〈財務省財務総合政策研究所「フィナンシャル・レビュー」令和６年第１号（通巻第 155 号）2024 年２月〉

「デジタル貿易」は「貿易協定」に何をもたらしたか？

―非貿易的関心事項を中心に―[*1]

飯野　文[*2]

要　約

経済や社会に広く浸透しつつあるデジタル化は貿易にも様々な影響を及ぼし，新たな課題をもたらしている。このため，貿易協定にも変容ないし対応のための進化が求められている。本稿は，貿易協定の変容ないし進化の様相の一端を明らかにし，自由貿易協定（FTA）を中心に形成されつつあるデジタル貿易のグローバルな規制環境について考察することを目途する。

そのため，まずデジタル貿易の概念を概観した上で，デジタル貿易の登場によって貿易に生じている主な影響と課題を考察する。次に，これらの課題に貿易協定がどの程度対応しているかについて WTO 協定と FTA を検討する。対象とする FTA は，デジタル貿易の規律形成を先導する「ルールメーカー」の国々の先進的な FTA（CPTPP，USMCA，DEPA，DEA，UKSDEA，EU・UKTCA，EUSDTP）と RCEP である。

検討の結果，第一にデジタル貿易の規律形成における協定間の相互作用の様相，第二にデジタル貿易がもたらした貿易協定の射程の拡大とそのインプリケーション，第三にデジタル貿易の規律に伴う「規制する権利」の存在感の向上と，それが貿易協定において定着しつつある状況，第四にデジタル貿易に関連してステークホルダーの参加機会を向上する必要性，を結論として提示している。

キーワード：デジタル貿易，電子商取引，越境データ移転，サイバーセキュリティ，個人情報保護，WTO，FTA，規制する権利

JEL Classification：F13, F15, K33

Ⅰ．はじめに

経済や社会に広く浸透しつつあるデジタル化は貿易にも様々な影響を及ぼし，新たな課題をもたらしている。特に技術の進展に伴って流通量が増大したデータ[1)]は，それ自体が取引対象であることに加え，サービス提供の手段（SNS，オンラインゲームなど）にも深く関わり，また

＊１　フィナンシャル・レビュー論文計画報告会，フィナンシャル・レビュー論文検討会議において貴重な質問及びコメントを下さった方々に謝意を申し上げる。

＊２　日本大学商学部教授

新しいサービス開発促進の手段（クラウド，生成 AI など）でもある。そして，このように新たな価値を生み出すものとして，国家間の比較優位の源泉にも影響している。その結果，データ関連の貿易措置など新たな貿易障壁が登場すると共に，越境移転するデータをめぐって，個人情報の保護やサイバーセキュリティを確保する必要性なども生じている。さらに，データは国境にとらわれずに移転する一方で各国の規制は国家毎に行われるため，国家間の規制上の相違がグローバルに事業を行なう企業にとってのコスト上昇や法的不安定性の増大，国家間の軋轢などにつながっている。このため，貿易協定にも変容ないし対応のための進化が求められることになる。

本稿は，貿易協定の変容ないし進化の様相の一端を明らかにし，自由貿易協定（FTA）[2] を中心に形成されつつあるデジタル貿易のグローバルな規制環境について考察しようとするものである。まず第Ⅱ節でデジタル貿易とは何かを概観する。第Ⅲ節では，デジタル貿易の登場によって貿易に生じている影響と課題を考察する。これらの課題に貿易協定がどの程度対応しているかについて，まず第Ⅳ節で WTO 協定を検討する。次に第Ⅴ節では，デジタル貿易の規律形成を先導する「ルールメーカー」の国々の FTA を中心に検討する。第Ⅵ節では，結論として，以上の検討から明らかとなった諸点を提示する。

Ⅱ．デジタル貿易とは何か

本節では，デジタル貿易が貿易関連の主要国際機関，研究者，主要国に現段階でどのように捉えられているか例示しながら，デジタル貿易の概念について検討する。

OECD によれば，「デジタル貿易に…単一の定義はないものの，デジタルで又は物理的に提供される，デジタル取引可能な物品及びサービスの貿易であって，消費者，企業，政府が関与するものを包含するというコンセンサスは高まって」おり，また「デジタル貿易はデータの移動で支えられ…データは生産手段であるだけでなく，それ自体が取引される資産」である[3]。WTO については，WTO の電子商取引（以下 EC）作業計画[4] で示された EC に係る概念がよく知られている。すなわち「作業計画の目的上…『EC』という用語は，電子的手段による物品及びサービスの生産，流通，マーケティング，販売又は引渡しを意味する」というものである[5]。デジタル貿易の統計的定義としては，IMF，OECD，国連，WTO が共同で「デジタ

1）本稿では，検討対象とする FTA で「データ」と「情報」が各々定義されていないことを踏まえて両者を互換的に用いている。

2）本稿では，簡易化のため関税同盟や必ずしも市場アクセスを伴わない二国間，複数国間の協定も含めて FTA と称する。また条文の記載については，紙幅の関係上，原則として第 1 条 1 項を 1.1 条のように表記する。

3）OECD <https://www.oecd.org/trade/topics/digital-trade/> なお，この概念は，Gonzalez and Jouanjean（2017）（OECD Trade Policy Papters）により最初に示されたものである。González and Jouanjean（2017）pp. 7，12. 以下，本稿では特記ない限り，英文は筆者訳出による。

4）WTO，WT/L/274, 30 September 1998.

5）WTO の EC-JSI 交渉では，デジタル貿易ないし EC の定義として，当該定義がドラフトテキストに掲載された経緯があるようである。Peng（2022）p. 772，ft.9.。なお，WTO が毎年公表する世界貿易報告では，デジタル貿易に係る合意された定義はないとしつつ，OECD の定義が引用された例がある。WTO（2018）Section B, ft.21.

ル的に発注され，及び／又は，デジタル的に納品される全ての国際貿易」と初めて定義している[6)]。

研究者の中では Peng（2022）が「デジタル貿易に確立した定義はなく，一般にデジタル技術によって可能となる国際貿易を包含する広義の意味で理解されており...『EC』や『EC の貿易的側面』といった用語と互換的に使用され...『データフロー』という用語もデジタル貿易と密接な関係にある」と述べている[7)]。

各国はどのように捉えているだろうか。FTA でデジタル貿易ないし EC を定義しているものはほぼ見当たらないが，各国の HP 等に参考となる記述がみられる。例えば，EU は「デジタル貿易とは，通信及び/又は ICT サービスといった電子的手段によって可能になる商取引を指し，物品とサービス両方の貿易を対象とする」と説明している[8)]。オーストラリアは「デジタル貿易戦略」において，デジタル貿易に含まれるものを挙げる形で当該戦略上の定義を示している。それによると，①輸出入（インターネット及び EC プラットフォームで販売される物品・デジタルコンテント（ソフトウェア，本，音楽，フィルム，アプリを含む）・デジタル対応サービス（法務，金融，教育，コンサルティングなど)），②貿易の電子的円滑化（電子貿易文書の受容・技術進歩に伴う“Regtech”ソリューションの採用など），③越境データ転送（事業活動・ビジネス支援）が含まれると説明される[9)]。ニュージーランドは，デジタル貿易に単一の受容された定義はないとしつつ，上述した OECD の定義についてはコンセンサスが高まっていると述べ，デジタル貿易とは「デジタル的か物理的に引き渡されるかどうかにかかわらず，デジタル技術により可能となるあらゆるものを指す。例えば，電子書籍の購入とデジタル配信だけでなく，オンライン・マーケットを通じた紙の書籍の購入と物理的な送付も含まれる」とする。そして，デジタル貿易と EC は互換的に用いられると説明している[10)]。

以上は一端を示すに過ぎないものの，これらを集約すると，デジタル貿易については，第一に，確立した定義がないが，デジタル的に又は物理的に提供されるデジタル取引可能な物品とサービスを含む広い概念で，第二に，デジタル貿易を下支えしているのはデータであり，第三に，デジタル貿易は EC と互換的に用いられることが多い，ことが共通項として指摘できる。これに依って，現段階のデジタル貿易の共通理解をまとめれば，少なくとも，デジタル化された物品とサービスの貿易（電子的に取引される物理的な物品も含む）で，データ自体の取引も含み，データに支えられるものと捉えられよう。いずれにせよ，技術革新の速さに鑑みればデジタル貿易の外縁もそれに応じて変化し得ると思われる。なお，デジタル貿易と EC の関係については，例えば WTO の EC の定義とオーストラリアのデジタル貿易の捉え方を比較すると示されるように，デジタル貿易が国際的な EC を包含するようではあるが[11)]，本稿では，ひとま

6）IMF, OECD, UN and WTO（2023）p. 5. 原文は，“all international trade that is digitally ordered and/or digitally delivered”。“digitally ordered trade” は，“the international sale or purchase of a good or service, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders”，“digitally delivered trade” は，“all international trade transactions that are delivered remotely over computer networks” とそれぞれ別途定義される。*Ibid.*，p. 6.

7）Peng（2022）pp. 772-773.

8）EU，“Digital trade” <https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en>

9）オーストラリア外務貿易省，“Digital Trade Strategy” <https://www.dfat.gov.au/trade/services-and-digital-trade/e-commerce-and-digital-trade/digital-trade-strategy>

10）ニュージーランド外務貿易省，“What is ‘the digital economy’ and ‘digital trade’?” <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/what-is-the-digital-economy-and-digital-trade/>

ずデジタル貿易と EC を互換的なものとして用　いる。

Ⅲ．貿易への影響と課題

デジタル貿易の登場によって，貿易にはどのような影響が生じているだろうか。前節でみたように，デジタル貿易では，データがこれを下支え，またデータ自体も取引対象となる[12)]。こうしたデータの重要性は，各国の比較優位の源泉，つまり「競争力」の源泉に変化をもたらし，さらに，そうしたデータの流れを確保するインフラも，比較優位の源泉の一部となる[13)]。主要なインフラである大容量ネットワークについては 5G の普及，衛星インターネットの発展[14)]，宇宙におけるレーザー光線の通信技術開発[15)]，北極圏の海底ケーブル敷設の試み[16)]，さらには量子通信技術の展開可能性などにより，今後も一層の技術の発展が想定されている。これまでのインターネット人口の増加トレンドも今後の当該人口の増加を示唆している[17)]。こうした発展により，データの重要性と比較優位の源泉の変化はさらに深化することが見込まれる。

このような「競争力」の源泉の変化に伴って，貿易には主に次のような課題が生じている。第一に，新しいタイプの貿易制限措置の登場である。データの重要性が高まるにつれて，自由なデータの越境移転が追求される一方で，国家の「競争力」保持の観点から，データの越境移転を制限ないし禁止する措置（データローカリゼーションと呼ばれる）が採用されるようになっている[18)]。必ずしも定義されないままに用いられているケースが多いが「デジタル保護主義」といった表現はこうした事態を含むと思われる。

第二に，いわゆる非貿易的関心事項の存在感の上昇である。データの越境移転の制限ないし禁止は，上記の「競争力」保持以外の理由でも行われ，特に個人情報保護ないしプライバシー保護の観点からの規制がデータの越境移転に係る国際ルール形成上の重要な論点の一つになっている。例えば，WTO の EC に関する有志国間交渉（Ⅳ－２参照）では個人情報保護ないしプライバシーの保護に係る合意が難しい状況が続いた経緯がある[19)]。

11）デジタル貿易と EC の概念的相違は，IMF, OECD, UN and WTO（2023）Figure 1.4 で分かりやすく説明されており，右によっても，国際的な EC の一部はデジタル貿易の一部に位置づけられている。IMF, OECD, UN and WTO（2023），p. 14.

12）実際，世界 GDP の発展に貢献する物品，海外直接投資，データのグローバルな流れのうち，既に 2014 年にはグローバルなデータの流れの貢献度合いが物品貿易を上回ったことが指摘されている。McKinsey Global Institute（2016）p. 75.

13）この点は，データは「21 世紀の石油」との表現にも表れている。The Economist（6 May 2017）. WTO は，2018 年に知的財産権，データの流れ，プライバシーに関する規制や，デジタルインフラの質などが，新たな比較優位の源泉として浮上し得ると指摘している。WTO（2018）p. 63.

14）例えば，2022 年 10 月からスターリンク社がアジアでは初めて日本でのサービス供給を開始したことをツイッター（現 X）で公表している。朝日新聞（2022 年 10 月 11 日）及び日刊工業新聞（2022 年 11 月 23 日）。

15）REUTERS（2022 年 6 月 3 日）。

16）REUTERS（December 2, 2022）.

17）インターネット人口は，2000 年に世界の 6％，2022 年に 70％（日本では 100％）に達している。ITU-D ICT Statistics，Facts and Figures <https://www.itu.int/itu-d/sites/statistics/>

18）*E.g.*, Digital Policy Alert, “Data Governance” <https://digitalpolicyalert.org/policy-area/data-governance?period=2020-01-01,2023-09-17>

また，新たな非貿易的関心事項も現れている。代表例としてサイバーセキュリティが挙げられる[20]。サイバーセキュリティという用語は既に広く用いられているが，普遍的に合意された定義は存在しないといわれる[21]。但し，国際的にも国内的にも定義は存在しており，代表的なものとしては，標準化の文脈における ISO/IEC や ITU の定義がある。ISO/IEC によればサイバーセキュリティは「サイバーリスクから人・社会・組織・国家を保護すること（注：保護とは，サイバーリスクを許容可能なレベルに保つこと）」である[22]。国内的な定義には米国国立標準技術研究所（NIST）の用語集[23] や日本のサイバーセキュリティ基本法（2014）によるもの[24] がある。

なお，サイバーセキュリティという用語は，政治的色彩を帯びやすく，インターネット主権と国家安全保障の問題として枠づけされやすい[25]。OECD は，デジタルセキュリティという用語を用いるなかで，サイバーセキュリティは「複雑で多面的な分野となっており，少なくとも，経済的・社会的，技術的，法の執行，国家及び国際的な安全保障という４つの側面がある」とし，このうち経済的・社会的側面がデジタルセキュリティであると説明する[26]。OECD のこの捉え方は，サイバーセキュリティが政治的色彩を帯び得ることをよく反映している。

このようなサイバーセキュリティの観点からの規制が貿易を制限する場合があるが，フィッシング対策や決済上のセキュリティ確保など，デジタル貿易の円滑かつ安全な実施に欠かせないものから，安全保障上の理由で導入されている措置もあり，サイバーセキュリティは広くデジタル貿易全体に関連する課題といえる。

第三に，新たな関係者（ステークホルダー）の登場ないし関与の高まりである。新たな「関係者」には以下が含まれる。まずデータの保有者としては，政府と一部のいわゆるプラット

19）*E.g.*, Inside US Trade（2023）.

20）*E.g.*, Digital Policy Alert, “Data Governance” <https://digitalpolicyalert.org/policy-area/data-governance?period=2020-01-01,2023-09-17>

21）Chang and Liu（2022）p. 186.

22）ISO/IEC 27032:2023（en）Cybersecurity — Guidelines for Internet Security <https://www.iso.org/obp/ui/#iso:std:iso-iec: 27032 :ed- 2 :v 1 :en>; ITU は，ITU-T X. 1205 （04 / 2008）<https://www.itu.int/itu-t/recommendations/rec.aspx?rec=9136> 参照。

23）NIST, Computer Security Resource Center, “Glossary” <https://csrc.nist.gov/glossary> サイバーセキュリティの定義の一つは「コンピュータ，電子通信システム，電子通信サービス，有線通信，及び電子通信（これらに含まれる情報を含む）に対する損害の防止，保護，修復を行い，その可用性，完全性，認証，機密性，及び否認防止を確保すること」である。

24）サイバーセキュリティ基本法（平成二十六年法律第百四号）第２条「電子的方式，磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され，又は発信され，伝送され，若しくは受信される情報の漏えい，滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ，その状態が適切に維持管理されていること」と定義される。

25）Chang and Liu（2022）p. 187. その例として，中国の関連法（Cybersecurity Law Article 1.（2017））とベトナムの関連法（Law on Cybersecurity of Viet Nam（2018））が挙げられている。例えば，ベトナムの関連法では，サイバーセキュリティは，サイバースペースにおける活動が，国家安全保障，社会秩序及び安全，または政府機関，組織及び個人の合法的な権利及び利益に害を及ぼさないことを保証することを意味すると定義される（2.1 条）。

26）The Global Forum on Digital Security for Prosperity（OECD）<https://www.oecd.org/digital/global-forum-digital-security/about/> 当該フォーラムは，OECD（2015）の宣言に基づいて 2018 年 12 月に創設されたもので，「当該分野におけるすべての利害関係者のコミュニティのための，国際的な多国間かつ学際的な環境」である。

フォーム企業[27]の影響力が高まっている。データ保有者としての政府の中には，「競争力」保持の観点からデータの囲い込みをはかる場合がみられるほか，監視・コントロール手段に利用する場合もあり，その意味では特に独裁的体制と親和性が高いといえ，国際的に規律すること自体が難しいことがある[28]。プラットフォーム企業の中には，データを基盤としてサービスを提供するため，データを貪欲に収集するものがある。また，プラットフォーム企業には個人情報保護や，フェイクニュース等の拡散防止などの観点から，規制上も一定の役割を果たすことが期待される場合がある[29]。

一般の消費者も，データの生成者として（SNS における発信，著作物の公開など），またオンライン取引の当事者として，デジタル貿易に直接関与することが増えている。さらには，AI の普及により，消費者はより深いレベルでこうした技術に影響を受ける側にもなっている。例えば，AI によるプロファイリングは人間の意思決定に影響を与え，さらには生成 AI によれば認知過程への介入も可能となり得る[30]。このように，データをめぐる技術（例えば AI）はこれまでの技術に比べて人間に深い部分で関わり得ることから，消費者は関連する規律策定に早い段階から関与していくことが重要になると思われる。貿易協定ではこれまでにも「市民社会（civil society）」などの表現で関与が規定される場合がある[31]。

第四に，デジタルデバイドの拡大とそれに対する懸念の高まりである。デジタルデバイドは，先進国と途上国の間の IT インフラなどの差や，ジェンダー間のインターネット普及率の差など様々な意味を包含する[32]。特に先進国と途上国間のデジタルデバイドについての懸念は高く，例えば WTO の第 12 回閣僚会議（MC12）においても特に開発的側面に沿って EC 作業計画を再活性化することが合意されている[33]。

27）プラットフォーム企業の定義は様々であるが，国際的な定義の一つとして「インターネットを介したサービスを通じて交流する 2 以上の異なるが相互依存するユーザ（企業か個人かを問わない）間の交流を促進するデジタルサービス（“a digital service that facilitates interactions between two or more distinct but interdependent sets of users（whether firms or individuals）who interact through the service via the Internet”）」がある。 OECD（2019）p. 21.

28）この点が貿易協定上で表れている例として，RCEP12.14 条及び 12.15 条（後掲 V-2-1 参照）。

29）例として，EU のデジタルサービス法 34 条及び 35 条。（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）（Text with EEA relevance），OJ L 277, 27.10.202. 両条は，非常に大規模な，オンラインプラットフォーム及びオンライン検索エンジンのプロバイダに，サービスとアルゴリズムシステムを含むその関連システムの設計又は機能，又はそのサービスの利用に起因する EU 域内のシステミックリスク（違法なコンテンツの拡散，基本的権利への悪影響など）の特定，分析，評価と緩和措置の導入を義務づける内容である。

30）例えば，生成 AI に対する質問への回答として国家が恣意的な回答を予め用意しておくと，人間がそれを学習してしまうことになる。

31）例えば，国際貿易又は投資に影響を及ぼす事項における腐敗行為の防止等に係る CPTPP26.10 条，USMCA27.5 条，貿易と持続可能な開発に係る日 EU・EPA16.16 条。

32）WTO（2018）pp. 43-49.

33）WT/MIN（22）/32（WT/L/1143），22 June 2022. 加えて，WTO の “Aid for Trade” の 2023-2024 計画では，デジタルコネクティビティが優先分野の一つに挙げられている。WT/COMTD/AFT/W/95，10 February 2023.

Ⅳ．貿易協定側のアダプテーション１：WTO

前節で捉えたデジタル貿易の登場とその課題に貿易協定側はどの程度対応できているだろうか。現行の貿易協定を大別すればWTO協定とFTAに分かれるが，結論を先取りすれば，WTOの現行のルールにおける対応は限定的なものにとどまっている。FTAではWTOの規律のギャップを埋めるようにデジタル貿易関連規律の発展が先行したが，その適用範囲は締約国にとどまり限定的である。さらに，FTAの規律は，その範囲及び約束の深さの点で「異質（“heterogeneous”）」である[34]。以下では，WTO協定及びFTAの順に検討する。

Ⅳ－１．WTO 協定と判例法

デジタル貿易とは，現段階で，デジタル化された物品とサービスの貿易（電子的に取引される物理的な物品も含む）で，データ自体の取引も含まれ，データに支えられるものと捉えられることは前述した。このうちデジタル化された物品ないしECが物品かサービスかという問題についてWTO加盟国間の合意はない。しかし，電子的手段により取引されるサービスについては，WTO紛争処理手続の先例に依ると，少なくともGATSの第１モード（越境取引）に該当し，加盟国が行ったGATS上の約束も非物理的形態で提供されるサービスをカバーし得る。すなわち*US – Gambling*でパネルは，GATSの第１モードには，インターネット等を含む全ての提供手段が含まれると結論し[35]，この点は技術的中立性の原則にも沿っていると述べている[36]。その際，パネルは技術的中立性の原則をWTOのEC作業計画の進捗報告から導出し[37]，この原則はWTO加盟国の間でほぼ共有されているようである（“seems to be largely shared among WTO Members”）と述べている[38]。なお，この点は本件で上訴されていない[39]。

加盟国のGATS上の約束については，*China – Publications and Audiovisual Products*（*AB*）において上級委員会が「中国のGATSの約束表の用語（「録音（“sound recording”）」と「配信（“distribution”）」）は十分に一般的であり，適用対象が時間とともに変化する可能性がある」こと，そして「配信」は有形・無形の製品の両方に適用されると述べている[40]。加えて，このような解釈は，*US-Shrimp*で「有限天然資源」を解釈する際に示したアプローチと一貫していると述べ[41]，いわゆる発展的解釈を示した[42]。

加えて，WTO協定をみても，政府調達協定

34）*E.g.*, Wu（2017）p. 8; Monteiro and Teh（2017）p. 71; Burri（2021）p. 20.

35）パネルは，第１モードにはインターネットを含め，すべての配送手段が含まれると判断した。Panel Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services（*US-Gambling*）, WT/DS285/R, para. 6.287.

36）*US-Gambling*, para. 6.285.

37）*US-Gambling*, footnote 836. Work Programme on Electronic Commerce – Progress Report to the General Council, adopted by the Council for Trade in Services on 19 July 1999, S/L/74, 27 July 1999. para. 4: “It was also the general view that the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied.”

38）*US-Gambling* para. 6.285.

39）Appellate Body Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services（*US-Gambling*（AB））, WT/DS285/AB/R, paras.219-220.

や貿易円滑化協定など，近年に改正か策定された協定でデジタル化への対応がみられる。例えば，政府調達協定（2012 年改正）では電子的手段を用いた調達（例，4.3 条），貿易円滑化協定は電子決済（17.2 条）などがある。上述した個人情報保護ないしプライバシーの保護についても，GATS の一般的例外条項に関連規定[43]，金融サービス規律に関連規定[44] が存在する。

以上のように，WTO では紛争処理手続の判断において技術的中立性の原則や発展的解釈といった概念を通じてデジタル貿易への適応が一定程度みられると共に，デジタル貿易にある程度対応する協定も限定的ではあるが存在する。

しかし，現行の WTO 協定が不十分である部分は多い。主な例を挙げれば，現行のサービス分類（W/120）は古く，再交渉の必要性が指摘されて久しい[45]。例えばクラウドサービスや SNS の新たなサービスやオンラインゲームはどの分類に該当するのか[46]，Uber，Zoom などの仮想会議サービス，LINE などのチャットサービス[47] の分類も必ずしも明らかでない。さらには，前節で指摘した新たな課題について，WTO 協定上のルールが存在しない場合もある。データの越境移転については限られたルールがあるのみで[48]，データローカリゼーション，サイバーセキュリティについてのルールはみられない[49]。加えて「新たな関係者」の登場も想定されていない。要するに 1995 年に合意された WTO 協定はその後一部に発展があったとはいえ，デジタル貿易に対応していないのである。

かような状況に WTO の紛争処理手続を通じて対応するにも限界がある。既述の通り，紛争処理手続を通じた対応は，技術的中立性，発展的解釈といった概念に依ることでもある。しかし，これらの概念はどこまで対応できるのか，その概念は十分に明確なのかは必ずしも明らかでない。例えば，技術的録音物の物理的配信とデジタル配信までは対応可能かもしれないが，AI によるサービス提供と人によるサービス提供はどうか。AI による医療画像診断サービス

40）“This lends support to interpreting the meaning of “distribution” as applying to both tangible and intangible products...”, “China’s GATS Schedule（“sound recording” and “distribution”）are sufficiently generic that what they apply to may change over time”. Appellate Body Report, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products（*China-Publications and Audiovisual Products*（AB））, WT/DS363/AB/R, paras. 395-396.　本件パネルは，中国の約束表上の “sound recording distribution services” に係る約束は，インターネット経由など，非物理的な形態で提供されるサービスにも及ぶと判断した。Panel Report, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products（*China-Publications and Audiovisual Products*）, WT/DS363/R, para. 7.1265.

41）*China-Publications and Audiovisual Products*（AB）, footnote 705.

42）「発展的解釈」とは次のように理解される。“In practice, what is described as evolutionary interpretation is in essence often an effort to ensure that the treaty remains relevant and effective over time. In other words, evolutionary interpretation may often be understood as a choice, at the time of the interpretation of a treaty（and thus not necessarily at the time of its conclusion）, to give meaning to a treaty taking into account developments subsequent to the conclusion of the treaty.” Damme（2019）p. 171.

43）GATS14 条 c.ii.

44）Understanding on Commitments in Financial Services, para.8, “Transfers of Information and Processing of Information”.

45）Peng（2022）p. 6.

46）Wu（2017）p. 5; Buri（2021）chapter.1.

47）Peng（2022）pp. 6-7.

48）Understanding on Commitments in Financial Services, para.8, “Transfers of Information and Processing of Information”.

49）Understanding on Commitments in Financial Services の例外規定にあるプライバシーの保護，及び安全保障例外（GATT21 条等）が措置の一部をカバーし得る。但し，サイバーセキュリティ対応措置が安全保障例外に該当し得るかは議論がある。後掲Ⅴ－２－２（３）参照。

は，単なる提供手段の相違として捉えてよいか。既に，生成 AI，なかでも ChatGPT については単なる情報提供サービスではないからこそ規制論が出ているのではないか[50]。

また，各概念には批判も存在する。まず技術的中立性については，*China – Publications and Audiovisual Products* のパネル手続中，中国は加盟国から公式に認められたことはないと主張し[51]，パネルは本件において中国の約束表の解釈に技術的中立性の原則を援用する必要はなく，もし非物理的配信がカバーされるかどうか疑義があれば当該原則が援用されたかもしれないと述べる一方で[52]，WTO におけるその地位がどうであれ本件では解釈に際して必要ないと述べた[53]。パネルは，技術的中立性の原則を肯定しているようでもあるが，地位の不明確性を示唆しているようにもみえる[54]。確かに，技術的中立性に言及した *US – Gambling* のパネルは，“largely shared” と述べるにとどまり，加盟国全体がこの原則を共有しているわけではない。しかも同パネルは，共有している「ようである（“seems to”）」とするに過ぎない。またパネルは EC 作業計画の進捗報告に技術的中立性の原則を見出したが，進捗報告に重きを置きすぎたとみることもできる[55]。研究者の中にも，技術的中立性の原則は WTO 協定上の位置づけが不明確であることに加え，既存の義務の範囲を予測不可能に拡大すると共に，各国が技術関連規制を採用する余地を狭めてしまうと指摘するものがある[56]。

また，発展的解釈についても賛否がある。*China – Publications and Audiovisual Products* における約束表の発展的解釈については，「前向きな展開（“positive development”）」ではあるものの，法的確実性の達成には必ずしも寄与しないとの指摘がある[57]。特にデジタル貿易の文脈では「WTO の判例法は，どのような状況で，どの程度，交渉時に存在した『技術の状態』が，約束の範囲を決定する上で関連するかについて完全に明確ではない」[58] のである。

いずれにせよ，本来的には「排他的解釈権限」と意思決定の権限を有する加盟国[59] が決定すべき点―例えばデジタル化に応じた約束表の約束の範囲のように―がこうした概念により対処されている面もある点に限界があるということだろう。

Ⅳ－２．WTO における作業と交渉

現行ルールの限界に鑑み，WTO ではデジタ

50）AI については，開発指針の必要性や，高度 AI によるサービス提供へのライセンス制の導入なども国際的に議論されており，G7 でも 2023 年５月の G7 サミットで合意された「広島 AI プロセス」に基づいて 2023 年内に AI の開発・利活用の方針が決定される予定である。
G7 Hiroshima Leaders' Communiqué May 20, 2023, para.38. <https://www.g7hiroshima.go.jp/documents/pdf/Leaders_Communique_01_en.pdf>

51）“(N) ever formally accepted by Members”, *China – Publications and Audiovisual Products*, para. 7.1249.

52）“we have no need to invoke a principle of technological neutrality...(t) he principle of technological neutrality might have come into play had we found that China's commitment covered distribution on physical media and that there was doubt about whether it also covered the distribution of content on non-physical media.” *China – Publications and Audiovisual Products*, para.7.1258

53）“...the principle of technological neutrality, whatever its status within the WTO, is likewise not needed in this case...”, *China – Publications and Audiovisual Products*, para.7.1264

54）上述のようにパネルの当該判断については上訴対象外である。*China – Publications and Audiovisual Products* (*AB*), paras 219-220.

55）進捗報告に規範を創出する効果を与えるものといえるが，他方で，確かに WTO の紛争処理手続でいくつかの “principles” が見出されてきたのも事実である。Mitchell (2008), pp. 32-33, Part II.

56）Gagliani (2020) pp. 731-738.

57）Burri (2021) p. 19.

58）Peng (2022) p. 778.

59）それぞれ WTO 設立協定 9.2 条及び 4.1 条。

ル貿易への対応が探求的作業と交渉という2トラックで行われてきた。前者はWTOで1998年に策定された「EC作業計画」に基づいて開始された多国間の取り組み（多国間トラック），後者は2017年のECに関する共同声明を契機に開始された有志国間の取り組み（複数国間トラック）である。

多国間トラックは，1998年のECに関する宣言において「ECに関連する全ての貿易関連問題を検討する作業計画」の策定と「電子的送信に関税を課さないという現在の慣行を継続」（関税モラトリアム）を加盟国が決定したことに端を発する[60]。その後EC作業計画が策定され，それに基づき議論が継続しているが，もともと交渉でなく探求的作業を行っているため新たなルールの策定に直結しない。但し，本作業は加盟国全てが参加する形をとる点で，また，加盟国のデジタル貿易に係る理解を促進したと思われる点で評価に値する。なお，関税モラトリアムについては，閣僚会議毎に当該慣行の継続が決定されており，直近では2022年MC12における閣僚決定を根拠にMC13まで継続される[61]。

第二の複数国間トラックは，2017年のMC11で有志71ヵ国がECに関する最初の共同声明を公表し，「将来のWTO交渉に向けた探求的作業の開始」を宣言したことが契機である[62]。共同声明イニシアチブ（以下EC-JSI）と呼ばれるこの取り組みは2019年に本格的に交渉に入り[63]，本稿執筆時点（2023年9月）までに統合テキストが4回作成されている[64]。

EC-JSI交渉の進捗状況は，当該交渉の“co-convener”であるオーストラリア，日本，シンガポールによって公表されている。それによると，2023年3月時点で参加国は89ヵ国となり，これで世界貿易の90%以上を占める[65]。交渉は，主にECの実現，オープンネスとEC，トラストとEC，横断的課題，電気通信，市場アクセス，範囲と一般規定をカバーする[66]。第3回の統合テキスト（2022年12月）には，ペーパーレス取引，電子契約，電子認証と電子署名，未承諾の商用電子メッセージ，オンライン消費者保護，オープンガバメントデータ，オープンなインターネットアクセス，透明性，サイバーセキュリティ，電子取引の枠組みといった10項目について収束済の規定が含まれ[67]，加えて，電子請求に係る規定もほぼ収束している[68]。他方で，データ関連イシュー（データの越境フロー，ローカリゼーション），関税モラトリアムの恒久化，プライバシー，ソースコード，暗号を使用するICT製品，水平的課題（前文，

60）WT/MIN（98）/DEC/2，25 May 1998.
61）WT/MIN（22）/32（WT/L/1143），22 June 2022.
62）WT/MIN（17）/60，13 December 2017.
63）WT/L/1056，25 January 2019.
64）INF/ECOM/62/Rev.1，14 December 2020; INF/ECOM/62/Rev.2，8 September 2021; INF/ECOM/62/Rev.3 22 December 2022; INF/ECOM/62/Rev.4，4 August 2023. なお第1回（2020），第2回（2021），第4回（2023）テキストはNGOによって公開されている。第4回テキストについて右参照 <https://www.bilaterals.org/?wto-2023-plurilateral-ecommerce-48862&lang=en>
65）WTO，Joint Initiative on E-commerce，<https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm>
66）“Joint Statement Initiative on E-commerce: Co-convener’s Update, December 2020”.
67）“WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia，Japan and Singapore，20 January 2023”.
68）WTO Press Release，16 February 2023，“E-commerce negotiations enter final lap，Kyrgyz Republic joins initiative” <https://www.wto.org/english/news_e/news23_e/ecom_17feb23_e.htm> 2023年10月に至り，「シングルウィンドウによるデータ交換とシステムの運用可能性／UCR（Unique Consignment Reference number: 単一貨物識別符号）を加えて，12項目で合意済となっている。WTO, Press Release, 7 October 2023, “E-Commerce Co-Convenors: We Must Lock in the Credible Package that We Have in Our Hands” <https://www.wto.org/english/news_e/news23_e/jsec_27oct23_e.htm>

定義，原則など）については，交渉を加速するとされている[69]。しかし，これらのイシューの多くは，米中間の技術的覇権をめぐる争いと深くかかわり，また，プライバシー保護の観点から個人データの越境移転に厳格な姿勢をとるEU，主として安全保障の保護を理由に[70] データの国内での囲い込みをはかる中国との間で合意が困難な領域である。これらの点については最新の第4回統合テキスト（2023年8月）においても大きな前進はないようである[71]。本交渉は有志国間の交渉ではあるが，多くの国が参加する点で妥結すれば多国間のルールが成立する有効なプロセスである。しかし，2023年末までの実質的な合意が目指されているなか[72]，今後の見通しは本稿執筆時点（2023年9月）でなお不透明である。

Ⅴ．貿易協定側のアダプテーション2：先進的なFTA

Ⅴ－1．FTAにおけるデジタル貿易規律の発展と「ルールメーカー」の登場

FTAは，WTO協定の間隙を埋めるようにデジタル貿易を規律する「実験室」[73] として機能してきた。これらの規律をFTA横断的に分析する先行研究も徐々に増えている。その先駆けの一つであるMonteiro and Teh（2017）[74] は，その時点で，第一にEC条項は増加傾向にあり，第二にこれらの規定が構造，用語，範囲の面で異質（“heterogeneous”）であり，第三に進化し続ける可能性があることを指摘している[75]。また，Burri（2022）は，2000-2022年に合意されたFTA370件のデジタル貿易関連規定を反映したTAPEDデータベースに基づき，203のFTAがデジタル貿易関連規定を含むことを指摘する[76]。Burri（2021）によれば，過去20年弱の間にデジタル貿易関連規定は数の面でも詳細さの面でも大幅に進化を遂げ，特に2010年以降に締結されたFTAではその7割弱にデジタル貿易関連規定があり，データ関連規定が含まれる場合もあるという[77]。同じTAPEDデータベースに基づいてFTAに含まれるデータフロー関連規定に着目したElsig and Klotz（2021）は，99件のFTA（EUを1として関係国数82ヵ国）がデータフロー関連規定を含み，また，それらの規定の範囲は異質（“heterogeneous”）であると述べている[78]。

以上のようにデジタル貿易関連の規律はこれまで発展してきているが，その傾向は直近でも継続している。第一に，デジタル貿易特化型の協定の登場である。この先駆けは日米デジタル貿易協定（2019署名・2020発効）であり，次に，

69）*Ibid.*
70）例えばINF/ECOM/19 24 April 2019，para 4.1.
71）*E.g.*，Inside US Trade（2023）.
72）WTO Press Release，28 July 2023，“E-commerce co-convenors to issue updated negotiating text”. <https://www.wto.org/english/news_e/news23_e/ecom_28jul23_e.htm>
73）*E.g.*，WTO（2018）p. 178.
74）1957-2017.5までにWTOに通報された発効済のFTA275件のうち，ECに明示的に言及するFTA75件を分析している。
75）Monteiro and Teh（2017）p. 71.
76）Burri（2022）p. 758. なお，TAPEDデータベースは，右参照 TAPED: A Dataset on Digital Trade Provisions <https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/>
77）Burri（2021）pp. 20-26.
78）Elsig and Klotz（2021）pp. 48-52.

DEPA[79]（デジタル経済パートナーシップ協定）が締結されている。また，デジタル経済協定が新たに締結されて既存のFTAのEC章がアップデートされる場合もある。DEA[80]（オーストラリア・シンガポールデジタル経済協定），UKSDEA[81]（英・シンガポールデジタル経済協定）がその例である。このほか米国の主導するIPEFでもデジタル貿易関連の規律を交渉中である。

第二に，数，詳細さ，範囲などの面でも，EUがEU・UKTCA[82]（EU英国貿易協力協定）で初めてデータ関連規定をFTAに含める発展がみられているほか，上述の特化型の協定ないし既存のFTAのアップデートのために締結された最近の協定では，AIやデジタルアイデンティティ（ID）などの新たなイシューが含まれる例がある。

第三に，協定よりもより緩やかな形態である「デジタル貿易原則」の策定もみられるようになっている。代表例はEUであり，主としてデジタル貿易分野での協力が中心的な内容である「パートナーシップ」の一環で，デジタル貿易原則に合意している[83]。EUSDTP[84]（EUシンガポールデジタル貿易原則）はその一例である。なお，こうしたデジタル貿易原則はG7も公表している[85]。

以上のようなデジタル貿易関連規定の進化には，中心となる国々が存在している。上記のように，同じデータベースに基づき，しかし異なるアプローチから分析を行ったBurri（2021）及びElsig and Klotz（2021）に依ると「中心的アクター」ないし「ルールメーカー」や「原動力」として共通するのは，米国，シンガポール，オーストラリア，最近のEU，カナダである[86]。

そこで，次節では主に上記の国々が最近締結したFTAをとりあげて，新たな課題への対応状況を検討する。より最近のFTAを検討する理由は，上述のように，FTAの規律が時間軸で見て発展してきている点にある。具体的な協定としては，CPTPP[87]，USMCA[88]，DEPA，DEA，UKSDEA，EU・UKTCA，EUSDTP，RCEPを対象とし，デジタル貿易特化型の協定でない場合には，当該協定のECないしデジタル貿易章及び関連規定（金融サービス章など）を主に検討する。RCEPは，この意味で先進的なFTAで

79）Digital Economy Partnership between Singapore, Chile and New Zealand（DEPA）.
80）Australia-Singapore Digital Economy Agreement（DEA）．両国間のFTA（SAFTA）の主にEC章をアップデートする内容である。
81）Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore（UKSDEA）．両国間のFTAの主にEC章をアップデートする内容である。
82）Trade and Cooperation Agreement between the United Kingdom of Great Britain and Northern Ireland, of the one part, and the European Union and the European Atomic Energy Community, of the other part（EU・UKTCA）.
83）例えばEUSDTPは，1）Preamble; 2）Digital Trade Facilitation; 3）Data Governance; 4）Consumer trust; 5）Business trust; 6）Cooperation on digital tradeという構成である。
84）EU-Singapore Digital Partnership / Digital Trade Principles（EUSDTP）.
85）G7が2021年に公表した原則は，1）open digital markets; 2）data free flow with trust; 3）safeguards for workers, consumers, and businesses; 4）digital trading systems, and 5）fair and inclusive global governanceという5つの領域をカバーしている。<https://www.meti.go.jp/press/2021/10/20211022008/20211022008-3.pdf>
86）Burri（2021）によれば，FTAのEC条項の多い順に，シンガポール（22），EU（22），オーストラリア（15），米国（14），チリ（13），カナダ（12）であり，EUのFTAは，いわゆる新世代FTAを中心に，充実化した内容となっている（括弧内はFTA数）。Burri（2021）pp20-21, ft.53. Elsig and Klotz（2021）によれば，データフローの観点から「中心的アクター」ないし「ルールメーカー」は，EU，米国，シンガポール，オーストラリア，カナダ，メキシコである。Elsig and Klotz（2021）p. 53.
87）The Comprehensive and Progressive Agreement for Trans-Pacific Partnership.
88）The United-States-Mexico-Canada Agreement.

はないが，これを含むことで，デジタル・ガバナンスを形成する三極の1つといわれる[89] 中国も含まれることになる。上記のうち，DEPA，DEA，UKSDEA，EUSDTPがデジタル貿易特化型であるが，DEA及びUKSDEAは締約国間で既に締結されているFTAのデジタル貿易規定ないし章を置き換えるものである。なお，CPTPP及びDEPAは，新規加入可能であり拡大可能性を有している点で注目に値する[90]。

これらの協定をデジタル貿易という観点から概観しておく。CPTPP（2018署名・同年12月発効（前身のTPPは2016署名））のEC章（14章，全18条）は，オーストラリアとシンガポールのFTAであるSAFTA（2003署名・発効）を基にしたといわれる[91]。14章は，締結時点では最も先進的といわれたEC関連ルールを定め，それは後のFTAのモデルともなった[92]。その主たる特徴は，データ関連規定（14.11条電子的手段による情報の越境移転，14.13条コンピュータ設備の設置）を定める点，一定のソフトウェアのソースコードの移転又はアクセス要求の禁止（14.17条）やサイバーセキュリティに係る協力（14.16条）など，それまでの貿易協定にあまり見られなかった新たな規定を含めた点，しかもこれらが紛争処理（28章）の対象であり，法的実効性を有する点にある。

USMCA（2018署名・2020発効）のデジタル貿易章（19章，全18条）はCPTPPが交渉ベースとして用いられたが，その内容を発展させている。主に，データ関連規定の強化，個人情報保護の強化，CPTPPにないオープンガバメントデータに係る規定（19.18条）の創設，サイバーセキュリティに係る規定（19.15条）の洗練で，これらを規定する19章は31章（紛争処理手続）の対象で法的実効性を有する。

DEPA（2020署名・2021発効）は，デジタル貿易特化型の協定である。全16の「モジュール」で構成され，デジタル関連の幅広いイシューを対象とする[93]。モジュールは貿易協定の章ないし節と同義とみなし得るもので，貿易協定に通常みられる各条が各モジュールに含められている。こうした「モジュール・アプローチ」の採用，すなわち「協定をデジタル経済の異なる問題領域の権利と義務をカバーする『モジュール』に分割する」[94] ことにより，他国が既存のFTAや関連する国内政策を更新する際にモジュールを利用できるため，上述した拡大可能性と併せて，DEPAの規範的影響力（“normative impact”）が高められるとの評価もみられる[95]。但し，各規定は協力促進義務や努力義務が中心で，拘束力があるとしても協力義務にとどまる。また，詳細な紛争処理手続（モジュール14）を有するが，データ関連規定のようにEC-JSI交渉で未決着であるなど議論の多いものは，モジュー

89）*E.g.*, Shaffer（2021）pp. 40-41.

90）DEPAでは2023年6月に韓国の加入が実質合意され，中国，カナダ，コスタリカ，ペルーも加入申請済である。Joint Press Release <https://www.mti.gov.sg/Newsroom/Press-Releases/2023/06/Joint-Press-Release-on-the-accession-of-the-Republic-of-Korea> 当初シンガポール，チリ，ニュージーランド，ブルネイが締結したP4協定の交渉に米国などが参加し，2016年のTPP締結を経て，2018年にCPTPPに結実した経緯を想起するとDEPAの拡大可能性は現実的なものである。

91）例えば，CPTPPのデジタルプロダクトの無差別待遇（14.4.1条），個人情報保護（14.8条）。Wu（2017）pp. 10, 20.

92）例えばCPTPPはUSMCA交渉のベースとして用いられた。Peng（2022）ft.77. 米国はTPP交渉に参加し，メキシコ，カナダはCPTPP締約国である故と思われる。

93）CPTPP及びUSMCAに含まれていない主な規定として，モジュール7のデジタルID（7.1条），モジュール8（エマージングトレンドと技術）のFintech（8.1条），AI（8.2条），政府調達（8.3条），競争政策の協力（8.4条），信頼あるデータ共有を検討するデータイノベーション（9.4条），デジタル分野における中小企業協力（モジュール10），及び市民社会等との協力可能性等を明示するデジタルインクルージョン（11.1条）がある。

94）Peng and Streinz（2021）, p. 19.

95）*Ibid*.

ル 14 の対象外か[96]，そもそも規定しない。例えば，金融サービスは対象外であり（1.1.2.b 条，電子決済（2.7 条）を除く），ソースコードやアルゴリズムに係る規定もない。一方，個人情報保護[97] については，詳細な義務が規定され（4.2 条），モジュール 14 の対象でもある。

DEA（2020 署名･発効）は SAFTA14 章（EC）を新 14 章（デジタル経済，全 38 条）におきかえるもので，データ関連規定を含め，デジタル貿易に係る規律で最も広範な規律対象範囲を有する協定の一つといってよい。章のタイトルが，デジタル貿易や EC でなく，「デジタル経済」である点にもそれが表れている。例えば，デジタル ID（29 条），AI（31 条）や Fintech（32 条）など DEPA を継承しているとみられる面があることに加え，コンピュータ設備の設置に係る規律に金融サービスを含めるほか（25 条），インフラの安定性確保の観点からの海底通信ケーブル（22 条），Fintech に加えて Regtech の協力（32 条）など，DEPA をしのぐイシューについて規律する。加えて競争政策の協力（16 条），ステークホルダーエンゲージメント（35 条）など，デジタル貿易ないしは広範なデジタル経済に特有の課題にも取り組むと共に，中小企業（36 条），キャパシティビルディング（37 条）などデジタルデバイド解消に向けた高い意識もみられる。具体的な義務を定める規定も多く，これらが 16 章（紛争処理）の対象であり，法的実効性を伴う。

UKSDEA（2022 署名･発効）の 8 章 F 節（「デジタル貿易及びデジタル経済」）は，DEA と並んで規律対象とするイシューが幅広く，同様に「デジタル経済」を対象とする DEA をしのぐ。DEA がカバーする点に加えて，デジタルインクルージョンのほか，新たに “Lawtech” を含めるなど，革新的な内容を含む。サイバーセキュリティに係る規定も，次節でみるように USMCA を基に拡充している（Ⅴ－２－２（3）参照）。また，義務規定も多く，しかもこれらは紛争処理章（14 章）の対象であり，法的実効性を有する。

EU・UKTCA（2020 署名・2021 発効）は，EU の貿易協定で初めてデジタル貿易の章を設けた協定で当該章は紛争処理手続の対象である。EU・UKTCA は大部に渡るが，デジタル貿易の中心的規律は，Part Two（貿易，輸送，漁業及びその他のアレンジメント）Heading One（貿易）Title Ⅲ（デジタル貿易）である[98]。上述した他の協定に比べて規定数及び対象イシュー数は限定されるほか，データ関連規律に係る独特の構造及び「規制する権利」に係る規定を有すると共に（Ⅴ－２－２（2）参照），個人データ・プライバシー保護の強調（Ⅴ－２－２（2）参照），サービス貿易との関係の重視[99]，規制問題の協力[100] を定めるといった特徴がある。

EUSDTP（2023 署名）は，「原則」であるため現段階では法的拘束力はないが[101]，規定ぶりを “shall be” に変更すればそのまま適用され得るような洗練された規定も含んでおり協定の原型のようである。実際両国は 2023 年 7 月に EUSDTP（及びその基であるデジタルパー

96）DEPA 附属書 14-A は，モジュール 14 の適用範囲を規定しており，これによれば 3.3 条（デジタルプロダクトの無差別待遇），3.4 条（暗号法を使用する ICT 製品），4.3 条（電子的手段による越境情報移転），4.4 条（コンピュータ設備の設置）は対象外である。附属書Ⅰ（本協定に関する了解）によれば，これらの規定は，締約国間にいかなる権利又は義務も生じさせない。

97）個人情報の定義（1.3 条）は，CPTPP と同一である。

98）Title Ⅲは 3 つの章，すなわち第 1 章一般規定（196～200 条），第 2 章データフロー及び個人データ保護（201，202 条），第 3 章特別の規定（203～212 条）で構成される（全 17 条）。このほか，サイバーセキュリティは，別途，分野別協力の一部として扱われ（Part Four（分野別協力）Title Ⅱ（サイバーセキュリティ）），紛争処理も別途（Part Six（紛争処理及び水平的規定）Title Ⅰ（紛争処理）），個人データ保護関連規定も数か所にある。

99）例えば「電子的送信」はサービスの提供とみなされることの確認規定（203.1 条），及び Title Ⅲ（デジタル貿易）において，「コンピュータ・サービス」の範囲の拡大に係る締約国の了解を規定する（212 条）。

100）EU・UKTCA Article 211 Cooperation on Regulatory Issues with regard to Digital Trade.

トナーシップ）における「協力と収束に基づいて」，デジタル貿易協定の交渉を開始すると公表している[102]。内容面では，AIや規格・適合性評価に係る詳細な規定など，EU・UKTCAが規律しないイシューを含み，先進的である。

RCEP（2020署名・2022発効）のEC章（12章，全17条）は，EC-JSI交渉で収束済のイシュー及びGATSで規定済のイシューを中心に基本的事項をカバーすると共に，データ関連規律（12.14条コンピュータ設備のロケーション，12.15条電子的手段による情報の越境移転）を含む。また，オンライン個人情報保護（12.8条）に係る規定も有する。しかしながら，後述するようにデータ関連規律に広い例外を定めるなど（Ⅴ－２－２参照），全体としてルールのレベルはそれほど高いと言えず[103]，現行では紛争処理手続（19章）も12章に不適用である（12.17.3条）。一方，画期的といえるのは，ECに関する対話（12.16条）に，産業界，専門家，学界その他の利害関係者（ステークホルダー）の参加を含むことができるとされ，ステークホルダーの関与の機会が提供されている点である。

以上を踏まえて，次節では，1）新しいタイプの貿易制限措置（データ関連規定），2）デジタル貿易関連の非貿易的関心事項，3）新たな関係者，4）デジタルデバイド，5）その他，に係る対応について協定横断的に検討する。検討に際して，本稿では協定の前文や締約国の「認識」を定める条項にも着目している。これらは締約国の権利義務を定めるものではないものの，一定の意義のあることが指摘されている。その一部について予め言及しておく。まず，前文については，第一に解釈上の文脈の一部を構成し[104]，第二に協定の目的，目標が明らかにされる点で，条約解釈に重要な影響を与え得る[105]。締約国の「認識」を定める規定については，締約国の相互の一般的な期待を基礎づけ，当該分野の将来の方向性も既定し得る点で価値のあるものであるほか[106]，こうした規定が，交渉時に行われた議論を推察する手がかりとなるとの指摘がある[107]。両者を含め，これらの規定は，拘束力を有しないものの締約国の行動に徐々に影響を与える有用な手段でもあり得る[108]。

Ⅴ－２．横断的検討

Ⅴ－２－１．新しいタイプの貿易制限措置への対応

データ関連規定である越境データ移転，及びローカリゼーション規律は，本稿で検討対象とした協定全てに含まれている。その主たる内容は，概ね，事業実施を目的とする情報の越境移転の許容と，事業実施の条件としての自国内におけるコンピュータ設備の利用又は設置要求の

101）Singapore and the European Union Sign Digital Partnership，1 February 2023 para.20. <https://digital-strategy.ec.europa.eu/en/library/eu-singapore-digital-partnership>; EUSDTP前文9th recital. 以下，「条」はEU側公表のデジタル貿易原則によるナンバリングに基づく。EU，“Digital Trade Principles” <https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en>

102）“Joint Statement on the Launch of Negotiations for an EU-Singapore Digital Trade Agreement” <https://policy.trade.ec.europa.eu/news/joint-statement-launch-negotiations-eu-singapore-digital-trade-agreement-2023-07-20_en>

103）デジタルプロダクト，ソースコード，金融サービスに係るコンピュータ設備のロケーション等は，今後の対話義務の対象として挙げられるにとどまる（12.16.1（b）及び（c）条）。12章を19章（紛争処理）の対象とするかも含めて，これらのイシューは，締約国間で別段の合意ない限り，RCEP発効から5年後に実施予定（その後は5年毎）の一般レビュー（20.8条）における検討対象であり，締約国には検討義務がある（12.16.1条）。

104）ウィーン条約法条約31条2項。

105）*E.g.*, Gleason and Titi（2022）p. 7.

106）サイバーセキュリティの文脈で，Whitsitt（2023）p. 18.

107）木村（2022）p. 1570.

108）Peng（2022）p. 786.

禁止である。これらの規定の原型はCPTPP（14.11条[109]，14.13条[110]）であるが，CPTPPは金融サービスを対象としない。金融サービスについては，越境データ移転はDEPA，EUSDTPを除く協定に，ローカリゼーションについては，CPTPP，DEPA，EUSDTP，RCEPを除く協定に関連規定がみられた（補論表1参照。以下横断的検討について適宜同表を参照のこと）。また，これらのデータ関連規定は，一定の条件の下で“legitimate public policy objectives”（LPPO：正当な公共政策目的）達成のための措置をとることを妨げられないとするLPPO「例外」を伴う（但し，USMCA，EU・UKTCAについては後述する通り）。一定の条件とは，例えば，(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，及び (b) 目的の達成のために必要である以上に情報の移転に制限を課すものではないこと，である（金融サービスについては異なる条件等が付されることがある）。なお，エンフォースメントについては，DEPA，RCEPのデータ関連規定が各々の紛争処理手続の対象外であるほかは，各紛争処理手続の対象である。

データ関連規定に関して，突出して強い義務を定めるのはUSMCAである。USMCAの情報の越境移転（19.11条）[111]は，CPTPPと同様にLPPO「例外」を認めるが，LPPO達成のために必要な措置の採用または維持を妨げられない，と「必要な」を入れて必要性を強調し，措

109）CPTPP 14.11 Cross-Border Transfer of Information by Electronic Means
1. The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

110）CPTPP Article 14.13: Location of Computing Facilities
1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

111）USMCA Article 19.11 Cross-Border Transfer of Information by Electronic Means
1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
(b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective. (*Footnote 5 omitted*)

置をとる国のハードルを高くしているようである。さらに，データローカリゼーション規律では他の協定に見られるようなLPPO「例外」をそもそも規定しない（同19.12条）[112]。

EU・UKTCAはデータ関連規律について独特の構造をとる。201条（越境データフロー）は，締約国に越境データフローの確保を求め（“are committed to”），締約国の一定の行為による締約国間の越境データフローの制限を禁じる。対象となる行為は，（データの）（a）処理のため，締約国内におけるコンピュータ設備又はネットワーク要素の使用要求，（b）保存または処理のため，締約国内へのデータのローカライズ要求，（c）他締約国内における保存又は処理の禁止，（d）自国内におけるコンピュータ設備又はネットワーク要素の使用，またはローカリゼーション要求を越境データ移転の条件とすること，である[113]。LPPO「例外」についても，これを「権利」と捉えて（198条「規制する権利」），他の協定と異なる形をとると共に，“legitimate policy objectives”（LPO：正当な政策目的）を例示する。これはLPPO「例外」よりも強い形ともいえるが，この点は次節でみるように別の問題を想起する（Ⅴ－２－２（1）参照）。

RCEPでは，他の協定よりも広いLPPO「例外」及び安全保障例外がデータ関連規定に定められている。RCEPでは，締約国に，対象者[114]に対して同国域内における事業実施の条件としてコンピュータ設備を域内で利用又は設置するよう要求することを禁止する（12.14.2条）。また，事業実施目的の場合の電子的手段による情報の越境移転の妨げを禁止する（12.15.2条）。但し，これらの禁止規定に違反する措置であっても，LPPO達成に「締約国が必要と考える」措置は，恣意的または不当な差別または偽装された貿易制限とならない態様で適用されることを条件に許容され（12.14.3.a，12.15.3.a条），必要性の判断は措置実施国によることを明示する（両条注）。現状ではEC章は19章（紛争処理）の対象でないが[115]，仮に本条が19章の対象になったとしても，LPPOの対象は広く，また必要性も措置実施国が判断することになり，争い得るのは適用条件の充足性のみということになる。加えて，安全保障については，締約国が安全保障上の重大な利益の保護に必要と考える措置をとることを妨げられず，当該措置は他締約国に争われてはならないことをも規定する（同12.14.3.b，12.15.3.b条）。つまりLPPO「例外」よりもさらに締約国の裁量は広く，係争の余地は少ない。こうしたRCEPの規定ぶりは法的不安定性につながり，ひいては禁止規定自体を無意味にしかねない。

以上のように，本稿で検討対象とした協定では新しいタイプの貿易制限措置に対応する規律がみられるが，金融サービスのローカリゼーション措置への対応など，規律を拡充する余地のあることが窺える。

112）USMCA Article 19.12 Location of Computing Facilities
No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory.

113）本規定の実施に係るレビューが義務とされており，協定発効後3年以内に規定の機能が評価される。また，締約国は（a）～（d）の見直しを他締約国に提案可能であり，被提案側は提案に妥当な考慮を払わなければならない（201.2条）。

114）端的には締約国の投資家，投資財産，サービス提供者をさす（但し，金融機関，公的機関，金融サービス提供者を除く）（12.1.b条）。

115）現行では紛争処理（19章）手続は12章（EC）に不適用である（12.17.3条）。仮に12章の解釈適用について締約国間の相違が生じた場合には，協議とRCEP合同委員会への問題付託（12.17.1及び同2）が可能であるのみである。19章の対象とするかどうかは締約国間で別段の合意がない限り，RCEP発効から5年後に実施予定（その後は5年毎）の一般レビュー（20.8条）の検討対象となっており，締約国には検討義務がある。但し，レビューで19章の12章への適用が合意されたとしても，その適用は合意した国に限定される（12.17.3条）。

Ⅴ－２－２．非貿易的関心事項への対応

（1）「規制する権利」と LPPO

非貿易的関心事項という観点から，まず指摘すべきは，締約国の「規制する権利」に対する意識の強化である。本稿で検討対象とした協定では，主として協定の前文において「規制する権利」への言及がみられた。前文では「規制する権利」と共に“legitimate public welfare objectives”（LPWO：公共の福祉に係る正当な目的）が示され，その内容が例示されている場合もある（CPTPP，USMCA，DEA，UKSDEA にみられる。例示しないものとして，DEPA，EUSDTP，RCEP）。例えば，CPTPP の前文では規制する権利と並列して LPWO を保護する決意の認識が謳われ，公衆衛生，安全，環境，有限天然資源の保存，金融システムの健全性及び安定性，公衆の道徳が例示されている。SAFTA の EC 章を置き換える DEA に関しては，SAFTA の前文では「規制する権利」に言及しなかったものが，DEA で SAFTA の前文も併せて置き換えて新たに当該権利に言及しており[116]，デジタル貿易の規律の導入が契機となったことが窺われる。また，締約国のこうした意識は，データ関連規律において LPPO「例外」が規定されている点にも見出すことができるといえよう。

なかでも EU はデジタル貿易の規律（EU・UKTCA Title III）で，LPO を達成するための締約国の「規制する権利」（198 条）を規定すると共に LPO を例示する[117]。併せて Title III の規定によって，締約国は，184 条（プルーデンシャルカーブアウト），412 条（一般的例外），415 条（安全保障例外）に規定される公益上の理由（public interest reasons）のためにこれらの規定に従った措置を採択又は維持することを妨げられない旨確認しており（199 条　例外）[118]，規制の自律性（autonomy）への意識は突出している。

とはいえ，「規制する権利」や LPPO の概念はそれほど明確ではない。データ関連規定における LPPO「例外」，前文で謳われる「規制する権利」と LPWO という概念があり，加えて EU・UKTCA では，類似の概念が LPO と表現されてその内容が例示されている[119]。各々は例示される場合もあり，その例示内容をみると似通っているが，微妙に相違もある。もちろんこれらは例示に過ぎないことに加え，そもそも何が正当な政策目的かは，各国の発展段階，経済状況，社会・文化的状況などに依って異なり得るため限定するのは困難である。但し，懸念されるのは，それによって「例外」の範囲が広がり，原則が意味をなさないほどに浸食される可能性である。

EU・UKTCA の「規制する権利」は，例外

116）DEA Annex B Preamble（関連部分，下線は筆者による）
“Recognising their inherent right to regulate and resolving to preserve their flexibility to set legislative and regulatory priorities, safeguard public welfare and protect legitimate public welfare objectives, such as public health, safety, the environment, privacy, the conservation of living or non- 37 living exhaustible natural resources, the integrity and stability of the financial system and public morals;”

117）EU・UKTCA Article 198 Right to regulate
The Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity.

118）EU・UKTCA Article 199 Exceptions
For greater certainty, nothing in this Title prevents the Parties from adopting or maintaining measures in accordance with Articles 184, 412 and 415 for the public interest reasons set out therein.

119）さらには，EU・UKTCA の前文では，LPPO 達成のための締約国の規制する権利と LPPO が例示される。（Preamble, “7. RECOGNISING the Parties’ respective autonomy and rights to regulate within their territories in order to achieve legitimate public policy objectives such as...”）

条項との関係という別の問題も提起し得る[120]。198条（規制する権利）は，LPO達成のために，締約国が自国内で規制する権利を有することを再確認すると規定する。LPOとして，公衆衛生，社会サービス，公教育，安全，気候変動を含む環境，公衆道徳，社会又は消費者保護，プライバシー及びデータ保護，又は文化多様性の促進及び保護が例示されている。同時に，199条（例外）では，上述の通り，TitleⅢの規定により，締約国は他章の例外規定（184，412，415条）が定める公益上の理由のため，これらの規定に従って措置を採択又は維持することを妨げられない旨規定する。LPOと「公益上の理由」の一部は重なるため，両者の関係がやや判然としない部分がある。例えばLPOの一つに文化多様性が挙げられているが，文化多様性の保護のために一部のデータの越境移転を制限する締約国の措置は，412条（一般的例外）で文化多様性を保護する措置が列挙されていないなかで，どのように理解されるのだろうか。権利として当然に当該措置が認められるのか，そうであればLPOの内容は例示に過ぎない中でそうした措置は無制限に広がるのか。特に，GATT20条を準用する412条との相違の一つは，いわゆるGATT20条の柱書に定められるような適用のための条件がない点にあり，濫用につながることも懸念される。それともEU・UKTCAの規制する権利は一定の制限を受けるのだろうか。さらにいえば，“LPPO”と“LPO”―違いは“public”の有無である―はどの程度の相違を生じさせるのだろうか。これらの諸点はさらなる検討に値しよう。

（2）個人情報保護

GATSでは例外事由の一つに例示されていたプライバシーの保護は，本稿で対象とした協定において，デジタル貿易の規律上「デジタル貿易の利用者」（例，USMCA19.8条）ないし「電子的取引に従事する者」（例，DEA17条）の個人情報を保護する法的枠組みの採用又は維持を締約国の義務とする（「原則」のEUSDTPを除く。また，後述のようにEU・UKTCAは権利とする規定ぶりである）。

なかでもDEPAは非常に詳細な規定を有しており，個人情報の越境移転を可能とする具体的な方法にも言及する。DEPA4.2条（個人情報保護）は，デジタル経済における個人情報保護の重要性に対する認識を規定し（1項），締約国にEC及びデジタル貿易の利用者[121]の個人情報保護を定める法的枠組みの採択又は維持を義務づける（2項第1文）。同枠組み策定にあたっては，関連国際機関の原則及びガイドラインの考慮を義務とし（2項第2文），同枠組みを支える原則として8つの原則が含まれるべきとして例示する（3項）。これらはいわゆるOECD8原則[122]に相当するものである。加えて，締約国に，自国内で発生する個人情報保護違反からEC利用者を保護するために非差別的な慣行を採用する義務（4項），同利用者に提供する個人情報に係る関連情報の公表義務（5項）を課す。さらに，個人情報保護のため締約国で異なる制度間の互換性及び相互運用性の促進メ

120）EU・UKTCA以外の協定では，一般的例外は，EUSDTPを除き，GATT20条及びGATS14条，又はGATS14条のみが全部又は部分的に準用される形となっている。環境関連部分などに拡充がみられる場合もある。EU・UKTCAにおいてもGATT20条は準用されるが，追加的な条件等が付加されている。GATS14条については言及されないものの，同条と類似の内容が一部規定される（412条）。

121）ECとデジタル貿易を書き分けているが，いずれも定義しない。

122）OECDガイドライン（OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）に含まれる原則で具体的には次の通り。1）Collection Limitation Principle，2）Data Quality Principle，3）Purpose Specification Principle，4）Use Limitation Principle，5）Security Safeguards Principle，6）Openness Principle，7）Individual Participation Principle，8）Accountability Principle.（邦訳すると順に，収集の制限，データの質，目的の特定，使用の制限，安全保護措置，透明性，個人の参加，説明責任））。

カニズム[123]の開発及び同メカニズムの適用に係る情報交換等を義務とする（6，7項）。また，締約国には，事業者によるデータ保護に係るトラストマークの採用奨励の義務（8項）及び当該マークの利用に関する情報交換と経験共有を義務とし（9項），越境情報移転を促進する有効な手段として他締約国のトラストマークの相互承認を努力義務とする（10項）。本条はDEPAモジュール14（紛争処理）の対象であり法的実効性を伴うものである。もともとFTAでは，環境や労働などの規律が含まれることで，規律対象範囲が広がる傾向があり，その際には貿易との関係の希薄化すらみられる場合もあった[124]。上記のDEPAの規定が示すように，デジタル貿易は貿易協定に個人情報保護を含む形でその傾向を強めているといえる。

また，個人情報保護との関係では，個人データ保護を基本的人権として捉える[125]EUの高い保護水準が知られている。EU・UKTCAでも，個人データ及びプライバシーの保護に対する強い意識がみられる[126]。Title III 第2章「データフローと個人データ保護」では，個人データ及びプライバシーの保護が個人の「権利」と明示され[127]，協定の別の章でもこの点が確認されている（769条個人データ保護）。

EUの高い保護水準はまた，米国などの比較的緩やかな姿勢と相違するため，デジタル貿易に係る国際的なルール形成上の課題の一つとなってきた。しかし，本稿で検討した貿易協定からは，本件の進展を期待させるような発展もみられた。従来，EUは個人データを貿易交渉の対象とすることができず，その背景には，欧州委員会の貿易総局と司法総局の間で，個人データの保護を確保しながら貿易協定でデータの越境移転に対処する方法をめぐる対立があったといわれている[128]。しかし，EUは2018年にEUの貿易協定における越境データフローと個人データ保護に係る横断的規定（以下，横断的規定）を承認した[129]。これらの条項に基づく交渉が二国間で奏功したものもあり，また，

123）方法として，規制結果の承認又は相互協定，より広範な国際的枠組み，トラストマークや認証，締約国間の個人情報移転のためのその他手段，を例示する。

124）例えばCPTPPとUSMCAでは，「締約国間の貿易又は投資に影響を及ぼす態様で」国内環境法の実効的な執行を怠らないことが締約国の義務であるが（CPTPP20.3.4条，USMCA24.4.1条），USMCAでは「締約国間の貿易又は投資に影響を及ぼす態様で」という要件は，そうでないことを被申立国が反証しない限り満たされたと推定されることとなり，大幅に緩和されている。

125）TFEU16.1条，Charter of Fundamental Rights of the EU 8.1条。なお，石井（2017）3-4頁も参照。

126）個人データは「データ対象者（data subject）に関する情報」（6.1.d条）と定義される。

127）EU・UKTCA Article 202 Protection of Personal Data and Privacy

1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade.
2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application1 for the protection of the data transferred. 3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains.

128）Aaronson and Leblond（2018）pp. 261-262. この結果，例えば，日EU・EPAは，データの越境移転については協定発効から3年以内に再度検討するというレビュー条項を含むのみであった（日EU・EPA8.81条）。その後，2022年10月に両国はこの点に係る交渉開始に合意している。外務省プレスリリース <https://www.mofa.go.jp/press/release/press6e_000412.html>；EUプレスリリース <https://policy.trade.ec.europa.eu/news/eu-and-japan-start-negotiations-include-rules-cross-border-data-flows-their-economic-partnership-2022-10-07_en>

129）“Horizontal Provisions on Cross-border Data Flows and Personal Data Protection” <https://ec.europa.eu/newsroom/just/items/627665>

EC-JSI交渉の文脈でも提案されているという[130]。EU・UKTCAにも，横断的規定の一部が反映されている。但し，欧州データ保護監察機関（EDPS）は，EU・UKTCAに横断的規定が全て反映されていないことを強く批判する意見を出しているほか[131]，横断的規定の活用については，依然としてEU加盟国の意見は分かれているとの見方もある[132]。それでもなお，EUが個人データ及びプライバシーの保護を貿易協定で扱うこと自体，この問題の進展を期待させるものである[133]。

米国の姿勢も変化しているようである。米国の立場が反映されたTPPをほぼ継承したCPTPPの個人情報保護（14.8条）規定は，EC利用者の個人情報保護を定める法的枠組みの採用又は維持義務を課すものの，その内容は比較的緩やかである。具体的には，同枠組み作成にあたり，締約国は関連国際機関の原則及び指針の考慮が求められるが，これは「考慮すべき」であるにすぎない。本稿で検討した協定の中には，こうした原則及び指針として，OECDガイドライン（2013）[134]やAPECプライバシーフレームワーク[135]を挙げる場合がみられるが，これらにも言及しない。この緩やかさの背景の一つには，米国において，プライバシー保護が，事業者から，というよりもむしろ政府からの保護に重点がおかれ，正式なデータ保護機関がないこともあいまって，自己規制やベストプラクティスがプライバシー保護の一般的な保護モデルであるといわれる[136]ことがあるように思われる。しかし，USMCAでは，締約国の個人情報保護義務は強化されている（19.8条）。具体的には，締約国は個人情報保護[137]のための法的枠組みを採択または維持する義務を負うが，その際に検討すべき関連する国際機関のガイドライン及び原則として，上記2つが例示され（19.8.2条），併せていわゆるOECD8原則を含む9原則[138]や個人情報保護措置の遵守及び当該情報の越境移転のリスク比例性の確保に対する重要性の認識，を挙げる。加えてデジタル貿易利用者に対する個人情報保護の関連情報（自然人が救済を追求する方法等）の公開義務を定める。USMCAでは，デジタル貿易に限定せずとも，個人情報保護の一般的な必要性が打ち出され，そこでも同様の規定がある（32.8条）[139]。以上に加えて，米国内における関連連

130）*E.g.*, “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, 12.7.2022, COM（2022）336 final”, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0336>

131）“opinion/ 22 Feb 2021” <https://edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_en>

132）Zhang（2021）pp. 7-8.

133）2023年7月に署名されたEUとニュージーランドのFTA（Free Trade Agreement Between New Zealand and the European Union（EU-NZFTA））にも横断的規定が含まれている。

134）OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data（2013）.

135）APEC Privacy Frameworkは2004年に導入され，2015年に改訂されている。<https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group>

136）Burri（2021）p. 753.

137）個人情報は，「特定された又は特定し得る自然人に関する情報（データを含む。）」（19.1条）と定義され，CPTPPと同一である。

138）USMCAでは，OECD8原則のうち6）Opennessに代えて“transparency”となり，更に“choice”が追加されている。

139）本条における個人情報の定義は「特定された又は特定し得る自然人に関する情報（データを含む。）（“information, including data, about an identified or identifiable natural person.”）」で，19章の定義と同じである。

邦法案の議会提出などの動向[140]をみても，米国の対応は変化しつつあるように見受けられる。

本稿で検討した貿易協定のうち，EU・UKTCAを除く協定では，個人情報保護規定に関してある程度の収束がみられる。CPTPPの後の協定では，法的枠組みの策定の際に，国際的原則又はガイドラインを考慮することが含まれ，上述のOECDやAPECの関連原則への言及がみられる場合もある。これらに具体的に言及せずとも，OECD8原則の内容が含まれることもあるほか（例，DEPA4.2条，DEA17.3条，UKSDEA8.61E条），APECのCBPR[141]が強く推進される場合もある（例，USMCA19.8.6条，DEA17.8及び17.9条）。上述したEUと米国のアプローチの相違にみるような各国の相違を踏まえ，個人情報保護にあたっては，異なるアプローチをとり得ること，及び異なるアプローチ間の相互運用性の確保の重要性とその具体的方法が規定される場合もある（例，DEPA4.2.6条，DEA17.7条，UKSDEA8.61E.6条）。

相互運用性確保の観点から近年の興味深い発展は，Global CBPRの稼働である。もともと個人情報の保護を確保しつつデータの越境移転を実現する仕組みの一つに，データの越境移転の前提としてデータ保護基準を満たしている企業等を認証する形がある[142]。この認証の既存の仕組みとしてAPECプライバシーフレームワークへの適合性を認証するAPEC CBPRが作られていたところ，2022年4月に参加国及び地域（日本を含む9ヵ国・地域）が，APECの枠にとらわれず，より広範囲での個人データの円滑な越境移転や各国の規律の相互運用性促進などを目的としてGlobal CBPRを設立することを公表した[143]。2023年4月にはGlobal CBPR Forum規約，Global CBPRフレームワークなどの組織体制等に関する文書の公表に至り[144]，新たな国や地域が参加する体制も整うこととなった。既に英国が参加要件の緩いアソシエイトとなることを求めて，認められている[145]。企業が重視する法的確実性の向上という観点からは[146]，Global CBPRと既存のAPEC CBPRとの関係，及び，APEC CBPRとの間で長年調整がはかられてきたEUの認証システムと，Global CBPRとの関係―特に認証を相互に承認するのか―をより明確にしていくことが課題となろう。

個人情報保護については，以上のような発展を踏まえて，一層の規律の収束に向かうか，今後の展開が注目される。

（3）サイバーセキュリティ

本稿で検討した協定には全てに何らかのサイ

140）第117回連邦議会に提出されたH.R.8152など。<https://www.congress.gov/bill/117th-congress/house-bill/8152/text>

141）APEC Cross-Border Privacy Rules. <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>

142）こうした仕組みには，主に説明責任原則，十分性認定，契約（モデル条項），BCR（Binding Corporate Rule），認証，同意の6タイプがあるといわれる。OECD（2023）pp. 23-30.

143）Global CBPR Forum, “About the Global CBPR Forum”. <https://www.globalcbpr.org/about/>

144）Global CBPR Forum, News, April 13, 2023 “Global CBPR Forum Welcomes Participation by Interested Jurisdictions”. <https://www.globalcbpr.org/global-cross-border-privacy-rules-cbpr-forum-welcomes-participation-by-interested-jurisdictions/>

145）Global CBPR Forum, News, July 6, 2023 “The Forum Welcomes the UK as an Associate”. <https://www.globalcbpr.org/the-forum-welcomes-the-uk-as-an-associate/>

146）データの越境移転と企業の経験を調査したOECD（2023）によれば，各国におけるデータ保護法制の増加は，プライバシー保護に資する一方で，様々な規制に服する義務が重なることで，企業にとっての規制リスクを増加させ得るという。企業にとっての課題として，データ移転要件の透明性の向上（データ管理者／処理者の区別や「第三国へのデータ移転」の定義の曖昧性など）と規制のセクター横断的一貫性（金融データとその他データ，重要な国家インフラ関係のデータとその他データなど）を含む法的不確実性の存在などが指摘されている。OECD（2023）pp. 11-18.

バーセキュリティ関連規定が含まれており，デジタル貿易の規律に先進的に取り組む国々を中心に各国の共通の関心事項であることが表れた[147]。但し，規定の洗練度合いとしては，EU・UKTCA を除き[148]，サイバーセキュリティの重要性等に係る締約国の認識のみ定める場合（CPTPP，DEPA，DEA，RCEP）と，認識に加えて協力なども定める USMCA（19.15 条サイバーセキュリティ）[149] ないし USMCA を拡充する場合（本節で USMCA 型と呼ぶ。USMCA，UKSDEA，EUSDTP）との２つに大きく分かれた。

USMCA 型の基本的要素は，主に，上記の認識に加えて，1）関連当局の対応キャパシティ向上，2）悪意あるコードの拡散の特定と軽減のための締約国間の協力，3）リスクベースのアプローチの採用と自国内企業による同アプローチの採用の奨励，である。UKSDEA8.61L 条は，このうち 2）を含まないものの USMCA（19.15 条）を拡充した内容で，検討対象とした協定の中で最も詳細である。同条は，締約国の認識と，自国内企業によるリスクベースアプローチの採用奨励の努力義務で構成されるが，いずれについても規定を詳細化している[150]。EUSDTP（4.2 条）では，USMCA（19.15 条）の要素，UKSDEA で USMCA を拡充した内容が一部含まれる[151]。EU についても，EUSDTP は USMCA 型が採用されているため，両国間のデジタル貿易協定の交渉の結果が興味深いところである[152]。

サイバーセキュリティへの対応は，一般にますますリスクベースになっているといわれ[153]，

147）貿易協定上のサイバーセキュリティ関連規定は，狭義では「サイバーセキュリティ」，「サイバーセキュリティに関する協力」といったタイトルを付した規定が該当するが，より広義には「安全なオンライン環境の創造」（DEA18 条“Creating a Safe Online Environment”）や「オンラインの安全性及びセキュリティ」（DEPA 5.2 条 “Online Safety and Security”）といった規定，サイバーセキュリティを理由とするソースコード（またはソースコード中のアルゴリズム）へのアクセス要求の可否に関連する規定（例えば USMCA19.16 条）なども含まれ得る。本稿では特に狭義の意味の関連規定及び後述する安全保障例外を検討対象とした。

148）EU・UKTCA では，協力対象事項の一部として規定される。

149）USMCA Article 19.15: Cybersecurity

1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:
   (a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and
   (b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.
2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

150）例えば，認識面では，サイバーセキュリティに関する（c）対話の維持，（d）消費者向け IOT 機器の基本的セキュリティ基準の相互承認，（f）R&D の協力等の重要性を追加している。また，リスクベースアプローチについては，（a）サイバーセキュリティリスク事象の検知，対応，回復，管理のため，及び（b）業界及び顧客の強度向上のため，オープンで透明な業界基準に依拠するアプローチの使用奨励義務を課す。

151）具体的には，締約国の認識（サイバーセキュリティ事象や脅威がデジタル貿易の信頼を損なうこと，ビジネスにとって安定的なデジタル貿易環境の必要性），悪意あるコードの拡散の特定と軽減のため関連当局のキャパシティ向上と情報交換及び協力の必要性，リスクベースのアプローチの有効性に鑑みた同アプローチ，及び，サイバーセキュリティリスク事象の検知，対応，回復，管理のためのリスク管理のベストプラクティスに係る自国内企業による採用奨励，である。

152）なお，EU-NZFTA のデジタル貿易章にはサイバーセキュリティ条項は見られない。

USMCA のように貿易協定にリスクベースのアプローチが規定される例も観察されるようになっている。サイバーセキュリティ対応措置は，予防的かつ長期的性格をもち，定期的なリスクの評価を必要とするダイナミックなプロセスであるため，すぐに古くなり得る「過度に記述的な規制（“overly prescriptive regulation”）」よりもリスクベースの対応が適切であるとされる[154]。リスクベースのアプローチは，少なくとも本稿で検討した協定では明確に定義されないが，そのアプローチでは「政府，組織，企業に攻撃のリスクを評価し，潜在的な被害を判断し，リスクや影響を軽減するための適切な対策を策定する」ことが求められる[155]。USMCA（19.16 条）も，同アプローチにおいては，「サイバーセキュリティのリスクの特定，それからの保護，サイバーセキュリティの事象の検出，対応，回復のために合意に基づく基準及びリスク管理のベストプラクティスに依拠する」と説明しており，同条も貿易協定に表れるリスクベースアプローチを理解する一助となる。以上をみると，このアプローチは端的にはリスクの存在を前提に，リスクに基づいて導入すべき措置を決定するものといえ，WTO の SPS 協定における危険性評価に基づく許容可能なリスクのレベルの決定とそれを達成する SPS 措置の導入，という一連の流れに類似する。しかし，サイバーセキュリティでは安全保障の要素が加味され得る点で，人動植物の生命健康の保護よりも情報開示が困難となり，第三者による調査も難しい[156]。そこで現状では，サイバーセキュリティ対応措置については，貿易協定上のサイバーセキュリティ条項による協力と，GATT21 条（ないし WTO 協定上の同条類似の規定）を改訂した安全保障例外（以下，安保例外）条項の採用で対処されている。そこで次に安保例外条項を見ておく。

貿易協定でよく知られている安保例外条項は GATT21 条である。しかし，GATT 違反のサイバーセキュリティ対応措置を同条により例外として許容する可能性については否定的な見方が多い[157]。その論拠は，概ね上述のように予防的，長期的性格をもち，定期的なリスクの評価を必要とするダイナミックなプロセスであるサイバーセキュリティ対応措置が「国際関係の緊急時（“taken in time of… other emergency in international relations”）（GATT21 条（b）（iii））」にとられる必要があるなど GATT21 条が規定する様々な条件を満たさないとするものである[158]。

一方，本稿で対象とした貿易協定の安保例外条項は CPTPP（29.2 条　安全保障のための例外）[159] と同一のタイプ（CPTPP，USMCA，DEPA，DEA）と，GATT21 条の構造（特に同条（b）の類型を維持）を保持するタイプ（UKSDEA，EU・UKTCA，RCEP）の 2 つに分かれる（EUSDTP を除く）。前者は，GATT21 条の類似の文言を採用するが，主として同条（b）が規定するような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（“action”）のリスト化を行わず措置の限定を取り払っており，例外の範囲を拡大し得

153）Meltzer（2019）pp. 1-2.

154）Meltzer（2019）p. 24. また米国，EU，オーストラリア，中国もこのアプローチを重視している。例えば，米国については，NIST（2018）p. 3.，EU については，Directive（EU）2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation（EU）No 910/2014 and Directive（EU）2018/1972, and repealing Directive（EU）2016/1148（NIS 2 Directive），オーストラリアは，Chang and Liu（2022）p. 195, ft.15, 中国については，Meltzer（2019）p. 12 参照。

155）Meltzer（2019）p. 1. OECD（2015）p. 5. NIST（2018）pp. 4-5.（特に 1.2 Risk Management and the Cybersecurity Framework）

156）Meltzer（2019）p. 26.

157）*E.g.*, Whitsitt（2023）pp. 8-13; Chang and Liu（2022）pp. 192-193; Meltzer（2019）pp. 20-23.

158）*E.g.*, Meltzer（2019）pp. 20-23.

る。一方，UKSDEA，EU・UKTCA，RCEPは，主としてGATT21条（b）の上記リストに追加的な要素を加えて例外の範囲を拡大する[160]。いずれによっても一般論としては，GATT21条よりもサイバーセキュリティ対応措置を正当化し易いと考えられる。類型のリストがある方が措置は限定されるため，抑制的といえる。

サイバーセキュリティ対応措置の例外としての許容可能性という観点からみると，特に，UKSDEA及びRCEPの規定が注目される。UKSDEAでは，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のリストに「重要な公共インフラ（一般公衆に不可欠な物品又はサービスを提供する通信，電力又は水のインフラに関連するもの）を，機能不能にし，又は破壊しようとする意図的な企てから保護するためにとる措置」が追加されている（16.11条（b）（iv））。RCEPでも，同リストに，通信，電力，水のインフラを含む重要な公共インフラ（公有か私有かを問わない）の保護のための措置，及び国家緊急事態に際しての措置，が追加されている（17.13条（b）（iii）及び（iv））[161]。両条項は，例えばサーバ攻撃から重要な公共インフラを保護するための措置を包含すると考えられ，GATT21条よりもサイバーセキュリティ対応措置が許容されやすいと捉えられる[162]。

サイバーリスクは，ネットワークでつながっている各国にとっての共通リスクであるため，各国間で協力して対応することが必要とされる。他方でサイバーセキュリティは安全保障に関連し得るために高度な規制の自律性も求められ，それが偽装された貿易制限措置につながりやすく，また無制約に措置がとられかねない危険性を有する面をもつ。この点で，本稿で検討対象とした貿易協定では，サイバーセキュリティ条項で協力を定めながら，安保例外条項でサイバーセキュリティ対応措置が例外として許容され得る余地を広げるという現実的な対応がとられているといえる。但し，安保例外条項は，

159）CPTPP Article 29.2: Security Exceptions
Nothing in this Agreement shall be construed to:
（a）require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or
（b）preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.

160）*E.g.*, UKSDEA ARTICLE 16.11 Security Exceptions（関連部分のみ）
Nothing in this Agreement shall be construed to:
…
（b）prevent either Party from taking any action which it considers necessary for the protection of its essential security interests:
（iv）taken in time of war or other emergency in international relations, or to protect critical public infrastructure（this relates to communications, power or water infrastructure providing essential goods or services to the general public）from deliberate attempts to disable or disrupt it;
…

161）RCEP Article 17.13: Security Exceptions（関連部分のみ）
Nothing in this Agreement shall be construed:
…
（b）to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests:
（iii）taken so as to protect critical public infrastructures7 including communications, power, and water infrastructures;
（iv）taken in time of national emergency or war or other emergency in international relations; or
…

162）*See.*, Whitsitt（2023）pp. 13-16.

結局のところケースバイケースでの援用であり不安定である。いずれ，貿易とサイバーセキュリティの関係をより親和的にする形のルールが必要になると思われる。

Ⅴ－２－３．新たな関係者

（1）オープンガバメントデータ

オープンガバメントデータに係る規定は，USMCA で導入されて以降，本稿で検討した協定においても，ほぼすべてにそのまま，あるいは発展させる形で含まれている（RCEP を除く）。USMCA（19.18 条）は，データの公開が経済社会の発展，競争力と技術革新の促進につながることの認識，及びデータを含む政府情報を一般に利用可能とする場合に，当該情報の機械での読み取りや検索等を可能とすると共に，当該情報へのアクセスと利用を拡大する方法の特定のため協力する努力義務を締約国に課す。

USMCA の規定は DEA で強化され，EU・UKTCA でもさらに発展した。DEA（27 条）は，USMCA とほぼ同趣旨で，データを含む政府情報が利用しやすい形で公開されることを目途するが，確保努力義務の対象である公開の態様がより具体的になっている[163]。EU・UKTCA210 条は，公開の態様をさらに詳細にしている[164]。

このようにオープンガバメントデータは，データの保有者ないし提供者としての政府の役割を明確化し，かつ改善する点で評価に値するが，一方で裨益するのはこうしたデータを活用する技術ないしはキャパシティを有する企業だけではないか，との批判もある[165]。政府データが公的に整備されることに鑑みれば，裨益者が限定されないことが望ましく，政府データの活用促進と同時に，このような批判への対応も必要であるように思われる。なお，この点に関連して，今後の発展が興味深いのは，EUSDTP（2.2 条）が「関心あるステークホルダーとの協議等を通じて，オープンガバメントデータの範囲を拡大する」ことに言及する点である。上記の批判に鑑み，関心あるステークホルダーがプラットフォーム企業などのデータ利用事業者にとどまらないことが期待される。

（2）ステークホルダーエンゲージメント

デジタル貿易ないしデジタル経済が広く一般社会にも影響することに鑑みると，既述の通り，様々なステークホルダーがデジタル貿易の規律検討に関与することは重要である。この点で注目すべきは，DEA と UKSDEA に取り入れられたステークホルダーエンゲージメントに係る規定である。両協定における関連規定の内容は同一であるので，DEA を概観する。DEA（35 条）は，主に，締約国間の「デジタル経済対話」の開催機会の追求義務，それを通じた関連協力努力の推進義務を規定する。当該対話には，適切な場合かつ両国が合意する場合に，ステークホルダーの参加（ステークホルダーは定義されないが，リサーチャー，学者，産業界，その他が例示される）を認め，また対話開催にあたってこれらと協力し得る旨を定めるものである。なお，既述の通り，RCEP においても「EC に関する対話（12.16 条）」を定めて当該対話へのステークホルダーの参加可能性を認めている。遵守確保の観点から，これらの規定の運用状況を注視していくことが必要であると思われる。

ステークホルダーの関与については，DEPA

163）具体的には次の通り。(a)「情報の適切な匿名化，記述的なデータの含有」追加，(b)「情報が可能な限り，信頼性が高く，使いやすく，自由に利用できる API を備えた空間的に利用可能なフォーマットで提供され，定期的に更新されること」。

164）具体的には次の通り。(a) 検索，取得，使用，再利用，再配布が容易な形式；(b) 機械的に読み取り可能かつスペース的に有効なフォーマット；(c) 記述的なメタデータを含み，それは可能な限り標準的であること；(d) 信頼性ある，ユーザーフレンドリーな，自由に利用できる API を介した提供；(e) 定期的な更新；(f) 差別的または不必要に再使用を制限する使用条件でないこと；(g) 各締約国の個人データ保護規則を完全に遵守した再利用であること。

165）Streinz（2021）pp. 178-179.

及び UKSDEA に規定されるデジタルインクルージョン（後述）もステークホルダーとの協議可能性を規定する。UKSDEA のように両方が含まれれば理想的である。

Ⅴ－２－４．デジタルデバイドへの対応

（１）デジタルインクルージョン

本稿で検討した協定の中でも，デジタルインクルージョンは DEPA と UKSDEA のみが規定する[166]。デジタルインクルージョンは定義されないものの，例えば DEPA では「女性，農村住民，社会経済的に低い集団，先住民族のデジタル経済への参加」が関連事項として挙げられており，少なくともこれらが含まれることが分かる（11.1.3 項）。さらに，UKSDEA では国家間のデジタルデバイドも言及される（8.61P 条）。

DEPA の規定は UKSDEA で発展している。まず，DEPA（11.1 条）は，デジタルインクルージョンの重要性，及び障壁除去によるデジタル経済の機会の拡大及び促進の重要性（先住民族間を含め文化的及び人と人とのつながりの強化，女性，農村住民，社会経済的に低い集団のアクセス改善を含み得る）に対する締約国の認識と，デジタルインクルージョンに係る締約国間の協力義務とその内容の例示，当該協力活動が締約国の関連機関，企業，労働組合，市民社会，学術機関及び NGO 等の連携を通じて実施され得る旨規定する。UKSDEA（8.61P 条）は，DEPA よりも認識や協力義務の例示を詳細にすることに加えて，国家間のデジタルデバイドに対する認識，それに対応するための締約国間の協力を強化する努力義務とその方法の例示，WTO などの国際機関におけるデジタル貿易におけるインクルージョン促進イニシアチブへの積極的な参加義務を新たに追加するなど，DEPA を拡充するものである。

DEPA 及び UKSDEA で興味深いのは，締約国域内に限定せず，一般的にデジタルインクルージョンの重要性を認め，そのための締約国の協力義務及び協力活動を例示すると共に，市民社会等の関与を明示する点である。ステークホルダーエンゲージメントと併せて，遵守確保の観点から，運用状況の検討が重要であると思われる。

（２）中小企業及び途上国

デジタルデバイド関連では，中小企業及び途上国のキャパシティ不足が特に懸念されている[167]。FTA では中小企業や途上国支援に関連する章が含まれることもあるものの，これらについてデジタル貿易章ないしデジタル貿易協定で規定しているのは，本稿が検討した協定のなかでも DEPA，DEA，UKSDEA のみである。なかでも DEPA が詳細であるので，関連規定をみておく。DEPA のモジュール 10（中小企業協力）は，デジタル経済における中小企業の貿易・投資機会の拡大及び雇用と成長の促進のため，締約国に様々な協力義務，情報公開義務，対話義務を課す。中小企業支援に多くの規定を割いている点で特徴的である[168]。

先進国と途上国間のデバイドについては，上述したデジタルインクルージョンが途上国対応の一部を構成しているといえよう。途上国支援

166）EUSDTP では，５節デジタル貿易に係る協力において，女性その他の低社会経済グループが直面するデジタル経済参加上の障壁への対処，中小企業支援が含まれており，類似する要素が規定されている。

167）WTO（2018）Section B.

168）10.1 条（一般原則）では，デジタル経済における中小企業の役割，中小企業関連の協力における民間企業の役割等の重要性に対する締約国の認識を規定し，10.2 条（デジタル経済における中小企業の貿易・投資機会強化のための協力）では，締約国間の関連情報交換等の協力義務と中小企業支援のプラットフォームへの自国内中小企業の参加奨励義務を課す。10.3 条（情報共有）では，中小企業向けの情報提供サイトの確立または維持義務とその内容の定期的の定期的なレビュー義務等，19.4 条（デジタル SME 対話）では，対話の開催義務（締約国の企業，NGO，学識者，その他の利害関係者を含み得るとされる）とそこから得られる知見の活用等が規定される。

に具体的には言及しないものの，例えば，DEPA（11.1 条）では，協力活動の一つに「デジタル経済へのあらゆる集団の参加促進のためのプログラム開発」が例示される（11.1.3.d 条）。また，上述のように UKSDEA（8.61P 条）は，国家間のデジタルデバイドに言及する。この点は他の協定にあまり見られないことに加え，対象範囲を締約国域内に限定していない点で示唆に富むと思われる。

なお，途上国に対する配慮は，途上国の締約国に協定上の義務実施の経過期間を付与する形でも表れる。この点は，CPTPP，USMCA，RCEP のように締約国に途上国を含む協定に見られた[169]。

Ⅴ－２－５．その他

（１）AI，デジタル ID，“Tech” 関係

以上のほか，本稿で検討した協定にみられた興味深い点は，貿易協定の対象範囲をさらに広げ得る新たなイシューに係る規定が含まれることである。なかでも，DEPA，DEA，UKSDEA に共通するのは，AI，デジタル ID，“Tech” 関係（Fintech，Regtech，Lawtech）である。

AI に係る規定は DEPA（8.2 条）で導入された後，DEA（31 条），UKSDEA（8.61R 条）で徐々に拡充されている。共通する主な構成要素は，1）AI の重要性等に対する認識，2）AI ガバナンス枠組みの策定（倫理的要素への言及を含む），3）その際の国際的に承認された原則またはガイドラインの考慮，である[170]。但し，AI については共通の定義が存在しないといわれており[171]，これらの協定においても AI は定義されない。

AI は，特に ChatGPT 等のいわゆる生成 AI が 2023 年春頃から急速に普及したことにより，それまで以上に広く関心を集め，また規律の必要性が国際的にも議論されている分野である。FTA で規律される例はこれまであまりなかったが，各国において規制が導入されつつある状況をみると，今後，FTA でも規律対象となる可能性の高いイシューの一つであると思われる。その際には，上述の共通の定義の欠如が課題となり得ることに加え，現行のデータ関連規制と同様に，一方で各国の規制と貿易障壁性との関係が問われつつ，他方で，規制が許容される範囲が焦点となると思われる。さらには，倫理的要素を含むガバナンス枠組みへの言及が示唆するように「倫理」との関連性も議論され得る。このことは，同時に FTA が対象とする「非貿易的関心事項」がさらに拡大する可能性のあることを示している。

デジタル ID については，DEPA で関連規定が導入された後，DEA で強化され，UKSDEA がこれを踏襲している。DEPA（7.1 条，デジタル ID）は，各国でデジタル ID の実施と法的アプローチが異なり得ること等を認識し，主として，締約国にその相互運用性を促進する努力義務を課すもので，共通基準の確立など，そのための具体的方法も例示する。但し，当該努力義務に反する措置であっても，LPPO 達成のための措置の採用又は維持は妨げられない。DEPA は，デジタル ID を定義しないが，例え

169）CPTPP や USMCA でも，一般的に中小企業を支援する中小企業章等がおかれているが，デジタル貿易に特化したものではない。

170）EUSDTP も AI を対象としており，1）～3）の要素に言及する。

171）*E.g.*，CRS（2021）pp. 1-2. AI に係る国内の規制で定義が示されている点で興味深いのは EU の関連法案である。21.4.2021 COM（2021）206 final 2021/0106（COD）Regulation of the European Parliament and of the Council Laying down Harmonized Rules on Artificial Intelligence（Artificial Intelligence Act）and Amending Certain Union Legislative Acts {SEC（2021）167 final} - {SWD（2021）84 final} - {SWD（2021）85 final}
Article 3 Definitions
“‘artificial intelligence system’（AI system）means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”.

ばOECD（2023）によれば「ユーザーについて特徴，資質，性質，または主張を証明するために使用でき，必要な場合にはそのユーザーの識別に使用できる，電子的に捕捉及び保存された属性及び／又は証明（credentials）の集合を指す」と説明される[172]。DEA（29条）は，DEPA（7.1条）と同趣旨であるが，次の点で強化するものである。第一に，デジタルIDについて締約国間で異なり得る法的・技術的アプローチについて適合性促進メカニズム策定を追求する義務を締約国に課す。第二に，そのような適合性促進のためのイニシアチブ促進努力義務も課し，第三に，DEPAが規定していたLPPO例外を規定しない[173]。

“Tech”関係の規定は，DEPAでFintech，DEAでRegtechが対象となり，UKSDEAではこれにLawtechが加わる[174]。これらの規定の主たる内容は締約国間の協力である。各々の用語の意味するところは，DEAによれば，Fintechは「金融サービスの提供及び利用の改善及び自動化のための技術の利用」（1.r条），Regtechは「規制プロセスの遵守の改善及び管理のためのIT技術の利用」（1.x条）であり，UKSDEAによると，Lawtechは「法律サービス提供のための従来の方法を支援，補完，代替することを目的とした技術」である（8.57.r条）。

（2）海底通信ケーブル

データの越境移転には，安定したインフラが欠かせないところ，海底通信ケーブルはそのインフラの一つである。貿易協定では，海底通信ケーブルに係る規定が含まれることはあったものの，その趣旨は，締約国の海底通信ケーブルの運営者や陸揚局の管理者が，他締約国の通信事業者に対して合理的かつ無差別な条件でアクセスを認めることを確保するよう当該締約国に求めるなど，主に通信サービスの競争促進であったといえる。本稿で検討した協定でも，CPTPP（13.15条），USMCA（18.13条），RCEP（附属書8-B-18条）は競争促進的観点からの規律を定める。一方，DEA及びUKSDEAの海底通信ケーブルに係る規定は，インフラの安定性の観点を含むもので新規性に富み，注目される。

特にDEA（22条，海底通信ケーブルシステム（STCS））は，インフラとしての海底ケーブルの重要性とその敷設，運用等の安定的確保の観点に着目する規定で，STCSの迅速，効率的な配置，保守，修理（以下，配置等）や保護に障害となり得る締約国の措置について締約国間の協議と協議要請の応諾義務も含む非常に詳細な内容を有している。

具体的には，まず，通信のコネクティビティにとってのSTCSの迅速かつ効率的な配置等の重要性に対する締約国の認識を定める。そして，他締約国のSTCSの運営又は所有又は管理者（以下，運営者等）が配置等のためのサプライヤ（非締約国の者を含む）を柔軟に選択できるよう確保する締約国の努力義務，及び他締約国の者が運営者等であるSTCSの配置等のために自国外の登録船舶に許可を求める場合に，主として手続的適正の観点から様々な事項[175]の確保義務を課す。さらに，他締約国の者が運営者等であるSTCSへの損害リスクの

172）OECD（2023），*Recommendation of the Council on the Governance of Digital Identity*，OECD/LEGAL/0491，p. 6.

173）加えてDEAには，締約国間の協力の実際的な手段を定めるMOUがあり，デジタルIDもその一つである。MOUのその他の対象分野は，データイノベーション，AI，貿易円滑化，電子請求，農産品の電子認証協力，個人データ保護である。

174）但し，UKSDEAは，Fintech及びRegtechについては締約国の協力のみ定める。両者は，UKSDEAで「金融サービス全般にわたる技術の利用の改善を伴う活動」を意味するとされる（UKSDEA8.53.2条注2）。

175）具体的には，（a）認可対象活動の公開，（b）要件と手続の公開，（c）評価基準の公開，（d）申請及び更新手続の合理的，客観的，公平な管理，（e）申請者に対する合理的期間内の決定通知，（f）設置等に十分な期間の確保，（g）手数料の合理性と透明性，必要額への限定性，である（22.2条）。

軽減努力義務と，そのための方法（STCS 位置情報を地図や海図で利用可能とすること等）を例示する。

UKSDEA（8.38 条，海底ケーブル陸揚局（SCLS）及びケーブルシステム（SCS））は，SCLS 及び SCS の迅速かつ効率的な配置等の重要性に対する締約国の認識と共に，公衆電気通信サービスとして SCS 運営が認可されている場合，SCLS 及び SCS へ合理的，無差別的，透明な条件でのアクセスを確保する締約国の義務，自国内で他締約国の者が運営等を行う SCLS 及び SCS への損害リスクの軽減を許容する規定，締約国間の協力義務を主に定める。

DEA が海底ケーブルの重要性とその敷設，運用等の安定的確保の観点をより重視しているのに比べ，UKSDEA は，SCLS 及び SCS へのアクセス確保をも締約国の義務とする点で，競争促進的要素も含むものである。海底通信ケーブルに係る規定は，デジタル貿易との関係上，データ関連規定に比べると現時点ではそれほど注目度は高くないようであるが，今後，データの流通量の一層の増大が予想されるなかで重要性を増していくと思われる。

（3）新たなイシュー

以上に加えて，本稿で検討した協定のうち最も直近に合意された EUSDTP では，非個人データの保護（2.1.5 条）や民間企業の有する個人データへのガバメントアクセス（2.1.7 条）への言及もみられた。いずれも比較的新しいイシューである。ガバメントアクセスについては OECD で 2022 年に初めて勧告が採択されたところであり[176]，それによれば，民間企業の有する個人データへのガバメントアクセスは「民間部門又はデータが自国の領域内に存在しない場合において当該民間部門に政府へのデータ提供を義務付ける法的枠組みによる権限を国家が有するという状況を含め，政府が自国の法的枠組みに従ってそれぞれの領域内で法執行及び国家安全保障の目的を追求する場合に，民間部門が保有又は管理する個人データへ政府がアクセスし，これを処理すること」を内容とする[177]。これらも今後，デジタル貿易規律上の重要なイシューとなる可能性がある。

Ⅵ．結論

本稿では，デジタル貿易が貿易に及ぼす主に 4 つの課題（及び，その他を含めれば 5 つの観点）及び貿易協定側の対応について，WTO の限界を踏まえ，デジタル貿易の「ルールメーカー」とされる国々の貿易協定を中心に検討した。検討を通じて明らかとなった諸点を提示する。

第一にデジタル貿易の規律形成における協定間の相互作用の様相である。本稿で対象とした協定は，デジタル貿易という観点からみれば，大きく，アジア太平洋型（CPTPP・USMCA・DEPA・DEA・UKSDEA），EU 型（EU・UKTCA・EUSDTP），その他（RCEP）ともいうべき 3 つのパターンに分けることができる。アジア太平洋型では，SAFTA が基になって CPTPP が形成され，それが USMCA，DEPA，DEA につながった。しかしそれらは全て UKSDEA に影響を及ぼしている。既述の

176）OECD，Declaration on Government Access to Personal Data Held by Private Sector Entities，OECD/LEGAL/0487. <https://www.ppc.go.jp/files/pdf/government_access_jp.pdf>

177）*Ibid.*，p. 6. 邦訳は，個人情報保護委員会による。<https://www.ppc.go.jp/enforcement/cooperation/international_conference/OECD_0412/>

通り，UKSDEAは，その新規性及び包括性で突出しており，デジタルインクルージョンなどDEPAの優れた点も継承する。同時に，サイバーセキュリティについてはUSMCAの関連規定を基にし，それを拡充している。さらに，ステークホルダーの参加，インフラの安定性の観点を含む海底通信ケーブル規定，CPTPPやUSMCA等に比べて抑制的な安全保障例外，新規イシューに対する積極的な取り組み（AI，Fintech，Regtech，Lawtechなど）がみられる。

他方，EUは，FTAを締結する際に，従来“サービス貿易，設立，EC”という章の中でECを扱う傾向があった[178]。しかしその傾向は，EU・UKTCA，及びEU-NZFTA（2023年7月署名）でデジタル貿易に係る独立した章が設けられることで変わりつつあるように見受けられる。新たな章の特徴は，データ関連規律の独特の構造を有するなどアジア太平洋型とは異なるものであるが，USMCAを原型とするオープンガバメントデータ規定がEU・UKTCAにおいて発展しているように，またEUSDTPではDEPA等と類似の要素を含むAI規定が含まれているように，両型間でも相互作用が存在することが分かる。

FTAのデジタル貿易ルールが継年的に進化してきたことは本稿で言及したが，今回の検討を通じて，ルール形成の最先端にあるルールメーカーの貿易協定も相互に影響し合いながら，規律を洗練させ，また充実させていることが窺われた。併せて，インフラの安定性確保の観点からの海底通信ケーブル規定，AI，“Tech”関係の規定など，現在創出されつつある規定や，ガバメントアクセス，非個人データのような新たなイシューが貿易協定上に表れつつあることも示された。これらに鑑みても，規律の発展，洗練の傾向は今後とも続いていくことが見込まれる。もちろん，本稿が示したのは現時点の一過性の姿に過ぎない。しかし，その姿は，先駆的な協定ないし規定のモデルが「ルールメーカー」によって提案され，それらが影響力をめぐって競争しているようでもあり，今後の関連ルールの形成に対して示唆に富む。

第二に，デジタル貿易による貿易協定の射程の拡大とそのインプリケーションである。デジタル化は，経済や社会に広く関わる故か，デジタル貿易の規律では，以前にもまして，「貿易関連性」が広く捉えられているようである。具体的には，必ずしも直接的な「貿易関連」ではない規律が含まれ，また，WTO協定では「非貿易的関心事項」として，例外として捉えられていた事項が直接の規律対象となる例がみられる。個人情報保護，サイバーセキュリティがその例である。FTAでは既に環境や労働分野でそうした規律は増加していたが，デジタル貿易の進展はその傾向を強めている[179]。この傾向は，本来，市場原理を前提とする貿易協定の規律に「非貿易的関心事項」をある意味統合するものとみることもでき，貿易と「非貿易的関心事項」，ないしは市場原理と非市場原理とのバランスをとりつつ，ひいては規律全体を持続可能なものとするという意味では積極的に評価される面もある[180]。但し，「非貿易的関心事項」により深く入りこむことで，締約国の「規制する権利」はより強調されるようになり，同時に，制度間の「相互運用性」「互換性」「協力」などが一層重視されるようになっている。

第三に，第二の点とも関連して，デジタル貿易の規律に伴う「規制する権利」の存在感の向上と，それが貿易協定において定着しつつある状況である。WTOの文脈における「規制する

178）Wu（2017）p. 9.

179）もちろんデジタル貿易のみがその原因ではない。環境，労働などの非貿易的関心事項の台頭（この点について松下・飯野（2021）pp. 4-6参照），安全保障と，経済ないし市場に係る問題を一層接近させる国家（例えば中国）の登場，なども影響していると考えられる。

180）但し，貿易と非貿易的，ないしは市場原理と非市場原理という捉え方自体が視座を経済的関心に置いているともいえる。

権利」に係る見方の一つは，「加盟国が自ら重要であると判断する政策目的を追求する裁量，又は，国内で受忍可能な危険性を設定する自由として具現化される」というものである[181]。しかし，WTO 協定では「規制する権利」そのものは，本稿で検討した FTA に見るほどの存在感はない。「規制する権利」は GATS の前文では言及されるが，本稿で検討した協定の前文が明示しているものと異なり，WTO 協定の前文では言及されない。もちろん，「規制する権利」の考え方は WTO 協定に反映されている。例えば GATT20 条や同 21 条の例外規定や，TBT 協定の前文（6th recital）は WTO の上級委員会によって当該権利の存在を反映ないし確認するものと捉えられた経緯があり[182]，さらに，SPS 協定も規制を含めて一定の措置をとる加盟国の「権利」を規定している[183]。一方，本稿で検討した FTA にみられる「規制する権利」は，国の規制空間（policy space）を表現する LPPO などの用語と共に存在感を増している。しかしその内容は，少なくとも各々の協定上はそれほど明らかではない。懸念されるのはこうした「規制する権利」や，LPPO ないし LPPO 類似の概念によって，原則が意味をなさないほど浸食される可能性があることである。このようにデジタル貿易との関連で「規制する権利」を通じて規制の自律性が強調される状況であれば，デジタル化が広く一般社会にも影響することに鑑みても，規律の正統性の確保及び規律の公平さの確保のため，規律の策定に様々なステークホルダーの関与が求められ，また策定後のレビューなども一層求められるのではないだろうか。

この観点から，ステークホルダーの参加に係る規定が重要であると思われるが，第四に，ルールメーカーの最近の協定においてもデジタル貿易に関連してステークホルダーの参加が規定される例は少なかった。また，データの越境移転の自由が主張されるのであれば，それを担保する環境への配慮も必要であるが，その面での課題であるデジタルデバイドについても同様に規定される例は限定的であった。これらの点は，デジタル貿易の国際通商ルールにおいてより強調されて然るべきであろう。

参 考 文 献

朝日新聞（デジタル）2022 年 10 月 11 日「スペース X の衛星ネット通信「スターリンク」，日本でもサービス開始」<https://www.asahi.com/articles/ASQBC6RCBQBCULFA026.html>（2023 年 9 月 15 日アクセス）

石井夏生利（2017）『新版　個人情報保護法の現在と未来：世界的潮流と日本の将来像』勁草書房

木村雅道（2022）「近時の通商協定に見られる金融サービス　分野におけるデータ関連の規律」『国際商事法務』Vol. 50，No. 12，pp. 1565-1570.

日刊工業新聞（デジタル）2022 年 11 月 23 日「スペース X が日本で「スターリンク」開始，「ライバルよりも有利な状況」の理由」<https://newswitch.jp/p/34697>（2023 年 9 月 15 日アクセス）

邵洪範（2019）『貿易自由化と規制権限：WTO 法における均衡点』東京大学出版会

松下満雄・飯野文（2021）「現代国際通商システ

181）邵（2019）2 頁。

182）Appellate Body Report，United States – Measures Affecting the Production and Sale of Clove Cigarettes，WT/DS406/AB/R，para.95; Appellate Body Reports，European Communities – Measures Prohibiting the Importation and Marketing of Seal Products，WT/DS400/AB/R / WT/DS401/AB/R，para.5.125.

183）SPS 協定 2.1 条。

ムのパノラマ」『国際商事法務』Vol. 49, No. 99, pp. 1-13.

REUTERS（デジタル）2022 年６月３日「ソニーが新会社設立，衛星レーザー光通信装置を製造へ」<https://jp.reuters.com/article/space-sony-group-idJPKBN2NJ24P>（2023 年９月 15 日アクセス）

Aaronson, S., and P. Leblond (2018), "Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO", *Journal of International Economic Law*, Vol. 21 No. 2, pp. 245-272.

Burri, M. (2021), "Chapter 1 Data Flows and Global Trade Law", in M. Burri (ed.), *Big Data and Global Trade Law*, Cambridge University Press, pp. 11-41.

Burri, M. (2022), "Chapter 28 Privacy and data protection", in D. Bethlehem, D. McRae, R. Neufeld, and I. Van Damme (eds.) , *The Oxford Handbook on International Trade Law, 2nd ed.*, Oxford University Press, pp. 745-768.

Chang, L. Y.-C., and H.-W. Liu (2022), "Chapter 8 Ensuring Cybersecurity for Digital Services Trade", in J. W. Kang, et al. (Asian Development Bank), *Unlocking the Potential of Digital Services Trade in Asia and the Pacific*, pp. 184-204.

Congressional Research Service (2021), Artificial Intelligence: Background, Selected Issues, and Policy Considerations, R46795・Ver. 3 . <https://crsreports.congress.gov/product/pdf/R/R46795>（2023 年９月 15 日アクセス）

Damme, I. V. (2019), "Chapter 16 Understanding the Choice for Evolutionary Interpretation", in G. Abi-Saab, K. Keith, G. Marceau, and C. Marquet (eds.), *Evolutionary Interpretation and International Law*, Bloomsbury, pp. 171-180.

Elsig, M., and S. Klotz (2021), "Chapter 2 Data Flow-Related Provisions in Preferential Trade Agreements Trends and Patterns of Diffusion", in M. Burri (ed.), *Big Data and Global Trade Law,* Cambridge University Press, pp. 42-62.

Gagliani, G. (2020), "Cybersecurity, Technological Neutrality, and International Trade Law", *Journal of International Economic Law*, Vol. 23, No. 3, pp. 731-738.

Gleason, T., and C. Titi (2022), "The Right to Regulate", Academic Forum on ISDS Concept Paper, 2022 / 2 <https://ssrn.com/abstract=4255605>（2023 年９月 15 日アクセス）

González, L. J., and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", OECD Trade Policy Papers, No. 205, OECD Publishing, Paris.

IMF, OECD, UN, and WTO (2023), *Handbook on Measuring Digital Trade: 2nd Edition*, WTO.

Inside US Trade (2023), "New WTO text on E-Commerce Shows Divisions over Privacy, Data Flows", August 14, (2023),

McKinsey Global Institute (2016), Digital Globalization: The New Era of Global Flows, McKinsey & Company.

Meltzer, J. P. (2019), "Cybersecurity and Digital Trade: What Role for International Trade Rules?", Global Economy and Development Working Paper 132 , the Brookings Institution.

Mitchell, A. D. (2008), *Legal Principles in WTO Disputes*, Cambridge University Press.

Monteiro, J.-A., and R. Teh (2017), "Provisions on Electronic Commerce in Regional Trade Agreements", WTO Working Papers ERSD-2017-11.

National Institute of Standards and Technology (NIST) (2018), *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*, NIST. <https://nvlpubs.nist.gov/nistpubs/

cswp/nist.cswp.04162018.pdf>（2023年9月15日アクセス）

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris.

OECD（2019）, *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris.

OECD（2022）, *Cross-border Data Flows: Taking Stock of Key Policies and Initiatives*, OECD Publishing, Paris.

OECD (2023), "Moving Forward on Data Free Flow with Trust: New Evidence and Analysis of Business Experiences", OECD Digital Economy Papers, No. 353, OECD Publishing, Paris.

Peng, S., C. F. Lin., and T. Streinz (2021), "Artificial Intelligence and International Economic Law: A Research and Policy Agenda", in S. Peng, C. F. Lin, and T. Streinz（eds.）, *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, Cambridge University Press, pp. 1-26.

Peng, S. Y.（2022）, "Chapter 29 Digital Trade", in D. Bethlehem, D. McRae, R. Neufeld, and I. Van Damme（eds.）, *The Oxford Handbook on International Trade Law*, 2nd ed., Oxford University Press, pp. 771-789.

REUTERS（digital）December 2, 2022 "Arctic Data Cable Linking Europe to Japan Secures First Investment" <https://www.reuters.com/technology/arctic-data-cable-linking-europe-japan-secures-first-investment- 2022-12 -02 />（2023年9月15日アクセス）

Shaffer, G.（2021）, "Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience" in S. Y. Peng, C. F. Lin, and T. Streinz（eds.）, *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, Cambridge University Press, pp. 29-53.

Streinz, T.（2021）, "International Economic Law's Regulation of Data as a Resource for the Artificial Intelligence Economy" in S. Y. Peng, C. F. Lin, and T. Streinz（eds.）, *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, Cambridge University Press, pp. 175-192.

The Economist（digital）May 6, 2017 "The World's Most Valuable Resource Is No Longer Oil, But Data" <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>（2023年9月15日アクセス）

Whitsitt, E.（2023）, "International Trade Law and Cybersecurity: Balancing Market-Oriented and Domestic State Regulation" in T. Ishikawa, and Y. Kryvoi（eds.）, *Public and Private Governance of Cybersecurity: Challenges and Potential,* Cambridge University Press（Forthcoming）<https://ssrn.com/abstract= 4309960 >（2023年9月15日アクセス）

WTO（2018）, *World Trade Report 2018: The Future of World Trade: How Digital Technologies are Transforming Global Commerce*, WTO.

Wu, M.（2017）, "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System", RTA Exchange, International Centre for Trade and Sustainable Development（ICTSD）and the Inter-American Development Bank（IDB）<www.rtaexchange.org/>（2023年9月15日アクセス）

Zhang, S.（2021）, "Protection of Cross-Border Data Flows Under International Investment Law", in J. Chaisse, L. Choukroune, and S.

Jusoh (eds.), *Handbook of International Investment Law and Policy*, Springer, pp. 1-23.

補論表１　デジタル貿易により生じた課題等への FTA の対応状況

EC: Electronic Commerce DT: Digital Trade DE: Digital Economy FS: Financial Service	CPTPP 2018 Chapter 14 EC	USMCA 2018/2020 Chapter 19 DT	DEPA 2020/2021	DEA（SAFTA） 2020 Chapter 14 DE	UKSDEA（UKSFTA） 2022 Chaper 8 Section F DT and DE	EU・UKTCA 2020/2021 Title III DT	EUSDTP 2023 *8	RCEP 2020/2022 Chapter 12 EC
データ越境移転	○	○	○ （CPTPP 類似）	○ （CPTPP/DEPA 同旨）	○ （DEA 同旨）	○	○	○
金融サービス	○（FS 章）	○（FS 章）	×	○	○（FS 節）	〈除外しない〉	〈言及しない〉	○（8 章附 FS）
LPPO「例外」	○	○	○	○	○	〈権利*2〉	〈言及しない〉	○
ローカリゼーション要求禁止	○	○	○ （CPTPP 類似）	○ （CPTPP/DEPA 同旨）	○ （DEA 同旨）	○ （4 類型禁止）	○	○
金融サービス	×	○（FS 章）	×	○	○（FS 節）	〈除外しない〉	〈言及しない〉	×
LPPO「例外」	○	×	○	○	○	〈権利*2〉	○	○
前文「規制する権利」	○*1	○*1	○*1	○*1	△*11	○	○	○
前文 LPPO/LPWO 例示	○*3	○*3	×	○*3	○（LPPO）*11	○（LPPO）	×	×
「規制する権利」規定	×	×	×	×	△*11	○ /LPO 例示	×	×
個人情報保護 法的枠組み採用又は維持義務	○	○	○	（USMCA 強化） ○	（DEA＋USMCA） ○	個人データ・ プライバシー保護 規定	データ保護言及	○
国際的原則・ガイドライン考慮	○ （非義務）	○ （非義務）	○ （義務）	○（同上） （義務）	○（同上） （義務）			○ （義務）
OECD/APEC 明示的言及	×	○	×	○（同上）	×			×
サイバーセキュリティ　締約国認識	○	○	○	○*9	○（USMCA 拡充）	△（協力）	○	○
当局キャパシティ向上	×	○	△（認識）	×	△（認識）	△（協力）	○	×
リスクベースアプローチ	×	○	×	×	○（同上）	△（協力）	○	×
安全保障例外	CPTPP 型	CPTPP 型*4	CPTPP 型*4	CPTPP 型*4	GATT21 条型*5	GATT21 条型*5	〈規定せず〉	GATT21 条型*5
オープンガバメントデータ	×	○	○	○（USMCA 強化）	○（DEA と同旨）	○（USMCA 拡充）	○	×
ステークホルダーエンゲージメント	×	×	×	○	○（DEA と同旨）	×	×	△*6
デジタルインクルージョン（DI）	×	×	○	×	○（DEPA 拡充）	×	×	×
途上国	△*7	△*7	○（DI）*10	○	○（DI）*10	×	×	△*7
中小企業	×	×	○	○	○	×	×	×
デジタル ID	×	×	○	○（DEPA 強化）	○（DEA と同旨）	×	×	×
AI　締約国認識	×	×	○	○	○	×	○	×
AI ガバナンス枠組み	×	×	○	○	○	×	○	×
国際的原則・ガイドライン考慮	×	×	○	○	○	×	○	×
協力	×	×	×	○	○	×	×	×
Fintech	×	×	○	○	○（FS 節で言及）	×	×	×
Regtech	×	×	×	○	○（FS 節で言及）	×	×	×
Lawtech	×	×	×	×	○	×	×	×

（出所）各協定より筆者作成。LPPO: legitimate public policy objective; LPWO: legitimate public welfare objective; LPO: legitimate policy objective.

*協定名下部の年号は署名／発効年を表す（区別ない場合には同年署名・発効）。協定下部の章は主な検討章を示す。原則として，縦軸の項目に係る個別規定の有無を示す。

*1：“inherent right…to regulate” を規定。*2：EU・UKTCA は「規制する権利」を規定（本文も参照）。*3：“LPWO” を例示　*4：CPTPP 型＝CPTPP と同一（本文も参照）

*5：GATT21 条型＝GATT21 条（b）のリスト維持型（本文も参照）　*6：EC 対話に係る規定中で言及。*7：経過期間。*8：非個人データ保護，民間企業の有する個人データへのガバメントアクセスも言及（本文も参照）。*9：オーストラリア・シンガポール間にはサイバーセキュリティの協力を内容とする MOU が別途存在する。*10：DI＝デジタルインクルージョンで規定（本文も参照）。*11：UKSFTA8.1 条（目的・適用範囲）で締約国が「規制する権利」保持する旨規定，前文で LPPO 例示。