RIETI Discussion Paper Series 22-J-004

デジタル貿易諸協定における個人情報保護法制とデータ・ガバナンス

石井 由梨佳
防衛大学校

RIETI
Research Institute of Economy, Trade & Industry, IAA
独立行政法人経済産業研究所
https://www.rieti.go.jp/jp/

RIETI Discussion Paper Series 22-J-004
2022 年 2 月

デジタル貿易諸協定における個人情報保護法制とデータ・ガバナンス*

石井 由梨佳（防衛大学校）

要　旨

デジタル貿易諸協定のうち、高水準の義務を定めるものは、事業実施のためのデータの越境移転の自由の確保、コンピューター関連設備の設置要求の禁止、ソースコードやアルゴリズム開示要求の禁止規定を置く。他方で協定締結とは別に、近年では、各国が個人情報やデータの保護法制を新たに制定したり、強化したりしている。

しかし、そのような各国法制には、上記のデジタル貿易諸協定の規則に抵触しうるものが含まれている。本稿では（1）個人情報保護法制及びデータ保護法制と、（2）データ・ガバナンスの一環として輸入国が事業者に対して取る措置、特にソースコードあるいはアルゴリズムの開示を求める規制が、デジタル貿易諸協定においてどのように位置づけられているかを実証に基づき検討する。

キーワード：デジタル貿易、個人情報保護、プライバシー、データ・ガバナンス、データ倫理、国際公法
JEL classification: K23, K33

*本稿は、独立行政法人経済産業研究所（RIETI）におけるプロジェクト「現代国際通商・投資システムの総合的研究（第Ⅴ期）」の成果の一部である。また本研究は JSPS 科研費（基盤 C）21K01173 の成果の一部である。本稿の執筆に当たっては、2021 年 10 月 14 日の研究会及び 11 月 25 日の DP 検討会に出席の方々から多くの有益なコメントを頂いた。ここに記して、感謝の意を表したい。

1. はじめに

今日、180を超える協定においてデジタル貿易が規律されている[1]。日米デジタル貿易協定等の二国間協定、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）[2]、 地域的な包括的経済連携協定（RCEP）[3]、米国・メキシコ・カナダ協定（USMCA）[4]等が締結されている他、2022年1月現在、世界貿易機関（WTO）においてデジタル貿易条約の交渉が進められている。

その具体的な規則内容は協定に応じて異なるものの、高水準の義務を定める諸協定は、最恵国待遇、市場アクセス義務、無差別待遇という一般原則に加えて、事業実施のためのデータの越境移転の自由の確保、コンピューター関連設備の設置要求の禁止、ソースコードやアルゴリズム開示要求の禁止規定を置く[5]。

他方、それとは独立した動きとして、各国が個人情報やデータの保護法制を新たに制定したり強化したりしている[6]。情報コンピューター技術（ICT）の飛躍的な発展を背景にして、事業者は多岐に渡る個人情報を大量に蓄積、統合、解析している。また人工知能（AI）技術が機械学習を通じて自律的にデータを用いることも増えている。従来の個人情報保護の必要性に加えて、そのようなビッグデータの利活用を規律する要請が強くなってきたためである。

しかし、そのような各国法制には、上記のデジタル貿易諸協定の規則に抵触し得るものが含まれている。本稿では事業者に課される（1）個人情報あるいはデータの域内保存義務、あるいは（2）政府の情報収集活動への協力義務（ガバメント・アクセス）が、デジタル貿易諸協定においてどのように位置付けられているかを実証に基づき検討する。

検討に先立ち、問題の所在を明らかにするために、域内保存義務とガバメント・アク

---

[1] University of Lucerne, 'TAPED: A New Dataset on Data-related Trade Provisions' <https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/> accessed 7 February 2022.

[2] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (sealed on 23 January 2018, entered into force on 30 December 2018) <https://mfatgovtnz2020.cwp.govt.nz/pl/trade/free-trade-agreements/free-trade-agreements-in-force/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-cptpp/>.

[3] Regional Comprehensive Economic Partnership Agreement (signed on 15 November 2020) <https://rcepsec.org/legal-text/>.

[4] United States–Mexico–Canada Agreement, *signed on* 30 November 2018 (revised on 10 December 2019, entered into force on 1 July 2020) <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>.

[5] デジタル貿易協定の分析については、TAPED (n 1); Digital Trade Estimates Project <https://ecipe.org/dte/> accessed 7 February 2022 参照。

[6] 個人情報ないしデータの定義は法制によって異なるが、特定の個人に関する情報であること、当該個人が生存していること、その情報によって個人を識別できるものであることを要素とする情報を一般的に指す。また、情報（information）とデータ（data）は同義ではないが、一般的には、情報（ある対象の属性、思考の内容等の意味内容）はデータ（符号、信号）によって表現されるものと捉えることができる。ただし、個人情報保護法制についての議論では両者が相互互換的に用いられることも少なくない。

セスの意義を示しておく。

1-1　個人情報の越境移転規制あるいはデータの域内保存義務

①　　個人情報保護法制における個人情報の越境移転規制

個人情報保護法制は、事業者の個人情報の取り扱いの他に[7]、データの越境移転を規律することが多い[8]。事業者がデータを他国領域に移転したとき、移転先でのデータの保護が十分でなければ、事業者が容易に移転元国の個人情報保護法制を潜脱しうるからである。また、国内外で事業者の負担が不均衡になることを防止するためでもある。現在、日本を含めた 70 カ国以上が、個人情報保護法制において何らかの形で越境移転の制限を行っている[9]。

厳格に移転を規制する法制は、原則として移転を禁止し、例外的に安全が確保されることが認められる場合にのみそれを認める。その代表的な例である、欧州連合（EU）の2016年の一般データ保護規則（GDPR）は、次のように定める。まずGDPRは欧州経済領域（EEA）域外の第三国への個人データの移転を原則認めない。その例外として、(1) 欧州委員会が特定の国や地域が個人データについて十分な保護水準を確保していると認定することがある（十分性認定）[10]、(2) 事業者が適切な保護措置

---

[7] 個人情報保護法制の内実は国によって異なるものの、OECD プライバシーガイドライン 8 原則は（1）データ収集の制限、（2）データの質、内容の管理、(3) 目的明確化、（4）利用制限、(5) 安全保護、(6) 収集方針等の公開、(7) 個人主体の参加、(8) 管理者の責任を定める。OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. また、主要国の国内法制については、個人情報保護委員会「外国における個人情報の保護に関する制度等の調査」<https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/>参照。また、個人情報保護委員会(調査委託先:株式会社野村総合研究所)「日米欧における個人データの越境移転に関する実態調査」（令和 4 年 1 月 27 日）<https://www.ppc.go.jp/files/pdf/nichibeiou_ekkyouiten_report.pdf>参照。

[8] 本稿では「情報が国境を越えて移転する」ことを越境移転としている。ただし、その形態は多様である。デジタル貿易協定が規律するデジタル産品の輸出にせよ、個人情報保護法が規律する外国第三者への個人情報の提供にせよ、データの越境移転と等価ではない。データの越境移転規制については、渡辺翔太「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―」REITI Discussion Paper Series 19-J-067（独立行政法人経済産業研究所、2019 年）<https://www.rieti.go.jp/jp/publications/nts/19j067.html>；同「欧州司法裁判所 Schrems II 事件判決が越境データ流通に与える影響の考察―我が国の推進する DFFT 構想への影響を中心にして―」RIETI Discussion Paper Series 21-J-035（独立行政法人経済産業研究所、2021 年）<https://www.rieti.go.jp/jp/publications/summary/21070017.html>参照。

[9] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 1.

[10] EU, The General Data Protection Regulation, 2016/679, 4 May 2016, OJ L119, 1-88 [GDPR] <https://eur-lex.europa.eu/eli/reg/2016/679/oj> art 45. 十分性認定に際して委員会が考慮する要素としては、移転先の国における法の支配、人権及び基本的自由の尊重がなされていること、データ保護法、職業上の準則及び保護措置（効果的で執行可能なデータ

を取っていること[11]、(3) データの移転を義務付ける国際合意があること[12]、(4) 特例に該当すること[13]が定められている。英国がEU離脱に際して制定したデータ保護法も、同様に、原則として越境移転を禁止としながらも、適切な保護が保障されている場合に移転を許容する[14]。

これに対して大多数の国は、データの越境移転自体は禁止せずに、移転に条件を付ける方式を取る。そのような条件として、本人の同意を求めることが通例である。しかし、事業者と利用者が持つ情報の非対称性や同意の形骸化に鑑み、同意があれば移転先の事業者や国の体制がどうであれ移転を許容する考え方には問題がある。そこで、移転先の法制が安全であることを移転元の政府が認めていることを求めたり、移転先の事業者が適切な安全管理措置を取っていることを求めたりすることが多い。その適切性を判断するのにあたり、アジア太平洋経済協力のAPEC越境プライバシー規則（CBPR）等の国際基準を参照する場合がある[15]。

主体の権利、その個人データが移転されるデータ主体のための行政上及び司法上の救済を求める権利等)、独立した監督当局が存在し、効果的に機能していること等がある。

[11] Ibid art 46. 保護措置として拘束的企業準則（Binding Corporate Rules、BCR)、標準データ保護条項（Standard Data Protection Clauses)、アドホック契約（Ad Hoc Clauses)、行動規範（Code of Conduct)、認証（Certification）がある。

[12] Ibid art 48.

[13] Ibid art 49. 十分性認定基準や、事業者の適切な保護措置についてはそれぞれ細かく基準が定められており、かつ関連する判例も出ているが、本稿では割愛する。Svetlana Yakovleva and Kristina Irion, 'Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade' (2020) 10 International Data Pritacy Law 201.

[14] United Kingdom, Data Protection Act 2018, c.12 <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> Section 73. 管理者は、個人データを第三国又は国際機関に移転することはできない。しかし、例外として次の場合には移転が認められる。第 1 に、(1) 転送が法執行目的のいずれかのために必要であること、(2) (a)移転が十分性認定（adequacy decision）に基づくものであること、(b)(a)でない場合、適切な保護措置があること、(c)(a)(b)でない場合、特別な状況として認められること、(3)意図された受領者が第三国の関連当局若しくは関連国際機関である国際機関であること、又は管理者が指定管轄機関である場合には、法定条件を充足することである。第 2 に、個人データが英国以外の加盟国によって管理者又は他の管轄機関に最初に送信又はその他の方法で利用できるようにされた場合には、当該加盟国、又は法執行指令の目的上の管轄機関である当該加盟国に拠点を置く者が、当該加盟国の法律に従って移転を承認していることである。ただし移転が加盟国若しくは第三国の公共の安全、又は加盟国の本質的な利益に対する緊急かつ深刻な脅威の防止のために必要である場合と、時間的に認可を得ることができない場合には例外が認められている。

[15] CBPR を基準とする国としてタイがある。Thailand, Personal Data Protection Act, 2019, Sec. 28. 非公式英訳として次を参照。Personal Data Protection Act, B.E.2562 (2019) (Unofficial Translation) (27 May 2019) <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf>. アジア諸国の実践を分析した研究として、Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014); Graham Greenleaf, 'Asia's Data Privacy Dilemmas: 2014-2019' (2019) 4 Revista Uruguaya de Protección de Datos Personales 49.

個人情報保護法制では、事業設備等を自国領域内に置く義務は課されないことが多い。ただし、越境移転規制が厳格であるため、実質的に域内保存義務と同じ効果を持つ場合もある[16]。

② データ保護法制におけるデータの域内保存義務

データ保護法制は、非個人情報も含めたデータの取り扱いについて、事業者の安全管理義務等を定める法制を指す[17]。産業振興や安全保障のためにデータの管理を事業者に義務付けることが主な目的である。その際に、事業者が自国で事業を行うために必要な設備や自国で収集したデータを国内に留めることを義務付けることがある。理由は国によって異なるが、そのような規制を課すことで他国企業の参入障壁を上げて自国産業を保護することや、安全保障上の理由から機微なデータを他国に持ち出すことを防止することが挙げられる。

このような法制には、(1) データの複製を自国内に保管しておくことを義務付けるもの、(2) データの加工や保管を自国内で行うことを義務付けるもの（他国内におけるデータの保管の禁止)、設備を自国内に設置することを義務付けるもの、(3) (2) の義務に加えてデータの自国外への持ち出しを禁止するものがある[18]。

個人情報保護法制における越境移転規制にせよ、データ保護法制におけるデータの域内保存義務にせよ、ある規制や措置がデジタル貿易協定に抵触するかをカテゴリカルに判断することはできず、その内容、目的、効果等から、実質的に審査することが必要だと言える。

1-2 政府による情報へのアクセスとデータ・ガバナンス措置

一般に政府は自国領域内にあったり自国管轄下の事業者が保有していたりするデータにアクセスすることができる。実際に、政府は競争法や租税法等の執行、あるいは刑事捜査のために事業者の保有するデータにアクセスしたり、デジタル産品のソースコードや解析アルゴリズムの開示を求めたりすることがある。

近年では、これらの措置が、データ・ガバナンスの一環で行われることがある。デジタル産品のうち、データによって駆動される、いわゆるデータ・ドリブンな（data-driven）技術は、大量のビッグデータを生成、記録、処理、共有、利用する。これは一方ではデジタル産業の飛躍的な拡大を促したが、他方で、それがもたらす危険性が認識されるようになっている。データを用いたプロファイリングがなされる結果、個人の自律的選択

---

[16] 例えば欧州連合司法裁判所（CJEU）は、民間事業者が要配慮個人データを持っている場合（sensitive data set)、そのデータに対する監視を可能にするために EU の域内に留め置かなくてはならないという判断を出している。CJEU, C-293/12 and C-594/12, The Digital Rights Ireland and Others, 8 April 2014, EU:C:2014:238, paras. 66-68; C-203/15 and C-698/15, Tele2 Sverige v. Tom Watson, 21 December 2016, ECLI:EU:C:2016:970, para. 122.

[17] 中国・データ安全法（中华人民共和国数据安全法（2021 年 6 月 10 日採択）<http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>）や、インド・情報技術法（Information Technology Act 2000, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011）等がある。

[18] Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future', (187) OECD Digital Economy Papers (OECD ed, 2011).

が難しくなったり、社会的差別が助長されたりして、人々のプライバシーや安全が害される恐れがあるためである。そこで、技術の設計やデータの収集、処理、国境を越えた移転に対する制限等について、データ倫理（data ethics）に基づいて法制定を行なったり政策を策定したりする例が増えている[19]。

これまでにOECDは2019年5月にAIに関する理事会勧告を採択し[20]、それを受けて2020年6月に日本を含む有志国とEUが「AIに関するグローバルパートナーシップ」（GPAI）というイニシアティブを立ち上げた[21]。また、欧州委員会は2021年4月にAIについての新しい規則の提案を行なった[22]。その他、OECD専門家ネットワークが設けられたり[23]、欧州評議会で特別委員会が設けられたり[24]、各国レベルで指針を策定したりする動きがある[25]。

これらに共通する、データ・ガバナンスの基本的な原則として、人権の保護及び尊重がなされること、設計が倫理的であること、事業者や設計者がアルゴリズムについて説明責任を負うこと、プライバシーと安全が守られることが含まれる。具体的には、人権を侵害し得る技術販売の禁止、機微に関わるデータの転送や処理の制限、企業が技術を国内市場で販売するためにアルゴリズムやソースコードを規制当局に開示して検証あるいは承認を受けることの義務付け、外国技術基準の使用制限、国内技術基準を用いることの義務付け、ライセンス取得の義務付け等が行われ得る。

もっとも、外国技術基準の使用制限等がなされると外国事業者の参入が事実上難しくなる。また、法執行のためにコードの開示が義務付けられるとそれによって外国政府から技術が盗まれる危険性が生じる。そこで、これらの措置が、デジタル貿易協定上の義務と抵触しうる[26]。

---

[19] Jessica Fjeld and others, 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' [2020] Berkman Klein Center for Internet & Society <http://nrs.harvard.edu/urn-3:HUL.InstRepos:42160420>. データ倫理とは、データと情報の生成、記録、キュレーション、処理、頒布、共有、利用を含む、アルゴリズムがもたらす問題を評価し、道徳的に望ましい方向性を策定するための倫理である。

[20] OECD, *Recommendation of the Council on Artificial Intelligence* (22 May 2019) OECD/LEGAL/0449 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

[21] The Global Partnership on Artificial Intelligence <https://gpai.ai> accessed 7 February 2022.

[22] EU, Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, COM/2021/206 Final <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>. European Commission, White Paper on Artificial Intelligence: a European approach to excellence and trust (19 February 2020) <https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en>も参照。

[23] OECD Network of Experts on AI (ONE AI) <https://oecd.ai/en/network-of-experts> accessed 7 February 2022.

[24] Council of Europe, CAHAI (Ad hoc Committee on Artificial Intelligence) <https://www.coe.int/en/web/artificial-intelligence/cahai> accessed 7 February 2022.

[25] 各国の動向についてはOECD AI Policy Observatory <https://oecd.ai> accessed 7 February 2022 参照。

[26] Mishra Neha, 'International Trade Law Meets Ethics: A Brave New World' (2021) 53 NYU Journal of International Law and Policy 303.

1-3　問題の所在

①　　各国法制の調和化の限界

戦後の自由貿易体制は、政府の施策を相互運用可能なものにしながら企業に他国における責任を課すという、分散的なアプローチを基礎とする[27]。WTO体制も、貿易の自由化と非貿易関心事項である政策価値との調整を図りながら発展した経緯を有する[28]。もっとも、WTOは国際経済全体を支えるレジームにはならなかった。WTOが発足した1990年代は、多国間主義に基づく国際関係の法化（legalization）が進められた時期である。しかし、各国の経済体制や価値体系が多様化し、大国の自国第一主義が台頭する中で、今日では、価値を組み込んだ貿易体制を構築することの限界が顕在化している。

デジタル貿易について言えば、それが公権力によるガバナンスが必要であることに異論はないと思われる。データ・ドリブン経済の深化によって、公的ないし私的な監視による社会管理がなされたり、国家、サイバーセキュリティ、個人プライバシーが脅威にさらされたりすることが生じるためである[29]。しかし、そのガバナンスの中核となる、個人情報保護政策やデータ・ガバナンスは、経済秩序のみならず人権、文化、安全保障をも左右する。そのため、デジタル貿易とこれらの価値との調整は、その性質上、国際的な調和（harmonization）が困難である。

i　　プライバシー権の保障

まず、プライバシー権の内実や射程は、それぞれの社会における歴史、政治、文化的価値を反映したものである[30]。例えばこの権利が他の法規則に優位する憲法上の権利であるか、あるいは包括的な個人情報保護法があるかは、国や地域によって異なる。EUではデータ保護についての権利がEU基本権憲章上保障されている[31]。これに対して、中国のように個人の権利保護だけではなく、国家主権の維持を目的として個人情報の活用を行う国もある[32]。米国では、IT企業にデータを活用させることで新しい技術や産業を作っていくことを重視している。同国は連邦レベルでの包括的なデータ保護法は持っておらず、規律領域、及び州のレベルにおいて関連法を設けている[33]。

プライバシー権は市民権規約をはじめ主要な国際人権条約に規定されているが、それは政府からの検閲を受けないことや、私生活を第三者にみだりに晒されない権利に留ま

---

[27] John Gerard Ruggie, 'International Regimes, Transactions, and Change – Embedded Liberalism in the Post-War Economic Order' (1982) 36 International Organization 379.

[28] 小寺彰「WTO 体制における『非貿易的関心事項』の位置」小寺彰編著『転換期の WTO 非貿易的関心事項の分析』（東洋経済新報社、2003 年）1 頁参照。

[29] データ・ドリブン経済が引き起こすリスクを論じたものとして Gregory Shaffer, 'Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience' (2021) 20 World Trade Review 259. がある。

[30] Joseph HH Weiler, *The Constitution of Europe: 'Do the New Clothes Have an Emperor?' and Other Essays on European Integration* (Cambridge University Press 1999) 101.

[31] Charter of Fundamental Rights of the European Union (adopted on 2 October 2000, entered into force on 7 December 2000) OJ C 326, 26.10.2012, 391-407, art 8.

[32] 本稿 12 頁参照。

[33] Robert Wolfe, 'Learning about Digital Trade: Privacy and E-Commerce in CETA and TPP' (2019) 18 World Trade Review 63, 77.

る[34]。それに対して、デジタル時代に対応したプライバシー権は、データが容易に移転流通し、かつ大量に蓄積され利活用されるという性質を持つものであることから、本人がより積極的に自己の情報を積極的に管理することを認めるものである[35]。そのようなデジタル時代に対応したプライバシー権は国際的にも確立しているとは言えない。

確かに、近年では、高水準のプライバシー権を国際的に確立しようとする動きもある[36]。第 1 に、2013 年に改正された経済協力開発機構（OECD）のプライバシー指針は、加盟国が遵守するべき基準を示したものである[37]。指針は越境移転規制自体については直接定めないが、次の OECD 理事会勧告が出ている[38]。まず、加盟国は自国と他国との間における個人データの国際流通について指針に一致する継続する保護のレベルを保つために、他国が指針を実質的に遵守している場合、又は効果的な執行メカニズム及びデータ管理者により導入される適切な措置を含め十分な保護措置がある場合、流通を制限することを控えるべきである[39]。そして、個人データの国際流通に対するいかなる制限も、顕在するリスクに比例した制限でなければならず、データの機微性並びに処理の目的及び状況を考慮しなくてはならない[40]。この勧告は越境移転の方式として参照されることが多い。しかし同勧告は拘束力を有さないだけではなく、中国を含めた OECD 非加盟国に影響を及ぼさない。

第 2 に、欧州評議会の 108 号条約改正議定書は、データの越境移転規制を含めたデータ保護規律を行う多数国間条約として詳述に値する[41]。条約 14 条は、データの越境移転に関して次のように定める。まず、締約国は個人データの保護のみを目的として、この条約の他の締約国の管轄下にある受取人への当該データの移転を禁止したり、特別な権限を与えたりしてはならない。ただし、(1) 他の締約国への移転、あるいは当該他の締約国から非締約国への移転が条約の規定を回避することにつながるという現実的かつ重大なリスクがある場合、又は (2) 締約国が、地域的国際機関に属している諸国によって共有された、調和化された保護規則に拘束されるのであれば、その限りではない。

---

[34] International Covenant on Civil and Political Rights (adopted on 16 December 1966, entered into force on 23 March 1976) 999 UNTS 171, art 19.

[35] 自己情報管理権について山本龍彦『プライバシー権を考える』(信山社、2017 年) 3、15 頁参照。プライバシーとデータ・プライバシーとを区別する見解として、Bygrave (n 21) 3.

[36] Lee Andrew Bygrave, *Data Privacy Law* (Oxford University Press 2014) 31.

[37] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013* <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

[38] OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), C(80)58/FINAL, 11 July 2013, C(2013)79.

[39] Ibid para. 17.

[40] Ibid para. 18.

[41] 欧州評議会の 1981 年のデータ保護に関する 108 号条約（The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108)）を改正した条約が 2018 年改正議定書である。Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, CETS No. 223.

そして、受取人がこの条約の締約国ではない国又は国際機関の管轄下にある場合、個人データの移転は、この条約の規定に基づく適切な保護レベルが確保される場合にのみ行うことができる。適切な保護レベルは（1）当該国の法律又は国際機関の条約等、（2）移転とそれ以降の処理に関与する者によって採用され実施される法的拘束力がありエンフォースできる文書において記載された個別の（*ad hoc*）、又は承認された標準化された保障措置によって確保することができる。

ただし、これらの規則に関わらず、次の場合には、各締約国は個人データの移転を行うことができる。すなわち、（1）データ主体が適切な保護措置がない場合に生じるリスクを知らされた上で、明示的、具体的かつ自由な同意をした場合、（2）データ主体が特定の利益のために特に必要とされる場合、（3）優先されるべき正当な利益、特に重要な公共の利益が法律で規定されており、当該移転が民主主義社会において必要かつ適切な措置である場合、（4）そのような移転が表現の自由のために、民主主義社会において必要かつ比例的な措置をなすことである。また加盟国は、監督当局がそのような移転を禁止、停止、あるいは条件付けできることを定める。

このように、改正 108 号条約は、越境移転の必要性を踏まえながら、データに対する権利を保障しようとするものとして評価できる。ただし同条約には、米国、中国をはじめとした主要国の参加が見込める状況ではない。

第 3 に、アジア太平洋経済協力（APEC）では、越境プライバシー保護ルール（CBPR）が採択されており、日本、米国、韓国、台湾等が参加している。CBPR は APEC から認定を受けた各国の認証機関が、個人情報保護に関する一定の条件を満たした事業者を認証する仕組みである。この認証を得ることによって、事業者の個人情報保護の信頼性を確保することができる。他方で、CBPR は加盟国に国内法の改正等を義務付けるものではなく、上記の条約とは性格を異にする。また 2015 年に改正されたものの、利用者保護の観点から十分な水準であるとは言えないという批判がある[42]。

他にも国際的なフォーラムにおける規範形成はなされているが[43]、いずれも拘束力がなかったり高水準ではなかったりして、デジタル貿易にインパクトを与えるものではない。

これに伴い、デジタル貿易協定においてプライバシー保護をどのように位置付けるかについての議論は収斂していない[44]。一方では、個人情報に対する権利は基本的人権であるとして、その優位性を維持する立場がある。これを支持する根拠の1つとして、経済的利益とデータ保護とを衡量することは、より強固に守られるべきデータ保

---

[42] Greenleaf, 'Asia's Data Privacy Dilemmas: 2014-2019' (n 15) 69. 改正前の批判として、Greenleaf, *Asian Data Privacy Laws* (n 15) 536.EU 委員会は、CBPR に基づく第三国への移転は日本の個人情報保護法で保障されるよりも明らかに低いレベルであると指摘している。Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, 19.3.2019, para. 79 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0419>.

[43] Bygrave (n 36) 31.

[44] Ibid 66; SA Aaronson and P Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 Journal of International Economic Law 245.

護の個人や社会の利益を軽視するという議論がある[45]。もっとも、このようにプライバシー保護の優位性に例外を認めない考え方には、批判も多い[46]。デジタル貿易の文脈においては、各国法制の相互適合性（compatibility）を確保する等の方式が取られることが多い。

ii　　安全保障

データ保護法制において事業者に安全管理義務を課したり、政府のデータへのアクセスを容易にしたりすることは、当該国の安全保障上の措置でもある。そのような措置は、貿易制限的になることがある。しかし、サービスの貿易に関する一般協定（GATS）14条の2をはじめ、通商協定では安全保障例外が設けられるのが通例である[47]。2019年ロシア・貨物通過に関する措置事件では、WTOパネルは、加盟国の貿易制限的措置が関税及び貿易に関する一般協定（GATT）21条の安全保障例外に当たるかは、当該加盟国の完全な自己判断によるのではなく、パネルの客観的審査に服することを示した[48]。しかし、ある国にとっての安全保障上の脅威が何であるか、定型的な基準はない。そのため、デジタル貿易協定において例外条項が濫用されるリスクは大きい[49]。

もっとも、特に高水準のデジタル貿易協定は加盟国間の信頼を基礎として締結される。データの自由流通が安全保障上の脅威になるとしたら当該国は協定の締結をしない。このことから協定上の義務と安全保障との緊張関係は表面化しにくいし、実際、デジタル貿易の文脈においても主要な争点にはなっていない。

---

[45] Svetlana Yakovleva and Kristina Irion, 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation' (2020) 114 AJIL Unbound 10 <https://www.cambridge.org/core/product/identifier/S2398772319000813/type/journal_article>.

[46] Yakovleva and Irion (n 13) 205. 2014 年に米国企業を対象に行われた調査において、約 8 割の企業が EU のデータ保護のために取らなくてはならない措置がビジネスをオンラインで行う際の最大の障壁だと考えているというものがある。U.S. Census Bureau, Foreign Trade, U.S. International Trade Data <https://www.census.gov/foreign-trade/data/index.html> accessed 7 February 2022.

[47] 関税及び貿易に関する一般協定についてのものであるが、安全保障例外の解釈については川瀬剛志「WTO 協定と安全保障貿易管理制度の法的緊張関係：2019 年日韓輸出管理紛争をめぐる覚書」『上智法学論集』64 巻 3・4 号（2021 年）75 頁参照。

[48] WTO, *Russia - Measures Concerning Traffic in Transit - Report of the Panel* (5 April 2019) WT/DS512/R, paras. 7.53-7.82. 解説として、川瀬剛志「【WTO パネル・上級委員会報告書解説㉛】 ロシア―貨物通過に関する措置（DS 512） ――安全保障例外（GATT21 条）の射程――」RIETI Policy Discussion Paper Series 20-P-004（独立行政法人経済産業研究所、2020 年）<https://www.rieti.go.jp/jp/publications/pdp/20p004.pdf>.

[49] 「安全保障に関する間主観的な理解が、国家と人間の安全保障の分断を容易にしている」ことを指摘するものとして、White Nigel D and Davies-Bright Auden, 'The Concept of Security in International Law' in Robin Geiß and Nils Melzer (eds.), *The Oxford Handbook of the International Law of Global Security* (Oxford University Press 2021) <http://opil.ouplaw.com/view/10.1093/law/9780198827276.001.0001/law-9780198827276-chapter-2>.

②　価値を基盤にした貿易体制構築の意義と限界

以上のように、デジタル貿易については、各国の価値を調和化させることが本質的に困難である。それに加えて、主要な経済圏が重視する価値をグローバルに普及させるアプローチが明確に異なっているという特徴もある。

まず、米国はデータの利活用は基本的に企業に委ねており、基本的に自由貿易体制の下でグローバルなデータ・ガバナンスを構築しようとしている。また米国にはプライバシーを規律する包括的な連邦法は存在せず、消費者保護としてオンラインプライバシーを規制している州が一部あるのに留まる[50]。後述するように、米国は非貿易的事項である個人情報保護やプライバシー規制については、各国の相違を容認しつつ、相互に運用可能であれば足りるとするアプローチを取る。

これに対して、EUは規範の拡散（norm diffusion）を通じて他国の法制に影響を及ぼす政策を2000年頃から展開している。すなわち、グローバルな大手企業をEUの高水準のガバナンスに服させることによって、企業の本国が同程度の法制を構築するように促す方式である。データの越境移転規制を定めるデータ保護指令とGDPRはそのような「ブリュッセル効果」の代表的な例である[51]。

他方で、EUはデジタル貿易の高度な自由化は部分的にしか行っていない。また、EU議会が2020年に提唱し始めた「デジタル主権」政策は、GDPR等を外国事業者に遵守させるのと同時に、米中に遅れを取るEUの事業者を育成する狙いもあり[52]、保護主義的な側面もあると言える。

米国とEUのアプローチは異質であるものの、表現の自由を含めた人権保障であるとか、民主主義の維持が重要であることについては共通の認識がある。そこで、2021年6月、米国とEUは貿易技術評議会（TTC）を設立し[53]、「共有された民主主義的価値」を基礎に貿易を進めることを謳っている。

これらとは対照的に、中国は、国有企業が中核となって、産業連関とサプライチェーンの高度化を主導し、中国の経済発展に必要な国際環境を構築する方向性を明らか

---

[50] カリフォルニア州などで、消費者保護としてオンラインプライバシー法がある(California Consumer Privacy Act, California Civil Code Sec. 1798.100, signed into law on 28 June 2018.)。連邦レベルでプライバシー保護を行う法案が提出されたことはあるが成立していない。

[51] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

[52] Sean Fleming, 'What is digital sovereignty and why is Europe so interested in it?,' (World Economic Forum, 15 March 2021) <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>.

[53] European Commission, Press Release, 15 June 2021, EU-US launch Trade and Technology Council to lead values-based global digital transformation (15 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990>.

にしている[54]。国家情報法[55]、インターネット安全法[56]、データ安全法[57]には、データを中国の国益のために用いる方針が明示されている。また電子商取引について、中国は、加盟国はインターネット主権（internet sovereignty）とサイバーセキュリティを尊重するべきであり、各国の法制、秩序に沿って行われるべきだという立場を明示している[58]。そのため、中国が当事国になるデジタル貿易協定は高水準の自由化を義務付けるものではない[59]。

他方で、中国は東南アジア、パキスタンやスリランカなどの南アジア、アフリカ、中南米地域などの途上国に道路、鉄道、港等のインフラを提供する「一帯一路」政策を実施している。そして2015年頃からその参加国において「情報回廊」の構築に注力している（デジタルシルクロード、数字丝绸之路）[60]。すなわち中国の大手IT企業らが、これらの参加国に海底ケーブルや通信衛星を含めた通信インフラを提供している。そこで参加国が中国のデータ・ガバナンスに倣うことがある。また、インフラの提供によって、通信機器の規格やネットワークプロトコル等についての中国の基準を対象国に導入することになる（「北京効果」）[61]。さらに、中国はインターネット等の標準や規則を策定するICANN、インターネット技術タスクフォース（IETF）や、国際通信を所轄する万国通信連合（ITU）などに積極的に参画することで、各フォーラム

---

[54] 渡邉 真理子 ＝加茂 具樹＝川島 富士雄＝川瀬 剛志「中国の CPTPP 参加意思表明の背景に関する考察」RIETI Policy Discussion Paper 21-P-016 （独立行政法人経済産業研究所、2021 年）<https://www.rieti.go.jp/jp/publications/summary/21090002.html> 参照。

[55] 中华人民共和国国家情报法 1 条、2017 年 6 月 27 日第十二届全国人民代表大会常务委员会第二十八次会议通过 <http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml>。

[56] 中华人民共和国网络安全法 1 条、2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过 <http://www.cac.gov.cn/2016-11/07/c_1119867116.htm>。

[57] 中华人民共和国数据安全法 1 条、2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过 <http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>。

[58] World Trade Organization, Joint Statement on Electronic Commerce, Communication from China, 24 April 2019, INF/ECOM/19, Section 3.3.

[59] 川瀬剛志「『ルール』から見た中台の TPP 加入へのハードル」（東洋経済オンライン、2021 年 9 月 30 日）<https://toyokeizai.net/articles/-/459107> 参照。

[60] 《推动共建丝绸之路经济带和 21 世纪海上丝绸之路的愿景与行动》（2015 年 3 月）<http://2017.beltandroadforum.org/n100/2017/0407/c27-22.html>参照。経緯については伊藤亜聖「中国の『デジタルシルクロード』構想 ～背景、関連文書、企業行動～」日本国際問題研究所『令和元年度外務省外交・安全保障調査研究事業 中国の対外政策と諸外国の対中政策』（令和 2 年 3 月）119、123 頁参照。「デジタルシルクロード」の分析として Jonathan Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (Profile Books Ltd 2021); 持永大『デジタルシルクロード』（日本経済新聞出版、2022 年）参照。

[61] Congyan Cai, *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously* (Oxford University Press 2019) 162; Matthew S Erie and Thomas Streinz, 'The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance' (2021) 54 New York University Journal of International Law and Policy 1, 36.

における規範形成に影響を及ぼしている[62]。これらの中国の政策は、長期的には途上国におけるデジタル貿易の水準を規定しうる。

中国の他にも、国家主導でデジタル貿易を規制しようとする動きが見られる。例えば、ロシア、インド、ベトナム等が同様にデータの越境移転を制約している[63]。

最後に、日本は「信頼性のある自由なデジタル流通」（DFFT）を標榜し、WTOの電子商取引交渉を主導している。これは、「プライバシーやセキュリティー、知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す」政策である[64]。しかしその「信頼」は、敢えて価値中立的に位置付けられている。日本は中国をはじめとして、必ずしも民主的ではない国家体制を持つ国とも貿易を強化する必要があることがその背景にある。日本のアプローチについては第4節で考察を加える。

③　　小括

個人情報保護にせよ、データ・ガバナンスあるいはデータ倫理にせよ、データの利活用に関して国際的に確立した基準はなく、各国法制には大きな相違がある。そのため、現状では同志国（like-minded countries）の間で高水準のデジタル貿易協定が締結される一方、一部の国ではデータローカライゼーションが強化されている。この限界を踏まえた上で、第2節ではデータの越境移転規制について、第3節ではデータ・ガバナンスについての、貿易協定における規律のあり方を検討する。

2.　データの越境移転規制

2-1　サービスの貿易に関する一般協定の意義と限界

データの越境移転は電子商取引としてGATSの適用対象になり得る。もっとも、GATSはプライバシー保護、サイバーセキュリティ、データ倫理等を直接には規律していない[65]。個人情報保護法制上の措置が、GATSが定める実体義務の違反に当たるのか

---

[62] Erie and Streinz (n 61) 44. また、中国が国際ルールの形成、援用を通じてグローバル経済秩序形成に影響力を高めていく「制度に埋め込まれたディスコース・パワー」（制度性話語権）を追求する姿勢について、渡邉 真理子＝加茂 具樹＝川島 富士雄＝川瀬 剛志「中国の CPTPP 参加意思表明の背景に関する考察」RIETI Policy Discussion Paper Series 21-P-016 （独立行政法人経済産業研究所、2021 年）<https://www.rieti.go.jp/jp/publications/summary/21090002.html>参照。

[63] 各国法制については、個人情報保護委員会「外国における個人情報の保護に関する制度等の調査」（令和4年）＜https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/>参照。瓜生・糸賀法律事務所編『個人情報越境移転の法務』（中央経済社、2020年）；西村あさひ法律事務所編他『個人情報保護法制大全』（商事法務、2020年）；西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」<https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf>参照。

[64] IT 総合戦略本部「デジタル時代の新たな IT 政策大綱」（2019 年 6 月 7 日決定）19 頁。

[65] GATS におけるデジタル貿易の規律については既に検討が尽くされていると思われるので本稿では取り扱わない。東條吉純「WTO 協定による越境データ流通の規律と限界」RIETI Discussion Paper Series 20-J-011（独立行政法人経済産業研究所、2020 年）<

を立証するためには、規制の対象になっている個々の電子商取引について、(1) それが約束書に含まれること (2) 含まれたとして、それがGATSの定める義務に違反すること[66]、かつ、(3) GATS14条で認められている一般的例外、若しくは14条の2で認められている安全保障例外に当たらないことを示す必要がある。従って、あるデータローカライゼーション措置がGATSに違反することを示すのは容易ではない。そのためこの協定は「グローバルな越境データ流通網の構築という観点からは、明らかに不十分であると言わざるを得ない」[67]。

2-2 デジタル貿易協定における個人情報保護法制の位置付け

デジタル貿易協定はこのようなGATSの限界を克服するために締結されている。ただし冒頭で述べたようにその水準は協定によって異なる。個人情報保護に関して、その内容は、(1) 各加盟国・地域に同等の保護水準確保を義務付けるもの、あるいは、調和化を義務付けるもの、(2) 相互運用性 (inter-operability) の強化を義務付けるもの (個人情報保護については各国が異なるアプローチを取り得ることを踏まえて、異なるレジーム間の適合性 (compatibility) を促進するもの)、(3) 各国の裁量を重視するものに大別することができる。これらは相互に排他的な分類ではなく、同じアプローチを取るものであっても、自由化の義務付け内容が異なる結果、加盟国が取るべき措置の内容が相違することもある。

① プライバシー権の高水準保護の維持

個人情報保護について最も厳格なアプローチを取るのが EU の締結する諸協定であり、それらは当事国に対して同等の保護水準を確保することを義務付ける。前述したように、EU は GDPR については妥協しない立場を取っている。欧州委員会は 2018 年 1 月に、EU が通商・投資協定を交渉する際に依拠するべき、データ流通と個人データ保護に関する共通条文を採択している[68]。

日＝EU 経済連携協定、メキシコ＝EU 自由貿易協定では、デジタル貿易についての規則採択は先送りにされた。他に、豪州、チリ、インドネシア、メキシコ、ニュージーランド、チュニジアとデジタル貿易協定の締結が予定されている。なお、EU は環大西洋貿易投資パートナーシップ (TTIP)[69]と新サービス貿易協定 (TiSA)[70]においてデジタ

---

https://www.rieti.go.jp/jp/publications/dp/20j011.pdf> ; 阿部克則「データローカライゼーション措置と国際経済法上の規律 : WTO と TPP における法的位置づけ」『フィナンシャル・レビュー』5 号 (2019 年) 25 頁; Susannah Hodson, 'Applying WTO and FTA Disciplines to Data Localization Measures' (2019) 18 World Trade Review 579; Neha Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?' (2020) 19 World Trade Review 341.

[66] GATS, art 6(1).

[67] 東條「前掲論文」(注 65) 2 頁参照。

[68] European Commission, Horizontal Provisions for Cross-Border Data Flows and For Personal Data Protection (in EU Trade and Investment Agreements) (18 May 2018) <https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf>.

[69] EU と米国間で、貿易投資の自由化を進める条約として、2014 年に交渉が開始されたが 2019 年 4 月に停止された。

[70] EU 及び日本、米国を含む 22 の国及び地域で、デジタル貿易の他、金融、医療、交通

ル貿易の自由化を進めようとしたが、いずれも締結には至らなかった。

EU＝英国通商協力協定

EU＝英国通商協力協定（TCA）第 2 部第 3 篇の 201 条は、越境データ流通を確保するために、越境データ流通は特定の方式で制限されてはならないことを定める[71]。

続いて、TCA202 条は個人データの保護とプライバシーについて次のように定める。双方当事者は、個人が、個人データの保護とプライバシーに対する権利を有しており、それらの高い水準がデジタル経済における信頼と貿易の発展に貢献することを認識する[72]。

そして協定は、締約当事者の法律が、移転データの保護のために一般的な適用条件の下で移転を可能にする手段を規定している場合には、個人データ及びプライバシーの保護に関する措置を締約国が採用又は維持することを妨げるものではないことを定める[73]。なお、ここでの一般的な適用条件とは、客観的に定式化された条件において、不特定多数の事業者に水平的に適用される[74]。このようにして EU と英国は自らの厳格な個人情報保護法の実施とデジタル貿易促進とを可能にしている。

カナダ＝EU 包括的経済連携協定

カナダ＝EU 包括的経済連携協定（CETA）16 章は、電子商取引について章を設ける[75]。もっとも CETA は TCA とは異なり、国際基準に則って基準の調和化を図る。

協定 16.2 条は、両当事者が、WTO 規則が電子商取引に適用されることを確認している。他方で、同条は、協定の他の規定に基づく締約国の義務に従った場合を除き、電子的手段により送信される配信を許可する義務を締約国に課すものではないとする。各締約国は、電子商取引に従事するユーザーの個人情報を保護するための法律、規制若しくは行政措置を採用し、又は維持すべきであり、その際には、両締約国が加盟する関連国際機関のデータ保護に関する国際基準を十分に考慮しなければならない。

協定 16.4 条は、各締約国は、電子商取引に従事する利用者の個人情報を保護するための法律、規制若しくは行政措置を採用し、又は維持しなければならないと定める。各

についての自由化を進める条約として、2014 年に交渉が開始されたが 2019 年に停止された。

[71] EU-UK Trade and Cooperation Agreement (signed on 30 December 2020, entered into force on 1 May 2021) OJ L 444, 31.12.2020, 14-1462. TCA, art 201. すなわち、第 1 に、加盟当事者の領域において、加工のためにコンピューター設備又はネットワーク要素（network elements）の使用を求めてはならない。 第 2 に、加盟当事者の領域において保管又は加工のためにデータのローカライゼーションを求めてはならない。第 3 に、相手加盟当事者の領域においてデータを保管又は加工することを禁止してはならない。第 4 に、加盟当事者の領域におけるコンピューター設備あるいはネットワーク要素の使用を越境データ移転の条件にしてはならない。

[72] TCA, art 202(1).

[73] Ibid.

[74] Ibid Note 34.

[75] Comprehensive Economic and Trade Agreement (signed on 30 October 2016, provisional application started on 21 September 2017) <https://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/>.

締約国は、電子商取引に従事する利用者の個人情報を保護するための法令若しくは行政措置を採用し、又は維持するものとし、その際には、両締約国が加盟する関連国際機関のデータ保護に関する国際基準を十分に考慮する。

②　相互運用性強化

これに対して、それぞれの国内法制が異なることを前提にしつつ、相互運用性（inter-operability）あるいは相互適合性（compatibility）を高めるアプローチがある。このアプローチは、国内法制が同じ高水準において個人情報を保護するところまでは求めてはいない点で、前節のアプローチとは異なる。

米国・メキシコ・カナダ協定及び米国自由貿易協定

米国が主導する条約は、概ねこの相互運用性を確保するアプローチを取る。その代表的な例は、米国・メキシコ・カナダ協定（USMCA）19 章である[76]。具体的には、協定 19.8 条 2 は、個人情報保護法をデジタル貿易の利用者のために作ること、その指針として CBPR と OECD のプライバシー指針を考慮することを加盟国に義務付けている。

さらに協定 19.8 条 6 は締約国が個人情報保護に関して異なる法的アプローチを取り得ることを認識し、これらの異なるレジーム間の適合性（compatibility）を促進するメカニズムの開発を奨励すると定めている。締約国は、それぞれの管轄におけるメカニズムについて情報交換し、適合性を高めるためにこれらのメカニズムを拡張したり他の適切な取り決めをしたりすることを検討すること、また、APEC・CBPR システムが個人情報を保護しつつ、越境情報移転を提供するのに有効なメカニズムであることを認識することについても定めがある。

そして協定 19.11 条は越境移転の禁止又は制限を原則禁止しつつ、正当な公共政策の目的を達成するために必要なものであって、恣意的若しくは不当な差別の手段又は偽装された貿易制限を構成しないこと、目的を達成するために必要な範囲を超えて、情報の移転に制限を課さないことを条件として、その例外を認めている。ただし、ある措置が、他の締約国のサービス供給者に不利益になるように競争条件を修正するような様態で、国境を越えて行われることのみを理由に異なる扱いを与える場合には、本項の条件を満たさない。

また、日本と米国はデジタル貿易協定を締結したが、そこでもこのアプローチが採用されている。協定 15 条 1 は「各締約国はデジタル貿易の利用者の保護者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」ことを定める。さらに 15 条 3 は「各締約国は、個人情報を保護するために各締約国が異なる法的な取組み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間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」として、法制度それ自体の調和化は求めていない。しかし、15 条 4 は「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

[76] United States-Mexico-Canada Agreement (entered into force on 1 July 2020) art 19.14 <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>.

識する」として、移転を規制することを当事国に認めている。

米国は他に、豪州、バーレーン、CAFTA（コスタリカ、ドミニカ共和国、エルサルバドル、グアテマラ、ホンジュラス、及びニカラグア）、チリ、コロンビア、韓国、モロッコ、オマーン、パナマ、ペルーとの FTA で電子商取引章を設けている[77]。ただし、豪州 FTA、オマーン FTA、ペルーFTA のように、消費者保護の重要性については規定を置くが、個人情報保護についての独立した規定を置いていないものもある[78]。また、韓国 FTA のように、個人情報保護の重要性を認識しつつ、情報流通に不必要な制約を課さないことを約するのに留まるものもある[79]。USMCA と日米デジタル貿易協定がプロトタイプになるかは、今後の進展を見る必要がある。

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 も相互適合性を維持するアプローチを取っている。締約国は「個人情報保護が経済的及び社会的な利益を向上させ、消費者の信頼向上に資すること」を認める。そのため、締約国は、電子商取引の利用者の個人情報の保護について定める法的枠組みを採用し、維持する。なお、締約国は、個人情報の保護のための法的枠組みを作成するに当たり、関係国際機関の原則及び指針を考慮すべきとされている。

CPTPP14.8 条はまず移転自体は自由に行うことを原則にして、しかし個人情報保護については適合性を促進することを奨励する。さらに 14.11 条は、データの越境移転での規制の例外については、移転そのものについて各国が規制要件を定めることと、かつ、公共政策目的においてその制限をすることを認めている。

次に、14.11 条は次のことを定める。締約国は、各締約国が情報の越境移転について条件を定めることを認める。ただし対象国の事業の実施のために行われる場合には、個人情報を含む情報の電子的手段による国境を越える移転を許可するものとされる。さらに、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、次の条件を満たすことを必要とする。すなわち、(1) 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、(2) 目的の達成のために必要以上に情報の移転に制限を課するものではないことである。

日英包括的経済連携協定

日英包括的経済連携協定（CEPA）も高いデータ保護基準を維持しながら、両国間の

---

[77] USTR, Digital Trade & E-Commerce FTA Chapters <https://ustr.gov/issue-areas/services-investment/telecom-e-commerce/e-commerce-fta-chapters> accessed 7 February 2022.

[78] Australia-US FTA (entered into force on 1 January 2005) <https://ustr.gov/sites/default/files/uploads/agreements/fta/australia/asset_upload_file508_5156.pdf>; Panama-US Trade Promotion Agreement (entered into force 31 October 2012) <https://ustr.gov/sites/default/files/uploads/agreements/fta/oman/asset_upload_file650_8842.pdf>.

[79] Korea-US Free Trade Agreement (entered into force on 15 March 2012) art 15.8 <https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf>.

データ流通を確保しようとする[80]。協定 8.80 条は個人情報保護について次のように定める。まず各締約国は、電子商取引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、又は維持すること、個人情報保護のための法的枠組みを構築するにあたり、関連する国際機関の原則及びガイドラインを考慮しなければならないことを定める。

しかし、各締約国は、個人情報を保護するために異なる法的アプローチを取る可能性があることを認識する。そして、その異なるレジーム間の適合性（compatibility）を確保するように努める。この仕組みを取ることには、英国にとって、保護水準の高いデータ保護法の枠組みを維持しながら、日本との電子商取引の自由化を進めることができるという利点がある。

チリ＝ニュージーランド＝シンガポール・デジタル貿易協定

チリ＝ニュージーランド＝シンガポール・デジタル貿易協定（DEPA）は、関連する国際団体の原則や指針を考慮して、個人情報保護のための法的枠組を策定することを義務付けている[81]。また DEPA は 4.2 条 2 の中でその基本原則を特定している。もっとも、4.2 条 5 は加盟国の法制に対するアプローチが異なることを認めて、その適合性と相互運用性を強化するための具体的なメカニズムを促進させることを定めている[82]。

③　裁量重視

デジタル貿易協定を締結する目的が貿易障壁を減らす、あるいは撤廃することにある以上、データ流通への制限に対して各国の裁量を広く認めるものは少ない。

しかし、その中でもRCEPはそのような協定として位置づけることができる。RCEPの電子商取引章は一方では、貿易促進のための協力義務を定める[83]。しかし、12.14条は「各締約国がコンピューター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」と定める。さらに12.15条は「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」を取ることを認め、それが電子商取引規則に違反しているかを紛争解決手続で争えないことを定める。

ただし、12.16条において、デジタル産品の扱いやソースコードの開示命令の禁止等

---

[80] Japan-UK Comprehensive Economic Partnership Agreement (signed on 23 October 2020, entered into force on 1 January 2021) <https://www.mofa.go.jp/files/100111408.pdf>. 情報の越境移転への制限禁止、設備の自国領域内設置要求の禁止、ソースコードや暗号情報の開示要求禁止等を規定する。

[81] Singapore, Chile and New Zealand, Digital Economy Partnership Agreement (signed on 12 June 2020) <https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement>. そのような原則として、収集への制限、データの質、目的の特定、使用の限定、安全セーフガード、透明性、個人の参加及びアカウンタビリティが挙げられている。

[82] DEPA は、デジタル包摂性の拡大にコミットする点でも、着目に値する。さらに、同協定は中小企業（SME）が利用できる仕組みの充実を図るものである（電子請求書、エクスプレス輸送、電子決済の相互運用性等がある）。

[83] 加盟国の領域から他の加盟国の領域へのサービス提供（サービス貿易の第 1 モード）については、締約国は自国の現在の慣行を維持する（12.11 条 1 項）。

についても対話をすること、協定発効後にデジタル取引の紛争解決の適用について見直しを行う義務も規定されている。また、12.17条は、締約国は誠実に協議を行う義務を負うこと、またそれによって意見の相違を解決することができない場合にRCEP合同委員会に付託することができることを定める。

確かに、RCEPは日本、中国、韓国との間で締結された初めての経済連携協定であるし、参加15カ国の国内総生産（GDP）の総計は世界GDPの3割であることから期待も大きい。しかしデジタル貿易については、その効果は限定的なものに留まっていると言える。

2-3　小括

デジタル貿易協定では自由化義務のレベルが協定によって異なっており、低水準のものであれば個人情報保護の問題は顕在化しない。しかし、高水準の協定を締結するときには、個人情報保護法制におけるデータの越境移転規制にせよ、安全保障目的等でのデータローカライゼーションにせよ、データ流通への制限について合意できるかは、協定締結の分岐点である。これまで締結された協定については、EUを別にすれば、個人情報保護法制の水準の相違は許容し、相互に信頼できる国との間で運用性を強化していくアプローチが取られることが多い。

3.　データ・ガバナンス措置

3-1　サービスの貿易に関する一般協定の意義と限界

次に、データ・ガバナンス措置について検討する。GATS6 条 1 項では、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義務を負う。そして、GATS6 条 5 項(a)は、「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」によって「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」と定める。また、GATS6 条 5 項(b)は、加盟国はこの義務を遵守しているかを決定するのにあたり「関係国際機関の国際的基準」を考慮することを定める。そこで、データ・ドリブン技術に対する規制が国際基準に沿っておらずその国独自のものであるなどして、「合理的に予想され得なかった」と言える場合には、この条項に違反し得る。

なお、ここでの「関係国際機関」とは、少なくとも WTO 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であるので、インターネット技術特別調査委員会（IETF）や電子電気学会（IEEE）等、国家の参加を認めていない標準設定機関は含まれない[84]。

もっとも、データ・ガバナンス規制は、GATS14 条 a 項が定める「公衆の道徳の保護」として正当化される余地が大きい。特に、データ・ドリブンな技術によって差別が助長されることを防いだり、技術の透明性を高めて設計者の説明責任を求めたりする規制については、例外として認められると思われる。

なお、ブラジル租税措置事件では、ブラジルが実施した、自動車に対する工業品税の

[84] Neha (n 26) 374; Gabrielle Marceau, 'Evolutive Interpretation by the WTO Adjudicator' (2018) 21 Journal of International Economic Law 791.

引き上げ、ブラジル国内での一定の製造工程の実施、研究開発への投資等と結び付け、情報通信機器分野における内外差別的な優遇税制措置等を巡り、日本がパネル設置を要請した[85]。上級委員会は、文脈依存的に政策上の問題に照らして条約を解釈し、社会的包摂を促進するために課された措置は、同条項の「公衆の道徳」の範囲に含まれるとした。各加盟国は、自国の価値観や制度に沿って、何が公共の道徳に反するかを決定する裁量を有している。この点について国によって道徳の内容は異なるため、リスクの存在を特定したり問題となっている道徳の基準の正確な内容を特定したりする必要はないとする指摘がある[86]。

また、前節の分析と重複するが、データ・ガバナンス規制は、GATS14 条 c 項 2 号が定める「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」のための法令の実施だとして正当化される余地もある。

3-2　デジタル貿易協定における位置付け

①　　ソースコード又はアルゴリズムの開示命令の禁止

このように例外事由が広いため、高度な自由化を進めるためには GATS のみでは限界がある。そこで、デジタル貿易協定においてデータ・ガバナンスについての具体的規定を置くものが出てきている。

冒頭に述べたように、高水準のデジタル貿易協定においては、ソースコード又はアルゴリズムの開示を自国におけるサービス提供の条件とすることは禁止される。これに対して、事業者の説明責任は基本的な原則として認められる。また、条約も法執行目的において例外を認めることが多い。例えば、USMCA19.16 条 2 は規制当局が個別の捜査、検証措置の実施、あるいは司法手続のために、ソースコード等へのアクセスを許容している。日米デジタル貿易協定 17 条 2 も、「特定の調査、検査、検討、執行活動又は司法手続のため」に同様にアクセスすることを認める。日英 CEPA8.73 条は、同旨の規定に加えて事業者の自発的な開示については、開示命令禁止規定は適用されないことを定める。これらはデジタル産品を提供する企業と輸入国の正当な公共の利益との均衡を取るものとして評価できる。

なお、法執行の一部としてソースコード等の開示を求めるのか、あるいは安全保障上の目的や技術を盗取することを目的として開示を求めるのかの区別を予め付けることはできない。権限ある規制当局あるいは司法当局による開示命令であれば前者だと推定されるが、ソースコード等がその目的通りに取り扱われる保障はない。もっとも後者の目的でデータ開示を求める国とは、高水準のデジタル貿易協定は締結しないであろうから、この点に関して具体的な問題は生じにくいと思われる。

---

[85] WTO, *Brazil - Certain Measures Concerning Taxation and Charges - Report of the Appellate Body* (13 December 2018) WT/DS472/AB/R. 解説として、東條吉純「【パネル・上級委員会報告書解説㉙】 ブラジル租税措置事件（DS472, 497）――内国税減免措置に対する WTO ルールの適用範囲――」RIETI Policy Discussion Paper Series 19-P-037（独立行政法人経済産業研究所、2019 年）<https://www.rieti.go.jp/jp/publications/pdp/19p037.pdf> 参照。

[86] Neha (n 26) 374.

②　データ倫理規定

データ・ドリブンな技術について特別な規定を置く協定もある。DEPA8 条 2 項では、当事国は「AI 技術の信頼性、安全性、及び責任ある利用のための倫理的枠組みと規律枠組みの経済的、社会的重要性を認識」することが謳われている。そして当事国は可能な限り AI 技術の採用と利用を促進するために相互理解を深め、「そのような枠組みを国際的に適合させる（align）ことが有益である」ことが確認されている。

同じく、シンガポール＝豪州デジタル経済協定（SADEA）31 条も、DEPA に類似した条項の他に、両国は(1)AI 技術に関する調査研究と産業慣行とそれらの規律について共有すること、(2)産業と社会において AI 技術の責任ある利用と採用を促進し維持すること、(3)研究者、学界、産業界において、商業化の機会と協力を奨励することについて協力することを定める。

これらはいずれも国際基準に沿って協力を行う努力規定に留まる。もっとも、双方とも政府、産業、学術領域などにおける対話を促進しようとしている点は特記に値する。データ倫理については政府のみならず、IT 企業やデータを管理する企業の間における協力が必要である。前述したように、GATS では民間が設定した標準は形式的には考慮されないことになるが、他方で、国家主導で AI を含むデータ・ドリブン技術のあり方を定めると、技術開発が妨げられるという懸念もある [87]。これらの規定は、WTO 体制の国家中心的な限界を克服するものとして評価することができる。

3-3　小括

データ・ガバナンス措置については各国内レベルでは法制に取り入れることが増えている。他方で、そのような措置の水準については、国際的に確立したものがなく、デジタル貿易協定において具体的な規則が入っている例は少ない。高水準のデジタル貿易協定を締結する場合には、少なくともDEPAやSADEAのように、適正な利用や、国際協力について努力義務規定を入れ、技術の変化に応じて柔軟な対応をすることが必要になる。

4.　日本の課題

以上の検討を踏まえて、日本の法政策について簡単なコメントを付す。日本における個人情報やその他の利用者情報の適正な取り扱いについては、個人情報保護法と電気通信事業法に定めがある。2020 年改正においてこれら 2 つの法律が日本の管轄に服する外国事業者にも適用がされるようになったり、個人情報保護法における個人情報の越境移転規制が強化されるようになったりして、グローバル化への対応が図られている。

個人情報保護法において、日本の管轄に服する事業者は、個人情報を外国にある第三者に提供する場合には、本人の同意を得なければならない[88]。ただし、個人情報保護委員会規則において（1）個人情報保護法制が個人の権利利益を保護する上で日本と

---

[87] ibid 373.

[88] 日本・個人情報の保護に関する法律（平成 15 年法律第 57 号）23、24 条。2020 年の法改正では個人の権利保障が強化されたが、越境移転についての基本的な規則は維持された。個人情報保護法の改正については、個人情報保護委員会「令和 2 年改正個人情報保護法について」<https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/> 参照。

同等の水準にあると認められる外国として定めるものと、(2) 個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして定める基準に適合する体制を整備している者については、本人同意取得義務が除外される。前者で除外されるのは現行ではEUと英国である。また、後者の適合性判断において、CBPRが用いられている。これに対して、非個人情報の越境移転についてはこれらの法律では特段の制約は設けられていない。

日本が諸国と今後デジタル貿易協定を締結していく上で、現行の法政策には少なくとも次の 2 つの課題がある。

第 1 に、デジタル貿易におけるプライバシーやデータ・ガバナンス措置の規律は、国内法レベルにおける諸問題と、必ずしも連続性をもって議論されているわけではない。

例えば、現行法ではプラットフォーム規制を含めた広義のデジタルサービスのガバナンスに関してカバーできていない諸問題が残っている。それらを論ずることは本稿の射程を越えるが、特にウェブサイトやアプリの利用者情報が、通信の秘密の保護対象から外れていることが特記に値する[89]。この点については、一方では、これらの情報については、保護対象から外れるとしても、事業者がそれを利用者の意思に反して取得、活用することには問題があるという指摘がある[90]。しかし、これらの情報取得や利活用に際して規制を設けることは、事業者に負担を課すものであることも一因となって、議論は収斂していない[91]。しかし、これらの見解の相違が、デジタル貿易を議論するときに参照されることは殆どない。

確かに、デジタル貿易協定が相互運用性を確保するアプローチを取る限りにおいて、

---

[89] 電気通信事業法 4 条 1 項参照。「通信の秘密」の範囲には、通信の内容のみならず、「個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、通信回数等これらの事項を知られることによって通信の意味内容を推知されるような事項」が含まれると整理されている。総務省・プラットフォームサービス研究会「中間報告書」(2019 年 4 月) 8 頁<https://www.soumu.go.jp/main_content/000613197.pdf>参照。他方で、通信ではないウェブの利用履歴情報などはここに含まれない。また、コミュニケーションを媒介する事業者(LINE 社など)は届出が必要な事業者に当たるが、オンライン・ショッピングなどの事業を提供する者はそれに当たらない。

[90] 同上、27 頁。令和 4 年 1 月、総務省・電気通信事業ガバナンス検討会「報告書(案)」に対する意見募集がなされた<https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000235.html>。「報告書(案)」47 頁以降は、利用者情報の適正な取り扱いに関する規程の策定、利用者情報統括管理者の選任、利用者情報の適正な取扱いに関わる方針の策定及び公表、及び、その取扱い状況に関する評価の実施と対策への反映を、利用者の利益に及ぼす影響が大きい事業者に対して求めていくことを述べている。また、総務省・プラットフォームサービスに関する研究会が、2021 年 9 月の中間報告書において、利用者情報の取扱いについて、各国法制を含めたグローバルな情勢の変化を踏まえること、分かりやすい通知や同意取得がなされるべきこと等を指摘している。総務省・プラットフォームサービスに関する研究会「中間とりまとめ」(令和 3 年 9 月) 100 頁<https://www.soumu.go.jp/main_content/000769270.pdf>参照。

[91] 本稿執筆時点において、政府は電気通信事業法の改正を目指しているが、異論もある。日本経済団体連合会「総務省『電気通信事業ガバナンス検討会報告書(案)』に対する意見」(2022 年 2 月 4 日)<https://www.keidanren.or.jp/policy/2022/012.html>参照。

これらの問題は協定とは独立した論点である。しかし、これらの情報が外国に移転する場合、それが輸出先の外国事業者にどのように利用されるのか、また、外国政府がそれらの情報にアクセスできるのかは、日本国内の利用者のプライバシーや安全に影響を与える。また、プライバシー権の保障について相互に高水準の規律を求める協定を締結する場合には、国内法制がその水準に適合しているかも問題となる。そのため、政府としては、データの越境移転を行う事業者側のニーズを踏まえながらも、それが利用者の権利を保障するための指針を策定するなどの対応が望ましいと言える。

第 2 に、1-3②で指摘したように、日本は DFFT を謳い「プライバシーやセキュリティー、知的財産権に関する信頼」を基礎に据えながらも、そこでの「信頼」に実体的価値を組み込んでいない。これは、交渉の幅を広げるという点では、効果的だとも評価できる。しかし、米国と EU が価値を基にしたアプローチを取る立場を表明している以上、価値中立的なアプローチを取ることで、却ってその方向性が曖昧になることも懸念される。

既にプラットフォーム規制を巡る議論では、ビッグデータの利活用などによって、個人の自律的選択が制約されたり、フェイク・ニュースの蔓延などによって国内の民主主義が脅かされたりする可能性が指摘されている。デジタル貿易の高水準の自由化を進める上では、それらのリスクを考慮する必要がある[92]。個人情報については2020年の個人情報保護法改正とガイドライン策定において手当がされているとも言えるが、それ以外の情報の移転も含めて、包括的な検討が必要だと思われる[93]。

5. 結語

本稿では、デジタル貿易協定においては、その性質上調和化が難しい、個人保護情報法制やデータ保護法制、ガバメント・アクセスを認める法制について、主に相互運用性を強化するなどして、データ流通の障壁を低くする方向性が打ち出されていることを実証した。

当面の国際的な動向としては、WTOの電子商取引交渉と、CPTPP、RCEPの経済圏を包含するアジア太平洋自由貿易圏（FTAAP）構想の展開が重要である。日本はいずれにおいても中心的な位置にいる。特に前者については、2021年12月に共同議長声明が発出され、その中で8つの条文について概ねのコンセンサスができたことが述べられ

---

[92] デジタル貿易ではないが、2016 年以降、LINE 社が通信サーバを韓国に置き、中国事業者がそのデータを管理していたことについては、違法性はないにせよ、利用者のプライバシー保障や日本の経済安全保障の観点から問題ではないかという指摘がなされた。Z ホールディングス・グローバルなデータガバナンスに関する特別委員会「最終報告」（2021 年 10 月）<https://www.z-holdings.co.jp/notice/20211018>参照。また、山本龍彦＝石井由梨佳＝河合優子「HOT issue(No.26) 鼎談 LINE 問題から考えるグローバルデータガバナンス」『ジュリスト』1565 号（2021 年）2, 48 頁参照。

[93] この点に関して、個人情報保護法 1 条は個人の権利利益を保護することを本法の目的としている。これは、憲法 13 条、21 条、35 条等における権利を保障するものである。また、電気通信事業法 4 条は事業者が通信の秘密は侵してはならないことが定められている。これは憲法 21 条 2 項が定める通信の秘密を保障するものである。しかし、それらでカバーされない情報を含めた包括的、体系的な規律は現行ではなされていない。

ている[94]。ただしその中には、プライバシーやデータ・ガバナンスについての項目は入っていないようである。後者については、中国のCPTPP加盟の可能性が排除されないことを踏まえなくてはならない[95]。いずれについても、本稿で検討した諸論点は回避できない問題であり、今後の展開を注視する必要がある。

[94] WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore, December 2021 <https://www.meti.go.jp/press/2021/12/20211214001/20211214001-1.pdf>.

[95] 川瀬剛志「中国の CPTPP 加入にどう向き合うか」経済産業研究所コラム（2021 年 9 月 22 日）<https://www.rieti.go.jp/jp/columns/a01_0662.html> 参照。