Review 13: 81–111. https://www.fclr.org/content/uploads/2021/09/Cavanagh_Macro_Final-jmf.pdf

Centre for International Trade and Policy (CITP) (2024) Interoperability of data governance regimes: challenges for digital trade policy. Centre for International Trade and Policy, 1–11. https://citp.ac.uk/publications/interoperability-of-data-governance-regimes-challenges-for-digital-trade-policy

Center for Strategic and International Studies (CSIS) (2019) North Koreans want external information, but Kim Jong-un seeks to limit access. CSIS, Washington, DC. https://www.csis.org/analysis/north-koreans-want-external-information-kim-jong-un-seeks-limit-access

Chen X, Gao X (2024) Norm diffusion in cyber governance: China as an emerging norm entrepreneur?, International Affairs 100(6): 2419–2440. https://doi.org/10.1093/ia/iiae237

Cheney CT (2021) The digital silk road: understanding China's technological rise and the implications for global governance. In: Chaisse J, Górski J (eds) Research handbook on the Belt and Road Initiative. Edward Elgar, Cheltenham, 88–101. https://www.academia.edu/74809503

Christakis T (2024a) The "zero risk" fallacy: International data transfers, foreign governments' access to data, and the need for a risk-based approach. Centre for Information Policy Leadership & Cross-Border Data Forum, 1–95. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_zero_risk_fallacy_-_t.christakis_feb24.pdf

Christakis T (2024b) Data free flow with trust: current landscape, challenges and opportunities. Journal of Cyber Policy 9(1): 95–120. https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2421838

Cleary Gottlieb (2019) U.S. CLOUD Act's potential impact on the GDPR. 3 September 2019. https://www.clearygottlieb.com/news-and-insights/publication-listing/us-cloud-acts-potential-impact-on-the-gdpr

Cochrane T (2021) Digital privacy rights and CLOUD Act agreements. Brooklyn Journal of International Law 47(1): 1–88. https://brooklynworks.brooklaw.edu/bjil/vol47/iss1/1/

Cochrane T (2022) Hiding in the eye of the storm cloud: how CLOUD Act agreements expand U.S. extraterritorial investigatory powers. Duke Journal of Comparative & International Law 32(1): 153–210. https://scholarship.law.duke.edu/djcil/vol32/iss1/4/

Cory N, Dick E, Castro D (2020) The role and value of standard contractual clauses in EU U.S. digital trade, 19. Information Technology and Innovation Foundation. https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade

Cory N, Dascoli E (2021) How barriers to cross-border data flows are spreading globally, what they cost, and how to address them. Information Technology and Innovation Foundation. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/?utm_source=chatgpt.com

Creemers R (2017) Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. Journal of Contemporary China 26(103), 85–100. https://doi.org/10.1080/10670564.2016.1206281

Creemers R (2021) China's cyber governance institutions. Leiden Asia Centre, Leiden, 1–22. https://leidenasiacentre.nl/wp-content/uploads/2021/01/Chinas-Cyber-Governance-Institutions-Layout-geconverteerd-1.pdf

Curran VG (2016) United States discovery and foreign blocking statutes. Louisiana Law Review 76: 1141–1149. https://digitalcommons.law.lsu.edu/lalrev/vol76/iss4/11/

Dai Y (2022) Cross-border data transfers regulations in the context of international trade law: a PRC perspective. Springer, Singapore.

Dale JG, Aizawa N (2024) Data Free Flow with Trust: Japan's struggle to integrate democracy and human rights into digital trade policy Frontiers in Sociology 9 Article 1397528, 1–8. https://www.frontiersin.org/articles/10.3389/fsoc.2024.1397528/full

de Bruin R (2022) A comparative analysis of the EU and U.S. data privacy regimes and the potential for convergence. University of Luxembourg Law Research Paper No. 2022–007, 127–166. https://papers.ssrn.com/abstract_id=4251540

Deibert R, Rohozinski R (2010) Beyond denial: introducing next-generation information access controls. In: Deibert R, Palfrey J, Rohozinski R, Zittrain J (eds) Access controlled: the shaping of power, rights, and rule in cyberspace. MIT Press, Cambridge, MA, 3–13. https://doi.org/10.7551/mitpress/8551.003.0006

Dekker B, Okano-Heijmans M, Zhang ES (2020) Unpacking China's Digital Silk Road. Clingendael Institute, 1–17. https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf

Del Giovane C, Ferencz J, López González J (2023) The nature, evolution and potential implications of data localisation measures. In: Organisation for Economic Co operation and Development, OECD Trade Policy Papers No 278. OECD Publishing, Paris. https://doi.org/10.1787/179f718a-en

Dike MC, Owusu RA (2024) China–Africa relationships: A systematic literature review and research agenda. Africa Journal of Management 10(4): 464–499. https://doi.org/10.1080/23322373.2024.2421709

Dimitropoulos G, Chen RC, Chaisse J (2025) Plurilateralism: a new form of international economic ordering? Journal of World Investment & Trade 26(1–2): 1–30. https://doi.org/10.1163/22119000-12340350

DLA Piper (2025a), Data protection laws in Russia. DLA Piper, London. https://www.dlapiperdataprotection.com/index.html?c=RU&t=about (accessed 22 February 2026).

DLA Piper (2025b) Data protection laws in Turkey. DLA Piper, London. https://www.dlapiperdataprotection.com/index.html?c=TR&t=about (accessed 22 February 2026).

Docksey C, Propp K (2023) Government access to personal data and transnational interoperability: An accountability perspective. Oslo Law Review 10(1): 1–34. https://doi.org/10.18261/olr.10.1.2

Dodge WS (2015) International comity in American law. Columbia Law Review 115: 2071–2146. https://columbialawreview.org/content/international-comity-in-american-law/

EDPB (2020a) Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, adopted 10 November 2020.

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
EDPB (2020b) Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, adopted 10 November 2020. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en
EDPB (2020c) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, adopted 20 October 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
EDPB (2020d) Guidelines 05/2020 on consent under Regulation 2016/679, adopted 4 May 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
EDPB (2021a) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18 June 2021. https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
EDPB (2021b) Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, adopted Nov. 18, 2021, last revised Feb. 14, 2023. https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf
Ensafi R, Fifield D, Winter P, Feamster N, Weaver N, Paxson V (2015) Analyzing the Great Firewall of China over space and time. Proceedings on Privacy Enhancing Technologies 2015(1): 61–76. https://doi.org/10.1515/popets-2015-0005
Epifanova A (2020) Deciphering Russia's "sovereign internet law": tightening control and accelerating the splinternet. DGAP Analysis 2/2020. Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V., 1–11. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law
Erie MS, Streinz T (2021) The Beijing effect: China's "Digital Silk Road" as transnational data governance. New York University Journal of International Law and Politics 54: 1–44. https://cld.web.ox.ac.uk/article/beijing-effect-chinas-digital-silk-road-transnational-data-governance
European Commission (2021) Commission implementing decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L 199) 31. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
European Commission (2023a) Adequacy decisions: how the EU determines if a non-EU country has an adequate level of data protection. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
European Commission (2023b) Commission implementing decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-U.S. data privacy framework, 2023 O.J. (L 231) 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023D1795
European Data Protection Board and European Data Protection Supervisor (2019) EDPB-EDPS joint response to the LIBE Committee on the impact of the US CLOUD Act on the European legal framework for personal data protection. 12 July 2019. https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en
European Data Protection Board (2024) Report on the first review of the EU-US Data Privacy Framework, 4 November 2024, European Data Protection Board. https://edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf (accessed 22 February 2026).
European External Action Service (EEAS) (2023) Joint statement on internet shutdowns on behalf of 54 countries, delivered at HRC 53, 3 July 2023. https://www.eeas.europa.eu/delegations/un-geneva/hrc53-joint-statement-internet-shutdowns-behalf-group-countries-0_en
European Union Institute for Security Studies (2021) China's data strategy. https://www.iss.europa.eu/publications/briefs/chinas-data-strategy

Federal Judicial Center (2015) Amendments to the federal rules of practice and procedure: Civil rules 2015—Proportionality and changes to the discovery process (video transcript), 1–7. https://www.fjc.gov/sites/default/files/2016/Proportionality%20%28Koeltl%29_0.pdf

Ferracane MF (2021) The costs of data protectionism. In: Burri M (ed) Big Data and Global Trade Law, 63–82. Cambridge University Press, Cambridge. https://doi.org/10.1017/9781108919234.005

Fisher S (2018) Testing the importance of information control to Pyongyang: How North Korea reacts to the diplomatic, information, military and economic tools of statecraft. International Journal of Korean Unification Studies 27(2): 67–111. https://repo.kinu.or.kr/bitstream/2015.oak/9823/4/3.%20Testing%20the%20Importance%20of%20Information%20Control%20to%20Pyongyang.pdf

Freedom House (2020) User privacy or cyber sovereignty? Human rights and data localization. Freedom House, Washington, D.C. https://freedomhouse.org/sites/default/files/2020-07/FINAL_Data_Localization_human_rights_07232020.pdf

Freedom House (2022) Freedom on the net 2022: countering an authoritarian overhaul of the internet. Freedom House, Washington, D.C. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

Freedom House (2023a) Egypt: Freedom on the Net 2023. Freedom House, Washington, D.C. https://freedomhouse.org/country/egypt/freedom-net/2023

Freedom House (2023b) Indonesia: Freedom on the Net 2023. Freedom House, Washington, D.C. https://freedomhouse.org/country/indonesia/freedom-net/2023

Freedom House (2023c) Turkey: Freedom on the Net 2023. Freedom House, Washington, D.C. https://freedomhouse.org/country/turkey/freedom-net/2023

Freedom House (2023d) Brazil: Freedom on the Net 2023. Freedom House, Washington, D.C. https://freedomhouse.org/country/brazil/freedom-net/2023

Freedom House (2024a) Freedom on the Net 2024: Russia Country Report. Freedom House, Washington, D.C. https://freedomhouse.org/country/russia/freedom-net/2024

Freedom House (2024b) Freedom on the Net 2024: Iran Country Report. Freedom House, Washington, D.C. https://freedomhouse.org/country/iran/freedom-net/2024

Freedom House (2024c) Freedom on the Net 2024: Turkey Country Report. Freedom House, Washington, D.C. https://freedomhouse.org/country/turkey/freedom-net/2024

Freedom House (2024d) Freedom on the Net 2024: India Country Report. Freedom House, Washington, D.C. https://freedomhouse.org/country/india/freedom-net/2024

Freedom House (2024e) Freedom in the World 2024: North Korea Country Report. Freedom House, Washington, D.C. https://freedomhouse.org/country/north-korea/freedom-world/2024

Gensler SS, Rosenthal LH (2013) The reappearing judge. University of Kansas Law Review 61: 849–875. https://digitalcommons.law.ou.edu/fac_articles/112/

Greenleaf G (2021) Global data privacy laws 2021: despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report 169: 10–13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

G7 Digital and Technology Ministers (2021), G7 Digital and Technology Ministers' Declaration, 28 April 2021. https://assets.publishing.service.gov.uk/media/608933688fa8f51b92e94d84/G7_Digital_and_Technology_Ministerial_Declaration.pdf

Gstrein OJ, Zwitter AJ (2021) Extraterritorial application of the GDPR: promoting European values or power? Internet Policy Review 10(3): Article 1576, 1–30. https://doi.org/10.14763/2021.3.1576

Gunitsky S (2015) Corrupting the cyber-commons: Social media as a tool of autocratic stability. Perspect Polit 13(1): 42–54. https://doi.org/10.1017/S1537592714003120

Gurkov A (2020) Personal data protection in Russia. In: Gritsenko D, Wijermars M, Kopotev M (eds) The Palgrave handbook of digital Russia studies. Springer, Cham, 95–113. https://doi.org/10.1007/978-3-030-42855-6_6

Hamlett JC (2017) The constitutionality of Russia's "undesirable" NGO law. UCLA Journal of International Law and Foreign Affairs 21: 245–282. https://www.jstor.org/stable/45302421

Han S (2024) Data and statecraft: why and how states localize data. Business and Politics 26: 263–288. https://doi.org/10.1017/bap.2023.41

Harkness TP, Moloo R, Oh P, Yim C (2015) Discovery in international civil litigation: a guide for judges, 1–124. Federal Judicial Center, Washington, DC. https://www.fjc.gov/content/309496/discovery-international-civil-litigation-guide-judges

Harwit E, Clark D (2001) Shaping the internet in China: evolution of political control over network infrastructure and content. Asian Survey 41(3): 377–408. https://library.fes.de/libalt/journals/swetsfulltext/14218789.PDF

Heldt A (2019) Reading between the lines and the numbers: An analysis of the first NetzDG reports. Internet Policy Review 8(2): 1–19. https://doi.org/10.14763/2019.2.1398

Hoda MJ (2018) The Aerospatiale dilemma: Why US courts ignore blocking statutes and what foreign states can do about it. California Law Review 106: 231–262. https://dx.doi.org/10.15779/Z38BZ6181D

Human Rights Watch (2016) Russia: "Big Brother" law harms security, rights (12 July 2016). https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights (accessed 22 February 2026).

Human Rights Watch (2020) Russia: growing internet isolation, control, censorship (18 June 2020). Human Rights Watch. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship (accessed 22 February 2026).

Human Rights Watch (2022) Turkey: Dangerous, dystopian new legal amendments. Human Rights Watch. https://www.hrw.org/news/2022/10/14/turkey-dangerous-dystopian-new-legal-amendments

Hung HT (2025) Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach. Journal of Computational Social Science 8, Article 24, 1–31. https://doi.org/10.1007/s42001-024-00346-8

Igaya S, Sudoh O (2025) Ignored discrepancies in the fundamental concepts of data protection laws in Japan and the EU. International Data Privacy Law 15(2): 171–185. https://doi.org/10.1093/idpl/ipaf015

Information Technology & Innovation Foundation (ITIF) (2025) Indonesia's data localization regulation. 9 June 2025. https://itif.org/publications/2025/06/09/indonesia-data-localization-regulation

Innis M, Wiyoso A (2018) General data localization requirements in Indonesia, 1–6. Baker McKenzie Insight, July 2018. https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al_generaldatalocalizationrequirements_july2018.pdf

International Telecommunication Union (ITU) (2025) Measuring digital development: Facts and Figures 2025. ITU, Geneva. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Internet Freedom Foundation (2021) How the intermediaries rules are anti-democratic and unconstitutional. 27 Feb 2021. https://internetfreedom.in/intermediaries-rules-2021/

Internet Society (2025) Policy Brief: Internet Shutdowns. Internet Society, Geneva. https://www.internetsociety.org/resources/policybriefs/2025/internet-shutdowns/

ITP Staff (2016) RTA and Huawei sign smart roads of the future deal. ITP.net, 20 October 2016. https://www.itp.net/news/609848-rta-and-huawei-sign-smart-roads-of-the-future-deal

Jackson JH (2003) Sovereignty modern: a new approach to an outdated concept. American Journal of International Law 97: 782–802. https://scholarship.law.georgetown.edu/facpub/110

Javed Y, Sajid A (2024) A systematic review of privacy policy literature. ACM Computing Surveys 57(2): 1–43. https://doi.org/10.1145/3698393

Jiang M (2024) Models of state digital sovereignty from the Global South: diverging experiences from China, India and South Africa. Policy Internet 16(4): 727–738. https://doi.org/10.1002/poi3.427

Kaya M, Shahid H (2025) Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. Interdisciplinary Studies in Society, Law, and Politics 4(2): 219–233. https://doi.org/10.61838/kman.isslp.4.2.20

King G, Pan J, Roberts ME (2017) How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. American Political Science Review 111(3): 484–491. https://doi.org/10.1017/S0003055417000144

Knockel J, Crete-Nishihata M, Ng J Q, Senft A, Crandall J R (2015) Every rose has its thorn: Censorship and surveillance on social video platforms in China. 5th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2015), Washington, D.C. 1–10. https://www.usenix.org/conference/foci15/workshop-program/presentation/knockel

Krupskiy M (2023) The impact of Russia's "foreign agents" legislation on civil society. Fletcher Forum of World Affairs 47: 65–82. https://sites.tufts.edu/fletcherrussia/the-impact-of-russias-foreign-agents-legislation-on-civil-society/

Kuner C (2011) Regulation of transborder data flows under data protection and privacy law: past, present and future. OECD Digital Economy Papers, No. 187. OECD Publishing, Paris, 1–31. https://doi.org/10.1787/5kg0s2fk315f-en

Kuner C (2015) Extraterritoriality and regulation of international data transfers in EU data protection law. International Data Privacy Law 5(4): 235–245. https://ssrn.com/abstract=2644237

Kuner C (2017a) Reality and illusion in EU data transfer regulation post Schrems. German Law Journal 18(4): 881–918. https://www.cambridge.org/core/journals/german-law-journal/article/reality-and-illusion-in-eu-data-transfer-regulation-post-schrems/0341A0D14DC345730F9B48A496A968D3

Kuner C (2017b) The Internet and the global reach of EU law. In: Cremona M, Scott J (eds) EU law beyond EU borders: The extraterritorial reach of EU law. Oxford University Press, Oxford, 83–102. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930

Lalova-Spinks T, Valcke P, Ioannidis J P A, Huys I (2024) EU-US data transfers: An enduring challenge for health research collaborations. NPJ Digital Medicine 7(1): 215, 1–5. https://doi.org/10.1038/s41746-024-01205-6

Lee JA, Liu CY (2016) Real name registration rules and the fading digital anonymity in China. Washington International Law Journal 25: 1–38. https://digitalcommons.law.uw.edu/wilj/vol25/iss1/3

Litvinenko A (2021) Re-defining borders online: Russia's strategic narrative on internet sovereignty. Media and Communication 9(4): 5–15. https://doi.org/10.17645/mac.v9i4.4292

Li W, Chen J (2024) From Brussels effect to gravity assists: understanding the evolution of the GDPR-inspired Personal Information Protection Law in China. Computer Law & Security Review 53: 106069, 1–14. https://doi.org/10.1016/j.clsr.2024.105994

Luisi M (2022) GDPR as a global standard? Brussels' instrument of policy diffusion. E-International Relations. https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/

Mahon A, Walker S (2024) Russia's digital repression landscape: Unraveling the Kremlin's digital repression tactics. Journal of Illiberalism Studies 4: 29–64. https://www.illiberalism.org/wp-content/uploads/2025/01/Anastassiya-Mahon-and-Scott-Walker-Russias-Digital-Repression-Landscape-1.pdf

Malkawi BH (2006) E-commerce in light of international trade agreements. MPRA Paper No. 90521, 1–17. https://ideas.repec.org/p/pra/mprapa/90521.html

Manners I (2002) Normative power Europe: a contradiction in terms? Journal of Common Market Studies 40(2): 235–258. https://www.princeton.edu/~amoravcs/library/mannersnormativepower.pdf

Marczak B, Weaver N, Dalek J, Ensafi R, Fifield D, McKune S, Rey A, Deibert R, Paxson V (2015)
China's Great Cannon. Citizen Lab Research Report No. 2015-34, University of Toronto, 1–19. https://citizenlab.ca/2015/04/chinas-great-cannon/

Master A, Garman C (2023) A worldwide view of nation-state internet censorship. Free and Open Communications on the Internet 2023(1): 1–21. https://www.petsymposium.org/foci/2023/foci-2023-0008.pdf

McCarthy LA, Rice D, Lokhmutov A (2023) Four months of "discrediting the military": Repressive law in wartime Russia. Demokratizatsiya 31: 125–150. https://muse.jhu.edu/article/889912

McMahan HB, Moore E, Ramage D, Hampson S, Agüera y Arcas B (2017) Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th international conference on artificial intelligence and statistics (AISTATS 2017), vol 54, 1273–1282. https://proceedings.mlr.press/v54/mcmahan17a/mcmahan17a.pdf

Miura H (2023) Japan's role and strategy in the formation of digital trade rules in the Indo-Pacific. NBR Commentary (January 10, 2023). https://www.nbr.org/publication/japans-role-and-strategy-in-the-formation-of-digital-trade-rules-in-the-indo-pacific/

Moerel L (2022) What happened to the risk-based approach to data transfers? Future of Privacy Forum Blog (Sept. 27, 2022). https://fpf.org/blog/what-happened-to-the-risk-based-approach-to-data-transfers/

Morishita S, Tschofenig H, Kühlewind M, Nottingham M, Schleizer S, Sy S (2023) RFC 9505: A survey of worldwide censorship techniques. Internet Research Task Force (IRTF), Privacy Enhancements and Assessments Research Group (PEARG). https://www.rfc-editor.org/rfc/rfc9505.html

Nanni R (2024) The false promise of individual digital sovereignty in Europe: Comparing artificial intelligence and data regulations in China and the European Union. Policy & Internet 16(3), 711–726. https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.424

New York City Bar Association, E-Discovery Working Group (2020) Cross-border e-discovery: Navigating foreign data privacy laws and blocking statutes in U.S. litigation. New York City Bar Association. https://www.nycbar.org/reports/cross-border-e-discovery-navigating-foreign-data-privacy-laws-and-blocking-statutes-in-u-s-litigation/

Nocetti J (2024) A splintered Internet? Internet fragmentation and the strategies of China, Russia, India and the European Union. IFRI. 1–32. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_internet_fragmentation_february_2024.pdf

OECD (2019a) Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies. OECD Publishing, Paris. https://doi.org/10.1787/276aaca8-en

OECD (2022a) Going digital to advance data governance for growth and well-being. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/going-digital-to-advance-data-governance-for-growth-and-well-being_246d8cab/e3d783b0-en.pdf

OECD (2022b) Cross-border data flows: Regulatory barriers and the need for proportionality. OECD Publishing, Paris. https://doi.org/10.1787/5031dd97-en

OECD (2022c) Fostering cross-border data flows with trust. OECD Digital Economy Papers No. 343. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/fostering-cross-border-data-flows-with-trust_617f8e3f/139b32ad-en.pdf

OECD (2022d) Going digital: Guide to data governance policy making. OECD Publishing, Paris. https://doi.org/10.1787/40d53904-en

OECD (2022e) Declaration on government access to personal data held by private sector entities. OECD/LEGAL/0487. Adopted 14 December 2022, OECD Legal Instruments, Paris. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

OECD (2023a) Moving forward on data free flow with trust: New evidence and analysis of business experiences. OECD Digital Economy Papers No. 353. Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/04/moving-forward-on-data-free-flow-with-trust_0f681e91/1afab147-en.pdf

OECD (2023b) The nature, evolution and potential implications of data localisation measures. OECD Trade Policy Papers No. 278. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf

Office of the High Commissioner for Human Rights (OHCHR) (2023) Russian court decisions on laws discrediting armed forces a "new low" in clampdown on expression. Press release, 28 August 2023. https://www.ohchr.org/en/press-releases/2023/08/russian-court-decisions-laws-discrediting-armed-forces-new-low-clampdown

Office of the United Nations High Commissioner for Human Rights (2022) Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights. Report A/HRC/50/55. https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-internet-shutdowns-trends-causes-legal-implications-and-impacts

Organization for Security and Co-operation in Europe (OSCE) (2015) Website blocking in France; other anti-terrorist legislation in some OSCE countries may curb free expression. OSCE Representative on Freedom of the Media, Vienna, 30 March 2015. https://www.osce.org/fom/148276

Pierucci F (2025) Sovereignty in the digital era: rethinking territoriality and governance in cyberspace. Digital Society 4:27, 1–19. https://doi.org/10.1007/s44206-025-00189-4

Polyakova A, Meserole C (2019) Exporting digital authoritarianism: The Russian and Chinese models. Brookings Institution, Washington, DC., 1–22. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

Quan E (2022) Censorship sensing: The capabilities and implications of China's Great Firewall under Xi Jinping. Sigma: Journal of Political and International Studies 39: 19–31. https://scholarsarchive.byu.edu/sigma/vol39/iss1/4

Raslan RAA (2024) Climbing up the ladder: technology transfer-related policies in China. Utrecht Law Review 20(1): 19–43. https://doi.org/10.36633/ulr.922

Reporters Without Borders (RSF) (2025) North Korea. https://rsf.org/en/country/north-korea (accessed 22 February 2026).

Ryngaert C, Taylor M (2020) The GDPR as global data protection regulation? AJIL Unbound 114: 5–9. https://doi.org/10.1017/aju.2019.80

Sant G (2015) Court-ordered law breaking: U.S. courts increasingly order the violation of foreign law. Brooklyn Law Review 81(1): 181–232. https://brooklynworks.brooklaw.edu/blr/vol81/iss1/5

Securiti (2024) Cross-border data transfer requirements under India DPDPA. https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdpa/ (accessed 22 February 2026).

Shishkina A and Issaev L (2018) Internet censorship in Arab countries: Religious and moral aspects. Religions 9(11): 358, 1–14. https://doi.org/10.3390/rel9110358

Snowden E (2019) Permanent record. Metropolitan Books, New York.

Stone R (2009) Internet blockade in Xinjiang puts a strain on science. Science 326(5959): 1471. https://doi.org/10.1126/science.326.5959.1471

Su R, Zhang D (2025) Adaptive sovereignty: China's evolving legislative framework for transnational data governance. Politics and Governance 13(1): 1–12. https://www.cogitatiopress.com/politicsandgovernance/article/view/10413/4479

Surbakti FPS (2025) Systematic Literature Review on Generative AI: Ethical Challenges and Opportunities. International Journal of Advanced Computer Science and Applications 16(5): 307–315. https://doi.org/10.14569/IJACSA.2025.0160530

Svanadze V, Iavich M, Lukashenko V (2025) Geopolitical and technical dimensions of Internet fragmentation. CEUR Workshop Proceedings 3991, 578–586. https://ceur-ws.org/Vol-3991/short3.pdf

Swire P, Hemmings JD (2017) Mutual legal assistance in an era of globalized communications: the analogy to the visa waiver program. New York University Annual Survey of American Law 71: 687–738. https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_swirehemmings.pdf

Swire P (2024) White Paper on Clarifying Definitions in the Protecting Americans' Data From Foreign Adversaries Act of 2024, Cross-Border Data Forum, pp. 1–10. https://www.crossborderdataforum.org/wp-content/uploads/2024/05/PADFAA-White-Paper-Appendix-May-7-2024.pdf (accessed 22 February 2026).

The Sedona Conference (2018) The Sedona Principles, Third Edition: Best Practices, Recommendations and Principles for Addressing Electronic Document Production. The Sedona Conference. https://thesedonaconference.org/publication/The_Sedona_Principles

The Sedona Conference (2024) Commentary on proportionality in cross-border discovery. The Sedona Conference Journal 25, 669–778. https://thesedonaconference.org/publication/Commentary_on_Proportionality_in_Cross-Border_Discovery

Thornburg EG (2006) Just say "no fishing": the lure of metaphor. University of Michigan Journal of Law Reform 40: 1–55. https://repository.law.umich.edu/mjlr/vol40/iss1/2/

UNCTAD (2021) Digital economy report 2021: Cross-border data flows and development – For whom the data flow. United Nations Conference on Trade and Development. https://unctad.org/system/files/official-document/der2021_en.pdf

UNCTAD (2022) Digital economy report pacific edition 2022: Towards value creation and inclusiveness. Geneva: United Nations Conference on Trade and Development. https://unctad.org/publication/digital-economy-report-pacific-edition-2022

UNESCO (2021) Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris. SHS/BIO/REC-AIETHICS/2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137

United Nations Human Rights Committee (2011) General Comment No. 34: Article 19 – Freedoms of opinion and expression. UN Doc. CCPR/C/GC/34. https://www.refworld.org/docid/4ed34b562.html

United Nations Human Rights Council (2014) Report of the commission of inquiry on human rights in the Democratic People's Republic of Korea. UN Doc A/HRC/25/63, 7 February 2014. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/108/66/PDF/G1410866.pdf

United Nations Human Rights Council (2022a) Report of the working group on the Universal Periodic Review: India. A/HRC/52/10, 27 December 2022. https://docs.un.org/en/A/HRC/52/11

United Nations Human Rights Council (2022b) Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights – Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/50/55, 13 May 2022. https://docs.un.org/en/A/HRC/50/55

United Nations Human Rights Council (2023), Report of the Special Rapporteur on the situation of human rights in Myanmar, A/HRC/52/21, 3 Mar 2023. https://undocs.org/A/HRC/52/21

UNIDIR (2023) Internet fragmentation and cybersecurity: a primer. United Nations Institute for Disarmament Research, 1–13. https://unidir.org/wp-content/uploads/2023/12/UNIDIR_internet_fragmentation_cybersecurity_primer.pdf

United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) (2008) Participant guide: international cooperation in cybercrime investigations. Cybercrime workshop rev. 2/28/08. https://www.oas.org/juridico/spanish/cyber/cyb22_coop_handout.pdf

UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2021) Internet shutdowns and human rights. United Nations. https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression

U.S. Department of State (2023) Country reports on human rights practices: North Korea. U.S. Department of State, Washington, D.C. https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/north-korea/

USTR (2018) Findings of the investigation into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under Section 301 of the Trade Act of 1974. Office of the United States Trade Representative, Washington, D.C. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

USTR (2023) National Trade Estimate Report on Foreign Trade Barriers (31 Mar 2023). https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf

USTR (2024) 2024 National Trade Estimate Report on Foreign Trade Barriers. Office of the United States Trade Representative, March 2024. https://ustr.gov/sites/default/files/2024%20NTE%20Report.pdf

Vila Seoane M (2021) Data securitisation: the challenges of data sovereignty in India. Third World Quarterly 42(8): 1733–1750. https://doi.org/10.1080/01436597.2021.1915122

Wang YA (2020) Exporting American discovery. University of Chicago Law Review 87: 2089–2160. https://chicagounbound.uchicago.edu/uclrev/vol87/iss8/2/

World Economic Forum (2022) Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows (White Paper). https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf

WTO (2021) Joint statement on electronic commerce: statement by ministers of Australia, Japan and Singapore, 14 December 2021. https://www.wto.org/english/news_e/news21_e/ji_ecom_minister_statement_e.pdf

Wu M, Ni Z, Wang Z, Hou Z, Amiri S, Levy D, Mislove A, Choffnes D (2023) How the Great Firewall of China detects and blocks fully encrypted traffic. In: Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, 1–18. https://gfw.report/publications/usenixsecurity23/en/

Xu J, Gong Q, Yin W (2022) Maintaining ideological security and legitimacy in digital China: Governance of cyber historical nihilism. Media International Australia 185(4): 387–401. https://doi.org/10.1177/1329878X221111826

Xu J (2024) Opening the 'black box' of algorithms: regulation of algorithms in China. Communication Research and Practice 10(3): 288–296. https://doi.org/10.1080/22041451.2024.2346415

Yakovleva S (2024) Governing cross-border data flows: reconciling EU data protection and international trade law. Oxford University Press, Oxford.

Zalnieriute M (2022) Data transfers after Schrems II: The EU-US disagreements over data privacy and national security. Vanderbilt Journal of Transnational Law 55(1): 1–48. https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss1/1/

Zambrano D (2016) A comity of errors: The rise, fall, and return of international comity in transnational discovery. Berkeley Journal of International Law 34: 157–206. https://chicagounbound.uchicago.edu/journal_articles/9931/

Zhang C (2024) China's privacy protection strategy and its geopolitical implications. Asian Review of Political Economy 3:6, 1–17. https://doi.org/10.1007/s44216-024-00028-2

Zhang D (2025) The EU's digital footprint: Shaping data governance in Japan and Singapore. Politics and Governance 13: Article 10422, 1–24. https://doi.org/10.17645/pag.10422

Zhou C, Jiang L (2024) Analysis of the legitimacy of China's data localization measures under the WTO framework. In: Shi L et al. (eds) Proceedings of the 4th International Conference on Public Administration, Health and Humanity Development (PAHHD 2024), 211–216. Atlantis Press. https://doi.org/10.2991/978-2-38476-295-8_26

Zou M, Zhang L (2025) Navigating China's regulatory approach to generative artificial intelligence and large language models. Cambridge Forum on AI: Law and Governance 1, e8, 1–16. https://doi.org/10.1017/cfl.2024.4

五十嵐隆幸（2024）「再考：中国の『デジタル権威主義』―デジタル技術を利用した『中国式の統治システム』の発展過程―」『問題と研究：アジア太平洋研究専門誌』第 53 巻第 1 号 139–171 頁.

片岡弘 (2024) 「米国ディスカバリの日本訴訟への越境的適用と国際的証拠収集のための情報法制上の対応の必要性」『情報法制研究』15 号 94–104 頁. https://www.jstage.jst.go.jp/article/alis/15/0/15_94/_article/-char/ja/

加藤尚徳（2023）「第 15 章 GDPR の十分性認定」指宿信・板倉陽一郎編『越境するデータと法―サイバー捜査と個人情報保護を考える』法律文化社 260–272 頁.

周靖（2021）「中国の国家サイバーセキュリティ戦略に関する一考察」『愛知大学法学部法学論集』第 55 巻 55–94 頁. https://aichiu.repo.nii.ac.jp/record/2000930/files/055-094 周.pdf

劉新宇・崔文英（2025）「中国における個人情報越境移転規制の新動向―『個人情報越境移転認証弁法』の実務解説」NBL 第 1304 号 28–33 頁.

渡辺翔太 (2019) 「ガバメントアクセス（GA）を理由とするデータの越境移転制限―その現状と国際通商法による規律、そして DFFT に対する含意―」RIETI ディスカッション・ペーパー・シリーズ 19-J-067; 1–40 頁. https://www.rieti.go.jp/jp/publications/dp/19j067.pdf

第Ⅲ部

越境的データガバナンス規範再構成の在り方

第Ⅲ部　越境的データガバナンス規範再構成の在り方

サイバー空間の分裂リスクは、各国が自国のデータ保護を根拠として、個別の制度原理に基づく越境的規制を適用し、同一のデータに複数の要求水準が競合する構造に起因している。自国の制度原理に依拠した越境的規制が一方的に適用される現状では、許容され得る保護措置の水準が国家間で大きく乖離し、その累積によって摩擦が制度化される。このような不整合を調整するためには、越境的移転条件を合理的に設定するための共通判断基準を確立する必要がある。越境的データガバナンス規範の再構成とは、制度原理の差異から生じる非互換性を是正し、国家間の規範競合を調整する中立的基盤を確立することを通じて、サイバー空間の分裂を回避し、その一体性と持続可能性を確保するための不可欠な方策である。

以上の認識を踏まえ、第Ⅲ部では、越境的データガバナンス規範再構成の在り方を検討する。まず、第 8 章では、地域貿易協定における大国の規範的対立を分析する。この分析の意義は、越境的データガバナンス規範に内在する制度的不整合の根源を、条文構造を手掛かりとして具体的に把握できる点にある。米国、EU、中国は、それぞれ自由なデータ移転、基本権保護、国家安全保障中心の統制といった異なる規範モデルを地域貿易協定において制度化しており、この乖離は、越境移転条件、個人データの取扱い、例外規定の射程という中核領域において深刻な接続不可能性を生じさせている。これらの構造的対立は短期的な調整可能性を欠き、既存の多国間枠組みによる是正も期待し難い。このため、越境的データガバナンスの制度的接続を再構築するには、大国間の対立点を具体的に析出する作業が不可欠である。他方で、現状の大国間の対立が容易に解消し得ないことを踏まえれば、その影響を回避するため、中堅国や新興国による有志国連携（plurilateral partnerships）が中立的かつ実務的な接続基盤として機能し得る点も明らかとなる。したがって、地域貿易協定における規範的対立の分析は、越境的データガバナンス規範再構成の前提条件を構築し、非大国主導の制度的イニシアティブの必要性を支える実践的意義を有する。

続く第 9 章では、越境的データガバナンス規範の具体化と実装について検討する。本章の目的は、理念的水準で論じられてきた越境的データガバナンスの原理を、制度設計に落とし込むための要素を明確にする点にある。具体的には、DFFT（Data Free Flow with Trust）を指導理念として位置づけ、データの性質と利用文脈に応じて移転条件を調整する枠組みを構想し、異なる国家制度を接続するための調和的基準の形成可能性を検討する。また、越境的データ移転規制に透明性と一貫性を確保する観点から、文脈的リスク評価に基づく運用規範の導入を探求し、国際的に運用可能な制度へと理念を転化するための基盤として、CRDM モデル（Contextual Risk-Based Data Minimization model）を提示する。

最後に第 10 章では、越境的データガバナンス規範再構成における有志国連携の意義と、「トウキョウ効果」の展開可能性を検討する。大国間の規範的対立により国際的統一規範の策定が困難となっている現状を踏まえ、中堅国および新興国による有志国連携を構築し、新たな国際フォーラムを通じて越境的データガバナンス規範を再構成することの制度的・政策的意義を明らかにする。さらに、このような枠組みから形成される規範が、日本の主導の下で大国へも波及し、国際的標準へと昇華し得る「トウキョウ効果」の展開可能性を検討し、その戦略的重要性を示す。

第 8 章

地域貿易協定における大国の規範的対立

第 8 章　地域貿易協定における大国の規範的対立

現在、越境的データ移転に関する国際的統一規範の策定については、WTO における交渉が停滞し、その他の多国間フォーラムでも実効性のある枠組みを確立することが難しい状況にある（前記第 2 章第 2 節参照）。このため、地域貿易協定（Regional Trade Agreement: RTA）などの二国間または地域的枠組みにおける協議が、実質的に中心的役割を担うようになっている[1]。WTO のデータベースによれば、2026 年 2 月 22 日現在、WTO に通知され、かつ発効済みの地域貿易協定は 380 あり、そのうち 132 において電子商取引（e-commerce）に関する規定が設けられている[2]。

地域貿易協定の電子商取引章において、越境的データ移転に関する総則的規定である「横断的条項（horizontal provision）」が初めて導入されたのは、2012 年 3 月に発効した「大韓民国とアメリカ合衆国との間の自由貿易協定」（KORUS）[3]である（第 15.8 条）。同条項は努力義務にとどまる非拘束的規定であったが（以下、参照条文は各項末尾に掲載する。）、米国はその後、拘束力のある条項の策定を目指して関係国への働きかけを強めた[4]。こうした動きを背景に、米国主導で「環太平洋パートナーシップ協定」（TPP 協定）[5]が推進され、2016 年 2 月には 12 か国が署名に至った。しかし、2017 年 1 月に米国トランプ政権（第 1 次）が離脱を表明したため[6]、米国を除く 11 か国[7]による交渉が継続され、2018 年 12 月に「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」（CPTPP 協定）として発効した[8]。なお、CPTPP 協定は、米国の離脱後も日本が主導的に推進してきた経済連携協定であり、2024 年 12 月には英国が正式加入するなど[9]、現在も米国不参加のまま、その制度的発展が継続している。

近年、米国、EU、中国といった大国は、自国の制度理念や価値観を反映した地域貿易協定を相次いで締結しており、その条文構造には各国の一国主義的主張が明確に示されている。米国が締約国として強い影響を及ぼした協定群は「米国モデル」と呼ばれ[10]、2020 年 1 月発効の「デジタル貿易に関する日本国とアメリカ合衆国との間の協定」（日米デジタル貿易協定）[11]、同

---

[1] Burri (2017), pp. 93–104, 113–117.

[2] WTO RTA Database. https://rtais.wto.org/UI/PublicMaintainRTAHome.aspx (accessed 22 February 2026).

[3] 「大韓民国とアメリカ合衆国との間の自由貿易協定」（Korea–United States Free Trade Agreement: KORUS）（2007 年 6 月 30 日署名、2012 年 3 月 15 日発効）.

[4] Yakovleva (2024), p. 156.

[5] 「環太平洋パートナーシップ協定」（Trans-Pacific Partnership Agreement: TPP 協定）（2016 年 2 月 4 日署名、未発効。12 か国が署名したが、2017 年 1 月に米国が離脱を表明）. USTR, TPP Full Text. https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text (accessed 22 February 2026).

[6] Office of the U.S. Trade Representative (2017), The United States officially withdraws from the Trans-Pacific Partnership (press release, Jan. 23, 2017). https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/january/US-Withdraws-From-TPP

[7] 日本、メキシコ、シンガポール、ニュージーランド、カナダ、オーストラリア、ベトナム、ペルー、マレーシア、チリ、ブルネイの 11 か国である（外務省「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（CPTPP）」）. https://www.mofa.go.jp/mofaj/ila/et/page23_002473.html

[8] 「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」（Comprehensive and Progressive Agreement for Trans-Pacific Partnership: CPTPP 協定）（2018 年 3 月 8 日署名、2018 年 12 月 30 日発効）.

[9] Department for Business and Trade (2024).

[10] Yakovleva (2024), pp. 23, 193–194.

[11] 「デジタル貿易に関する日本国とアメリカ合衆国との間の協定」（Agreement between the United States of America and Japan concerning Digital Trade: 日米デジタル貿易協定）（2019 年 10 月 7 日署名、2020 年 1 月 1 日発効）.

年 7 月発効の「米国・メキシコ・カナダ協定」（USMCA）[12]が典型例である。また、EU の強い影響下で締結された協定群は「EU モデル」と呼ばれ[13]、EU が 2018 年 5 月に策定した越境的データ移転の横断的規定モデル（以下「EU モデル条項」という。）[14]は、2019 年 2 月発効の「経済上の連携に関する日本国と欧州連合との間の協定」（日 EU・EPA）[15]の改正交渉（2024 年 7 月改正[16]）でも用いられた[17]。これに対し、2022 年 1 月発効の「地域的な包括的経済連携協定」（RCEP 協定）[18]は ASEAN 加盟国に加えて日本や中国も参加する協定であり[19]、中国の規制的アプローチが条文構造に色濃く反映されていることから、「中国モデル」の特徴を備えた協定と位置づけられる[20]。これらの三つのモデルは、用いる概念に一定の共通性を有しつつも、その規範的スタンスは根本的に異なっている。そのため、場合によっては鋭い対立を生じさせ、越境的データガバナンスにおける規範的分断をさらに深化させている。

本章では、この三つのモデルの相違点を中心に検討する。まず、第 1 節では、越境的データ移転に関する三つの基本原則を定める条項の規定内容について三つのモデルを対比して整理し、第 2 節ではそれら条項に関する適用除外規定および例外規定に着目し、大国間の規範的対立の重要点を明らかにする。そのうえで、第 3 節では大国の規範的対立を踏まえた越境的データガバナンス規範再構成の方向性を提示する。

【参照条文】

大韓民国とアメリカ合衆国との間の自由貿易協定（KORUS）

第 15.8 条（電子的情報の国境を越える流通）

両締約国は、貿易の促進における情報の自由な流通の重要性を認識し、及び個人情報の保護の重要性を認めつつ、国境を越える電子的情報の流通に対して不必要な障害を課し、又は維持することを差し控えるよう努めるものとする。

---

[12] 「米国・メキシコ・カナダ協定」（United States-Mexico-Canada Agreement: USMCA）（2018 年 11 月 30 日署名、2020 年 7 月 1 日発効）.

[13] Yakovleva (2024), pp. 23, 187-197.

[14] European Commission (2018), Horizontal Provisions on Cross-Border Data Flows and Personal Data Protection in EU Trade and Investment Agreements, European Commission, Brussels, 18 May 2018. https://ec.europa.eu/newsroom/just/items/627665/en

[15] 「経済上の連携に関する日本国と欧州連合との間の協定」（Agreement between the European Union and Japan for an Economic Partnership: 日 EU・EPA）（2018 年 7 月 17 日署名、2019 年 2 月 1 日発効）.

[16] 電子商取引に関する規定の再評価により、越境的データ移転に関する条項が改正され、2024 年 7 月に発効した（Protocol Amending the Agreement Between the European Union and Japan for an Economic Partnership, EU-Japan, 2024 年 1 月 23 日署名、2024 年 7 月 1 日発効）. https://www.mofa.go.jp/mofaj/files/100615101.pdf

[17] European Commission (2022), COM (2022) 336 final - Recommendation for a Council Decision authorising the opening of negotiations for the inclusion of provisions on cross-border data flows in the Agreement between the European Union and Japan for an Economic Partnership, Brussels, 12 July 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:336:FIN

[18] 「地域的な包括的経済連携協定」（Regional Comprehensive Economic Partnership Agreement: RCEP 協定）（2020 年 11 月 15 日署名、2022 年 1 月 1 日発効）.

[19] RCEP 協定の加盟国は、ASEAN10 か国（署名・発効当時）に加え、日本、オーストラリア、中国、韓国、ニュージーランドである（外務省「地域的な包括的経済連携（RCEP）協定」）. https://www.mofa.go.jp/mofaj/gaiko/fta/j-eacepia/index.html (accessed 22 February 2026).

[20] Yakovleva (2024), pp. 23, 194.

第 1 節　越境的データ移転に関する三原則条項

CPTPP 協定をはじめ、日本が近年締結した複数の経済連携協定[21]には、越境的データ移転に関する基本原則を体系的に定める三つの条項（以下「三原則条項」という。）が盛り込まれている[22]。

三原則条項の内容は、

① 事業遂行のための越境的データ移転に対する制限を禁止する条項（以下「越境的データ移転制限禁止条項」という。）

② 自国での事業遂行の条件として、コンピュータ関連設備の自国内での設置または利用を要求することを禁止する条項（以下「コンピュータ設備等要求禁止条項」という。）

③ 自国における製品等の輸入・頒布・販売・利用の条件として、製品等のソースコードの移転またはソースコードへのアクセスを要求することを禁止する条項（以下「ソースコード移転等要求禁止条項」という。）

の三つから構成されている。

三原則条項は、CPTPP 協定に続き、2020 年 1 月発効の日米デジタル貿易協定および同年 7 月発効の USMCA にも盛り込まれた。その後、米国が締約当事国ではない協定にも三原則条項が取り入れられ、2021 年 1 月発効の「日本国とグレートブリテン及び北アイルランド連合王国との間の包括的経済連携に関する協定」[23]、同月発効の「デジタル経済連携協定」（DEPA）[24]、そして 2024 年 7 月に改正規定が発効した日 EU・EPA[25]などにも反映されている。

以下では、「米国モデル」「EU モデル」および「中国モデル」の各協定における三原則条項の取扱いを検討し、条文構造の比較を通じて[26]、越境的データ移転をめぐる大国間の主張の対立を明らかにする。

第 1 項　越境的データ移転制限禁止条項

三原則条項のうち越境的データ移転制限禁止条項は、事業遂行のための越境的データ移転に対する制限を禁止する趣旨の規定であり、国境を越えたデータ流通の自由を確保し、データ

---

[21] 外務省は、「経済連携協定（EPA/FTA）」という表現を用いている。外務省「我が国の経済連携協定（EPA/FTA）等の取組」. https://www.mofa.go.jp/mofaj/gaiko/fta/ (accessed 22 February 2026).

[22] この三原則条項は、もともと米国の主導により TPP 協定に盛り込まれたものであり、当時は「TPP 三原則」とも称されていた。日本貿易振興機構 (JETRO) (2019).

[23] 「日本国とグレートブリテン及び北アイルランド連合王国との間の包括的経済連携に関する協定」(Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan for a Comprehensive Economic Partnership) (2020 年 10 月 23 日署名、2021 年 1 月 1 日発効).

[24] 「デジタル経済連携協定」(Digital Economy Partnership Agreement: DEPA)(2020 年 6 月 12 日署名、2021 年 1 月 7 日発効). 加盟国はシンガポール、ニュージーランド、チリの三か国である. Ministry of Trade and Industry Singapore, The Digital Economy Partnership Agreement (DEPA). https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement

[25] 日 EU・EPA は、電子商取引に関する規定の再評価により、越境的データ移転に関する条項が改正され、2024 年 7 月に発効した（Protocol Amending the Agreement Between the European Union and Japan for an Economic Partnership, EU-Japan, 2024 年 1 月 23 日署名、2024 年 7 月 1 日発効）. https://www.mofa.go.jp/mofaj/files/100615101.pdf

[26] CPTPP 協定は、附属書 IV において凍結の対象とされた規定を除き、TPP 協定の条文構造（章立て及び条番号）を基本的に踏襲している。本稿では、条文を引用する際には「CPTPP 協定第〇条」と表記する。

保護主義的措置を抑制するための基本的条項である。2012 年 3 月に発効した KORUS 第 15.8 条は努力義務的な非拘束的規定にとどまっていたが、2018 年 12 月発効の CPTPP 協定以降の協定ではより明確な拘束的義務として規定されるようになった[27]。

越境的データ移転制限禁止条項は、「米国モデル」「EU モデル」「中国モデル」のいずれにも法的拘束力を有する形で規定されており、条文上は、それぞれの大国がデータ保護主義の抑制およびデータの自由な流通の促進に賛同しているかのように見える。しかし、いずれの協定にも適用除外規定や例外規定が盛り込まれており（後記第 2 節参照）、その適用範囲の広さや運用の不透明さを踏まえると、越境的データ移転制限禁止条項の実効性確保には懸念が残る。

また、越境的データ移転制限禁止条項の対象となるデータ（すなわち越境移転の自由が保障されるデータ）に個人データが含まれるか否かについて、「米国モデル」では、日米デジタル貿易協定第 11 条第 1 項および USMCA 第 19.11 条第 1 項が、越境的データ移転制限禁止の対象となる「情報」について「情報（個人情報を含む。）」と明記し、個人データも越境的データ移転制限禁止条項の対象に含まれることを明示している。RCEP 協定（「中国モデル」）も第 12.15 条第 2 項において越境的データ移転制限禁止条項を定めており、条文の文理上、個人データを対象から除外する明示的文言は存在せず、個人データも越境的データ移転制限禁止条項の適用対象に含まれると解するのが自然である。

これに対し、「EU モデル」では個人データの越境移転について、ビジネス目的のデータ移転とは区別して規制する立場を明確にしている。すなわち、EU モデル条項は、個人データについて、一般的な越境移転規律を定める第 A 条とは切り離し、個人データおよびプライバシーの保護について規定する第 B 条を特別規律として適用する構造を採用している。そのため、個人データは制度設計上、越境移転自由化の対象から外れる。具体的には、EU モデル条項第 A 条第 1 項は「締約国間における越境的データ流通」について、「次の手段によって制限されてはならない」と規定し、(i)から(iv)においてデータローカライゼーション要求等を限定的に列挙しているものの、個人データの越境移転制限を禁止する規定は存在しない。他方、第 B 条第 2 項は「各締約国は、個人データ及びプライバシーの保護を確保するために、自らが適切と認める保護措置（越境的な個人データの移転に関する規則の採用及び適用を含む。）を採用し、維持することができる。」と定め、個人データの越境的移転制限を明示的に許容している。これは、「米国モデル」と対照的に、個人データを越境的データ移転制限禁止条項の適用対象から除外し、基本権としての個人データ保護を優先させる EU の立場を示すものである。日 EU・EPA 第 8.81 条第 4 項も同様の構成をとり、個人データ保護を理由とする越境移転制限措置の導入を各締約国に認めている。なお、JSI 安定化テキスト（前記第 2 章第 2 節参照）第 25 条も同様の規定振りを採用し「EU モデル」に沿った条文構造となっている。

以上のように、越境的データ移転制限禁止条項については、個人データをその適用対象とするか否かの点で、「米国モデル」と「EU モデル」との間で基本的な立場の相違が存在する。さらに、適用除外規定や例外規定の運用次第では、原則と例外が逆転し、越境的データ移転制限が制度的に常態化する可能性がある。このように、越境的データ移転制限禁止条項との関係では、データ保護主義的施策の禁止などについて必ずしも国際的な合意が形成されているとはいえず、原則と例外の関係も協定ごとに大きく異なる。

[27] Yakovleva (2024), pp. 155–157.

【参照条文（越境的データ移転制限禁止条項）】

CPTPP 協定

第 14.11 条（情報の電子的手段による国境を越える移転）

1. 締約国は、各締約国が情報の電子的手段による移転に関する自国の規制上の要件を課することができることを認める。
2. 各締約国は、対象者の事業の実施のために行われる場合には、情報（個人情報を含む。）の電子的手段による国境を越える移転を許可する。

（以下省略）

日米デジタル貿易協定

第 11 条（情報の電子的手段による国境を越える移転）

1. いずれの締約国も、情報（個人情報を含む。）の電子的手段による国境を越える移転が対象者の事業の実施のために行われる場合には、当該移転を禁止し、又は制限してはならない。

（以下省略）

USMCA

第 19.11 条（情報の電子的手段による国境を越える移転）

1. いずれの締約国も、情報（個人情報を含む。）の電子的手段による国境を越える移転が対象者の事業の実施のために行われる場合には、当該移転を禁止し、又は制限してはならない。

（以下省略）

EU モデル条項

第 A 条（越境的データ流通及びコンピュータ関連設備の設置）

1. 締約国は、デジタル経済における貿易を促進するために、越境的なデータ流通を確保することに対し、コミットする。そのため、締約国間における越境的データ流通は、次の手段によって制限されてはならない。

（(i)～(iii)は後記第 2 項末尾に掲載）

(iv) 越境的なデータ移転を、締約国の領域内におけるコンピュータ関連設備若しくはネットワーク要素の使用、又は当該領域内でのローカライゼーション要件の遵守を条件とすること。

（以下省略）

第 B 条（個人データ及びプライバシーの保護）

1. 各締約国は、個人データ及びプライバシーの保護が基本的権利であること、そしてこの点における高い基準がデジタル経済に対する信頼及び貿易の発展に寄与することを認識する。
2. 各締約国は、個人データ及びプライバシーの保護を確保するために、自らが適切と認める保護措置（越境的な個人データの移転に関する規則の採用及び適用を含む。）を採用し、維持することができる。本協定のいかなる規定も、締約国がそれぞれの保護措置によって提供する個人データ及びプライバシーの保護を損なうものではない。

日 EU・EPA

第 8.81 条（情報の電子的手段による国境を越える移転）

1. 両締約国は、情報の電子的手段による国境超える移転が対象者の事業の実施のために行われる場合には、当該移転を確保することを約束する。
2. このため、一方の締約国は、1に規定する情報の電子手段による国境を越える移転を次のことを行うことによって禁止し、又は制限する措置を採用し、又は維持してはならない。

((a)～(c)は後記第 2 項末尾に掲載)

(d) 一方の締約国の領域におけるコンピュータ関連設備若しくはネットワーク構成要素の利用又は一方の締約国の領域におけるローカライゼーションの要求を情報の国境を越える移転の条件とすること。

(e) 一方の締約国の領域への情報の移転を禁止すること。

(f) 他方の締約国の領域への情報の移転の前に一方の締約国の承認を要求すること。

(3 は後記第 2 節第 2 項(1)および(2)末尾に掲載)

4. この条のいかなる規定も、締約国が、個人データ及びプライバシーの保護に関する措置(情報の国境を越える移転に関するものを含む。)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、当該締約国の法律が、移転される情報の保護のために一般に適用される条件の下で移転を可能とする手段について定めていることを条件とする。

RCEP 協定

第 12.15 条(情報の電子的手段による国境を越える移転)

1. 締約国は、各締約国が情報の電子的手段による移転に関する自国の規制上の要件を課することができることを認識する。

2. 締約国は、情報の電子的手段による国境を越える移転が対象者の事業の実施のために行われる場合には、当該移転を妨げてはならない。

(3 は後記第 2 節第 2 項および第 3 項末尾に掲載)

JSI「安定化テキスト」

第 25 条(個人データ保護の例外)

この協定のいかなる規定も、締約国が、個人データ及びプライバシーの保護に関する措置(情報の国境を越える移転に関するものを含む。)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、当該締約国の法律が、移転される情報の保護のために一般に適用される条件の下で移転を可能とする手段について定めていることを条件とする。

第 2 項　コンピュータ設備等要求禁止条項

三原則条項のうちコンピュータ設備等要求禁止条項は、自国での事業実施の条件として、他国企業に対し自国内におけるコンピュータ関連設備の利用または設置、あるいはデータの自国内保存・処理を義務づける措置を禁止するものであり、データローカライゼーション措置に対する規律手段として理解されている[28]。

まず、「米国モデル」では、日米デジタル貿易協定第 12 条第 1 項および USMCA 第 19.12 条第 1 項が、「自国の領域において事業を実施するための条件」として、「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」と定めている。また、RCEP 協定第 12.14 条第 2 項も同様にコンピュータ設備等要求禁止条項を定めている。さらに、EU モデル条項第 A 条第 1 項は、(i)から(iv)で禁止対象行為を限定的に列挙し、「一方の締約国の領域内にあるコンピュータ関連設備又はネットワーク要素の使用を要求すること」「一方の締約国

[28] González et al. (2022), pp. 12–15, 22–25.

の領域内でのデータの局地的保存（ローカライゼーション）を要求すること」「越境的なデータ移転を、締約国の領域内におけるコンピュータ関連設備若しくはネットワーク要素の使用、又は当該領域内でのローカライゼーション要件の遵守を条件とすること」などを禁止しており、データローカライゼーション措置要求を明文で禁ずる構成を採用し、日 EU・EPA 第 8.81 条第 2 項も同様の規定を置いている。

以上のように、コンピュータ設備等要求禁止条項については、各モデルで条文構成に違いはあるものの、「米国モデル」「EU モデル」および「中国モデル」のいずれにも規定されている。そのため、大国の間でデータローカライゼーションを原則的に禁止することについて大きな対立は存在しないように見えるが、例外規定（後記第 2 節参照）との関係で依然として懸念が残る。特に、RCEP 協定は公共政策目的や安全保障を理由とする広範な例外を認めているため、制度設計としては米国モデル・EU モデルに比して拘束性が弱い構成となっている。このように、各協定で原則条項を定めたとしても、例外規定の適用によって、結果的に広範なデータローカライゼーション措置が認められる可能性がある。したがって、データローカライゼーション措置の禁止について必ずしも国際的なコンセンサスが成立しているわけではない。

【参照条文（コンピュータ設備等要求禁止条項）】

CPTPP 協定

第 14.13 条（コンピュータ関連設備の設置）

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。

（以下省略）

日米デジタル貿易協定

第 12 条（コンピュータ関連設備の設置）

1. いずれの締約国も、自国の領域において事業を実施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。

（以下省略）

USMCA

第 19.12 条（コンピュータ関連設備の設置）

1. いずれの締約国も、自国の領域において事業を実施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。

（以下省略）

EU モデル条項

第 A 条（越境的データ流通及びコンピュータ関連設備の設置）

1. 締約国は、デジタル経済における貿易を促進するために、越境的なデータ流通を確保することに対し、コミットする。そのため、締約国間における越境的データ流通は、次の手段によって制限されてはならない。

(i) データの処理のために、一方の締約国の領域内にあるコンピュータ関連設備又はネットワーク要素の使用を要求すること(当該設備や要素が当該締約国の領域内で認証又は承認されているものの使用を課す場合を含む。);
(ii) データの保存又は処理のために、一方の締約国の領域内でのデータの局地的保存(ローカライゼーション)を要求すること;
(iii) データの保存又は処理を、他方の締約国の領域内で行うことを禁止すること;
(iv) 越境的なデータ移転を、締約国の領域内におけるコンピュータ関連設備若しくはネットワーク要素の使用、又は当該領域内でのローカライゼーション要件の遵守を条件とすること。

(2 省略)

日 EU・EPA

第 8.81 条(情報の電子的手段による国境を越える移転)

1. 両締約国は、情報の電子的手段による国境超える移転が対象者の事業の実施のために行われる場合には、当該移転を確保することを約束する。
2. このため、一方の締約国は、1に規定する情報の電子手段による国境を越える移転を次のことを行うことによって禁止し、又は制限する措置を採用し、又は維持してはならない。

(a) 情報の処理に関して、一方の締約国の領域におけるコンピュータ関連設備又はネットワーク構成要素の利用を要求すること(一方の締約国の領域において認証され、又は承認されたコンピュータ関連設備又はネットワーク構成要素の利用を要求することを含む。)。
(b) 情報の保存又は処理に関して、一方の締約国の領域における情報のローカライゼーションを要求すること。
(c) 他方の締約国の領域における情報の保存又は処理を禁止すること
(d) 一方の締約国の領域におけるコンピュータ関連設備若しくはネットワーク構成要素の利用又は一方の締約国の領域におけるローカライゼーションの要求を情報の国境を越える移転の条件とすること。

((e)・(f)は前記第 1 項末尾に掲載)

(3 は後記第 2 節第 2 項(1)および(2)末尾に掲載)

RCEP 協定

第 12.14 条(コンピュータ関連設備の設置)

1. 締約国は、各締約国がコンピュータ関連設備の利用又は設置に関する自国の措置(通信の安全及び秘密を確保することを追求するための要件を含む。)をとることができることを認識する。
2. いずれの締約国も、自国の領域において事業を実施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 は後記第 2 節第 2 項(2)および第 3 項末尾に掲載)

第 3 項　ソースコード移転等要求禁止条項

三原則条項のうちソースコード移転等要求禁止条項については、留保的規定の適用の余地が大きいほか、「中国モデル」には盛り込まれておらず、その実効性に疑問が生じる。

まず、「米国モデル」では、日米デジタル貿易協定第 17 条第 1 項および USMCA 第 19.16 条第 1 項が、「他の締約国の者が所有するソフトウェア又は当該ソフトウェアを含む製品」の「輸入、流通、販売又は使用」の条件として、「当該ソフトウェアのソースコードの移転若しくは当該ソースコードへのアクセス、又は当該ソースコードにおいて表現されるアルゴリズムの移転若しくは当該アルゴリズムへのアクセス」を要求してはならない旨を定めている。

また、EU モデル条項にはソースコード移転等要求禁止条項は盛り込まれていないものの、日 EU・EPA 第 8.73 条第 1 項では「他方の締約国の者が所有するソフトウェアのソースコードの移転又は当該ソースコードへのアクセスを要求することができない」と規定し、ソースコード移転等要求禁止条項を明文で採用している。ただし、「米国モデル」とは異なり、アルゴリズムについては規定していない。

他方、RCEP 協定は第 12.16 条においてソースコードに関する「対話」の実施を定めるにとどまり、ソースコード移転等要求禁止条項自体を置いていない。このように RCEP 協定が対話規定にとどめ、禁止条項としての拘束力を付与していない点は、「中国モデル」がソースコード移転等要求禁止条項を制度的要素として位置づけないという特徴を象徴するものである。

さらに、ソースコード移転等要求禁止条項については、明文規定を欠く RCEP 協定を除き、各協定において司法手続や規制当局による手続（以下「司法手続等」という。）に関する留保的規定が置かれている。すなわち、日米デジタル貿易協定第 17 条第 2 項および USMCA 第 19.16 条第 2 項は、「一方の締約国の規制機関又は司法当局」が「特定の調査、検査、検討、執行活動又は司法手続のために、ソフトウェアのソースコード又は当該ソースコードにおいて表現されるアルゴリズムを保存し、又は入手可能なものとすることを要求すること」を禁止の対象外としている。また、日 EU・EPA 第 8.73 条第 2 項は、ソースコードの移転等要求について、「競争法令の違反を是正する司法裁判所、行政裁判所又は競争当局による要求」や「知的財産権の保護及び行使に関する司法裁判所、行政裁判所又は行政当局による要求」を禁止の対象外としている。これらの規定は、司法手続等におけるソースコード移転等要求を禁止規定の適用範囲から除外することを明確にするものである。特に、司法手続に限らず、規制当局や競争当局によるアクセスを容認する規定はガバメントアクセス（前記第 5 章参照）に通じるものであり、将来的には大国を中心にガバメントアクセスが濫用的に運用されるリスクにも留意する必要がある。これらの留保規定は、禁止条項の制度的拘束力を実質的に減殺し得る重要な要素であり、各国の司法当局・規制当局によるアクセス要求の範囲や運用次第で、条項の実効性は大きく左右される。

このように、ソースコード移転等要求禁止条項については、各モデル（主要国）の間でスタンスに大きな違いが見られるとともに、司法手続等に関する留保規定が盛り込まれており、その運用次第ではソースコード移転等要求が広く認められる実情となるおそれもある。したがって、ソースコード移転等要求禁止条項について、主要国間で制度設計や適用範囲に関する共通理解が十分に形成されているわけではない。

【参照条文（ソースコード移転等要求禁止条項等）】

CPTPP 協定

第 14・17 条（ソースコード）

1. いずれの締約国も、他の締約国の者が所有するソフトウェア又は当該ソフトウェアを含む製品の自国の領域における輸入、頒布、販売又は利用の条件として、当該ソフトウェアのソースコードの移転又は当該ソースコードへのアクセスを要求してはならない。
2. この条の規定の適用上、1の規定の対象となるソフトウェアは、大量販売用ソフトウェア又は当該ソフトウェアを含む製品に限定するものとし、中枢的な基盤のために利用されるソフトウェアを含まない。

（以下省略）

日米デジタル貿易協定

第 17 条（ソースコード）

1. いずれの一方の締約国も、他の締約国の者が所有するソフトウェア又は当該ソフトウェアを含む製品の一方の締約国の領域における輸入、流通、販売又は使用の条件として、当該ソフトウェアのソースコードの移転若しくは当該ソースコードへのアクセス又は当該ソースコードにおいて表現されるアルゴリズムの移転若しくは当該アルゴリズムへのアクセスを要求してはならない。
2. この条の規定は、一方の締約国の規制機関又は司法当局が、他方の締約国の者に対し、特定の調査、検査、検討、執行活動又は司法手続のため、ソフトウェアのソースコード又は当該ソースコードにおいて表現されるアルゴリズムを保存し、又は入手可能なものとすることを要求することを妨げるものではない。ただし、当該ソースコード及び当該アルゴリズムを許可されていない開示からの保護の対象とすることを条件とする。

（以下省略）

USMCA

第 19.16 条（ソースコード）

1. いずれの締約国も、他の締約国の者が所有するソフトウェア又は当該ソフトウェアを含む製品の他の締約国の領域における輸入、流通、販売又は使用の条件として、当該ソフトウェアのソースコードの移転若しくは当該ソースコードへのアクセス又は当該ソースコードにおいて表現されるアルゴリズムへのアクセスを要求してはならない。
2. この条の規定は、一方の締約国の規制機関又は司法当局が、他方の締約国の者に対し、特定の調査、検査、検討、執行活動又は司法手続のため、ソフトウェアのソースコード又は当該ソースコードにおいて表現されるアルゴリズムを保存し、又は入手可能なものとすることを要求することを妨げるものではない。ただし、当該ソースコード及び当該アルゴリズムを許可されていない開示からの適切な保護の対象とすることを条件とする。

（以下省略）

日 EU・EPA

第 8.73 条（ソースコードの移転又はアクセス）

1. いずれの一方の締約国も、他方の締約国の者が所有するソフトウェアのソースコードの移転又は当該ソースコードへのアクセスを要求することができない。この1のいかなる規定も、商業的に交渉された契約においてソースコードの移転若しくはソースコードへのアクセスの付与に関する条件を含め、若しくは当該条件を履行すること又は例えば政府調達に関連してソースコードを自主的に移転すること若しくはソースコードへのアクセスを自主的に付与することを妨げるものではない。
2. この条のいかなる規定も、次の要求又は権利に影響を及ぼすものではない。

(a) 競争法令の違反を是正するための司法裁判所、行政裁判所又は競争当局による要求

(b) 知的財産権の保護及び行使に関する司法裁判所、行政裁判所又は行政当局による要求（ソースコードが当該知的財産権によって保護される範囲に限る。）

（以下省略）

RCEP 協定

第 12.16 条（電子商取引に関する対話）

1　締約国は、電子商取引の発展及び利用を促進するに当たっての対話（適当な場合には、利害関係者との対話を含む。）の重要性を認識する。締約国は、当該対話の実施に当たり、次の事項を検討する。

((a)省略）

(b) 現在の及び新たな問題（デジタル・プロダクトの待遇、ソースコード、データの国境を越える流通及びコンピュータ関連設備の設置であって金融サービスにおけるもの等）

（以下省略）

第 2 節　適用除外規定および例外規定

三原則条項を定めた地域貿易協定においては、それらの条項に関する適用除外規定や例外規定が設けられるのが一般的であるが、その要件や適用範囲は協定ごとに異なっている。このような適用除外規定や例外規定が広範に認められる場合、三原則条項は実質的に名目的な規定にとどまり、むしろデータ保護主義的な運用を正当化する手段として機能するおそれがある[29]。

以下では、電子商取引における個人情報保護に関する適用除外規定、公共政策例外規定、安全保障例外規定について、大国間における基本的スタンスの違いを中心に、その問題点を整理する。

第 1 項　電子商取引における個人情報保護に関する適用除外規定

電子商取引章における個人情報保護規定は、越境的データ移転の自由と個人の権利保護との均衡をいかに図るかという根源的課題を反映している。この規定の在り方は、デジタル貿易の自由化を志向する通商政策と、基本的人権としての個人情報・プライバシー保護を重視する人権政策との交錯点に位置している。

個人情報保護については、日米デジタル貿易協定第 15 条第 1 項および USMCA 第 19.8 条第 2 項が、それぞれ、個人情報を保護するための「法的枠組み」の採用・維持について規定している。また、RCEP 協定第 12.8 条第 1 項も「個人情報の保護を確保する法的枠組み」の採用・維持について規定している。

これに対し、EU モデル条項第 B 条は、第 1 項で「個人データ及びプライバシーの保護が基本的権利であること」を明記したうえで、第 2 項において「本協定のいかなる規定も、締約国がそれぞれの保護措置によって提供する個人データ及びプライバシーの保護を損なうものではない」と規定し、個人データおよびプライバシーの保護を優先する立場を明確にしている。これは、GDPR が第三国の事業者に対しても法的拘束力を及ぼすことを通じて、個人データを越境移転保障の対象外とするという EU の立場を明らかにしたものと位置づけられる。なお、この点に関しては、日 EU・EPA 第 8.82 条第 1 項も、「個人が自己の個人情報及びプライバシーの保護についての権利を有すること」を規定したうえで、「一方の締約国は、他方の締約国が自国の定める措置によって個人情報及びプライバシーの適切な保護の水準を決定する権利を有することを認める」としている。これにより、実質的に、個人情報およびプライバシーの保護を優先させ、デジタル貿易規律の適用を制限する趣旨を定めている。

このような EU の立場に対し、日米デジタル貿易協定第 15 条第 4 項は、「個人情報の国境を越える流通に対する制限が当該流通によりもたらされる危険性との関係で必要であり、かつ、当該危険性に比例したものであることを確保することの重要性を認識する。」と規定し、リスクベースアプローチの考え方を条文上明示している。同趣旨の規定は USMCA 第 19.8 条第 3 項にも置かれており、「米国モデル」の特色ということができるが、これらは EU に対する明確なメッセージになり得る。すなわち、EU の個人情報保護当局の一部が、個人データの越境移転に関して個別のリスク評価に基づく移転を認めるリスクベースアプローチを明示的に否定し、移転先国の

[29] Burri (2017), pp. 87–99, 126–132; UNCTAD (2021), pp. 114–116, 174–176; Chin and Zhao (2022), section 6.3.

法制度について抽象的な制度的リスクが想定される場合には越境移転そのものを違法とみなす立場をとっていることから[30]、それに対する批判的な意義を有するものと位置づけられる。

以上のように、各モデルはいずれも個人情報保護のための法的枠組みの採用・維持を求める点では共通しているものの、個人データの越境的移転に関する規律構造には、「米国モデル」と「EU モデル」との間で重要な相違が見られる。

【参照条文（個人情報保護関連規定）】

日米デジタル貿易協定

第 15 条（個人情報の保護）

1. 各締約国は、デジタル貿易の利用者の個人情報の保護を規定する法的枠組みを採用し、又は維持する。

（2 省略）

3. 各締約国は、個人情報を保護するために両締約国が異なる法的な取組方法をとることができることを認識しつつ、このような異なる制度の相互運用性を促進する仕組みの整備を奨励すべきである。
4. 両締約国は、個人情報を保護するための措置の遵守を確保すること及び個人情報の国境を越える流通に対する制限が当該流通によりもたらされる危険性との関係で必要であり、かつ、当該危険性に比例したものであることを確保することの重要性を認識する。

USMCA

第 19.8 条（個人情報の保護）

1. 締約国は、デジタル貿易の利用者の個人情報を保護することが経済的及び社会的利益をもたらすこと、並びにそれがデジタル貿易における消費者の信頼を高めることに寄与することを認識する。
2. この目的を達成するため、各締約国は、デジタル貿易の利用者の個人情報を保護するための法的枠組みを採用し、又は維持しなければならない。かかる法的枠組みの整備にあたっては、APEC プライバシー・フレームワーク及び「プライバシー保護と個人データの越境移転に関する指針（2013）」を含む、関係する国際機関の原則及び指針を考慮することが望ましい。
3. 各締約国は、第 2 項に従い、主要な原則には、収集の制限、選択、データの品質、目的の特定、利用の制限、安全保護措置、透明性、本人の関与、及び説明責任が含まれることを認識する。各締約国は、個人情報を保護するための措置の遵守を確保すること、並びに個人情報の国境を越える流通に対するいかなる制限も、提示されるリスクに照らして必要かつ比例的であることを確保することの重要性を認識する。

EU モデル条項

第 B 条（個人データ及びプライバシーの保護）

1. 各締約国は、個人データ及びプライバシーの保護が基本的権利であること、そしてこの点における高い基準がデジタル経済に対する信頼及び貿易の発展に寄与することを認識する。
2. 各締約国は、個人データ及びプライバシーの保護を確保するために、自らが適切と認める保護措置（越境的な個人データの移転に関する規則の採用及び適用を含む。）を採用し、維持することができる。本協定のいかなる規定も、締約国がそれぞれの保護措置によって提供する個人データ及びプライバシーの保護を損なうものではない。

[30] Kuner (2017a), pp. 886–895, 899–909; EDPB (2021a), paras. 41–49; EDPB (2021b), paras. 6–16.

日 EU・EPA

第 8.82 条（個人情報の保護）

1. 両締約国は、各締約国の法令に従い個人が自己の個人情報及びプライバシーの保護についての権利を有すること並びにこの点に関する高い基準がデジタル経済における信用及び貿易の発展に寄与することを認める。一方の締約国は、他方の締約国が自国の定める措置によって個人情報及びプライバシーの適切な保護の水準を決定する権利を有することを認める。

（第 2 項省略）

3. 各締約国は、電子商取引に関連する個人情報の保護について定める法的枠組みを採用し、又は維持する。各締約国は、個人情報及びプライバシーの保護のための自国の法的枠組みの策定において、関係国際機関の原則及び指針を考慮すべきである。両締約国は、また、民間が保有する情報への政府のアクセスに関するプライバシー及び情報の保護の高い基準（例えば、民間部門の主体が保有する個人情報への政府のアクセスに関する経済協力開発機構の原則に規定する基準）がデジタル経済における信用に寄与することを認める。

（4 省略）

RCEP 協定

第 12.8 条（オンラインの個人情報の保護）

1. 各締約国は、電子商取引の利用者の個人情報の保護を確保する法的枠組みを採用し、又は維持する。

（以下省略）

第 2 項　公共政策例外規定

近年締結された地域貿易協定では、越境的データ移転制限禁止条項およびコンピュータ設備等要求禁止条項が規定される場合には、それらに対する例外規定を併せて設けることが一般的である。そのような例外規定の中でも最も重要なものの一つが、「公共政策の正当な目的」に基づく例外を認める規定（以下「公共政策例外規定」という。）である。以下では、越境的データ移転制限禁止条項との関係と、コンピュータ設備等要求禁止条項との関係に分けて整理する。

(1)　越境的データ移転制限禁止条項と公共政策例外規定

越境的データ移転制限禁止条項に関する公共政策例外規定は、CPTPP 協定第 14.11 条第 3 項、日米デジタル貿易協定第 11 条第 2 項、および USMCA 第 19.11 条第 2 項に定められている。これらはいずれも、各締約国が「公共政策の正当な目的を達成するため」に必要な措置を講ずることを認めたうえで、ただし書において「恣意的若しくは不当な差別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」および「目的の達成に必要な範囲を超えて情報の移転に制限を課するものでないこと」を定めている。また、EU モデル条項には個人情報保護関係の規定（前記第 1 項参照）を除いて公共政策例外規定は盛り込まれていないが、日 EU・EPA 第 8.81 条第 3 項は、各締約国が「公共政策の正当な目的を達成するため」にデータの越境移転を制限することを認めたうえで、ただし書において「同様の条件の下

にある国の間において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しないこと」および「目的の達成に必要な範囲を超えて情報の移転に制限を課するものではないこと」を定めている。これらの公共政策例外規定は、越境的データ移転制限禁止条項の例外として、各締約国が「公共政策の正当な目的」を達成するためにデータの越境移転を制限することを容認する趣旨である。もっとも、「公共政策の正当な目的」が具体的に何を意味するかについては、条文上明確に定義されておらず、各協定の紛争解決手続におけるパネル等の判断の積み重ねを待つ必要がある。現時点では、公共政策例外に関する国際的な解釈・運用の蓄積は十分ではなく、各締約国がその解釈を恣意的に拡張することで例外措置を広範に適用し、協定全体の実効性を著しく損なうリスクがある[31]。

これに対し、RCEP 協定は第 12.15 条第 3 項(a)で公共政策例外規定を設けたうえで、「注」として、「(a)の規定の適用上、締約国は、正当な公共政策の実施の必要性については実施する締約国が決定することを確認する。」と規定している。さらに、「米国モデル」や「EU モデル」に見られる「目的の達成に必要な範囲を超えて情報の移転に制限を課するものでないこと」という比例原則の趣旨を定める規定も設けられていない。加えて、RCEP 協定第 12.17 条第 3 項では、公共政策例外に関する争いを同協定の紛争解決システムの対象から明示的に除外しており、これらを総合すれば、他国が例外措置の正当性について制度上異議を唱えることができない構造となっている。このような構造は「中国モデル」の特徴の一つと位置づけられるが、これらを前提にすると、「公共政策の正当な目的」が具体的に何を意味するのかについては明らかにされないまま、各締約国の自己判断により公共政策例外が適用されることになり、越境的データ移転制限禁止条項の実効性確保に対する懸念を生じさせる。

【参照条文（公共政策例外規定①：越境的データ移転制限禁止条項関係）】

CPTPP 協定

第 14.11 条（情報の電子的手段による国境を越える移転）

（1・2 は前記第 1 項末尾に掲載）

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。

(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) 目的の達成に必要である以上に情報の移転に制限を課するものではないこと。

日米デジタル貿易協定

第 11 条（情報の電子的手段による国境を越える移転）

（1 は前記第 1 節第 1 項末尾に掲載）

2. この条のいかなる規定も、1 の規定に適合しない措置であって、締約国が公共政策の正当な目的を達成するために必要なものを採用し、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。

[31] Cory and Dascoli (2021), pp. 3–9, 11–14; Yakovleva (2024), pp. 82–97, 154–166, 206–215; Dimitropoulos et al. (2025), pp. 7–15.

(a) 恣意的若しくは不当な差別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) 目的の達成に必要な範囲を超えて情報の移転に制限を課するものでないこと。

USMCA

第 19.11 条(情報の電子的手段による国境を越える移転)

(1 は前記第 1 節第 1 項末尾に掲載)

2. この条のいかなる規定も、1の規定に適合しない措置であって、締約国が公共政策の正当な目的を達成するための措置を採用し、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。

(a) 恣意的若しくは不当な差別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) 目的の達成に必要な範囲を超えて情報の移転に制限を課するものではないこと。

日 EU・EPA

第 8.81 条(情報の電子的手段による国境を越える移転)

(1・2 は前記第 1 節第 1 項および第 2 項末尾に掲載)

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 1 及び 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。

(a) 同様の条件の下にある国の間において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しないこと。

(b) 目的の達成に必要な範囲を超えて情報の移転に制限を課するものではないこと。

(4 以下省略)

RCEP 協定

第 12.15 条(情報の電子的手段による国境を越える移転)

(1・2 は前記第 1 節第 1 項末尾に掲載)

3. この条のいかなる規定も、締約国が次のいずれかの措置を採用し、又は維持することを妨げるものではない。

(a) 2 の規定に適合しない措置であって、締約国が公共政策の正当な目的を達成するために必要であると認めるもの。ただし、当該措置が恣意的若しくは不当な差別の手段となるような態様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を条件とする。

注: (a)の規定の適用上、締約国は、正当な公共政策の実施の必要性については実施する締約国が決定することを確認する。

((b)省略)

第 12.17 条(紛争の解決)

(1・2 は省略)

3. いずれの締約国も、この章の規定の下で生ずる問題について、第 19 章(紛争解決)の規定による紛争解決を求めてはならない。締約国は、第 20.8 条(一般的な見直し)の規定に従って行うこの協定の一般的な見直しの一部として、第 19 章(紛争解決)の規定のこの章の規定への適用について見直しを行う。第 19 章(紛争解決)の規定は、当該見直しが完了した後、その適用に合意した締約国の間で、この章の規定について適用する。

(2) コンピュータ設備等要求禁止条項と公共政策例外規定

コンピュータ設備等要求禁止条項との関係についても、CPTPP 協定第 14.13 条第 3 項および RCEP 協定第 12.14 条第 3 項(a)に公共政策例外規定が設けられている。また、日 EU・EPA 第 8.81 条第 3 項の公共政策例外規定は、同条第 2 項に規定されたコンピュータ設備等要求禁止条項にも適用される。もっとも、ここでも「公共政策の正当な目的」が具体的に何を意味するかについて条文上は明確に定義されておらず、各締約国が恣意的に解釈し広範な例外措置を講じることによって、当該協定の実効性を著しく損なうリスクを含んでいる[32]。

他方、日米デジタル貿易協定および USMCA では、コンピュータ設備等要求禁止条項について公共政策例外規定が設けられていない。したがって、日本、メキシコおよびカナダは、米国との関係では、「公共政策の正当な目的」を根拠として自国のデータに関しデータローカライゼーション措置を講じることは認められないことになる。これは、これら三国の企業等が米国の IT 企業によるクラウド・インフラ等にデータの多くを保管しているという実態を反映するものであり、そのような状況を制限することとなるデータローカライゼーション措置を講じることは、米国との関係において許容されないことを意味する。以上の点から、これら三国が米国の市場支配モデル（Market dominant model）に基づく協定を締結させられているとも評価できる。他方、EU と米国の間では、データローカライゼーション措置を禁止する協定は締結されていない。むしろ、EU が GDPR によって自らデータ移転条件を管理する関係にあることから、米国は EU 基準への制度的譲歩を余儀なくされており、この点で、米国の市場支配モデル（Market dominant model）と EU の規範統制モデル（Normative control model）という対照的な構造がせめぎ合っているといえる。

これらに対して、RCEP 協定は、コンピュータ設備等要求禁止条項との関係でも、第 12.14 条第 3 項(a)に公共政策例外規定を設けたうえで、「注」として、「この(a)の規定の適用上、締約国は、正当な公共政策の実施の必要性については実施する締約国が決定することを確認する。」と規定している。さらに、「米国モデル」や「EU モデル」に見られた「目的の達成に必要な範囲を超えて情報の移転に制限を課するものでないこと」という比例原則の趣旨を定める規定は設けられていない。加えて、同協定第 12.17 条第 3 項では、公共政策例外に関する争いを同協定の紛争解決システムの対象から明示的に除外しており（前記(1)参照）、これらを総合すれば、他国が例外措置の正当性について制度上異議を唱えられない構造となっている。したがって、この枠組みでは「公共政策の正当な目的」が具体的に何を意味するのかについては明らかにされないまま公共政策例外が適用されることになり、コンピュータ設備等要求禁止条項の実効性確保に対する懸念を生じさせる。

【参照条文（公共政策例外規定②：コンピュータ設備等要求禁止条項関係）】

CPTPP 協定

第 14.13 条（コンピュータ関連設備の設置）

（1・2 は前記第 1 節第 2 項末尾に掲載）

[32] Cory and Dascoli (2021), pp. 3–9, 11–14; Yakovleva (2024), pp. 82–97, 154–166, 206–215; Dimitropoulos et al. (2025), pp. 7–15.

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。

(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。

日 EU・EPA

第 8.81 条（情報の電子的手段による国境を越える移転）

（1・2 は前記第 1 節第 1 項および第 2 項末尾に掲載）

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 1 及び 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。

(a) 同様の条件の下にある国の間において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しないこと。

(b) 目的の達成に必要な範囲を超えて情報の移転に制限を課するものではないこと。

（4 以下省略）

RCEP 協定

第 12.14 条（コンピュータ関連設備の設置）

（1・2 は前記第 1 節第 2 項末尾に掲載）

3. この条のいかなる規定も、締約国が次のいずれかの措置を採用し、又は維持することを妨げるものではない。

(a) 2 の規定に適合しない措置であって、締約国が公共政策の正当な目的を達成するために必要であると認めるもの。ただし、当該措置が恣意的若しくは不当な差別の手段となるような態様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を条件とする。

注: (a)の規定の適用上、締約国は、正当な公共政策の実施の必要性については実施する締約国が決定することを確認する。

((b)は後記第 3 項末尾に掲載）

第 3 項　安全保障例外規定

三原則条項に対する例外規定のうち、最も広範に適用され得る規定が「自国の安全保障上の重大な利益」を保護するための例外を認める規定（以下「安全保障例外規定」という。）である。

安全保障例外規定については、大国の間で基本的スタンスが大きく異なっている。米国は、GATT 第 21 条および GATS 第 14 条の 2 の安全保障例外（前記第 2 章第 1 節第 5 項参照）の適用については、各締約国の自己判断に委ねるべきものであり、WTO の紛争処理制度の審査対象とはならないと主張してきた。たとえば、Russia – Traffic in Transit 事件における米国の第三者意見において、米国は GATT 第 21 条を自己判断的条項と解釈し、各国が自国の安全保障

上の利益を理由としてとる措置はWTO紛争処理制度の審査対象外であると主張した[33]。当該事件においてWTOパネルは、GATT第21条(b)の文言(「締約国が自国の安全保障上の重大な利益の保護のために必要であると認める」)が各国に一定の裁量を与えることを認めつつも、その裁量は無制限ではなく、同条の適用要件(例外の発動要件が「戦時その他の国際関係の緊急時」に関連していること等)については客観的審査が可能であると判示した[34]。この判断により、安全保障例外を定めたGATT第21条は完全な自己判断的条項ではなく、一定の限界の下でWTO紛争処理手続の審査対象となることが確認された。

安全保障例外についての自己判断性を主張する米国の立場は、CPTPP協定第29.2条、日米デジタル貿易協定第4条およびUSMCA第32.2条にも反映されており、これらの条文構造からすれば、それら協定における安全保障例外規定の適用は各締約国の自己判断に委ねられ、紛争処理制度の適用外と解される[35]。これに対し、EUは、安全保障例外規定の適用要件(以下「例外適用要件」という。)の充足性が各協定上の紛争処理制度において審査対象となり得るとの考えに立脚していると解される。

この点について、日EU・EPA第1.5条第1項とCPTPP協定第29.2条の条文を比較する。日EU・EPA第1.5条第1項は、GATS第14条の2に類似した条文構造をとりつつ、例外適用要件を限定列挙している。すなわち、同項(b)(i)～(iv)において、例外適用要件として、(i)核分裂性物質・核融合性物質関連の措置、(ii)武器・弾薬および軍需品関連の措置、(iii)軍事施設へのサービス提供に関する措置、(iv)戦時その他の国際関係の緊急時にとる措置のいずれかに限定している。このような規定構造から、WTOのパネルがGATT第21条に関して示した上記判断に照らせば、日EU・EPA第1.5条第1項の安全保障例外規定の例外適用要件の充足性については、同協定の紛争解決手続において審査の対象となり得るものと解される[36]。

これに対し、CPTPP協定第29.2条は、同様に(b)において「国際の平和若しくは安全の維持又は回復に関する自国の義務の履行」あるいは「自国の安全保障上の重大な利益の保護」のために必要であると当該締約国が認める措置と定めてはいるものの、日EU・EPA第1.5条のように(b)の(i)～(iv)で例外適用要件を限定列挙する構造はとっていない。このCPTPP協定29.2条の規定構造は、例外適用要件の充足性についての判断は各締約国の自己判断に委ねるという米国の主張に沿ったものと解される。

【参照条文(安全保障例外規定①:日EU・EPA第1.5条およびCPTPP協定29.2条)】

日EU・EPA	CPTPP協定
第1.5条(安全保障のための例外) 1. この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。 ((a)省略)	第29.2条(安全保障の例外) この協定のいかなる規定も、次のように解されてはならない。 ((a)省略)

[33] Panel Report (2019), Russia – Measures Concerning Traffic in Transit, WTO Doc. WT/DS512/R (26 April 2019), paras. 2.4–2.6 (Third-Party Submission of the United States). https://ustr.gov/sites/default/files/enforcement/DS/US.3d.Pty.Stmt.%28as%20delivered%29.fin.%28public%29.pdf

[34] Panel Report (2019), Russia – Measures Concerning Traffic in Transit, WTO Doc. WT/DS512/R (adopted 26 April 2019), paras. 7.100–7.102, 7.108–7.114, 7.130. https://www.wto.org/english/tratop_e/dispu_e/512r_e.pdf

[35] 堀見裕樹(2019)335–360頁; Yakovleva (2024), pp. 154–162, 215–220.

[36] 堀見裕樹(2019)335–360頁; Yakovleva (2024), pp. 154–162, 215–220.

(b) 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを妨げること。 (i) 核分裂性物質若しくは核融合性物質又はこれらの生産原料である物質に関する措置。 (ii) 武器、弾薬及び軍需品の生産又は取引並びに軍事施設に供給するため直接又は間接に行われるその他の貨物及び原料の生産又は取引に関する措置。 (iii) 軍事施設のための直接又は間接に行われるサービスの提供に関する措置。 (iv) 戦時その他の国際関係の緊急時にとる措置。 (c) 締約国が国際の平和及び安全の維持のための国際連合憲章に基づく義務に従う措置をとることを妨げること。	(b) 国際の平和若しくは安全の維持又は回復に関する自国の義務の履行あるいは自国の安全保障上の重大な利益の保護のために必要であると当該締約国が認める措置をとることを妨げること。

また、日米デジタル貿易協定第 4 条および USMCA 第 32.2 条も、実質的に CPTPP 協定と同様の条文構造による安全保障例外規定を定めており、その文言構造(「締約国が・・・認める」)に照らせば、「自国の安全保障上の重大な利益」についての判断は、各締約国の自己判断に委ねられるものと解される[37]。なお、JSI の安定化テキスト(前記第 2 章第 2 節参照)では、第 23 条で「安全保障例外」として、「GATT 第 21 条および GATS 第 14 条の 2 の規定は、必要な変更を加えた上で適用されるものとする。」と規定しており、安全保障例外の例外適用要件充足性が紛争解決手続において審査され得るものと解される構成になっている[38]。米国は、この安定化テキストに対して、安全保障例外についての米国の主張が反映されていないとして、同テキストへの支持を表明しなかった[39]。

これらに対し、中国は、米国による追加関税措置をめぐる WTO 紛争(たとえば、China – Additional Duties on Certain Products from the United States〔DS558〕[40]など)において、GATT 第 21 条の安全保障例外の適用可能性が WTO 紛争処理制度の審査対象となり得るとの前提に立

[37] Yakovleva (2024), pp. 154–166, 215–220.
[38] Joint Statement Initiative on Electronic Commerce, WTO Doc. INF/ECOM/87 (July 26, 2024). https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True
[39] U.S. Mission to the International Organizations in Geneva (2024) Statement by Ambassador María L. Pagán on the WTO E-Commerce Joint Statement Initiative (26 July 2024), para. 4. https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative/
[40] WTO (2019) China – Additional Duties on Certain Products from the United States, WT/DS558/R, Panel Report, 15 November 2019. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/558R.pdf

って主張を展開している[41]。しかし、他方で RCEP 協定においては、より強力な安全保障例外規定が採用されている。すなわち、RCEP 協定第 12.14 条第 3 項および第 12.15 条第 3 項は、それぞれ越境的データ移転制限禁止条項およびコンピュータ設備等要求禁止条項に関して安全保障例外を定めつつ、その(b)において「締約国が自国の安全保障上の重大な利益の保護のために必要であると認める措置」について他の締約国は「争ってはならない。」と規定し、他国が当該措置の正当性を争う余地を明文で排除している。加えて、同協定第 12.17 条第 3 項では、同協定の電子商取引章に関する紛争全般が紛争解決手続の対象から除外されており（前記第 2 節第 2 項(1)参照）、これらを総合すれば、安全保障例外規定の適用について完全に実施国の自己決定に委ねる条文構造となっている。

以上のように、安全保障例外規定は、越境的データ移転を含む電子商取引規定に広く適用可能であるが、例外措置の実施について締約国に自己判断の権限を与える場合には、その濫用によって事実上のデータ保護主義が正当化されるリスクがあり、その結果、国際的なルールの一貫性を損ない、制度秩序の空洞化を招きかねない[42]。

【参照条文（安全保障例外規定②）】

日米デジタル貿易協定

第 4 条（安全保障のための例外）

本協定のいかなる規定も、次のことと解されてはならない。

(a) 締約国に対し、その開示が自国の安全保障上の重大な利益に反すると当該締約国が決定する情報の提供又はそのような情報へのアクセスを要求すること。

(b) 締約国が国際の平和若しくは安全の維持若しくは回復に関する自国の義務の履行又は自国の安全保障上の重大な利益の保護のために必要であると認める措置を適用することを妨げること。

USMCA

第 32.2 条（重大な安全保障）

1. 本協定のいかなる規定も、次のように解してはならない。

(a) 締約国に対し、その開示が自国の安全保障上の利益に反すると当該締約国が判断する情報の提供又はアクセスを認めることを要求するもの。

(b) 締約国が国際の平和若しくは安全の維持若しくは回復に関する自国の義務の履行又は自国の本質的安全保障上の利益の保護のために必要であると認める措置を適用することを妨げるもの。

RCEP 協定

第 12.14 条（コンピュータ関連設備の設置）

（1・2 は前記第 1 節第 2 項末尾に掲載）

3. この条のいかなる規定も、締約国が次のいずれかの措置を採用し、又は維持することを妨げるものではない。

((a)は前記第 2 節第 2 項末尾に掲載）

[41] WTO (2019) Russia – Measures Concerning Traffic in Transit, Panel Report, WT/DS512/R, circulated 26 April 2019, paras. 7.32–7.35 (China's third-party submission).
https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/512R.pdf

[42] Aaronson and Leblond (2018), pp. 257–266; Cory and Dascoli (2021), pp. 3–9, 11–14; Yakovleva (2024), pp. 154–166, 215–220.

(b) 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める措置。他の締約国は当該措置については、争ってはならない。

第 12.15 条(情報の電子的手段による国境を越える移転)

(1・2 は前記第 1 節第 1 項末尾に掲載)

3. この条のいかなる規定も、締約国が次のいずれかの措置を採用し、又は維持することを妨げるものではない。

((a)は前記第 2 節第 2 項末尾に掲載)

(b) 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める措置。他の締約国は当該措置については、争ってはならない。

JSI「安定化テキスト」

第 23 条(安全保障例外)

本協定の目的のために、GATT 1994 第 21 条及び GATS 第 14 条の 2 の規定は、必要な変更を加えた上で(mutatis mutandis)適用されるものとする。

第 3 節　大国の規範的対立を踏まえたデータガバナンス規範再構成の方向性

越境的データガバナンスの国際的規律は、国家主権、経済活動、基本権保障が交錯する領域であり、近年の地政学的緊張や規制強化の影響を受け、制度的複雑性が急速に高まっている。既存の地域貿易協定では、越境的データ移転制限禁止条項、コンピュータ設備等要求禁止条項、ソースコード移転等要求禁止条項といった三原則条項が整備されてきたものの、大国間の規範的対立を反映して、個人情報保護に関する適用除外規定、公共政策例外規定、安全保障例外規定が重層的に組み込まれた結果、これら規定が原則規定の実効性を構造的に掘り崩す現象が顕在化している[43]。この構造は、越境的データ移転の自由と国家による主権的統制との調整枠組みが制度的に実効性を欠くことを示すものであり、制度全体の予見可能性を損なう要因となっている。

本来、地域貿易協定における三原則条項は、データの自由な流通を制度的に支える中核的規定である。しかし、これらの条項に対する例外規定の適用が各国の一方的な自己判断に委ねられ、それが非大国の間にも拡大すれば、保護主義的運用が世界的に助長され、国際的データガバナンス体制は分断の危機に直面する。

本章で示したように、公共政策例外規定については国際的な解釈の蓄積が不十分であり、各国が例外の範囲を広く主張できる余地が残されている[44]。さらに、安全保障例外規定については、米国が自己判断性を強く主張する一方、EU は審査可能性を重視するという方向性の相違が構造的緊張を生んでいる[45]。一国主義的な例外規定の運用は、越境的データ移転を事実上制限し、結果としてデータ保護主義を制度的に正当化する作用をもたらす危険がある。特に、RCEP 協定のように例外措置への異議申立てが制度的に封じられる設計では、例外が恒常化し、原則条項の機能が弱体化する事態が想定される[46]。

大国を中心に各国が例外規定の適用や規制措置の正当化について広い裁量を行使する現状を踏まえると、今後の越境的データガバナンスに関する国際的枠組みにおいては、各措置の正当性や必要性を検証するための客観的かつ再現可能な評価基準を確立することが不可欠となる[47]。従来の抽象的な規律だけでは、例外規定の恣意的運用を抑制しきれず、国際的相互信頼を確保するには不十分である[48]。この課題を克服し、協定の実効性を担保するためには、データの性質、利用文脈、アクセス主体、受入国の制度構造といった具体的に可視化し得る複数要素を総合的に踏まえて各国の措置を評価する仕組みが必要となる。越境的データガバナンス規範の再構成には、抽象的条項の運用に依存した従来型モデルを超え、リスクに基づく透明で中立的な評価枠組みを中心に据える制度的転換が不可欠である。

もっとも、この点に関し、日本は、米国、EU、中国といった主要国と、それぞれ異なる規範構造を採用する経済連携協定を締結してきたことから、越境的データガバナンスに関する基本姿

---

[43] Aaronson and Leblond (2018), pp. 257–266; Cory and Dascoli (2021), pp. 3–9, 11–14; Chin and Zhao (2022), section 6; Yakovleva (2024), pp. 82–97, 154–166.
[44] Cory and Dascoli (2021), pp. 3–9, 11–14; Yakovleva (2024), pp. 82–97, 154–166.
[45] 堀見裕樹（2019）335–360 頁; Yakovleva (2024), pp. 154–166, 215–220.
[46] Aaronson and Leblond (2018), pp. 257–266; Cory and Dascoli (2021), pp. 3–9, 11–14; Chin and Zhao (2022), section 6.
[47] Aaronson and Leblond (2018), pp. 257–266; Cory and Dascoli (2021), pp. 3–9, 11–14; OECD (2022c), pp. 13–15, 27–32; Yakovleva (2024), pp. 82–97, 154–166.
[48] Aaronson and Leblond (2018), pp. 257–266; OECD (2022c), pp. 31–32; Yakovleva (2024), pp. 82–97, 154–166.

勢の一貫性が他国から見えにくいという構造的課題を抱えている。越境的データガバナンス規範再構成にあたっては、価値体系と政策スタンスの異なる複数のモデルに同時に向き合う必要があり、国際的信頼の確保には、国内制度と国際的コミットメントの整合性を示す明確な方針が求められる。この点を曖昧にしたままでは、日本が中堅国や新興国に対して主導的役割を果たす際に、説得力や信頼性を欠くことになる[49]。

このような日本の立場を活かすには、日本が異なる価値体系の橋渡しを行い、制度的・政策的対立を緩和する調整役となることである[50]。これを実現するためには、特定の大国による規範的統制に依拠する発想から離れ、DFFT の指導理念の下で、中立的なリスクベースアプローチを運用規範とし、信頼に基づく評価枠組みを国際協議の中心に据えることが不可欠となる[51]。そこでは、利用文脈に即したリスク評価の手法を導入し、例外規定の行使に一貫性と透明性を確保することで、越境的データガバナンスにおける制度的相互信頼を高める基盤を構築する必要がある。

[49] Burri (2017), pp. 126–132; Bacchus et al. (2024), pp. 3–9.
[50] Burri (2017), pp. 126–132; OECD (2022c), pp. 31–32; Bacchus et al. (2024), pp. 3–9; 石井夏生利(2025)240–245 頁.
[51] World Economic Forum (2020), pp. 7–8, 12–18, 28–36, 38–42; OECD (2022a), pp. 20–23, 34–35, 40–42.

第 9 章

越境的データガバナンス規範再編成の具体化と実装

第 9 章　越境的データガバナンス規範再構成の具体化と実装

本章では、越境的データガバナンス規範再構成の具体化と実装について検討する。近年の地政学的変動や国家主権意識の高まりに伴い、これまで国際的基本原理として機能してきた「Free Flow of Data（データの自由な流通）」は、その規範的機能を失いつつある（前記第 2 章第 1 節参照）。各国は、自国の法制度や政策目的に基づき、越境的データ移転に対する制限を強化する傾向を示しており、その結果として国際的にデータ保護主義が拡大している。

この状況は、従来の越境的データガバナンス規範が領域主権を前提とした静態的な規制モデルに依拠してきたこと、ならびに、実質的リスクの内容・発生可能性・重大性を十分に精査しないまま、形式的な規制枠組みや一方的な国益判断に基づいてサイバー空間に適用されてきたことに起因する構造的問題である。越境的データガバナンス規範の再構成にあたっては、こうした構造的問題を克服するため、DFFT（Data Free Flow with Trust）を指導理念として位置づけ、国家主権と国際的相互運用性の間に生じる緊張を調整しつつ、信頼性・透明性・実効性を制度的に確保し得る枠組みを構築することが必要となる。DFFT は制度の多様性を前提としつつ、越境的データ移転に対する評価基準や政策手続の透明化を促進し、国際的な信頼構築を支える理念的基盤として機能し得る。

越境的データガバナンス規範再構成にあたっては、次の四つの要素が重視される。

第一に、国際的データガバナンスの分断を阻止し、サイバー空間の分裂を回避するためには、「Free Flow of Data」に代わる新たな指導理念の下で、各国の主権的統制を尊重しつつ国際的相互運用性を確保し得る新たな規範が不可欠となる。日本が提唱してきた DFFT を指導理念とし、これを具体化する規範再構成が重要となる。

第二に、データの性質および利用文脈に基づく比例的かつ柔軟な規制調整を可能とする規範構造の構築が必要となる。形式的な移転禁止を中核とする枠組みから、リスクに応じて移転条件を段階的に調整する枠組みへ移行することにより、制度間の摩擦を最小化しつつ、各国の公共目的と越境的データ流通の両立を図ることが可能となる。

第三に、ガバメントアクセスを含む国家的介入について、透明性、説明責任および独立監督を制度的原理として国際的に位置づける必要がある。これは越境的データ移転に対する信頼性を支える基礎条件であり、相互監視ではなく制度的信頼の構築を志向する視座を提供する。

第四に、既存の貿易協定や地域協定の限界を超え、技術的、制度的および規範的論点を統合的に扱う新たな国際的協調枠組みの構築が求められる。データは経済財の域を超え、社会的、安全保障的および技術基盤的性格を有することから、従来の貿易法モデルのみでは十分に規律し得ない。したがって、より包摂的な新たな国際フォーラムの創設が必要とされる。

以上の再構成アプローチは、制度的ブロック間の対立を緩和し、サイバー空間の国際的公共性を維持するための現実的方策となる。サイバー空間の分裂を回避し、持続可能で信頼し得る国際的データガバナンスを形成するためには、各国が自国の制度的利害を超え、共通原理に基づく協調的で相互運用可能な規範の再構成に取り組むことが求められる。

本章では、第 1 節で越境的データガバナンス規範再構成のための指導理念および運用規範を検討し、第 2 節で新たな規範の実装の在り方として CRDM モデルを提案する。

第 1 節　越境的データガバナンス規範再構成のための指導理念および運用規範

越境的データガバナンス規範の再構成を論じるにあたっては、従来の国際的指導理念が果たしてきた役割と、その規範的限界を明確にする必要がある。これまで「Free Flow of Data」は、国境を越えるデータ流通を原則的に促進する理念として、国際的デジタル経済の拡大と技術革新を支える基盤的規範の機能を果たしてきた。この理念は、1990 年代に米国が提唱したインターネット自由市場モデルに由来し、越境的データ移転の自由が経済成長と技術革新の主要な駆動力であるとの認識の下で発展してきた[52]。米国は巨大 IT 企業の発展を背景に、この原則を通商政策の中核に据え、他国との貿易協定において越境的データ移転の制限禁止やデータローカライゼーション措置の禁止といった条項の普及を通じ、その国際的浸透を主導してきた[53]。

しかし、この理念は、国家によるデジタル主権主張の強化、ガバメントアクセスの拡大、国家安全保障政策の優位化といった現代的変化に直面し、規範的普遍性が損なわれて実質的な調整機能を低下させている（前記第 2 章第 1 節参照）。その結果、各国が自国の価値観や制度的論理に基づいてデータ流通を規律する状況が常態化し、越境的データガバナンスは、地政学的多極化の下で規範の再構成を迫られている[54]。OECD の企業調査でも、各国規制の不整合により企業が相反する義務を課される事例が多数生じていることが報告されており[55]、越境的データガバナンスに関する国際的統一規範の策定が求められている。

このような状況の下では、越境的データ移転を市場開放の延長として捉える従来の発想のみでは、各国が抱える公共的利益や制度的多様性を十分に包摂することが困難である。したがって、越境的データガバナンス規範の再構成にあたっては、自由な流通を無条件の規範目標として維持するのではなく、信頼性、比例性、透明性といった制度的価値を中核に据えた新たな指導理念の確立が求められる。本稿では、従来の自由流通原則を越えて、制度的相互信頼を基礎としたデータ流通の原理を再構成するため、DFFT を指導理念として位置づけ、その具体的な運用原則としてリスクベースアプローチに基づく枠組みの構築を提示する。

本節では、第 1 項において DFFT を指導理念とする規範再構成の方向性を検討し、第 2 項においてリスクベースアプローチによる運用規範の再構成について論じる。

第 1 項　DFFT を指導理念とする規範再構成の方向性

DFFT は、制度の多様性を前提としつつ信頼に基づく協調を可能にする理念として[56]、G7 や OECD をはじめとする国際的場面で承認されてきた。近年では、DFFT の理念を具体的制度へと転換する国際的取組が進展している[57]。日本は、2019 年の世界経済フォーラム年次総会（ダボス会議）において DFFT 構想を提唱して以降[58]、G7 および OECD における制度議論を継続的に

[52] Aaronson (2018), pp. 4–17. Meltzer (2015), pp. 91–101.
[53] Aaronson (2018), pp. 7–17; Meltzer (2015), pp. 91–101; Burri (2017), pp. 99–105, 110–122, 126–132.
[54] López González (2021), pp. 7–16; Dimitropoulos et al. (2025), pp. 2–15.
[55] OECD (2023b), pp. 17–24.
[56] OECD (2022c), pp. 8–9, 16–18, 31–32.
[57] OECD (2022c), pp. 31–32； G7 Digital and Tech Ministers (2023a); 藤井康次郎・根本拓・福島惇央 (2024)112–136 頁.
[58] Abe (2019).

主導してきた。G7 では、2021 年および 2023 年に、越境的データ移転の透明性向上、データ分類の共通枠組み、ガバメントアクセスに関する評価基準の整理などを提唱し、制度的枠組みの形成を促進した[59]。2023 年の G7 群馬高崎デジタル大臣会合においては、日本の主導により、DFFT を制度的に運用するための協力枠組みとして IAP（Institutional Arrangement for Operationalizing DFFT）を設置することが合意され、各国当局間での制度比較、政策手続の透明化、リスク評価手法の共有などを実施する枠組みが提唱された[60]。IAP は、越境的データガバナンスに関わる実務課題を扱う国際的プラットフォームとして位置づけられており、DFFT の理念を制度運用の段階へと具体化する機能を担う枠組みとして理解される。

OECD においても、日本はガバメントアクセス制度の比較可能性向上の必要性を提起し、2022 年 12 月の「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」[61]（以下「OECD ガバメントアクセス宣言」という。）に係る議論を主導した。同宣言は、透明性、必要性、比例性、独立監督といった原則を国際的基準として提示し、越境的データ移転に伴う制度的信頼性を確保するための共通基盤を提供するものである。さらに OECD は、IAP との連携も視野に、OECD ガバメントアクセス原則の国内実装状況のレビュー、制度的相互運用性を強化するための実務ガイドラインの策定、越境的データ移転に関するリスク評価手法の共通化について検討の必要性を示している[62]。

加えて、日本は APEC の CBPR（Cross-Border Privacy Rules）制度[63]の国際展開（Global CBPR）においても主導的役割を果たし、企業レベルの越境的データ移転認証制度の多国間展開を促進している[64]。これらの国際的取組は、DFFT の理念を政策的標語にとどめることなく、制度的信頼性、可視性および相互運用性を支える国際的枠組みへと発展させる基盤を形成している。

もっとも、DFFT を指導理念として位置づける規範再構成の方向性を検討するにあたっては、その概念自体に多義性が内在する点に十分留意する必要がある。経済安全保障の観点から自国データの越境移転を制限する措置が「with trust」の理念と整合的であると主張され得る一方で、それが「Data Free Flow」の側面との緊張関係に立つ可能性も否定できない。このように、DFFT の具体的内容は、各国の安全保障政策、法制度およびデジタル産業構造の相違により異なる解釈を許容する構造を有している。このため、DFFT の理念を国際的に実装するにあたっては、価値観の相違が制度的緊張へと転化することを抑制しつつ、信頼性、透明性および相互運用性を確保する慎重かつ精緻な制度設計が不可欠となる[65]。

したがって、DFFT の理念を実効的に具現化するためには、その運用に関する共通の基本原則を国際的に明確化し、各国の制度に定着させるための共通枠組みを構築することが必要となる。越境的データガバナンスにおける運用上の基本原則としては、これまで目的限定（Purpose

[59] G7 (2021a); G7 (2021b); G7 Digital and Tech Ministers (2023b).
[60] G7 Digital and Tech Ministers (2023a).
[61] OECD（2022e）.
[62] G7 Digital and Tech Ministers (2023a); OECD (2022e); OECD (2023a), pp. 15–17, 19–21.
[63] APEC (2015).
[64] Global CBPR Declaration (2022),
[65] OECD (2022a), pp. 34, 40–41; OECD (2023a), pp. 15–17, 19–21; 根本拓（2023）2–12 頁、16–22 頁.

Limitation）、必要性（Necessity）、比例性（Proportionality）、データ最小化（Data Minimization）、透明性（Transparency）、説明責任（Accountability）などが認知されてきた[66]。

これらの原則は、主として EU において、EU 基本権憲章[67]や GDPR の運用を通じて具体化されてきたが、その一部は形式主義的または過度に硬直的な適用に傾斜する傾向があり[68]、非大国や非 EU 諸国にとって制度的・技術的・運用的な負担や適応困難性をもたらす場合がある。このため、各国の制度的多様性および国際的相互運用性に配慮しつつ、これらの原則を柔軟かつ実効的に再構成することにより、特定の大国モデルの一方的普遍化ではなく、共有可能な国際規範として位置づけることが求められる。これは、DFFT の理念を制度的に実装するうえで不可欠な段階であり、有志国連携（後記第 10 章第 3 節参照）の制度的基盤を形成するものである。

第 2 項　リスクベースアプローチによる運用規範の再構成

国家間で統治体制・価値観・データガバナンスの制度設計が大きく異なる現状において、各国の主権的統制を尊重しつつ国際的相互運用性を備えた枠組みを構築するには、政治的・主観的な価値判断を介在させない中立的な判断基準の導入が不可欠である。この観点から、越境的データガバナンスにおいて、目的限定・必要性・比例性といった中核的基本原則を実務上で実効的に適用するための制度的枠組みとして、リスクベースアプローチは重要な意義を持つ。リスクベースアプローチとは、対応すべきリスクの内容・重大性・発生可能性を精査し、それに対する規制措置の実質的な均衡性を評価する方法論である[69]。この方法論は、法文化や政策目的の相違を超えて各国が共通に採用可能な判断基盤を提供し、各国の主権的統制を確保しつつ、国際的な整合性と相互信頼の構築を両立させるものである。

リスクベースアプローチが有効である理由は三点に整理できる。

第一に、各政策領域で問題となるリスクの種類は異なり、画一的・形式的な規制では状況に適合しないものの、いずれもデータの性質や利用文脈に依存して変動する性格を持つ。リスクベースアプローチは、データの性質や利用文脈に応じて保護と規律の水準を段階的に調整できるため、各国の政治体制や統治構造から中立的な判断基準を提供することが可能となる。

第二に、越境的効果を有する規制措置については、各国の国内制度において、他国から見ても恣意的でないことが確認できる制度的信頼性を確保することが不可欠であり、この信頼は透明性・説明責任・独立監督の制度化によって支えられる。リスクベースアプローチは、リスク評価の手続を明確化し、規制理由と必要性を合理的に説明する枠組みを提供するため、制度間の信頼構築に寄与する。

---

[66] GDPR art. 5(1)(a)–(f)（合法性、公正性、透明性、目的限定、データ最小化等の原則を規定。必要性および比例性は判例および指針により具体化）; OECD (2013), paras. 7–13（透明性、説明責任等の原則を提示）; Organization of American States (2021)（透明性、目的限定、データ最小化、説明責任、比例性等の原則を規定）.

[67] Charter of Fundamental Rights of the European Union, 2012 O.J. C 326/391.

[68] Kuner (2017a), pp. 886–905, 910–913（Schrems 判決後の EU 域外データ移転規制において、CJEU（欧州連合司法裁判所）の判断枠組みが高度に抽象化された保護基準を要求する結果、制度設計と実務運用との乖離を生じさせ、企業にとって実務上達成が困難な規制構造を形成している点を批判的に論じている。）.

[69] Article 29 Data Protection Working Party (2014), points 3–7, 9 and 11.

第三に、制度的ブロック間の非対称性を緩和し、国際的断片化を抑制するためには、各国の規制措置を相互に比較・評価可能な形で位置づける枠組みが必要である。リスクベースアプローチは、この相互評価の基準を提供し、各国が自国制度の合理性を国際的に説明可能な形で位置づけることを可能とする。

近年の国際的議論においては、越境的データガバナンスに関し、リスクベースアプローチ導入の必要性が広く認識されつつある。たとえば、OECD 改訂プライバシー・ガイドライン（2013 年改訂）第 18 パラグラフは、プライバシー保護と自由なデータ流通の利益の均衡を企図し、越境的データ移転に対する制限はリスクに比例したものでなければならないと明記しており[70]、越境的データ移転規制の設計指針の一つを提供している。さらに、近年の OECD は、DFFT の制度化に向けた分析の中で、各国が採用する移転評価手法の不透明性・多様性が企業のコンプライアンス負担を増大させている点を指摘し、越境的データ移転に関する評価基準について、リスクに応じて一貫的かつ透明なものとする必要性を強調している[71]。また、OECD ガバメントアクセス宣言は、ガバメントアクセスに関する透明性・必要性・比例性の原則を国際的基準として提示し、実質的にはリスクベースアプローチの制度的基盤を国際的に整備する方向性を示したものである[72]。近年の地域貿易協定にも、リスクベースアプローチを規範的基礎とする条文が盛り込まれつつある（前記第 8 章第 2 節参照）。

学問的議論においても、越境的データガバナンスにおけるリスクベースアプローチ導入の必要性を支持する見解が広がっている。たとえば Breitbarth（2021）は、リスクの発生可能性と保護措置の有効性の双方を考慮した柔軟な規制枠組みの構築が不可欠であることを強調し、データ移転に対する制限についても、このアプローチに即して柔軟に適用されるべきであると論じている[73]。また、Christakis（2024a）は、GDPR は国際的なデータ移転や EU 域内に所在するデータに対するガバメントアクセスのリスク評価に関してリスクベースアプローチを支持していると理解すべきであるとして、その解釈を EU 法の比例原則に根拠づけている[74]。これらは EDPB（European Data Protection Board：欧州データ保護理事会）が従来強調してきた形式的な遵守要件（第三国移転に一律の高度暗号化や契約条項を義務づける）を重視する方針[75]に対し、その見直しを促すものである。すなわち、EDPB は、GDPR の域内適用においては、個別のデータ処理行為を単位として、その性質および利用文脈に応じたリスクベースアプローチを広く認め、比例原則に基づく柔軟な評価を許容している。他方で、第三国への越境移転に関しては、Schrems Ⅱ 判決を踏まえ、当該移転行為それ自体のリスクよりも、受入国法制度全体の「実質的同等性」を中心基準とする枠組みを維持している。この結果、域内では処理行為ベースのリスクベースであるのに対し、域外では制度ベース・形式的評価に傾斜するという非対称性が生じている[76]。

こうした国際的・学問的な動向の中で、2024 年 7 月、ドイツ・トラウンシュタイン地方裁判所は、グローバルなソーシャルネットワーク事業者による米国への個人データの移転につき、GDPR 第

[70] OECD (2013), Part Four, para. 18.
[71] OECD (2022a), pp. 34, 40–42; OECD (2023a), pp. 15–17, 19–21, 23–25.
[72] OECD (2022e), principles I–II.
[73] Breitbarth (2021), pp. 541–547.
[74] Christakis (2024a), pp. 24–38, 42–56.
[75] EDPB (2021a), paras. 42–46, 79–88 and Annex 2（第三国法制の評価義務、実質的同等性確保のための補完措置の要求、ならびに暗号化・仮名化等の技術的補完措置の具体例を提示）.
[76] EDPB (2020c), paras. 6–8, 11–15, 28; EDPB (2021a), paras. 6–13, 23, 28–46; EDPB (2021b), paras. 6–16.

6 条第 1 項(b)（契約履行）および GDPR 第 V 章の要件を満たしていることから適法であるとして、データを EU 域内に保存すべきであるとの EU 当局側の主張を退けた[77]。この裁判例は、GDPR 第 V 章の個人データの域外移転に関してリスクベースアプローチを採用したものと解され、EU 司法における制度的転換の端緒を画する重要な判決と位置づけられている[78]。

[77] Landgericht Traunstein, judgment of 8 July 2024, Case No. 9 O 173/24. https://gdprhub.eu/index.php?title=LG_Traunstein_-_9_O_173/24.
[78] Christakis et al. (2024).

第 2 節　文脈的リスク評価に基づくデータ最小化モデル（CRDM モデル）による実装

越境的データガバナンス規範の再構成にあたっては、新たに策定される規範を国際的な協定またはガイドラインの形で実装し、その相互運用性と実効性を確保することが極めて重要である。本節では、リスクベースアプローチに基づく運用規範の実装方策として、文脈的リスク評価に着目し、これとデータ最小化原則を併用することにより、各国の主権的統制と国際的相互運用性を調整する新たなモデル（CRDM モデル）を提案する。

第 1 項　文脈的リスク評価

リスクベースアプローチを明示的に条文に規定した先例として、EU の AI 法[79]が挙げられる。同法は、AI システムの利用文脈に応じた段階的かつ文脈依存的なリスク評価に基づき、第 6 条第 2 項および附属書Ⅲにおいて分野別の「高リスク AI ユースケース」を列挙するなど、リスクの程度に応じた柔軟かつ階層的な規制対応を制度化している。具体例として、高リスクに分類されるものには、①バイオメトリクス分野（例：遠隔識別、属性分類、感情認識）、②重要インフラ分野（例：公共交通、エネルギー・水道等の安全運用）、③教育・職業訓練分野（例：入学選抜、試験評価）、④雇用・労働管理分野（例：採用・昇進・解雇の判断）、⑤法執行分野（例：犯罪リスク評価、ポリグラフ使用）などがある[80]。これらに該当する場合には、基本的権利侵害の可能性が高いため、透明性、監査可能性、説明責任などの厳格な義務が課される[81]。他方、中リスクまたは低リスクに分類されるシステムには、比例的かつ適合的な緩和措置が適用される[82]。

このようなデータの利用文脈に応じたリスク評価（contextual risk assessment）は、越境的データガバナンス規範の制度設計においても重要な示唆を与える。越境的データ移転においても、データの利用文脈に応じた文脈的リスク評価を導入することで、従来の移転先制度に依拠した適正性評価モデル（例：GDPR の十分性認定）よりも、柔軟性と中立性を備え、地政学的対立の影響を受けにくい制度設計が可能となる。これにより、データの性質に基づくリスク分類（高リスクデータ、中リスクデータ、低リスクデータ）と利用文脈（法執行、医療研究、統計など）に基づくリスク分類（高リスク文脈、中リスク文脈、低リスク文脈）を交差的に評価し、比例原則を適用して段階的な移転条件を整備することができる[83]。

リスクベースアプローチに基づく運用規範の再構成は、一律的な制度適正性評価への依存を避けつつ、個別のリスク文脈に応じた移転許容性判断を可能とするものであり、実務的柔軟性と制度的信頼性の両立を図ることができる。また、文脈的リスク評価と比例原則に基づく枠組みは、画一的基準ではなく段階的かつ柔軟な対応を促し、DFFT の中核理念である信頼に基づく

---

[79] Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union L 168, 12 July 2024, p. 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[80] Artificial Intelligence Act, art. 6(2), Annex Ⅲ (listing high-risk use cases).

[81] Artificial Intelligence Act, art. 6(2), Annex Ⅲ, and arts. 8–29, 51.

[82] Artificial Intelligence Act, art. 50, Recital 70.

[83] OECD (2019b), Section 1, Principle 1.2（人間中心の価値および公正性）, Principle 1.4（頑健性・安全性・セキュリティ）; European Regulation and Innovation Forum (2019), pp. 1–4.

自由な流通の具体化にも資する[84]。このアプローチは、従来の移転先制度中心の枠組みが抱えていた硬直性と地政学的依存性を克服し、各国の制度的多様性を前提にしつつ、信頼に基づく越境的データ流通を制度的に可能とする。さらに、このアプローチは、目的限定性、必要性、比例性といった越境的データガバナンスの中核的原則を具体的運用が可能な制度へと落とし込むものであり、透明性および説明責任の確保についても、段階的な説明義務や監督制度の導入によって担保し得る。

【参照条文（AI 法のハイリスク AI システム）】

AI 法附属書 Ⅲ（第 6 条第 2 項に定めるハイリスク AI システム）

第 6 条第 2 項にいう高リスク AI システムとは、次の分野のいずれかに該当する AI システムをいう。

1. バイオメトリクス（当該利用が EU 法又は加盟国法により認められている限度で）
   (a) 遠隔バイオメトリクスシステム。なお、特定の自然人が自己の申告どおりの人物であることを確認するという唯一の目的で用いられるバイオメトリック検証のための AI システムは含まれない。
   (b) センシティブ又は保護される属性・特性を推論によって識別し、それに基づき分類するために使用される AI システム。
   (c) 感情認識のために使用される AI システム。
2. 重要インフラ
   重要なデジタルインフラ、道路交通、水・ガス・暖房・電力の供給に関する管理及び運用において、安全性確保のための構成要素として使用されることを目的とする AI システム。
3. 教育及び職業訓練
   (a) あらゆる水準の教育機関又は職業訓練機関へのアクセス又は入学の可否を決定し、又は自然人を当該機関に配属するために使用されることを目的とする AI システム。
   (b) 学習成果を評価するために使用される AI システム（当該成果が教育機関又は職業訓練機関において自然人の学習過程の方向付けに利用される場合を含む）。
   (c) あらゆる水準の教育機関又は職業訓練機関の文脈において、個人が受ける、又はアクセスし得る教育水準の適切性を評価するために使用される AI システム。
   (d) あらゆる水準の教育機関又は職業訓練機関での試験に際し、学生の禁止行為を監視・検知するために使用される AI システム。
4. 雇用、労務管理及び自営業へのアクセス:
   (a) 自然人の採用又は選考のために使用される AI システム。特定対象に向けた求人広告の提示、応募書類の分析・フィルタリング、候補者の評価に用いられるもの。
   (b) 就業関係に関する条件、就業契約関係の昇進又は終了に影響を及ぼす決定を行うため、又は個々の行動、個人的特性に基づき業務を割り当てるため、あるいは当該関係にある者の業務遂行状況及び行動を監視・評価するために使用される AI システム。
5. 不可欠な民間サービス及び公共サービス・給付へのアクセス及び享受

[84] European Regulation and Innovation Forum (2019), pp. 1–4; OECD (2022a), pp. 40–42; OECD (2022e), Principles Ⅱ–Ⅲ, Ⅵ–Ⅶ; OECD (2023a), pp. 19–25, 26–31.

(a) 公的機関又はその委託先が、自然人の不可欠な公的支援給付及びサービス（医療サービスを含む）の受給資格を評価し、又は当該給付・サービスを付与・減額・取消し・返還請求するために使用する AI システム。

(b) 自然人の信用力を評価し、又は信用スコアを算定するために使用される AI システム。ただし、金融詐欺の検知を目的とする AI システムを除く。

(c) 生命保険及び医療保険において、自然人に関するリスク評価及び保険料算定に使用される AI システム。

(d) 自然人からの緊急通報を評価・分類するため、又は警察・消防・医療救助を含む緊急初動サービスの派遣やその優先順位付け、さらに緊急医療における患者トリアージシステムのために使用される AI システム。

6. 法執行（当該利用が EU 法又は加盟国法により認められている限度で）

(a) 自然人が犯罪被害者となるリスクを評価するために、法執行当局又はその委託先、もしくは法執行当局を支援する、又はその委託を受けた EU の機関・機構・事務所・庁が使用する AI システム。

(b) 法執行当局又はその委託先、あるいは法執行当局を支援する EU の機関・機構・事務所・庁が、ポリグラフその他これに類する装置として使用する AI システム。

(c) 法執行当局又はその委託先、あるいは法執行当局を支援する EU の機関・機構・事務所・庁が、犯罪の捜査又は訴追の過程における証拠の信頼性を評価するために使用する AI システム。

(d) 法執行当局又はその委託先、あるいは法執行当局を支援する EU の機関・機構・事務所・庁が、自然人が犯罪を行う、又は再犯するリスクを評価するために使用する AI システム。ただし、2016/680/EU 指令第 3 条 4 項にいう自然人のプロファイリングのみに基づくものではないものに限る。また、自然人又は集団の性格的特性や過去の犯罪行為を評価するために使用されるものも含む。

(e) 法執行当局又はその委託先、あるいは法執行当局を支援する EU の機関・機構・事務所・庁が、犯罪の検知・捜査・訴追の過程において、2016/680/EU 指令第 3 条 4 項にいう自然人のプロファイリングに使用する AI システム。

7. 移民、庇護及び国境管理（当該利用が EU 法又は加盟国法により認められている限度で）

(a) 適格公的機関又はその委託先、あるいは EU の機関・機構・事務所・庁が、ポリグラフその他これに類する装置として使用する AI システム。

(b) 適格公的機関又はその委託先、あるいは EU の機関・機構・事務所・庁が、加盟国領域に入国しようとする、又は既に入国した自然人がもたらすリスク（安全保障上のリスク、不法移民のリスク、健康上のリスクを含む）を評価するために使用する AI システム。

(c) 適格公的機関又はその委託先、あるいは EU の機関・機構・事務所・庁が、庇護、ビザ又は在留許可に関する申請や関連する不服申立ての審査を支援するために使用する AI システム。これには、当該地位を申請する自然人の適格性に関する審査や、証拠の信頼性に関する評価も含まれる。

(d) 適格公的機関又はその委託先、あるいは EU の機関・機構・事務所・庁が、移民、庇護又は国境管理の文脈において、自然人の検知・認識・識別のために使用する AI システム。ただし、渡航書類の検証を目的とするものは除く。

8. 司法及び民主的プロセスの運営

(a) 司法当局によって、又は司法当局のために使用され、事実及び法の調査・解釈、ならびに具体的事実関係への法適用を支援する AI システム。あるいは、代替的紛争解決手続においてこれと同様の方法で使用される AI システム。

(b) 選挙又は国民投票の結果、あるいは自然人が選挙・国民投票において投票行動を行う際の行動に影響を与えるために使用される AI システム。ただし、自然人がその出力に直接さらされない AI システム、すなわち政治キャンペーンを行政的又は後方支援的観点から整理・最適化・構造化するために使用されるツールは含まれない。

第 2 項　CRDM モデルの意義

本稿では、リスクベースアプローチによる規範再構成の実装手法として、文脈的リスク評価とデータ最小化原則を組み合わせた CRDM モデル（Contextual Risk-Based Data Minimization model：文脈的リスク評価に基づくデータ最小化モデル）を提案する。CRDM モデルは、越境的データ移転の制度設計において、データの性質や利用文脈に基づいてリスクを評価し、その結果に応じてデータ処理および規制措置の範囲を必要最小限に限定することを基本とする。ここでいうリスク評価は、データの性質自体に内在するリスクに加え、処理主体、利用目的、影響を受け得る権利・利益の性質、被害発生の蓋然性およびその重大性等の要素の相互関係を総合的に考慮して行う文脈依存的な判断であり、当該判断は事前的かつ継続的に見直され得る。

データ最小化原則は、狭義には、データの収集・処理・保存の各段階において、対象となるデータの内容および量が目的達成にとって最小限であることを求める原則であり[85]、データ流通の初期段階から過剰なデータ処理を予防する役割を担うものである。これに加えて、本稿におけるデータ最小化原則は、越境的データ移転に関し、目的達成のために必要と認められる範囲を超えて義務・制約・統制を課してはならないという原則を含む[86]。すなわち、実質的リスクに照らして、より侵害性の低い代替措置が存在する場合にはそれを優先すべきであるという必要性評価を中核とし、低リスクのデータ又は利用文脈に対して過剰な移転制限を課すことを制度的に排除することを含意する。

このように CRDM モデルでは、制度的に拡張された広義のデータ最小化原則を採用し、比例原則の下で「より制限的でない他の方法」の存否を主要な判断要素とする。これは比例原則のうち、特に必要性審査の要素を制度設計の中心に据えるものであり、当該方法が存在する場合には、当該データの取得や移転に対する規制は必要最小限の措置とは認められず、許容されない。

リスクベースアプローチとデータ最小化原則を統合することにより、形式的・一律的な禁止措置に依拠するのではなく、個人データ・非個人データを問わず、越境的データ移転に柔軟かつ合理的に対応し得る持続可能な制度的枠組みを構築できる。これは、規制の正当化根拠をデータの類型そのものではなく、当該処理がもたらし得る権利侵害リスクの程度に求めるため、データの法的分類を超えた統合的評価を可能にし、規制の正当化構造そのものを再編することに

[85] GDPR art. 5(1)(c); EDPB (2020c), paras. 11–15, 28.

[86] 越境的データ移転制限についても最小化原則を導入する必要性については、以前から指摘されてきた。Meltzer (2015), pp. 101–102.

よる。この点に関し、伝統的に憲法上の人格権などとして強固な保護が想定されてきたプライバシー権についても、その保護強度を一律のものとしてではなく、段階的に捉えるべきであるとする理論が示されている[87]。当該段階理論は、保護や規制の強度を一律ではなく段階的に構成すべきであるという点において、データ保護（特に、個人データ保護）におけるリスクベースアプローチと共通する発想に立つものであり、CRDM モデルはこの発想をデータ処理の文脈において具体化して段階的な保護措置を論ずるものと位置づけることができる。

CRDM モデルは、呼称自体は本稿独自のものであるが、OECD 改訂プライバシー・ガイドライン（2013 年改訂）[88]や CBPR[89]などを基盤とするものである。これらの国際モデルは、越境的データ移転に関する規制についてリスクベースアプローチを基本理念として共有し、データの性質等によるリスクの程度に応じて規制を柔軟に調整しつつ、相互運用性の確保と信頼に基づくデータ流通の促進を目的としている。もっとも、既存の国際モデルでは「より制限的でない他の方法」に関する判断の位置づけが必ずしも明確ではない。CRDM モデルでは、この点を踏まえ、越境的データ移転規制の審査において「より制限的でない他の方法」の存否を明示的かつ具体的な判断要素として位置づけ、これにリスクの性質や利用文脈に応じた階層的評価を統合することで、透明性と予見可能性を確保する枠組みを提示するものである。このように、CRDM モデルは、OECD ガイドラインや CBPR など既存の国際モデルを発展的に継承しつつ、越境的データ移転に関する規制適用の透明性を確保するとともに、規制当局・事業者双方にとっての予見可能性を実質的に高めることを意図する。

CRDM モデルの実装にあたっては、共有可能なリスク分類とそれに対する保護措置の関係を明示することが不可欠である。データの性質（識別性[90]、機微性など）に応じたリスク分類（高リスクデータ、中リスクデータ、低リスクデータ）や利用文脈によるリスク分類（高リスク文脈、中リスク文脈、低リスク文脈）は、移転可否判断の予見可能性・一貫性・透明性を確保する制度的判断基準を構成する。これらのリスク分類と保護措置との対応関係を法令条文や監督当局のガイドラインで明文化・標準化することで、各国の制度的多様性を前提としながらも相互運用性を確保できる[91]。実務面では、各国間でリスク分類や保護措置に関する共通語彙を整備することにより、制度運用上の誤解を回避し、一貫性ある審査基盤を確立することができる。こうした共通原則を制度的に機能させるためには、国際協定や合意文書に明記することが不可欠である。特に、リスク分類に応じた段階的な強度の保護措置を導入することで、目的の正当性・手段の適合性・制約の必要性・利益衡量に基づく柔軟かつ実質的に均衡のとれた判断を可能にする。このように各国が審査枠組みを共有することで、静的な制度適正性への依拠を回避し、動的で信頼性の高い越境的データガバナンスの共通基盤を形成できる[92]。

CRDM モデルは、従来の制度適正性審査（adequacy-type evaluation）とは異なり、個別のデータ処理文脈に即したリスク評価を規制適用の基準とする点において、審査対象および審査単

---

[87] 村上康二郎（2023）Ⅱ-1-Ⅱ-22 頁.
[88] OECD (2013).
[89] APEC (2015).
[90] 識別性とは、個人を特定可能とする情報属性の程度を指し、氏名・顔画像等の高識別性データから、匿名化・集計済みデータ等の低識別性データまで、技術的手段や補完情報の有無等も含めて段階的に評価される。Regulation (EU) 2016/679 of the European Parliament and of the Council, Recital 26, 2016 O.J. L 119, 1; 個人情報の保護に関する法律（平成 15 年法律第 57 号）第 2 条.
[91] OECD (2013); Stone Sweet and Mathews (2008), pp. 86-97.
[92] OECD (2019a), pp. 25-34, 77-89, 92-93.

位を構造的に転換するものである。この点、従来の TIA（Transfer Impact Assessment）は GDPR の下で発展してきたが、その評価対象が移転先国の制度状況に限定され、データの性質や利用文脈が制度的審査枠組みに組み込まれていないという構造的限界がある[93]。これに対し、CRDM モデルでは、①データのリスク特性（例：識別性、機微性）、②利用目的（例：法執行、医療研究、統計）、③保護措置（例：説明義務、安全性確保義務、監督義務）などを審査枠組みに明確に位置づける。たとえば、高リスクデータが高リスク文脈に用いられる場合には最大強度の保護措置が要求されるのに対し、低リスクデータが低リスク文脈に用いられる場合には最小強度の保護措置で足りることになる。これにより、越境的データ移転において柔軟で実質的に均衡のとれた判断を可能にする。

第 3 項　CRDM モデルにおけるリスク評価と保護措置

CRDM モデルでは、データの性質に基づくリスク評価とデータの利用文脈に基づくリスク評価を交差的に用いたうえで、それらに対応する保護措置の強度を段階的に決定する。その保護措置は、説明義務、安全性確保義務、監督義務という三つの要素の組合せによって体系的に表すことが可能である。この構造は、越境的データガバナンス規範の再構成において、理論的にも実務的にも有意義な枠組みを提供する。

第一に、この三義務構造は、リスク評価の結果を具体的な制度設計へと結びつける翻訳装置として機能する。越境的データ移転において、リスクの高低を示すだけでは実務上の行動指針にはならないが、三義務の組合せという明確な措置体系に接続することで、移転主体は必要な対応を直ちに把握できる。すなわち、どのようなデータがどの文脈で利用されるのかという抽象的評価を、説明の深度、技術的措置の強度、監督の厳格性という具体的義務に変換することが可能となり、規範運用の予見可能性が高まる。

第二に、説明・安全性確保・監督という三要素は、各国制度の基本構造に共通するため、制度間の異質性を緩和し、相互運用性を向上させる。GDPR が説明責任・技術的安全性確保・再委託監督を中核義務として構成し[94]、OECD ガバメントアクセス原則が透明性・必要性（比例性）・独立監督という三基軸を掲げ[95]、米国のセクター別法制も通知・安全性措置・サービス提供者監督を柱としているように[96]、異なるブロックが事実上同じ三層モデルに収斂している。このため、CRDM モデルが三義務の組合せを保護措置体系の基礎とすることは、特定大国の制度や規範を輸出するのではなく、既存制度の共通部分を抽象化する形で国際的な合意可能性を高める。

第三に、この枠組みは、セクター別の規制モジュールに対して柔軟に適用でき、制度設計における拡張性と長期的持続性を確保する。異なるセクター（法執行、医療、金融、研究、AI 利用など）は、求められるリスク水準も規制目的も異なるが、説明・安全性確保・監督の三義務は、その強度を調整することで、各セクターに固有の要請を過度な複雑化なく反映できる。これにより、

---

93 EDPB (2021a), paras. 14–25; Juliussen et al. (2023), pp. 227–235.

94 GDPR arts. 5(2), 12–14, 24, 25, 28, 32 and recital 39（透明性・安全性・責任原則の基礎）.

95 OECD (2022e), Principles Ⅱ, Ⅴ and Ⅵ.

96 GLBA (1999), 15 USC § § 6801(b), 6802–6803; FTC (2021), Standards for Safeguarding Customer Information, 16 CFR Part 314, sec. 314.4(a)–(d).

データ技術が高度化し新たな利用文脈が生じた場合でも、枠組みを改定することなく三義務の階層を調整するだけで規律を適応させることができる。

以上により、CRDM モデルが採用する三義務の組合せに基づく保護措置体系は、リスク評価と規範運用の間を接続する構造として機能すると同時に、ブロック横断的な共通基盤を提供し、分野別制度や将来的技術発展にも対応可能な柔軟性を備える点で、越境的データガバナンス規範の再構成にとって極めて有意義である。

CRDM モデルにおける三義務（説明義務・安全性確保義務・監督義務）の組合せが有意義である理由は、データの性質と利用文脈という二つの軸によって導かれるリスク評価を、具体的な保護措置の強度へと的確に還元できる点にある。たとえば、国家の治安維持を目的として個人の DNA 情報を収集する場合、当該データは高度な機微性を有し、データ主体の基本権への影響も極めて大きいという意味でデータの性質として高リスクである。また、その利用文脈も国家の強制力が介在し濫用のリスクも大きい領域であるため高リスク文脈に該当する。こうした二重の高リスク状況では、移転主体が負うべき義務は最大となり、説明義務については詳細な情報開示と手続的保障、安全性確保義務については高度な暗号化・厳格なアクセス管理・分散管理手法など最適化された措置、監督義務については事前承認を含む厳格管理・第三者監査・独立監督機関による継続的検証などが必要となる。つまり、高リスクデータ×高リスク文脈の組合せは、三義務すべてにおいて最大レベルの介入を正当化する。

これに対し、公表されている個人情報を匿名化による統計目的でインターネット上の公開サイトから収集する場合には、データの性質として機微性は非常に低く、本人識別可能性の点でも限定的であるため低リスクに分類される。利用文脈についても、政策立案や研究の補助を目的とした匿名化による統計的処理であり、当該データが直接個人の権利利益に深刻な影響を及ぼす可能性は低い。このような低リスクデータ×低リスク文脈では、求められる保護措置も最小限で足り、説明義務としては利用目的と取得方法の一般的説明、安全性確保義務としては通常の技術的・組織的管理措置、監督義務としては最低限の再委託管理や内部監査が適切となる。

さらに、CRDM モデルでは、義務の水準についても最小化原則が適用される点が重要である。すなわち、リスク評価に基づく義務づけは、目的達成のために必要最小限に限られ、より侵害性の低い手段が存在する場合には、過剰な説明義務・過度に重い技術的措置・不必要に厳格な監督義務を課すことは許容されない。言い換えれば、三義務の強度はリスクに応じて増減し得るが、その上昇は常に「より制限的でない他の方法」の存否を前提とするため、義務の賦課が自己目的化して濫用されることを制度的に防止する構造となっている。

このように、データの性質と利用文脈に応じて三義務の強度を論理的かつ比例的に調整し、かつ義務づけについても最小化原則を通じて過剰な介入を排除できる点が、CRDM モデルの制度設計上の意義である。単一の規制基準を画一的に適用するのではなく、データの性質や利用文脈に応じて必要最小限の義務を設定することにより、権利保護とデータ活用の双方の観点から合理的で持続可能な越境的データガバナンスを構築することが可能となる。

第 4 項　CRDM モデルにおけるモジュール構造

CRDM モデルにおけるモジュール構造は、一般原則および紛争処理手続を共通の義務的モジュールとして確保したうえで、利用セクター（例：法執行、医療研究、金融）ごとのモジュールに

区分し、各セクターにおけるリスク水準に応じた規制を適用する設計である。この構造を採用する利点は、セクターごとのリスク特性や規制目的に応じて、文脈的リスク評価に基づく最小限かつ適合的な措置を柔軟に設計できる点にある。各国は自国の制度的・技術的能力に応じて、自国に適合する特定セクターのモジュールへの参加が可能となる。また、一般原則および紛争処理手続を共通の義務的モジュールとして確保する点については、たとえば、WTO 協定では、DSU（Dispute Settlement Understanding）はすべての加盟国にとって義務的に適用される共通手続であり、各協定のセクター別義務とは独立して、加盟国間の紛争が発生した場合には一律にこの了解事項に従って処理されることが制度的に担保されている[97]。このように、セクター別の柔軟な参加を許容しつつも、共通の紛争処理手続を全加盟国に義務づける点は、紛争処理モジュールへの義務的参加という CRDM モデルの設計思想と構造を共通にするものであり、制度の実効性と予見可能性を支える基盤的要素として位置づけられる。さらに、各モジュールについては、それぞれのセクターの専門家や企業等のステークホルダーが規範形成過程に関与することにより、実践的な内容の規範を策定し得る。

しかし、モジュールの細分化や階層化が過度に進むと、制度全体が複雑化し、各国における理解や運用の負担が増大するおそれがある。特に行政資源が限られる非大国にとっては、制度参加の障壁となり、実効性や包摂性を損なうリスクが高い。制度的過密化を回避しつつ、必要な柔軟性と技術的な対応力を確保するためには、セクターの数を限定し、中核的な規律のみをモジュール本体（国際協定の本文）に明記する一方、詳細な技術的要件や実装方針はガイドラインとして文書化する方式が有効である。ガイドラインは、各国が文脈的リスク評価に基づき、国内法や技術インフラに応じて必要な措置を選択・実装する際の共通基準として機能し、制度の透明性と柔軟性を確保する役割を果たす[98]。モジュール本体は簡素で明確な構造を保ちつつ、ガイドラインを通じて実務上の多様性と柔軟な対応を補完する二層的運用により、利用文脈に応じた必要最小限の措置に限定できる。さらに、ガイドラインは時代や技術の進展に応じて逐次改訂可能であるため、制度の将来的な適応性を高める利点もある。

たとえば、民間の医療分野のモジュールの例として GA4GH（Global Alliance for Genomics and Health）があり[99]、その制度設計は、中核的な倫理原則やデータ共有の基本原則をフレームワークとして共通化する一方で、具体的な技術標準や実装手順をガイドラインとして柔軟に規定する構造を採用している。この枠組みは、分散型環境における相互運用性と自律性の両立を可能にする連合型データガバナンス（後記第 5 項参照）の先行事例として位置づけられる。

このようなモジュール構造は、特定の価値観や制度モデルに依拠することなく、中立性と公平性に基づいた越境的データガバナンスの枠組みの構築を可能にする。今後の国際的合意形成において、この枠組みは、柔軟性と技術的進化の双方を踏まえた現実的モデルとして、有志国連携（後記第 10 章第 3 節参照）の柱となり得るものであり、モジュールによる参加選択制は、各国の制度的差異を吸収し得る仕組みとなる。

---

[97] WTO (1994) Understanding on Rules and Procedures Governing the Settlement of Disputes, arts. 1(1), 3(2), 23(1).
[98] OECD (2013), Part Three, para. 15, Part Four, paras. 16–18, and Part Six, para. 21.
[99] Knoppers (2014), pp. 1–3 (framework purpose and governance), pp. 3–5 (foundational principles).

第 5 項　連合型データガバナンスの有用性と課題

CRDM モデルの実装を技術的側面から支えるものとして、連合型データガバナンス（Federated data governance）が注目される。これは、元データを所在国内に保持したまま、分散処理アーキテクチャを用いて多国間での協働分析を可能にする新たな管理モデルである[100]。フェデレーテッド・ラーニング（Federated Learning）[101]やセキュア・マルチパーティ計算（Secure Multiparty Computation）[102]などの分散処理技術を活用することにより、各主体がデータ管理責任を維持したまま、モデルパラメータや集計結果のみを共有する構成とし、制度的自律性およびデータ最小化を実現しつつ相互運用性を確保することができる[103]。

この連合型データガバナンスは、データの受入国における法制度を基準とするのではなく、処理や利用に伴うリスクを基準とした評価軸を導入する点に特徴がある。すなわち、データの物理的移転を伴わずとも信頼に基づく協働を可能にする枠組みであり[104]、多様な制度環境下においても実践的かつ有効な国際モデルとしての意義を有する。近年では、EU の GAIA-X（European Association for Data and Cloud AISBL）[105]に見られるように、分散処理アーキテクチャの社会実装が進展しており、高機微データ領域を含む多様な分野において国際的に重要なモデルとして評価されつつある[106]。したがって、連合型データガバナンスは、CRDM モデルの制度的基盤を支える技術的実装例として位置づけられる。

もっとも、現行法制度においては、連合型アーキテクチャによる国際連携であっても「越境移転」とみなされる場合があることに留意を要する。たとえば、生データを移転せず統計情報や仮名化情報のみを共有する場合であっても、GDPR 第 44 条以下の規制対象となり得る。EDPB も、統計情報であっても再識別の可能性が残存する限り個人データの「移転」とみなし、第三国からアクセス可能であれば越境移転規制（越境移転の原則的禁止）が適用されるとの見解を示している[107]。このような形式的解釈は、低リスクかつ信頼性の高い分散構成の実装を妨げる要因となる。これに対し、CRDM モデルは、「越境移転」という形式基準ではなく、実質的リスク評価に基づいて条件付きで移転を許容する。たとえば、患者データを仮名化処理し、医療研究目的で必要最小限の範囲に限って移転する場合には、リスクに応じた保護措置の下で移転が許容される。このように、連合型データガバナンスの導入は、CRDM モデルの理念を技術的に具現化する手段として、制度的柔軟性と法的安定性を両立させるうえで重要な意義を持つ。

---

[100] McMahan et al. (2017), pp. 1273–1274; Truong et al. (2021), sections 2–4; Barbereau et al. (2025), sections 3–4.

[101] McMahan et al. (2017), pp. 1273–1274; Aledhari et al. (2020), pp. 140699–140702.

[102] Lindell (2021), pp. 86–89.

[103] McMahan et al. (2017), pp. 1273–1274; Mansouri et al. (2023), pp. 140–148; Barbereau et al. (2025), sections 3–4.

[104] OECD (2013), Part Three, para. 15, Part Four, paras. 16–18, and Part Six, para. 21; Knoppers (2014), pp. 1–3 (Framework purpose and governance), pp. 3–5 (Foundational Principles and Core Elements); OECD (2023a), pp. 19–30.

[105] Gaia-X European Association for Data and Cloud AISBL (2022), Introduction, Architecture Overview, Data Sovereignty, Trust Framework, and Interoperability Framework.

[106] Otto (2022), pp. 44–45; Vankayalapati et al. (2025), pp. 80–83, 85–88.

[107] EDPB (2021a), paras. 6–13, 23, 28–42; EDPB (2021b), Annex, Example 12 (third country authority access constitutes transfer); EDPB (2025), paras. 16–22.

第 6 項　CRDM モデルのフレームワークの具体例

本項では、CRDM モデルのフレームワークの具体的構成を例示する。CRDM モデルは、データの性質に基づくリスク評価と、データの利用文脈に基づくリスク評価を交差的に用い、それぞれの状況に応じて適切な強度の保護措置を適用する構造をとる。この場合、評価軸や保護措置の区分が過度に複雑化することを避けるため、分類は適度な範囲に抑えることが望ましい。

ここでは例として、越境的データ移転の制御を対象に、データの性質によるリスク評価を三分類（高リスクデータ・中リスクデータ・低リスクデータ）、データの利用文脈によるリスク評価も三分類（高リスク文脈・中リスク文脈・低リスク文脈）とする。この二軸を交差させてマトリックス化すると、九つのセルが形成される（表 14-1 参照）。各セルに該当する具体的状況に応じて、要求される保護措置の強度が段階的に設定されるものとする（後記(2)参照）。

【表 14-1：CRDM モデルにおける越境的データ移転制御リスク評価マトリックス（例）】

データの性質（行）／ 利用文脈（列）	高リスク文脈	中リスク文脈	低リスク文脈
高リスクデータ			
中リスクデータ			
低リスクデータ			

(1)　三つの保護措置

次に、各セルに適用すべき保護措置の強度を検討する。ここでは一例として、三段階の強度を用いる。保護措置は、説明義務、安全性確保義務および監督義務の三つであり、説明義務は透明性の確保を通じた予見可能性の担保を目的とし、安全性確保義務は技術的・組織的措置による実体的保護を目的とし、監督義務は独立した外部統制および救済手続の確保を通じた制度的信頼の担保を目的とする。これら三つの義務は相互に補完的かつ累積的に適用される。

各措置についてそれぞれ三段階の強度（A：最大、B：中間、C：最小）を割り当てる。A は高リスク状況に対応する最大限の制度的統制を意味し、B は通常のリスク状況に対応する標準的統制、C は低リスク状況に対応する基本的統制を意味する。各保護措置の内容は、以下のとおりである。

ア　説明義務

説明義務とは、移転主体が、当該データの性質、処理目的、処理経路、受領主体が講じる安全措置、ガバメントアクセスの可能性、監督・救済手続、データ保持期間その他の関連情報を、移転の前後を通じて明確かつ容易に理解できる形式で提示する義務である。この義務は、移転

プロセス全体の可視性を確保するとともに、受領国における制度的信頼性の評価を可能にすることで、越境的データ移転の正当性と予見可能性を担保するものである。説明義務における三段階の強度は表 14-2 のとおりである。なお、具体的措置の内容は、附属書又はガイドラインにおいて定めることを前提とする。

【表 14-2：説明義務における三段階の強度の措置内容】

説明義務における三段階の強度の措置内容
A（最大） 移転主体は、移転の前後を通じて、当該データの性質、利用目的、処理経路、受領主体が講じる安全措置、ガバメントアクセスの可能性、監督・救済手続、データ保持期間その他の関連情報を網羅的かつ詳細に記載した包括的移転情報報告書を作成し、関係当局及び関係主体に対し事前に提供しなければならない。また、移転後の状況を定期的に更新し、変更点を速やかに通知しなければならない。具体的措置の内容は、附属書又はガイドラインにおいて定める。
B（中間） 移転主体は、データの性質、利用目的、受領主体が講じる主要な安全措置、ガバメントアクセスの可能性、監督・救済手続に関する基本情報その他の関連情報を、関係当局及び関係主体に対し移転前に文書で提示し、移転後に重要な変更が生じた場合にはこれを通知しなければならない。具体的措置の内容は、附属書又はガイドラインにおいて定める。
C（最小） 移転主体は、データの性質、利用目的、受領主体の属性及び基本的な安全措置に関する情報を、基本的かつ合理的な範囲で提供しなければならない。具体的措置の内容は、附属書又はガイドラインにおいて定める。

イ　安全性確保義務

安全性確保義務とは、移転主体および受領主体が、当該データの性質および利用文脈に照らして、技術的・組織的安全措置を講じ、無権限アクセス、漏えい、改ざん、目的外利用その他の侵害のリスクからデータを保護する義務である。この義務には、暗号化、アクセス管理、監査ログ、データ分離、機微データの追加的保護措置など、リスク水準に応じた複層的セーフガードの実施が含まれ、移転後の継続的な安全性維持を含めた全期間を対象とする。安全性確保義務における三段階の強度は表 14-3 のとおりである。なお、具体的措置の内容は、附属書又はガイドラインにおいて定めることを前提とする。

【表 14-3：安全性確保義務における三段階の強度の措置内容】

安全性確保義務における三段階の強度の措置内容
A（最大） 移転主体及び受領主体は、当該データの性質及び利用文脈に照らし、無権限アクセス、漏えい、改ざん、目的外利用その他の侵害を防止するため、合理的に利用可能な最高水準の技術的・組織的

安全措置を講じなければならない。合理的に利用可能な最高水準とは、当該時点の技術水準、実装可能性、コスト、侵害リスクの重大性等を総合考慮して判断される。これらの措置は、リスク評価に基づき体系的に設計され、安全性を確保するために必要と認められる範囲で継続的に維持及び更新されなければならない。具体的措置の内容は、附属書又はガイドラインにおいて定める。

B（中間）

移転主体及び受領主体は、当該データの性質及び利用文脈に照らし、無権限アクセス、漏えい、改ざん、目的外利用その他の侵害を防止するため、標準的な技術的・組織的安全措置を講じるとともに、定期的なリスク評価に基づき必要な追加措置を導入するものとする。具体的措置の内容は、附属書又はガイドラインにおいて定める。

C（最小）

移転主体及び受領主体は、当該データの性質及び利用文脈に照らし、無権限アクセス、漏えい、改ざん、目的外利用その他の侵害を防止するため、基本的かつ合理的な技術的・組織的安全措置を講じるものとする。具体的措置の内容は、附属書又はガイドラインにおいて定める。

ウ　監督義務

監督義務とは、移転主体および受領主体が、越境的データ移転に関連する監督・検証・救済の手続を整備し、移転の適法性や安全性に疑義が生じた場合に、独立した監督機関による審査、苦情処理、是正命令、救済措置などを通じて適切かつ迅速に対応する義務である。この義務は、制度的説明責任を担保し、移転主体・受領主体の遵守状況を外部的に確認可能とすることで、越境的データ移転の信頼性を確保する役割を果たす。監督義務における三段階の強度は表 14-4 のとおりである。なお、具体的措置の内容は、附属書又はガイドラインにおいて定めることを前提とする。

【表 14-4：監督義務における三段階の強度の措置内容】

監督義務における三段階の強度の措置内容

A（最大）

移転主体及び受領主体は、移転プロセス全体について独立した監督機関による継続的審査を受け、苦情処理、異議申立て、是正命令の履行、迅速な救済措置を確保しなければならない。独立した監督機関とは、組織的・機能的・財政的独立性を備え、移転主体および受領主体から実質的に影響を受けない機関をいう。また、自主監督体制を整備し、第三者認証取得及び年次報告を実施しなければならない。具体的措置の内容は、附属書又はガイドラインにおいて定める。

B（中間）

移転主体及び受領主体は、監督機関による審査・照会に誠実に協力し、苦情処理、異議申立て、是正命令の履行、迅速な救済措置を確保しなければならない。監督機関による審査は、当該データの性質及び利用文脈に照らして合理的に必要と認められる頻度及び範囲で実施されるものとする。具体的措置の内容は、附属書又はガイドラインにおいて定める。

C（最小）

移転主体及び受領主体は、監督機関が必要と認める範囲で情報を提供し、基本的な苦情処理、異議申立て、是正命令の履行、迅速な救済措置を確保する。ただし、定期的監査や年次報告は任意に実施するものとする。具体的措置の内容は、附属書又はガイドラインにおいて定める。

(2)　リスク評価別保護措置の強度に関するマトリックス

説明義務、安全性確保義務および監督義務の三つの保護措置にはそれぞれ三段階の強度を割り当てており、たとえば、三つの保護措置とも最大の強度が要求される場合は「AAA」と表記し、三つの保護措置とも最小の強度で足りる場合は「CCC」と表記する。いずれのリスク区分においても、三つの義務は最低限 C 水準以上で適用されるものとする。

説明義務については、利用文脈に基づくリスクに沿って強度が決まり、高リスク文脈については A（最大）の強度の保護措置、中リスク文脈については B（中間）の強度の保護措置、低リスク文脈については C（最小）の強度の保護措置が求められる。

安全性確保義務については、データの性質に基づくリスクに沿って強度が決まり、高リスクデータについては A（最大）の強度の保護措置、中リスクデータについては B（中間）の強度の保護措置、低リスクデータについては C（最小）の強度の保護措置が求められる。

監督義務の強度は、説明義務及び安全性確保義務のいずれか高い水準に一致するものとする。すなわち、説明義務または安全性確保義務について A（最大）の強度の保護措置が求められる場合には、監督義務については A（最大）の強度の保護措置が必要となる。また、説明義務または安全性確保義務について B（中間）の強度の保護措置が求められる場合には、監督義務については B（中間）の強度の保護措置が必要となる。さらに、説明義務および安全性確保義務について C（最小）の強度の保護措置で足りる場合には、監督義務も C（最小）の強度の保護措置で足りることになる。

以上により、リスク評価の交差を示す九つのセルに対応して、三つの保護措置の強度の組合せを示すと、表 14-5 のとおりとなる。

【表 14-5：CRDM モデルにおける越境的データ移転制御のリスク評価別保護措置の強度（例）】

データの性質（行）／利用文脈（列）	高リスク文脈	中リスク文脈	低リスク文脈
高リスクデータ	AAA	BAA	CAA
中リスクデータ	ABA	BBB	CBB
低リスクデータ	ACA	BCB	CCC

表 14-5 では、タテ軸（データの性質）とヨコ軸（利用文脈）の双方をそれぞれ三段階（高・中・低）で分類している。この二つの軸のいずれかが一段階でも低くなると、いずれかの保護措置の強度が減じられるという構造をとるため、次の特徴がある。すなわち、マトリックスの左上セル（高

リスクデータ　×　高リスク文脈）に対応する保護措置の強度の組合せは「AAA」となり、中央のセル（中リスクデータ　×　中リスク文脈）に対応する保護措置の強度の組合せは「BBB」となり、右下セル（低リスクデータ　×　低リスク文脈）に対応する保護措置の強度の組合せは「CCC」となる。その他のセルについては、いずれも下方または右方のセルに移動すれば、対応する保護措置の強度はいずれかの保護措置について減少する。また、CRDM モデルでは、保護措置の強度は最小化原則に基づき、目的達成に必要最小限の範囲に限定されるため、低リスク領域に過剰な義務を課すことは制度的に排除される。このように、マトリックスを下方向または右方向へ移動するにつれて保護措置の強度が段階的に減じられ、右下の「低リスクデータ　×　低リスク文脈」のセルでは、保護措置の強度が「CCC」となり、最小の保護措置セットに限定される。

たとえば、高リスクデータ（例：センシティブな個人データ）を高リスク文脈（例：公的機関による人物評価）の目的で越境移転する場合、マトリックスは左上の「AAA」のセットに該当し、いずれの保護措置についても最大の強度が求められる。すなわち、「AAA」の強度の保護措置が確保されない場合には越境的データ移転の禁止が制度的に許容される。他方、低リスクデータ（例：公開されている個人データ）を低リスク文脈（例：匿名化される統計利用）の目的で越境移転する場合、マトリックスは右下の「CCC」のセットに該当し、いずれの保護措置についても最小の強度で足り、これ以上の強度の保護措置を要求することは認められない。すなわち、最小限の保護措置による（最も自由な）越境的データ移転が認められなければならない。

(3)　データ主体の同意の取扱い

CRDM モデルにおいては、データ主体の同意は、越境的データ移転の可否を形式的に決定する独立の要件として位置づけられるものではない。同意の存在は、それ自体として保護措置の強度を減少させる効果を有しない。すなわち、同意は、移転の適法性を直接決定する要件ではなく、利用文脈のリスク評価に影響を及ぼし得る補助的評価要素として位置づけられる。その理由は、同意が存在するか否かは、当該移転に伴う実質的リスクの程度を直接的に示す指標とはならず、同意が取得されていても、利用文脈や権力関係、ガバメントアクセスの可能性といった構造的要因により、データ主体の権利侵害リスクが依然として高い場合が少なくないためである。むしろ、同意は、文脈的リスク評価において考慮され得る一要素として機能し、その存在や内容が、当該利用文脈のリスク水準や、説明義務・監督義務の強度に影響を及ぼし得ることになる。これは、規制強度を実質的リスクの程度にのみ連動させるという CRDM モデルの基本原理に基づくものである。この点で、CRDM モデルは、同意の有無をもって移転を一律に許容または禁止する従来型の形式的枠組みから距離を置き、実質的リスクに着目した評価構造を採用している。同意が存在する場合であっても、それが自由意思に基づくものであるか、利用目的が具体的かつ限定されているか、撤回可能性が確保されているか、国家権力や経済的優越関係が介在していないかといった要素を総合的に検討しなければ、当該利用文脈のリスクが低減されたとは評価されない。特に、法執行、行政サービス、雇用関係など、構造的な権力関係が存在する文脈においては、形式的な同意があっても高リスク文脈に該当し得る。このため、同意の存在のみをもって、説明義務や監督義務を軽減することは、CRDM モデルの下では正当化されない。

このような同意の評価は、各国の法文化や制度設計によって大きく異なり得るため、その具体的要件や評価基準を附属書において一律に条文化することは適切ではない。附属書は、あくまでデータの性質と利用文脈に基づくリスク分類、三義務の強度配分、過剰規制の排除といった共通かつ拘束的な枠組みを示す役割を担うべきであり、同意については、利用文脈のリスク評価において考慮され得る要素の一つとして位置づけるにとどめるのが相当である。

これに対し、同意の具体的取扱いは、ガイドラインにおいて詳細に定められるべき事項である。ガイドラインでは、同意がリスク低減要素として評価され得る場合とそうでない場合の判断基準、同意が説明義務の内容や深度にどのように反映されるか、監督機関が同意の実質的有効性をどのように検証するかといった運用上の指針を柔軟に示すことが可能となる。すなわち、附属書は規制構造を固定し、ガイドラインは評価方法を適応的に更新する役割を担う。この二層構造により、CRDM モデルは、国際的相互運用性と制度的安定性を確保しつつ、各国の制度的多様性や将来的な実務変化にも対応し得る枠組みを維持することができる。

(4)　条文化（例）

表 15 では、リスク評価別保護措置の強度に関するマトリックス（表 14-5 参照）について条文化した例を「附属書 X」として示す。この附属書は、越境的データ移転に関する国際協定において定めることが想定される。

【表 15：附属書 X（越境的データ移転における保護措置）】

附属書 X（越境的データ移転における保護措置）

第 1 条（目的）

1　本附属書は、越境的データ移転に関し、データの性質及び利用文脈に応じて必要となる移転条件及び保護措置の強度を、文脈的リスク評価に基づき段階的に設定するための基準を定める。

2　本附属書は、各締約国が自国制度の下で本モデルを実施する際の共通基準を明確化することを目的とする。

第 2 条（定義）

本附属書において、次の用語は、それぞれ以下のとおり定義する。

1 「データの性質」とは、移転対象となるデータが有する機微性、秘匿性、個人・組織への潜在的影響度その他の固有特性をいう。

2 「利用文脈」とは、データが利用される制度的・技術的・運用的環境をいい、当該利用における権力関係、目的の正当性及び限定性、関係主体の関与の在り方その他当該利用に伴う実質的リスクに影響を及ぼす要素を含むものとする。

3 「文脈的リスク評価」とは、越境的データ移転に伴うリスクを、移転対象となるデータの性質及び利用文脈を総合的に考慮して評価し、その評価結果に応じて、説明義務、安全性確保義務及び監督義務の強度を段階的に決定する評価手法をいう。

4 「保護措置」とは、説明義務、安全性確保義務又は監督義務の総称をいう。

5 「説明義務」とは、移転に関する情報提供及び透明性確保のための保護措置をいう。

6 「安全性確保義務」とは、移転に関する技術的・組織的安全性確保のための保護措置をいう。

7 「監督義務」とは、監督機関による検証、監査、是正措置に関する保護措置をいう。

8　保護措置の強度「A」とは、合理的に可能な最高水準の保護措置の強度をいう。

9　保護措置の強度「B」とは、標準的な頻度及び範囲の保護措置の強度をいう。

10　保護措置の強度「C」とは、必要最小限の合理的水準の保護措置の強度をいう。

第 3 条（リスク分類）

1　データの性質及び利用文脈は、それぞれ「高」「中」又は「低」の三段階に分類する。

2　保護措置の強度（A、B 又は C）は、それぞれの保護措置について、データの性質と利用文脈の組合せによって決定される。

3　保護措置の強度の決定は、別表に定めるマトリックス（高・中・低 × 高・中・低）に従う。

4　データ主体の同意の有無又はその取得形式は、前各項に基づくリスク分類を自動的に変更するものとはならない。

第 4 条（保護措置の強度の割当て）

1　各セル（データの性質 × 利用文脈）の位置に応じて、保護措置の強度の組合せ（AAA から CCC まで）を割り当てる。

2　左上セル（高リスクデータ × 高リスク文脈）は AAA とし、右下セル（低リスクデータ × 低リスク文脈）は CCC とする。

3　各保護措置の強度（A、B 又は C）内容は、次のとおりとする。

（1）説明義務「A」：包括的移転情報報告書の作成・事前提供・定期更新及び即時通知

（2）説明義務「B」：標準的範囲での合理的情報提供・更新

（3）説明義務「C」：最低限必要な情報提供

（4）安全性確保義務「A」：最高水準の技術的・組織的措置の導入及び継続的更新

（5）安全性確保義務「B」：標準的水準の技術的・組織的措置

（6）安全性確保義務「C」：最小限必要な技術的・組織的措置

（7）監督義務「A」：独立監督機関による継続的審査、第三者認証及び定期報告

（8）監督義務「B」：標準的頻度・範囲の監査及び報告

（9）監督義務「C」：最小限必要な監督措置

4　前各項に基づき割り当てられた保護措置の強度は、データ主体の同意の存在のみを理由として軽減されるものではない。

第 5 条（措置の適用）

1　締約国は、別表に基づき、当該移転が位置づけられるセルの保護措置の強度（ABC の組合せ）を適用するものとする。

2　本附属書の保護措置は、締約国が国内法制の下で同等の保護水準を確保する形で実施されることを妨げない。

3　締約国は、越境的データ移転に関し、本附属書に定める保護措置の強度に照らして過剰な条件を付してはならない。

4　締約国は、越境的データ移転に関し、当該データの移転主体又は受領主体が講じる保護措置が本附属書に定める保護措置の強度に満たないと認めるときは、当該越境的データ移転を禁止することができる。

第 6 条（透明性及び監督）

1　締約国は、保護措置の履行状況に関する透明性を確保し、必要に応じて情報共有を行う。

2　監督機関は、保護措置の適切な履行を確保するため、必要な検証及び是正措置を実施することができる。

第 7 条（ガイドライン）

本附属書に定める越境的データ移転制御のリスク評価別保護措置の実施に関する細則及び技術的事項（データ主体の関与の在り方に関する評価指針を含む。）は、ガイドラインで定める。

第 8 条（見直し）

本附属書は、技術的・制度的状況の変化に応じ、締約国会合の合意により見直すことができる。

別表（リスク評価マトリックス）

行は、データの性質に基づくリスク評価、列はデータの利用文脈に基づくリスク評価を示す。また、各セルの保護措置の強度の組合せは、説明義務・安全性確保義務・監督義務の組合せを示す。

	高リスク文脈	中リスク文脈	低リスク文脈
高リスクデータ	AAA	BAA	CAA
中リスクデータ	ABA	BBB	CBB
低リスクデータ	ACA	BCB	CCC

第 10 章

有志国連携による規範再構成と「トウキョウ効果」の展開

第 10 章　有志国連携による規範再構成と「トウキョウ効果」の展開

国際的データガバナンスの現状を踏まえると、現在進行中の趨勢として、また今後さらに深化し得る現実的シナリオとして、国際的データガバナンスのブロック化が想定される。すなわち、米国、EU、中国を中心とする三つの制度的ブロックが、それぞれ異質な法的・技術的・価値的枠組みを形成するとともに、各ブロックでは一定程度の相互接続性を保ちながらも、外部との連携が選択的・条件的に行われる構造が固定化し、制度的分断が進行する可能性がある。このような分断が深まれば、サイバー空間の統合性は大きく損なわれ、国際通信インフラ、デジタルサービスの相互接続、技術標準の整合性といった基盤領域において断片化の危険が高まる。その結果、国境を越えるデータ流通の可用性や信頼性が低下し、世界的なデジタルエコシステムの分裂という深刻な事態が生じ得る[108]。

サイバー空間の分裂は、技術的問題にとどまらず、国際経済秩序、民主的統治、基本的人権、国家安全保障など、多層的領域に直接的な影響を及ぼす[109]。大国が自らの規範を外部に投射しようとする構造が強まれば、制度的相互運用性は一層低下し、国際協調の余地はますます狭められる[110]。このような構造的危機を回避するには、従来の多国間制度が前提としてきた自由化・均衡化・相互互恵といった理念のみでは不十分であり、多元的ブロックの境界を調整し得る新たな規範基盤を設計することが不可欠である[111]。

以上を背景として、本章では、まず第 1 節で現実的シナリオとしての国際的データガバナンスのブロック化の進行について整理し、第 2 節で従来の多国間フォーラムに代わる新たな国際フォーラムの必要性と課題を論じる。そのうえで第 3 節において、有志国連携を中核とする制度的アプローチと、再構成された越境的データガバナンス規範の国際標準化に向けた戦略として「トウキョウ効果（Tokyo Effect）」の展開可能性を検討し、第 4 節で越境的データガバナンス規範再構成のロードマップを提示する。有志国連携によって越境的データガバナンス規範を再構成し、日本の主導の下で当該規範が国際的受容性を高め、大国の参加をも促すことで、やがて国際標準へと収斂していく動態は、協調的な規範波及の仕組みとして「トウキョウ効果」と位置づけられる。このアプローチは、特定国の価値体系による規範投射ではなく、多様な制度的ブロックを媒介し、信頼に基づく調整可能性を確保する点において独自の意義を有する。

[108] Burri (2017), pp. 93–99, 126–132; Aaronson and Leblond (2018), pp. 245–257, 259–263; UNCTAD (2021), pp. 100–111, 114–116, 174–176.
[109] Aaronson and Leblond (2018), pp. 245–263. UNCTAD (2021), pp. 43–46, 86–88, 100–111, 114–116.
[110] Burri (2017), pp. 93–105, 126–132; Aaronson and Leblond (2018), pp. 245–263.
[111] Burri (2017), pp. 93–99, 126–132; Aaronson and Leblond (2018), pp. 245–263; UNCTAD (2021), pp. 114–116, 174–176; Christakis (2024a), pp. 24–76.

第 1 節　現実的シナリオ（国際的データガバナンスのブロック化の進行）

現在の国際的データガバナンスを取り巻く環境は、米国、EU、中国を中心とする複数の制度的ブロックが並立し、それぞれの制度構造が固定化しつつある点に特徴がある（前記第 1 章第 3 節参照）。この制度的硬直は、国際的データガバナンスが複数の制度的ブロックへと分裂し、相互調整の機能が著しく損なわれるという現実的シナリオの中核をなす。

ブロック化が深化した場合、最も懸念されるのはサイバー空間そのものの分裂である[112]。サイバー空間は、国際通信、経済活動、医療・学術研究、災害対応、民主的討議など、現代社会の基盤的機能を支える高度に相互依存的な仕組みによって構成されている。その統合性が失われれば、国境を越える社会的・経済的・技術的連携は断片化し、世界規模で蓄積されてきた知識循環の基盤が広範に劣化する。制度的ブロックごとの分裂は、技術的互換性の低下にとどまらず、通信インフラの分断、研究データの孤立、民主的プロセスの弱体化など、人類社会の持続に不可欠な領域に深刻な影響を及ぼし得る[113]。

この分裂が人類にとって危険と評価される理由は明確かつ深刻である。

第一に、ブロック間の相互信頼が喪失すれば、共同研究、医療データ共有、環境監視、証拠協力といった国際協調の前提条件が揺らぎ、地球規模課題に対処する能力が決定的に低下する[114]。

第二に、技術開発や標準形成がブロックごとに乖離することにより、環境問題や国際的疾病対策など、越境的な情報共有と協調対応を制度的前提とする領域では、深刻な機能的障害が生じる[115]。

第三に、各制度的ブロック内部でガバメントアクセスの強化や情報統制の制度化が進めば、データ主体の権利保障がブロック間で不均衡となり、国際的な権利保障水準の調和が大きく損なわれる[116]。

したがって、国際的データガバナンスのブロック化は、技術面・制度面の双方において回避すべきシナリオである。その防止のためには、ブロック間の対立構造を前提として分断を固定化するのではなく、制度的相互運用性と国際的信頼形成を再構築する新たな国際的枠組みを設計することが不可欠である[117]。

---

[112] UNIDIR (2023), pp. 2–4, 9–12; 実積寿也ほか (2023) 72–94 頁.
[113] UNCTAD (2021), pp. 114–116, 174–176; UNIDIR (2023), pp. 2–4, 9–12; 実積寿也ほか (2023) 72–94 頁.
[114] Aaronson and Leblond (2018), pp. 245–263; UNCTAD (2021), pp. 43–46, 81–84, 158–163, 174–176; UNIDIR (2023), pp. 9–12.
[115] UNCTAD (2021), pp. 114–116, 158–163; UNESCO (2023), pp. 20–27.
[116] UNCTAD (2021), pp. 69–71, 86–90, 114–116, 174–184, 189–190; United Nations Human Rights Council (2022), pp. 2–16; UNESCO (2023), pp. 20–27; Christakis (2024a), pp. 24–76.
[117] Burri (2017), pp. 93–99, 126–132; Aaronson and Leblond (2018), pp. 245–263; UNCTAD (2021), pp. 114–116, 174–176; UNESCO (2023), pp. 20–27; Christakis (2024a), pp. 24–76.

第 2 節　新たな国際フォーラムの必要性と課題

越境的データ移転は、市場アクセスや競争条件の調整に収斂できる領域ではなく、相手国の法制度、ガバメントアクセスの運用、監督体制の整備状況といった、国家内部の統治構造と密接に結びついた領域である。したがって、越境的データガバナンスにおいては、相手国制度の信頼性やリスク構造を個別に検証しなければならず、市場アクセス中心の貿易原則が前提とする共通の比較基盤を適用することが難しい（前記第 2 章第 2 節参照）。しかし、現行の国際フォーラムはいずれも制度差の調整機能を十分に備えておらず、越境的データガバナンスに固有の課題に対応し得る制度基盤とはなっていない。そのため、国家間の制度差を前提としつつ、相互の制度的信頼性を評価する仕組みを組み込んだ新たな規範構造が不可欠となる。

第 1 項　従来型の国際フォーラムの限界と新たな国際フォーラムの必要性

越境的データガバナンスは、電子商取引にとどまらず、プライバシー、基本的人権、国家安全保障、技術的互換性など、相互に緊張関係にある多元的価値の調整を要する高度に複雑な政策領域である[118]。急激な地政学的変動下にある現状を踏まえれば、WTO や地域貿易協定といった従来型の経済フォーラムの枠組みでは、こうした複合的課題に十分に対応できず、今後の越境的データガバナンスの規範再構成を担うには限界がある[119]。この点について、Burri（2017）は、データガバナンスの領域では従来の貿易法モデルでは扱い切れない多元的価値が交錯し、WTO や既存の地域協定が依拠してきた自由化と無差別原則だけでは制度的限界を克服できないと指摘している[120]。また、Aaronson and Leblond（2018）は、データが公共財的性質を有し、同時に国家安全保障および人権保障に直結するため、データに関する国際ルール形成は従来の貿易交渉の枠組みに収まらないとし、より包括的かつ中立的な制度的枠組みの必要性を論じている[121]。さらに、UNCTAD（2021）は、国際的データ流通が経済・社会的基盤と不可分に結びついた今日において、貿易協定中心の規律は制度的射程に限界があり、より広範なステークホルダーを含み得る新たな国際フォーラムの構築を推奨している[122]。

このように、より包括的かつ中立的な原則に基づく新たな国際フォーラムの構築が求められている。その役割は、既存の経済協定を補完するにとどまらず、国際的な規範競争において中立的な対話の場を提供することにある。このフォーラムでは、データを社会的信頼に支えられたデジタル公共財として位置づけ[123]、国際的な相互運用性を確保するため比例性、透明性、審査可能性の各原則を制度的枠組みの中核に据える必要がある。

その際、求められる国際フォーラムは、従来の貿易交渉を中心とする場ではなく、データガバナンスの多面的課題に対応する総合的な制度基盤を備えたものでなければならない[124]。越境

---

[118] UNCTAD (2021), pp. 43–46, 69–71, 89–90, 120–123, 174–176; 城山英明（2023）147–159 頁.
[119] 川瀬剛志（2015）10–16 頁; Burri (2017), pp. 87–99, 126–132; Aaronson and Leblond (2018), pp. 245–248, 253–258, 266–269; Irion et al. (2020), sections II–III.
[120] Burri（2017）, pp. 87–99, 126–132.
[121] Aaronson and Leblond （2018）, pp. 245–248, 253–258, 266–269.
[122] UNCTAD（2021）, pp. 174–176, 182–184.
[123] UNCTAD (2021), pp.174–176, 178–179; OECD (2022e), Principles I–II, V; Digital Public Goods Alliance (2023); Purtova and van Maanen (2024), pp. 8–17, 19–28, 33–38.
[124] Burri (2017), pp. 87–99, 126–132; Irion et al. (2020), sections II–III; UNCTAD (2021), pp. 174–176, 182–184.

的データ移転の問題は、貿易自由化に関わる市場アクセス論に還元できるものではなく、個人データ及びプライバシーの保護に関する人権法的規範、サイバーセキュリティ及び情報セキュリティに関する技術的規範、公共政策目的の実現に関わる規制政策、並びに国家安全保障に関する主権的規範という、複数の制度領域にまたがる課題を包含している[125]。これらを実質的に調整するには、複数の領域が交差する問題を扱い得る新しい国際フォーラムが必要となる[126]。このフォーラムは、リスク評価等の共通基準策定、データローカライゼーションやガバメントアクセス等の運用状況の把握、例外規定適用の審査、第三者監査、能力構築支援（capacity building）など、多角的な機能を併せ持つことによって、多様な国家の制度差を埋め、相互運用性を制度的に確保するための基盤となる[127]。多面的な制度調整機能を備えた場が形成されることにより、断片化が進む国際的データガバナンスの再接続が可能になり、越境的データ移転に内在する複合的なリスクと規範的課題に国際的に対応できる枠組みが生まれる[128]。

第 2 項　新たな国際フォーラムの課題と方向性

越境的データガバナンス規範再構成にあたっては、各国の制度的多様性を前提に、データの性質と利用文脈に基づくリスク評価に応じた比例的かつ柔軟な制度設計を通じて、透明性と相互運用性を制度的に担保する新たな国際枠組みを構築することが求められる[129]。しかし、そのような制度差を前提とした規範再構成には、いくつかの課題が存在する。

第一に、移転先の制度環境に依存して判断が変動するという構造が、国際的な一貫性や予見可能性を確保する際の障害となる。多様な制度を抱える国々の間で、どの程度の保護水準を国際的に共有し得るのか、また、その水準をどのように制度運用に反映させるのかという問題が浮上する。

第二に、国家安全保障、公安、刑事法執行などに関連するガバメントアクセスの制度運用は、公開される情報が限定される傾向があり、相手国制度への評価を困難にする。特にガバメントアクセスの仕組みは移転条件に大きな影響を与えることから、この不透明性をどのように補い、国際的な基準形成に接続するのかが重要となる。各国が独自に主張する公共政策例外や安全保障例外が広範化すれば、制度の断片化が進み、越境的な相互運用性が損なわれる危険が高まる。

第三に、制度差を前提とする評価は、制度的に脆弱な国を不利に扱う結果を招く可能性がある。監督機関の整備状況や法制度の成熟度が低い国は、国際的なデータ流通の枠組みから排除されやすく、国際的なデータ格差や能力格差が広がる懸念がある[130]。この問題に対応するた

---

[125] OECD (2013), Part Two-Part Four, Supplementary Explanatory Memorandum, p. 29; Burri (2017), pp. 87–99, 126–132; Aaronson and Leblond (2018), pp. 254–258; Irion et al. (2020), sections II–III; UNCTAD (2021), pp. 43–46, 69–71, 89–90, 120–123.

[126] Aaronson and Leblond (2018), pp. 245–266; UNCTAD (2021), pp. 174–176, 182–184.

[127] UNCTAD (2021), pp. 174–184, 189–190; OECD (2023a), pp. 15–30; Christakis (2024a), pp. 24–76.

[128] Burri (2017), pp. 93–99, 126–132; Aaronson and Leblond (2018), pp. 245–263; UNCTAD (2021), pp. 174–184; Christakis (2024a), pp. 24–76.

[129] UNCTAD (2021), pp. 174–184; OECD (2023a), pp. 15–30; Christakis (2024a), pp. 24–38, 42–56.

[130] Aaronson and Leblond (2018), pp. 254–261; UNCTAD (2021), pp. 114–116, 174–176.

めには、制度の成熟を待つのではなく、制度改善を支援する能力構築など、国際協力の仕組みを規範構造の一部として組み込む必要がある[131]。

このような課題を踏まえると、越境的データガバナンス規範再構成においては、各国の制度差を前提としながらも、制度的信頼、透明性、一貫性を制度要件として組み込み、国家間の制度調整を可能とする枠組みを構築する必要がある[132]。既存の貿易法モデルに依拠するだけでは、データ移転を取り巻く制度環境、ガバメントアクセス、監督体制、技術的安全性といった多領域にまたがる問題群を包括的に扱うことが難しい[133]。越境的データ移転に特有の制度構造を踏まえれば、法的規範と技術的評価を統合しつつ、各国の統治構造とデータ流通の調整を制度的に支える新たな枠組みの確立が中心的課題となる[134]。

以上に述べた課題は、制度差を前提とする越境的データガバナンス規範再構成が本質的に抱える限界を示すものではなく、適切な設計原理を備えた枠組みによって対応し得る課題であり、CRDM モデルはこれらの課題に対する体系的な解決可能性を内包している。

第一に、判断の変動性や予見可能性の低下という課題について、CRDM モデルは、データの性質および利用文脈という共通の評価軸に基づき、リスク水準と対応措置との関係を構造化することにより、各国の制度差を前提としつつも国際的に共有可能な判断枠組みを提供する。この構造により、個別判断の恣意性を抑制し、制度運用の透明性と一貫性を確保することが可能となる。

第二に、ガバメントアクセスをめぐる不透明性の問題についても、CRDM モデルは、当該制度の存否や内容そのものを一律に評価対象とするのではなく、アクセスの目的、範囲、統制手段といった文脈的要素をリスク評価の対象として位置づけることにより、制度比較を可能とする分析枠組みを提示する。この点で、CRDM モデルは、国家安全保障や公共政策に関する各国の主張を排除するのではなく、それらを相対化し、国際的に検証可能な形で制度調整を行うための基盤を提供する。

第三に、制度的に脆弱な国が不利に扱われるという包摂性の課題についても、CRDM モデルは、制度成熟度そのものを参加条件とするのではなく、必要最小限の措置水準を段階的に設定し、能力構築を通じて制度改善を支援する余地を組み込む設計を採用している。この段階的かつ支援型の構造は、制度格差を固定化するのではなく、長期的に縮減する方向へと誘導するものであり、包摂的な国際フォーラムの形成に資する。

以上のとおり、CRDM モデルは、制度差を前提とする越境的データガバナンス規範再構成が直面する主要な課題に対し、リスク評価、比例性、データ最小化を統合した設計原理として応答するものであり、新たな国際フォーラムの制度的中核として位置づけることができる。

越境的データガバナンスの分野では、大国間でデジタル主権や個人情報保護をめぐる規範的対立が先鋭化し、統一的な国際ルールの形成は停滞している。このような情勢の下、各大国が自国モデルの国際標準化を推進しており、異なる法体系の間で調整可能な共通原則の構築は一層困難となっている。したがって、越境的データガバナンス規範再構成にあたっては、規範

[131] Aaronson and Leblond (2018), pp. 253–262; UNCTAD (2021), pp. 174–184, 189–191; OECD (2023a), pp. 11–22.
[132] Burri (2017), pp. 93–99, 126–132; UNCTAD (2021), pp. 174–184; OECD (2023a), pp. 15–30; Christakis (2024b), pp. 96–113.
[133] Burri (2017), pp. 87–99, 126–132; Irion et al. (2020), sections II–III; Christakis (2024a), pp. 24–76.
[134] Burri (2017), pp. 87–99, 126–132; Chin and Zhao (2022), section 6; UNCTAD (2021), pp. 174–184.

的対立を先鋭化させている大国の制度的関与を初期段階では想定せず、志を同じくする中堅国や新興国が連携して制度間の調整可能性を高め得る共通基盤を形成することにより、国際的に受容可能な共通原則の策定を促進することが重要となる[135]。ここでは、DFFT を指導理念としつつ、共通の問題意識と制度構築への志向性を共有する有志国連携を基盤とすることで、特定の大国や制度的ブロックの価値観に依拠せず、相互運用性と実効性を兼ね備えた柔軟な規範の形成が可能となる[136]。

第 3 項　実効的な紛争処理制度の必要性

新たな国際的データガバナンスにおいては、制度的信頼、透明性、一貫性を制度要件として組み込み、国家間の制度調整を可能とする枠組みの構築が不可欠となる。そのためには、実効的な紛争処理制度を義務的制度として枠組み全体に実装することが必須となる。CRDM モデルは、越境的データ移転に関して、データの性質と利用文脈のリスク評価に応じて移転条件を段階的に設定する制度設計であり、柔軟かつ合理的な越境的データガバナンスの実現を志向するものである。しかし、たとえこのような制度設計が国際協定として明文化されたとしても、実際の移転は関係国の国内制度に基づいて実施される。そのため、各国が協定上の原則や例外規定を自国の判断で一方的に解釈・適用すれば、CRDM モデルに基づく調和的な運用は損なわれかねない。こうした事態を回避し、その実効性を担保するには、共通の評価基準を備えた中立的な運用機関の整備が不可欠である。たとえば、ある国が越境的データ移転を制限した場合、他国はその措置が協定上の原則に照らして過剰であると主張し、公共政策例外や安全保障例外といった根拠が実際のリスクに比して均衡を欠くことを論証できるようにすることが制度的に重要である[137]。制度への信頼を確立するには、リスク分類や移転条件の整備と並行して、客観的かつ第三者的な判断を求めることができる手続的保障が不可欠であり、実効性のある紛争処理制度を構築しなければならない[138]。

したがって、越境的データガバナンスにおける紛争処理制度は、各国の国内制度に委ねられるべきではなく、協定に基づいて設置される中立的かつ独立した国際的機関によって担われる必要がある[139]。この点について、Kuner（2017a）は、データ移転に関する各国の国内判断に依拠するモデルでは、国際的制度調和を確保できず、透明性・予見可能性を担保するには国際的な制度的一貫性を確保する枠組みが必要であると指摘している[140]。また、Chaisse（2024）は、越境的データ保護紛争は複数の法域にまたがり、国内制度のみでは中立的かつ実効的な解決が困難であることから、国家の枠組みを超えた独立した第三者的紛争解決メカニズムの整備が不可欠であると論じている[141]。さらに、Dimitropoulos et al.（2025）は、プルリラテラルな国際協力制度

[135] Aaronson and Leblond (2018), pp. 245–263; UNCTAD (2021), pp. 174–184, 189–191; Christakis (2024a), pp. 39–56; Dimitropoulos et al. (2025), pp. 19–26.
[136] Hoekman and Sabel (2021), pp. 50–58; Bacchus et al. (2024), pp. 3–9; Dimitropoulos et al. (2025), pp. 2–7, 19–25.
[137] Hoekman and Sabel (2021), pp. 50–58; UNCTAD (2021), pp. 111–116, 174–176; Christakis (2024a), pp. 15–28, 39–56.
[138] Bacchus et al. (2024), pp. 3–9; Dimitropoulos et al. (2025), pp. 7–15, 19–25.
[139] Alford (2011), pp. 702–725, 741–749; Hoekman and Sabel (2021), pp. 50–58; Chaisse (2024), pp. 535–545; Dimitropoulos et al. (2025), pp. 7–15, 19–25.
[140] Kuner (2017a), pp. 886–895, 899–909.
[141] Chaisse (2024), pp. 535–545.

の実効性は、履行確保と制度的信頼を支える紛争処理メカニズムに依拠しており、第三者的審査を伴う制度的枠組みがなければ安定的な国際的協調は維持できないと指摘している[142]。

越境的データガバナンス規範再構成にあたっては、規範的原則やガイドラインの策定にとどまらず、異議申立て、調停、是正、救済といった手続を備えた国際的な第三者機関を制度化することが、協定の一貫性を担保し、各国による一方的な解釈・適用を防止するための中核的仕組みとなる。このような枠組みは、特定国による一方的な解釈・適用を制度的に抑制し、相互主義に基づく透明で予見可能なデータガバナンスを支える制度的基盤となる[143]。例外規定に対する規範的拘束力の制度化と、異議申立て・調停・救済などを含む第三者的紛争処理制度の整備は、一国主義的措置の拡散を抑制し、法の支配と中立性に基づく国際的枠組みの確立を可能にする制度的条件となる[144]。

[142] Dimitropoulos et al. (2025), pp. 7–15, 19–25.
[143] Bacchus et al. (2024), pp. 3–9.
[144] Slaughter (2000), pp. 1104–1123; UNCTAD (2021), pp. 111–116, 174–176; Dimitropoulos et al. (2025), pp. 7–15, 19–25.

第 3 節　有志国連携と「トウキョウ効果」の展開

志を同じくする中堅国や新興国が連携する有志国連携は、国際的データガバナンスの枠組み形成において極めて重要な戦略的要素となる[145]。

第一に、越境的データ移転における許容条件や例外規定の客観的適用基準を共通原則として策定するに際し、大国の一国主義的な影響を抑制することで、公平で予見可能な規律モデルを構築できる。また、有志国間の合意（プルリラテラル協定）は、自己判断的な例外規定の適用が非大国にまで拡大することを制度面から抑止し、国際的分断の回避に資する[146]。

第二に、例外規定の適用可否を含む解釈・運用上の争点を紛争処理制度の対象とすることで、異なる法制度間においても信頼を基盤とした相互運用性を確保できる[147]。

第三に、新たな規律モデルの策定後は、オープンエンド型の構成とすることで大国の参加にも門戸を開き、包摂性と一貫性を備えた国際秩序としての正統性を確立できる[148]。

このような枠組みは、自己判断的な例外規定の濫用を抑止し、共通基準に基づく安定的な運用を実現する基盤となる。有志国連携による多国間フォーラムの創設は、越境的データガバナンス規範再構成に向けた制度設計上の要請であると同時に、国際秩序の再構築を見据えた戦略的課題でもある。有志国連携が信頼性・実効性・相互運用性を中核原理として国際的規範形成を主導することにより、大国主導の規範支配を是正し、深まりつつある規範的分断を克服するための国際秩序の新たな方向性を提示し得る[149]。

歴史的にも、非大国が主導して提起した規範が、国連などの多国間交渉を経て最終的に大国を取り込み、国際的合意として定着した例が見られる。このような現象は「下からの規範形成（bottom-up norm-building）」と呼ばれ[150]、①非大国による問題提起、②国連等での制度化に向けた集団交渉、③大国による最終的受容、という三段階の過程を経て国際規範として確立される特徴を持つ（表 16 参照）。たとえば、1982 年の国連海洋法条約（UNCLOS）では、排他的経済水域（EEZ）の概念が小島嶼国や沿岸発展途上国の要請によって国際議題化され、第三次国連海洋法会議での大規模な交渉を経て制度化され、最終的に米国・ソ連・日本も受け入れた[151]。また、1992 年のリオ地球サミットで採択された「共通だが差異ある責任（Common But Differentiated Responsibilities: CBDR）」原則は、途上国グループ（G77 + 中国等）の主張を基礎として形成され、京都議定書およびパリ協定において国際制度として定着した[152]。さらに、持続

---

145 Hoekman and Sabel (2021), pp. 50–58; Dimitropoulos et al. (2025), pp. 2–7, 19–25.

146 Alford (2011), pp. 702–706, 725–749; Burri (2017), pp. 87–99, 126–132; Hoekman and Sabel (2021), pp. 50–58; Dimitropoulos et al. (2025), pp. 2–7, 19–25.

147 Slaughter (2000), pp. 1104–1123; Alford (2011), pp. 702–706, 725–749; Dimitropoulos et al. (2025), pp. 2–7, 19–25.

148 Burri (2017), pp. 87–99, 126–132; Hoekman and Sabel (2021), pp. 50–58; Dimitropoulos et al. (2025), pp. 7–15, 19–25.

149 Alford (2011), pp. 702–706, 725–749; Burri (2017), pp. 87–99, 126–132; Hoekman and Sabel (2021), pp. 50–58; Dimitropoulos et al. (2025), pp. 2–7, 19–25.

150 Finnemore and Sikkink (1998), pp. 895–905.

151 Koh (1982); Oxman (1994), pp. 353–366; Lewis (2025), pp. 3–7, 15–19.

152 Rio Declaration on Environment and Development, princ. 7, UN Conference on Environment and Development, A/CONF.151/26/Vol. I, June 14, 1992. https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf; Harris (1999), pp. 27–42; Kyoto Protocol to the United Nations Framework Convention on Climate Change, Dec. 11, 1997, 2303 UNTS 148, arts. 3, 10. https://unfccc.int/resource/docs/convkp/kpeng.pdf; Paris

可能な開発目標（SDGs）は、コロンビアやグアテマラを中心とする途上国の提案に端を発し、オープン・ワーキング・グループで非大国が積極的に議題設定を主導し、最終的に 193 か国の支持を得て国際的政策枠組みとして採択されたものである[153]。

【表 16：「下からの規範形成（bottom-up norm-building）」の例】

「下からの規範形成（bottom-up norm-building）」の例

1982 年国連海洋法条約（UNCLOS）における EEZ 導入の経緯

排他的経済水域（EEZ）は、小島嶼国や沿岸発展途上国が主導した「下からの規範形成」の代表例であり、現在の国際海洋秩序の中核概念である。UNCLOS 以前の伝統的海洋法は領海 12 海里を超える海域を公海として自由利用とし、先進海洋国のみが遠洋漁業や資源利用の利益を享受する構造で、発展途上国は自国周辺資源の活用が困難であった。

1970 年代、カリブ海・中南米・アフリカ・太平洋の島嶼国や沿岸発展途上国は、この不平等状態に対する危機感から、自国沿岸から 200 海里までの資源に主権的権利を認める制度を求め始めた。中南米諸国が早期に宣言していた「200 海里主権宣言」がその中心的な先例となり、G77 全体の要請として国際的議論に発展した。

1973 年開始の第三次国連海洋法会議では、先進海洋国が公海自由の制限に慎重姿勢を示す一方、発展途上国は資源利用の公平性を強く主張し、EEZ 創設を中心に大規模な集団交渉が行われた。交渉の結果、沿岸国が 200 海里以内の天然資源に主権的権利を持つ一方、航行の自由など公海原則も維持する折衷案が形成され、EEZ が国際制度として採用された。

当初は抵抗していた米国・ソ連・日本などの大国も、航行の自由が確保されること、発展途上国の集団的要求が国際的に広く支持されたことなどを背景に最終的に受容した。こうして EEZ は、発展途上国が提唱した規範が大国を巻き込みながら定着した典型例として、1982 年 UNCLOS において正式に国際法化された。

CBDR（共通だが差異ある責任）原則の形成と国際的定着の経緯

CBDR（共通だが差異ある責任）原則は、1992 年リオ地球サミットを契機に国際的に確立したものであり、発展途上国が主導して形成した規範が先進国に受容された典型例である。背景には、温室効果ガス排出の歴史的責任の大部分が先進国にあること、途上国には経済発展という優先課題があることなど、構造的不平等に対する強い問題意識があった。途上国グループ（G77＋中国、インド、ブラジル等）は、環境保全がすべての国に共通する課題である一方、負担の程度は各国の能力や歴史的排出に応じて差異化されるべきと主張した。

1992 年リオ宣言原則7は、この途上国側の立場を正式に国際原則として採択した最初の文書であり、CBDR の国際的承認を示す象徴的な転機となった。続く 1997 年京都議定書では、先進国のみに法的拘束力を伴う削減義務を課し、途上国には義務を課さないという形で、CBDR が具体的に制度化された。これは差異化された責任を明確に反映した最も典型的な適用例である。

Agreement, Dec. 12, 2015, art. 2(2), T.I.A.S. No. 16-1104.
https://unfccc.int/sites/default/files/english_paris_agreement.pdf.

[153] United Nations (2012), paras. 245-251; United Nations (2014), paras. 1-4 and Annex (Membership of the Open Working Group); United Nations General Assembly (2015), paras. 1-5, 53-59.

2015 年パリ協定においても CBDR は維持されたが、運用はより柔軟になり、すべての国が排出削減目標を提出しつつ、各国の能力や事情に応じて貢献水準を決めるという形式へ発展した。これにより、CBDR は途上国の主張に基づく規範から、国際社会全体に共有される包括的原則へと再構築された。

この形成・受容の過程は、非大国が主導して提起した規範が、大国の同意を得て普遍的な国際基準へと昇華した事例であり、ボトムアップ型の規範形成が実際に国際秩序を動かし得ることを示す代表例である。

SDGs（持続可能な開発目標）形成の経緯

SDGs は、非大国の開発課題を国際基準へと昇華させた典型例である。その形成の端緒は、2000 年の MDGs が先進国主導で策定され、途上国の政策優先順位や持続可能性の課題を十分に反映していないとの不満が広がったことにあった。こうした状況を踏まえ、2012 年のリオ+20 会議では、コロンビアとグアテマラを中心とする途上国が、持続可能性・包摂性・開発の統合を目指す新たな国際目標として SDGs の創設を提案し、G77+China の強い支持の下で国際的合意に至った。

その後の国連総会オープン・ワーキング・グループでは、小島嶼国や後発開発途上国を含む非大国が積極的に議題設定に関与し、気候変動への適応、海洋保全、不平等削減、技術移転など独自の優先課題を組み込んだ。こうして SDGs は、開発課題を特定国の問題に限定せず、すべての国が取り組むべき普遍的政策枠組みとして構築され、2015 年国連総会で 193 か国により全会一致で採択された。

この形成過程は、非大国主導の規範形成が最終的に国際的合意へと結実した事例であり、有志国連携による制度構築の可能性を示す歴史的先例となっている。

これらの事例は、非大国であっても創意と連携戦略を通じて大国の一方的支配に対抗し、信頼性・実効性・相互運用性を備えた国際秩序を築き得ることを示している。越境的データガバナンスにおける有志国連携もまた、複数の制度的ブロックが併存する現代的状況において、特定の大国モデルに依拠しない中立的基盤を形成する点に意義がある。すなわち、有志国が共通原則と運用基準を整備することで、制度的信頼性を中核とする新たな規範モデルを提示し、それを国際的に普及させるための起点となる制度的枠組みを構築することができる[154]。

さらに、有志国連携により形成された規範モデルは、国際取引や制度連携における前提条件として多数国で実装と運用が積み重ねられることにより、大国にとっても無視し得ない基準として認識されるようになる[155]。実際、UNCLOS や CBDR の例が示すように、非大国発の規範であっても、制度的合理性と包摂性を備えた場合には、最終的に大国の受容を経て国際基準として定着する。この点で、有志国連携は、大国への対抗軸としてではなく、国際社会全体の利益に資する新たな選択肢を提示する仕組みとして機能する。

この枠組みにおいて日本は、DFFT の提唱者であり JSI の共同議長国でもある立場を背景として、制度設計の中心的担い手および大国との調整役となる潜在力を有している[156]。事務局等

[154] Slaughter (2000), pp. 1104–1123; Hoekman and Sabel (2021), pp. 50–58; Bacchus et al. (2024), pp. 3–9; Dimitropoulos et al. (2025), pp. 7–15, 19–25.

[155] Finnemore and Sikkink (1998), pp. 895–905; Slaughter (2000), pp. 1104–1123; Parson and Ernst (2013), pp. 320–330; Hoekman and Sabel (2021), pp. 50–58.

[156] WTO (2019); Miura (2023); Digital Agency Japan (n.d.).

の常設機関を東京に設置することは、単なる象徴的措置ではなく、制度的専門性の蓄積、参加国間の継続的協議の枠組み、透明性と審査可能性の担保といった具体的機能を提供する点で大きな意義を持つ。これにより、日本は理念的指導力だけでなく、制度構築と運用の両面で実質的貢献を果たすことができる。

CRDM モデルの各モジュールで策定される規範については、それを主導した国や都市にちなんで、セクターごとに、「シンガポール・ルール」「シドニー・ルール」「ソウル・ルール」などと命名することも考えられる。また、有志国連携によって形成された規範が、日本の媒介と制度的支援により徐々に大国にも受容され、国際基準として定着するという動態は、「トウキョウ効果（Tokyo Effect）」と称することができる。この「トウキョウ効果」は、ブリュッセル効果のように規範を一方的に押し広げる構造とは異なり、多様な制度的ブロックを包摂しつつ相互運用性を実現する協調的モデルである。このような非対抗的かつ段階的な規範定着の過程は、越境的データガバナンスに内在する制度的非対称性を緩和し、国際社会全体にとって持続可能な規範秩序を構築するための現実的かつ有効なアプローチとして、越境的データガバナンスにおける新たな規範形成の力学として位置づけられる。

第 4 節　越境的データガバナンス規範再構成のロードマップ

本節では、越境的データガバナンス規範再構成について、理念的構想から制度的実装へと段階的に展開するロードマップを提示する。この関係では、DFFT の具体的実現のためのロードマップ（以下「DFFT ロードマップ」という。）が、2021 年 4 月に英国で開催された G7 デジタル・技術大臣会合において初めて包括的文書として提示され[157]、同年 6 月の G7 コーンウォール・サミットにおいて首脳レベルで正式に承認された[158]。DFFT ロードマップは、G7 が「自由なデータ流通」と「信頼」を両輪とする国際的データガバナンスの基本構想として DFFT を推進するに当たり、制度化に向けた具体的行動領域を体系的に示したものである[159]。

DFFT ロードマップでは、データの越境移転をめぐる規制の差異や不透明性が国際的な相互運用性を損なう主要因であるとの認識に基づき、(1)データの域内保管義務等の国内措置に関する協調、(2)プライバシー・セキュリティ関連規制の国際的整合性、(3)各国当局によるガバメントアクセスの透明化・必要性・比例性の確保、(4)医療・災害対策・サプライチェーンなどの優先分野における国際的データ共有の円滑化、という四つの重点領域を特定している[160]。DFFT ロードマップは、これらの領域において制度的・技術的両面からの協力を積み上げることにより、相互信頼を基盤とした国際的データ流通秩序の形成を段階的に進めるという G7 の合意を明確化する機能を果たした[161]。

DFFT ロードマップが越境的データ移転の規範策定において果たす中核的役割は、各国の異質な法制度・監督手続・技術基準が交錯する領域に、相互運用性と信頼性を確保するための共通原理を導入しようとする点にある。DFFT ロードマップは、越境的データ移転をめぐる現行制度が、国内規制の不透明性、政府当局のアクセス手続の差異、監督機関間の連携不足など複数の制度的摩擦を抱えているとの問題意識から出発し、これらの摩擦を制御するための国際的枠組みを段階的に整備する方針を示している。具体的には、プライバシー・サイバーセキュリティ・監督・救済といった要素について、必要性・透明性・比例性・説明可能性の原理を適用し、越境移転の適法性評価に関して各国が参照し得る共通の判断基準を構築することを目指している。また、政府当局による越境的データアクセスの在り方についても、制度的信頼を損なう不確実性を解消するため、各国がアクセス要件・手続保障・独立監督・事後的救済の枠組みを明示し、相互に共有可能な透明性基準を整備することを求めている。これにより、従来の一方的・形式的な越境移転規制とは異なる、制度間の比較衡量と文脈評価に基づく協調的な規範策定プロセスが可能となり、国際的に断片化したデータ移転ルールの調整が進むことが期待されている。さらに、医療、災害対応、研究開発など特定分野におけるデータ共有を想定した実務的枠組みの整備も併せて進めることで、単層的な法的整合性ではなく、多層的な制度的連携を支える越境移転規範の基盤を構築する方向性を示している[162]。

---

[157] G7 (2021a).
[158] G7 (2021b), para. 4.
[159] G7 (2021a), Introduction, Areas for Cooperation.
[160] G7 (2021a), Areas for Cooperation.
[161] G7 (2021a), Introduction.
[162] G7 (2021a), Introduction, Areas for Cooperation, Government Access to Data, Cross-border Data Use in Priority Sectors.

現状では、DFFT の理念提示から一定期間を経て、国際制度としての骨格（IAP）が整いつつあり、実務の土台も一定の進展をみせている[163]。もっとも、DFFT ロードマップは法的強制力を欠く協力指針にすぎず、制度的非対称性を根本的に解消するには限界がある。DFFT ロードマップは、必要性・比例性・透明性といった基本原理を基軸として制度間の相互運用性を高める方向性を示しているが、各国の監督権限、ガバメントアクセスの手続、国家安全保障概念の射程、民間部門に対する規律の構造が大きく異なる以上、共通原理の抽象度は高く、具体的運用段階での調整力は限定的である[164]。さらに、DFFT ロードマップが前提とする協調メカニズムは、主として G7 の先進国間における制度的整合性を念頭に置いており、制度的成熟度の異なるアジア・アフリカ・中南米諸国を包摂する枠組みは十分に確立されていない[165]。この構造は、むしろ既存規範圏の論理を維持したまま非対称性を内在化させる危険を伴っている。また、ガバメントアクセスの在り方についても、各国が自国法の正当性を主張し続ける限り、透明性基準に一定の共通性を見いだすことはできても、制度そのものの再設計や権限構造の調整に踏み込むことは困難である。その結果、DFFT ロードマップは越境移転のリスク管理を改善する一定の意義を有するものの、制度的非対称性の源泉を解消するには不十分であり、包括的な是正のためには新たな制度的枠組みや中立的フォーラムの構築が不可欠となる[166]。

このような DFFT ロードマップの課題を踏まえ、表 17 では、本稿の CRDM モデルによる新たな規範の実装を前提に、当初段階（当初の数年間）、中期段階（約 5 年程度）、長期段階（約 10 年程度）の三段階に分けて、そのロードマップを提示する。

【表 17：越境的データガバナンス規範再構成のロードマップ】

越境的データガバナンス規範再構成のロードマップ

1. 当初段階（当初の数年間）

当初段階では、既存の多国間交渉が制度的限界に直面している現状を踏まえ、有志国連携による規範的基盤の形成が最優先課題となる。この段階の目的は、統一的制度を即時に構築することではなく、各国が共有可能な原理的共通基盤を明確化することである。具体的には以下の点が特に重要となる。

ア　有志国連携の制度化準備

日本、シンガポール、オーストラリア、韓国など、地政学的に中立的かつ技術的信頼性を有する国々を中心に、中堅国および新興国で構成される有志国連携の常設的協議体（有志国フォーラム）を設立し、将来的なプルリラテラル協定（Plurilateral Agreement on Cross-Border Data Governance）の基盤となるネットワークを整備する。東京に国際事務局を設置し、DFFT 原則の普及、技術標準化、紛争解決支援、能力構築支援などの恒常的機能を担わせる。

イ　共通原理の明確化

[163] 内閣官房 (2023).
[164] G7 (2021a), Introduction, Areas for Cooperation, Government Access to Data; OECD (2022d), pp. 21–33, 35–45.
[165] Christakis (2024b), pp. 96–105, 107–113; Dale and Aizawa (2024), Introduction; Discussion (sections discussing Global South concerns and limits of alternative governance options); UNCTAD (2024), pp. 21–22, 53–64, 179–183, 208–212.
[166] OECD (2023a), pp. 7–9, 11–30; Christakis (2024a), pp. 39–56, 70–76, 86–95.

DFFT を指導理念とし、リスクベースアプローチを中核として運用規範を構成し、CRDM モデルによって実装するという共通原理を早期に確立する。ここでは、データの性質に基づくリスクと利用文脈に基づくリスクを評価軸とし、越境的データ移転の条件を比例的調整の対象として位置づける点について、各国間で共通理解を形成する。当初段階で最初に着手すべき事項は、各国が共有可能な共通評価軸の確立である。すなわち、「どのようなデータ・文脈が高リスクとみなされるのか」「どのような条件下で越境移転が許容されるのか」を分類・定義する CRDM モデルの国際的共通言語化を先行的に実施し、それを後続段階の制度設計の前提条件とする。

ウ　初期段階における大国の非関与

越境的データガバナンス規範の再構成を実効的に進めるためには、制度形成の初期段階において大国の参加を前提としない設計とし、中堅国および新興国による自律的設計空間を先行的に確立することが重要である。これは、政治的対立を煽る意図によるものではなく、制度形成を早期に硬直化させる外生的圧力から交渉枠組みを保護するための方法論的措置である。法理念、市場構造、安全保障観が異なる大国モデルを同時に枠内へ呼び込めば、概念対立が先鋭化し、合意内容は抽象化して実装可能性が低下する。したがって、まずは中堅国および新興国間で限定的合意を積み上げ、後発的に大国を招き入れる段階設計とする。

この自律的設計空間の確保は、共通の運用基盤を先に可視化することによって実現される。リスクベースアプローチを軸に、文脈的リスク評価とデータ最小化の手続を標準化し、データの性質と利用文脈に応じた移転条件を階層化する。重要なのは、価値概念としての信頼（with trust）を統一定義することではなく、それを監査可能な運用パラメータへ分解し、第三者検証や相互認証に接続する点にある。理念の調和ではなく、手続と検証可能性の整備を先行させることにより、政治的対立を回避しつつ最小公倍数の運用基盤が形成される。

2. 中期段階（～5 年）

中期段階では、当初段階で確立された原理的基盤をもとに、モジュラー構造を持つプルリラテラル協定を具体的な法形式へ落とし込む。この段階では、参加国の制度的成熟度や産業構造の差異を考慮しつつ、段階的かつ柔軟に参加できる制度設計が必要である。この段階の目標は、協定発効と並行して、データガバナンスの制度的相互運用性を実装することにある。主要課題は以下のとおりである。

ア　モジュールの試行

一般原則および紛争処理手続を共通の義務的モジュールとして確保したうえで、セクター別の小規模モジュールによる試行を実施する。医療、教育などのセクターごとに、共通の評価軸、監査指標、是正メカニズムを定めたテンプレートを整備し、参加国が選択的にオプトインできる設計とする。これにより、各国の制度成熟度や産業構造の差異を包摂しつつ、実務面の相互運用性を段階的に拡張できる。試行モジュールの運用実績は、紛争解決の前例や監査知見を蓄積し、後の条文化と常設化の素材となる。

制度の持続性を担保するには、技術標準と手続規範の中立化が鍵となる。特定の大国の法制度に依存しない形で、国際標準化の成果や既存の認証枠組みを基盤として用い、相互承認の最小条件を明文化する。これに紛争解決の義務的モジュールを組み合わせることで、過度な政治化を避けつつ、可視性と予見可能性を確保できる。

当初の試行対象として最も適しているのは医療セクターと教育セクターである。これらのセクターは、個人データを扱う点で高いリスクを伴う一方、公益性が明確で社会的正統性を得やすい。医療

データの国際的二次利用や教育研究データの共有は、公共目的の実現と密接に関連するため、越境的データ移転の枠組みを試行するにあたり適合性が高い。

ただし、既存の OECD、WHO、UNESCO といった国際機関の枠組みをそのまま参照すれば、大国が主導して形成してきた規範構造を追認する結果となり得る。したがって、それらの指針を政策的前提として採用するのではなく、有志国フォーラムにおいて批判的かつ分析的に検討することが不可欠である。この批判的検討とは、文書の内容自体を評価するだけでなく、その背後にある規範形成の力学や制度的前提を相対化する作業を含む。既存文書の構造的偏りを見極め、どの理念がどの地政学的利益を反映しているのかを可視化したうえで、各国の制度的成熟度と社会的文脈に応じて再構成可能な独自の評価基準を策定すべきである。これは既存文書を否定するものではなく、批判的素材（critical references）として再利用し、政治的中立性と技術的整合性の両立を図る試みである。医療や教育など公共性の高いセクターでこのような制度モデルを実証すれば、大国の規範的影響を最小化しつつ、信頼に基づく均衡的な越境的データガバナンスの原型を提示できる。

イ　紛争解決手続の義務化

WTO DSU 型の紛争処理を参考に、プルリラテラル協定内に義務的紛争解決モジュールを導入し、制度の実効性と予見可能性を確保する。紛争解決機関については、グローバルサウスなどの当事国関係者の出廷の便宜を考慮し、シンガポールに設置する案が考えられるが、事案の性質や当事国の構成に応じて、適切な国・地域にアドホックにパネルを設置する方式も検討し得る。

ウ　監査・認証制度の整備

加盟国間の信頼構築を制度的に担保するため、第三者監査機関および相互認証制度を設置し、越境的データ移転に関する透明性と検証可能性を確保する。この場合、日本が関与してきた国際認証基準（CBPR、OECD Trust Framework など）を技術的基盤として参照することは有効であるが、真に中立的な制度設計を志向するのであれば、これらの枠組みをそのまま移植するのではなく、技術的要素および手続的構造を抽出し、政治的文脈を切り離した形で再構成する必要がある。日本が果たすべき役割は、これらを制度設計の素材として再構築し、有志国連携型の標準化モデルを提示することである。この再構成的アプローチにより、日本が関与するプルリラテラル協定は、名目的な主導にとどまらず、実質的に自律した制度的方向性を確立することが可能となる。

3. 長期段階（～10 年）

長期的には、プルリラテラル協定を基盤として、より包括的なグローバル・フォーラムへと発展させることを展望する。この段階では、制度的・技術的双方における恒久的枠組みの確立が焦点となる。

ア　セクター別モジュールの策定

医療、教育、金融、AI、訴訟関連データなど、リスク水準の異なるセクターごとに個別モジュールを設定し、専門家等のステークホルダーも参加して実効的な規範を策定する。このセクター別モジュールは、各加盟国が自国の制度成熟度に応じて選択的に参加できる柔軟な構造を形成する。各モジュールで策定された規範は、それを主導した国や都市にちなんで、セクターごとに、たとえば、「シンガポール・ルール」「シドニー・ルール」「ソウル・ルール」などと命名する。

イ　包括的ガバナンス構造の構築

プルリラテラル協定をオープンエンド型の構成とし、一定の段階を経た後に大国の参加を認めることで、より包括的な国際ガバナンス体制へと接続させる。また、一定の制度成熟を経た段階で、WTO 電子商取引交渉、OECD デジタル政策枠組み、UN グローバルデジタルコンパクト等との制度

的接続を段階的に行う。これにより、WTO、OECD、APEC、UN など既存の多国間枠組みとの制度的接合を進め、断片化した規範構造の統合を図る

ウ　グローバルサウスとの包摂的連携

発展途上国・新興国に対し、リスク分類や技術的基準への適合を支える能力構築（capacity building）を体系的に提供し、規範格差の縮減と制度的包摂性の向上を図る。この段階では、各国の制度的多様性を前提としつつ、信頼・比例性・透明性の原理に基づき越境的データ移転を管理する新たな国際秩序の確立が最終的目的となる。

エ　国際制度への昇華（「トウキョウ効果」の実現）

東京を中核とする国際事務局がこの多層的枠組みを恒常的に支えることにより、「トウキョウ効果」は理念的象徴にとどまらず制度的現実として結実する。越境的データガバナンスは、一国主導や政治的支配に依拠せず、信頼・透明性・比例性の原理に基づき安定的に運用される国際制度として確立される。

参考文献（第Ⅲ部）（本文との対応関係は各頁に脚注番号で表示）

Aaronson SA (2018) Data is different: Why the world needs a new approach to governing cross-border data flows. CIGI Papers No. 197, Centre for International Governance Innovation, Waterloo, ON, Canada, November 2018, 1–22. https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows/

Aaronson SA, Leblond P (2018) Another digital divide: The rise of data realms and its implications for the WTO. Journal of International Economic Law 21(2): 245–272. https://doi.org/10.1093/jiel/jgy019

Abe S (2020) Special address by prime minister Shinzo Abe at the World Economic Forum annual meeting 2020, Davos, 21 January 2020. Prime Minister of Japan and His Cabinet. https://japan.kantei.go.jp/98_abe/statement/202001/_00001.html

Aledhari M, Razzak R, Parizi RM, Saeed F (2020) Federated learning: a survey on enabling technologies, protocols, and applications. IEEE Access 8: 140699–140725. https://doi.org/10.1109/ACCESS.2020.3013541

Alford RP (2011) The self-judging WTO security exception. Utah Law Review: 697–759. https://scholarship.law.nd.edu/law_faculty_scholarship/330

APEC (2015) APEC cross-border privacy rules (CBPR) system. APEC Secretariat, Singapore. https://cbprs.org (accessed 22 February 2026).

Article 29 Data Protection Working Party (2014) Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, 1–4 (Feb. 27, 2013; adopted May 30, 2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Bacchus J, Borchert I, Morita-Jaeger M, Ruiz Diaz J (2024) Interoperability of data governance regimes: challenges for digital trade policy. CITP Briefing Paper 12, Centre for Inclusive Trade Policy, 1–11. https://citp.ac.uk/wp-content/uploads/CITP-Briefing-Paper-12-Interopability-of-Data-Governance-Regimes-Challenges-for-Digital-Trade-Policy.pdf

Bradford A (2020) The Brussels effect: How the European Union rules the world. Oxford University Press.

Barbereau T, Delgado Fernandez J, Potenciano Menci S (2025) The governance of federated learning: a decision framework for organisational archetypes. Data and Policy 7: e53–1–e53–14. https://doi.org/10.1017/dap.2025.10020

Breitbarth P (2021) A risk-based approach to international data transfers. Eur. Data Prot. L. Rev. 7: 539–549. https://edpl.lexxion.eu/data/article/17963/pdf/edpl_2021_04-010.pdf

Burri M (2017) The governance of data and data flows in trade agreements: the pitfalls of legal adaptation. UC Davis L. Rev. 51: 65–132. https://lawreview.law.ucdavis.edu/issues/51/1/Symposium/51-1_Burri.pdf

Chaisse J (2024) Arbitration in cross-border data protection disputes. Journal of International Dispute Settlement 15: 534–548. https://doi.org/10.1093/jnlids/idae018

Chin YC, Zhao J (2022) Governing cross-border data flows: international trade agreements and their limits. Laws 11(4): 63, 1–22. https://doi.org/10.3390/laws11040063

Christakis T (2024a) The "Zero Risk" fallacy: international data transfers, foreign governments' access to data and the need for a risk-based approach. Centre for Information Policy Leadership / Cross-Border Data Forum Paper Series, 1–79. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_zero_risk_fallacy_-_t.christakis_feb24.pdf

Christakis T (2024b) Data free flow with trust: current landscape, challenges and opportunities. Journal of Cyber Policy 9(1): 95–120. https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2421838

Christakis T, Felz D, Swire P (2024) German court decision signals move towards risk-based approach to data transfers. Cross-Border Data Forum, October 16. https://www.crossborderdataforum.org/german-court-decision-signals-move-towards-risk-based-approach-to-data-transfers/

Cory N, Dascoli L (2021) How barriers to cross-border data flows are spreading globally, what they cost, and how to address them. Information Technology and Innovation Foundation, Washington D.C. https://itif.org/sites/default/files/2021-data-localization.pdf

Dale C and Aizawa M (2024) "Data Free Flow with Trust": Japan's struggle to integrate democracy and human rights into digital trade policy. Frontiers in Sociology 9: Article 1397528. https://www.frontiersin.org/articles/10.3389/fsoc.2024.1397528

Department for Business and Trade (2024) £2 billion boost to growth as UK joins major trade group. 15 December 2024. https://www.gov.uk/government/news/2-billion-boost-to-growth-as-uk-joins-major-trade-group

Digital Agency Japan (n.d.) Data Free Flow with Trust (DFFT). https://www.digital.go.jp/en/policies/dfft (accessed 22 February 2026).

Digital Public Goods Alliance (2023) Digital Public Goods Standard. https://digitalpublicgoods.net/standard/

Dimitropoulos G, Chen RC, Chaisse J (2025) Plurilateralism: a new form of international economic ordering? Journal of World Investment & Trade 26(1-2): 1-30. https://doi.org/10.1163/22119000-12340350

EDPB (2020a) Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, adopted 10 November 2020. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

EDPB (2020b) Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, adopted 10 November 2020. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en

EDPB (2020c) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, adopted 20 October 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

EDPB (2020d) Guidelines 05/2020 on consent under Regulation 2016/679, adopted 4 May 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

EDPB (2021a) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18 June 2021. https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

EDPB (2021b) Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR, adopted Nov. 18, 2021, last revised Feb. 14, 2023. https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf.

EDPB (2025) Guidelines 01/2025 on Pseudonymisation, Jan. 16, 2025. https://edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf.

European Regulation and Innovation Forum (2019) Highlights Note 12: Proportionality principle and the management of risk, 1-4. https://www.eriforum.eu/uploads/2/5/7/1/25710097/erif_highlights_12_-_proportionality_principle.pdf

Finnemore M, Sikkink K (1998) International norm dynamics and political change. International Organization 52(4): 887-917. https://www.jstor.org/stable/2601361

Gaia-X European Association for Data and Cloud AISBL (2022) Gaia-X architecture document - 22.10 release. Brussels. https://docs.gaia-x.eu/technical-committee/architecture-document/22.10/

Global CBPR Declaration (2022) Annex to Ministry of Economy, Trade and Industry (METI) and Personal Information Protection Commission (PPC), Press release「グローバル越境プライバシールール（CBPR）フォーラム設立に向けた宣言をすることに合意しました」, 21 April 2022. https://www.meti.go.jp/press/2022/04/20220421001/20220421001.html

González J L, Casalini F and Porras J (2022) A preliminary mapping of data localisation measures. OECD trade policy paper no. 262. OECD Publishing, Paris. https://www.oecd.org/en/publications/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en.html

G7 (2021a) G7 Roadmap for Cooperation on Data Free Flow with Trust. G7 Digital and Technology Ministers' Meeting, 28 April 2021.

https://assets.publishing.service.gov.uk/media/609cf5e18fa8f56a3c162a43/Annex_2_Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf
G7 (2021b) Carbis Bay G7 Summit Communique, 12 July 2021. https://www.gov.uk/government/publications/carbis-bay-g7-summit-communique/carbis-bay-g7-summit-communique
G7 Digital and Tech Ministers (2023a) Ministerial declaration: The G7 digital and tech ministers' meeting, Takasaki, Gunma, 29–30 April 2023. Ministry of Internal Affairs and Communications, Tokyo. https://www.soumu.go.jp/joho_kokusai/g7digital-tech-2023/topics/pdf/pdf_20230430/ministerial_declaration_dtmm.pdf
G7 Digital and Tech Ministers (2023b) Ministerial declaration: the G7 digital and tech ministers' meeting, Takasaki, Gunma, 29–30 April 2023. Government of Japan, Tokyo. https://www.soumu.go.jp/joho_kokusai/g7digital-tech-2023/topics/pdf/pdf_20230430/ministerial_declaration_dtmm.pdf
Harris PG (1999) Common but differentiated responsibility: the Kyoto Protocol and United States policy. NYU Environmental Law Journal 7: 27–48. https://www.nyuelj.org/wp-content/uploads/2019/07/Harris_Common_But_DIfferentiated_Responsibility.pdf
Hoekman B, Sabel C (2021) Plurilateral cooperation as an alternative to trade agreements: innovating one domain at a time. Global Policy 12(S3): 49–60. https://doi.org/10.1111/1758-5899.12923
Irion K, Kaminski ME, Yakovleva S (2020) Privacy peg, trade hole: why we (still) shouldn't put data privacy in trade law. University of Chicago Law Review Online. https://lawreview.uchicago.edu/online-archive/privacy-peg-trade-hole-why-we-still-shouldnt-put-data-privacy-trade-law
Juliussen BA, Kozyri E, Johansen D, Rui JP (2023) The third country problem under the GDPR: enhancing protection of data transfers with technology. International Data Privacy Law 13(3): 225–243. https://doi.org/10.1093/idpl/ipad013
Knoppers BM (2014) Framework for responsible sharing of genomic and health-related data. Hugo Journal 8(1):3. https://doi.org/10.1186/s11568-014-0003-1
Koh TB (1982) A constitution for the oceans. Remarks by the President of the Third United Nations Conference on the Law of the Sea, 6 December 1982. United Nations. https://www.un.org/depts/los/convention_agreements/texts/koh_english.pdf
Kuner C (2017a) Reality and illusion in EU data transfer regulation post Schrems. German Law Journal 18(4), 881–918. https://www.cambridge.org/core/journals/german-law-journal/article/reality-and-illusion-in-eu-data-transfer-regulation-post-schrems/0341A0D14DC345730F9B48A496A968D3
Kuner C (2017b) The internet and the global reach of EU law. LSE Law, Society and Economy Working Paper No. 4/2017; University of Cambridge Faculty of Law Research Paper No. 24/2017, 1–37. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930
Lewis R (2025) The 'constitution for the oceans'? The law of the sea convention as a living treaty. International and Comparative Law Quarterly 74(1): 1–31. https://doi.org/10.1017/S0020589325000120
Lindell Y (2021) Secure multiparty computation. Communications of the ACM 64: 86–96. https://doi.org/10.1145/3387108
López González J (2021) Trade and cross-border data flows. OECD Going Digital Toolkit Notes, No. 11, OECD Publishing, Paris. https://doi.org/10.1787/7bc12916-en
Mansouri S, Elayan H, Oueis J, Conti M, Al-Nemrat A (2023) SoK: secure aggregation based on cryptographic schemes for federated learning. Proceedings on Privacy Enhancing Technologies 2023: 140–164. https://doi.org/10.56553/popets-2023-0009
McMahan HB, Moore E, Ramage D, Hampson S, y Arcas BA (2017) Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS 2017), PMLR 54:1273–1282. https://proceedings.mlr.press/v54/mcmahan17a.html
Meltzer J P (2015) The internet, cross－border data flows and international trade. Asia & Pac Pol'y Stud 2(1): 90–102. https://doi.org/10.1002/app5.60
Miura H (2023) Japan's role and strategy in the formation of digital trade rules in the Indo-Pacific. NBR Commentary, January 10, 2023. https://www.nbr.org/publication/japans-role-and-strategy-in-the-formation-of-digital-trade-rules-in-the-indo-pacific/

OECD (2013) The OECD Privacy Framework, including the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing, Paris. https://www.afapdp.org/wp-content/uploads/2018/06/oecd_privacy_framework.pdf
OECD (2019a) Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies. OECD Publishing, Paris. https://doi.org/10.1787/276aaca8-en
OECD (2019b) Recommendation of the Council on Artificial Intelligence (adopted 22 May 2019), OECD/LEGAL/0449. OECD, Paris. https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf
OECD (2022a) Going digital to advance data governance for growth and well-being. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/going-digital-to-advance-data-governance-for-growth-and-well-being_246d8cab/e3d783b0-en.pdf
OECD (2022b) Cross-border data flows: Regulatory barriers and the need for proportionality. OECD Publishing, Paris. https://doi.org/10.1787/5031dd97-en
OECD (2022c) Fostering cross-border data flows with trust. OECD Digital Economy Papers No. 343. OECD Publishing, Paris. https://doi.org/10.1787/139b32ad-en
OECD (2022d) Going digital: Guide to data governance policy making. OECD Publishing, Paris. https://doi.org/10.1787/40d53904-en
OECD (2022e) Declaration on government access to personal data held by private sector entities. OECD/LEGAL/0487, adopted 14 December 2022. OECD Legal Instruments, Paris. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487
OECD (2023a) Moving forward on data free flow with trust: New evidence and analysis of business experiences. OECD Digital Economy Papers, No. 353. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/04/moving-forward-on-data-free-flow-with-trust_0f681e91/1afab147-en.pdf
OECD (2023b) The nature, evolution and potential implications of data localisation measures. OECD Trade Policy Papers No. 278. OECD Publishing, Paris. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf
Organization of American States (2021) Updated principles on privacy and the protection of personal data. OAS, Washington, DC. https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf
Otto B (2022) A federated infrastructure for European data spaces. Communications of the ACM 65(4): 44-45. https://doi.org/10.1145/3512341
Oxman BH (1994) The rule of law and the United Nations Convention on the Law of the Sea. European Journal of International Law 7(3): 353-371. https://academic.oup.com/ejil/article/7/3/353/394782
Parson EA, Ernst LN (2013) International governance of climate engineering. Theoretical Inquiries in Law 14: 307-338. https://doi.org/10.1515/til-2013-015
Purtova N, van Maanen G (2024) Data as an economic good, data as a commons, and data governance. Law, Innovation and Technology 16: 1-42. https://doi.org/10.1080/17579961.2023.2265270
Slaughter A-M (2000) Judicial globalization. Virginia Journal of International Law 40: 1103-1124. https://slaughter.scholar.princeton.edu/document/211
Stone Sweet A, Mathews J (2008) Proportionality balancing and global constitutionalism. Columbia Journal of Transnational Law 47: 72-149. https://insight.dickinsonlaw.psu.edu/fac_works/222/
Truong N, Sun K, Wang S, Guitton F, Guo YK (2021) Privacy preservation in federated learning: an insightful survey from the GDPR perspective. Computers & Security 110: Article 102402. https://doi.org/10.1016/j.cose.2021.102402
UNCTAD (2021) Digital economy report 2021: Cross-border data flows and development – For whom the data flow. United Nations Conference on Trade and Development. https://unctad.org/system/files/official-document/der2021_en.pdf
UNCTAD (2024) Digital economy report 2024: Governing data and AI for development. United Nations, Geneva. https://unctad.org/publication/digital-economy-report-2024
UNESCO (2023) Global internet governance report 2023: fragmentation of the internet. UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000386859

United Nations (2012) The future we want. Outcome document of the United Nations Conference on Sustainable Development (Rio+20), A/RES/66/288. https://undocs.org/A/RES/66/288
United Nations (2014) Report of the Open Working Group of the General Assembly on Sustainable Development Goals. A/68/970. https://undocs.org/A/68/970
United Nations General Assembly (2015) Transforming our world: the 2030 agenda for sustainable development. GA Res 70/1, Sept 25, 2015. https://docs.un.org/en/A/RES/70/1
United Nations Human Rights Council (2022) The right to privacy in the digital age: report of the United Nations High Commissioner for Human Rights. UN Doc A/HRC/51/17, 4 August 2022. United Nations, Geneva. https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf
UNIDIR (2023) Internet fragmentation and cybersecurity: a primer, 1–14. UN Institute for Disarmament Research, Geneva. https://unidir.org/wp-content/uploads/2023/12/UNIDIR_internet_fragmentation_cybersecurity_primer.pdf
Vankayalapati R K, Korupalli V, Karthik S and Sravya P (2025) Federated edge computing for privacy-preserving analytics in healthcare and IoT systems. International Journal of Computer Trends and Technology 73: 80–90. https://doi.org/10.14445/22312803/IJCTT-V73I1P110
World Economic Forum (2020) A roadmap for cross-border data flows: Fostering data free flow with trust. World Economic Forum, Geneva. https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross-Border_Data_Flows_2020.pdf
WTO (2019) Joint statement on electronic commerce, WT/L/1056. World Trade Organization. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/1056.pdf
Yakovleva S (2024) Governing cross-border data flows: reconciling EU data protection and international trade law. Oxford University Press, Oxford.
石井夏生利（2025）「各国のプライバシー・データ保護法の理解と国際協調の可能性」音無知展・山本龍彦編『講座 情報法の未来をひらく：AI 時代の新論点 第 3 巻 プライバシー』法律文化社 229–59 頁.
川瀬剛志（2015）「WTO 協定における無差別原則の明確化と変容」RIETI ディスカッション・ペーパー・シリーズ 15-J-004; 1–33 頁. https://www.rieti.go.jp/jp/publications/dp/15j004.pdf
実積寿也，前村昌紀，白畑真，堀越功，小宮山功一朗，水越一郎（2023）「スプリンターネットを巡る議論」『情報法制研究』13: 72–94 頁. https://www.jilis.org/report/2023/jilisreport-vol5no2.pdf
城山英明（2023）「グローバルなデータガバナンスにおける多様な公共政策目的の調整」『経済安全保障に関する研究報告書』日本国際問題研究所 147–159 頁. https://www.jiia.or.jp/pdf/research/R04_Economic_Security/01-11.pdf
内閣官房（2023）[仮訳]附属書:「DFFT 具体化のための国際枠組み（Institutional Arrangement for Partnership: IAP）の設立及び G7 の期待に関するコンセプトペーパー」. https://www.cas.go.jp/jp/seisaku/digital/dfftiap_annex_jp.pdf
日本貿易振興機構（JETRO）（2019）電子商取引の「TPP3 原則」と中国・韓国の法制度の比較. 2019 年 5 月 20 日. https://www.jetro.go.jp/biz/areareports/2019/13a43c86eed15d2c.html
根本拓（2023）「信頼性のある自由なデータ流通（DFFT）を促進するための多様なアプローチの分析 ―OECD マッピングレポートの紹介を通じて―」経済産業研究所ポリシー・ディスカッション・ペーパー 23-P-006; 1–33 頁. https://www.rieti.go.jp/jp/publications/pdp/23p006.pdf
藤井康次郎・根本拓・福島惇央（2024）「越境データ移転規制における透明性の確保―国際的な制度構築に向けて―」石井由梨佳（編）『講座 情報法の未来をひらく：AI 時代の新論点 第 7 巻 安全保障』法律文化社 112–136 頁.
堀見裕樹（2019）「第 11 章 安全保障例外条項と紛争処理の限界―司法判断適合性の観点から―」阿部克則・関根豪政編『国際貿易紛争処理の法的課題』信山社 335–360 頁.
村上康二郎（2023）「情報プライバシー権の類型化に向けた一考察」『情報通信政策研究』第 7 巻第 1 号 Ⅱ-1-Ⅱ-22 頁.

おわりに

おわりに

本稿では、サイバー空間分裂回避のための越境的データガバナンス規範再構成について論じた。第Ⅰ部で越境的データガバナンス規範再構成の必要性と課題を検討し、第Ⅱ部で国際的データガバナンスの分断をもたらす五つの国家施策を分析したうえで、第Ⅲ部で越境的データガバナンス規範再構成の在り方を提示した。

まず第Ⅰ部では、国家のデジタル主権行使により国際的データガバナンスが分断され、伝統的基本原則の実効性が失われつつある状況と、国際的統一規範の不存在を指摘した。各国はデータという非領域的対象をめぐり、自国の統制をサイバー空間へ拡張しており、その結果、規範的主張の衝突と閉鎖的なデータ保護主義が拡大している。データ流通が地政学的境界線に沿って断片化すれば、サイバー空間全体が制度的ブロックごとに分裂するリスクが高まる。米国、中国、EU といったデータ大国はそれぞれ独自の規範的統制を及ぼしつつ対立しており、越境的データガバナンスに関する国際的統一規範の策定は停滞している。多国間フォーラムでも共通原則や調整メカニズムの構築は十分に進んでいない。その間に、各国は自国の価値観や安全保障上の懸念に基づく規制を展開し、制度間の非対称性はむしろ拡大している。

越境的データガバナンスには、大国間の規範的対立に起因する「ヨコの非対称性」と、大国と非大国との権力・ガバナンス格差に基づく「タテの非対称性」が併存する。規範のブロック化が進行すると、各ブロック内で大国が主導的地位を強め、垂直的な従属構造が固定化される。この構造的非対称性を克服するには、ブロック横断的な相互運用性と、大国・非大国間の規範的衡平性を備えた新たな越境的データガバナンス規範の再構成が必要となる。

越境的データガバナンスは、相手国制度の信頼性やリスク構造を個別に検証することを要する領域であり、平等な市場アクセスの確保を中心とする貿易原則が想定する共通の比較基盤を欠いている。最恵国待遇・自由化原則・内国民待遇といった GATS の基本原則は、各国制度を形式的に比較することを前提とする制度構造に基づくものである。これに対し、越境的データガバナンスは、相手国制度の差異を実質的に評価することを不可避とする。このため、GATSの基本原則を越境的データガバナンスにそのまま適用することは、その制度的前提との間に齟齬を生じ、妥当性を欠く。したがって、国家間の制度差を前提としつつ、制度的信頼性を評価する枠組みを備えた新たな規範構造が求められる。

このような観点から、第Ⅱ部では、国際的データガバナンスの分断をもたらす五つの国家施策―大国による規範輸出、データローカライゼーション、ガバメントアクセス、越境的ディスカバリ、国家によるデータ流入規制―に焦点を当て、それぞれの背景と制度的影響を分析した。これらは、国家がサイバー空間における主権を拡張し、または自国の規範領域を防衛する過程で表出した制度的形態であり、その相互作用を通じて国際的データガバナンスの分断が深化している。越境的データガバナンスにおいては、断片化した制度構造の累積により、各国が異なる制度原理と価値観に基づき併存・競合する多極化したデータ秩序が形成されている。そのため、断片化した制度間の齟齬を是正し、国際的相互運用性を回復するための取組として、越境的データガバナンス規範の再構成が不可欠となる。本稿で分析対象とした諸領域に共通する要請は、データの性質および利用文脈に応じて、規制と保護の水準を調整し得る制度的枠組みを整備し、分断された国際秩序を再び接続するための基盤を確立する点にある。今後は、各国の制度的

多様性を前提としつつ、複層的なリスク評価に基づく制度設計を通じて、透明性と相互運用性を持続的に確保し得る新たな国際的枠組みを構築していくことが求められる。

これらの分析を踏まえ、第Ⅲ部では、地域貿易協定における大国の規範的対立を明らかにしたうえで、越境的データガバナンス規範再構成の具体化と実装、有志国連携による規範再構成と「トウキョウ効果」の展開を検討した。規範再構成の在り方として、DFFT を指導原理とし、リスクベースアプローチによる運用規範の意義を確認したうえで、文脈的リスク評価とデータ最小化原則を統合した CRDM モデル（Contextual Risk-Based Data Minimization model）を提案した。CRDM モデルは、データの性質と利用文脈に応じてリスクを評価し、その結果に従ってデータ処理および規制措置の範囲を必要最小限に限定することを基本とする。CRDM モデルでは、形式的一律の禁止ではなく、リスクと必要性に即した柔軟な対応が要請され、比例原則に基づき「より制限的でない他の方法」が存在する場合には、当該データ移転や取得に対する規制は正当化されない。これにより、個人データ・非個人データを問わず、越境的データ移転に対して持続可能で合理的な制度枠組みを構築することが可能となる。

また、CRDM モデルに基づく規範再構成を前進させるうえで、中堅国や新興国による有志国連携は戦略的に重要である。規範的対立を先鋭化させている大国主導の枠組みへの過度な依存を回避しつつ、中堅国や新興国の主導により、各国の主権的統制を尊重しながら国際的相互運用性を確保し得る新たな国際規範を策定する必要がある。有志国連携により形成された規範が、国際取引や制度連携における前提条件として多数国で実装と運用が積み重ねられることにより、大国にとっても無視し得ない基準として認識されるようになる。この点で、有志国連携は、大国への対抗軸としてではなく、国際社会全体の利益に資する新たな選択肢を提示する仕組みとして機能する。

この枠組みにおいて日本は、DFFT の提唱者であり JSI の共同議長国であるという立場を背景に、制度設計の中心的担い手および大国との調整役となる潜在力を有する。有志国連携による規範が、日本の媒介と制度的支援を通じて大国にも徐々に受容され、国際基準として定着していく動態は、「トウキョウ効果（Tokyo Effect）」と称することができる。このトウキョウ効果は、ブリュッセル効果のように一方的に規範を押し広げる構造とは異なり、複数の制度的ブロックを包摂しつつ相互運用性を実現する協調的モデルとして、越境的データガバナンスにおける新たな規範形成の力学を示すものである。

本稿では、以上の検討を通じて、越境的データガバナンスにおける制度的非対称性を克服し、サイバー空間の分裂を回避するための越境的データガバナンス規範再構成の理論的枠組みと実装戦略を提示した。すなわち、国家間の制度差を前提としつつ相互運用性を確保する規範構造として CRDM モデルを提案し、さらに有志国連携による段階的制度形成とトウキョウ効果という動態的規範形成メカニズムを理論化した点に、本研究の学術的貢献がある。今後は、各モジュールの制度設計や運用評価を通じて実証的検証を進めることが課題となるが、本稿が提示した枠組みは、分断が進行する国際的データ秩序を再接続するための基礎理論を提供するものである。

（完）

謝辞

本論文の作成にあたり、多くの方々から貴重なご指導とご支援を賜りました。ここに心より御礼申し上げます。

まず、指導教員である後藤厚宏先生（前学長）には、修士論文の段階から本論文の完成に至るまで、終始丁寧かつ的確なご指導を賜りました。深い学識に基づくご助言と温かいご配慮により、本研究を完成させることができました。心より感謝申し上げます。

また、主として個人情報保護の観点から貴重なアドバイスをいただきました村上康二郎先生に深く御礼申し上げます。

さらに、審査にあたり貴重なご指摘とご助言を賜りました桑名栄二学長、大久保隆夫研究科長に深く御礼申し上げます。

2026 年 3 月

片岡　弘