RIETI Discussion Paper Series 24-J-018

ガバメントアクセスに焦点を当てた DFFTの具体化に向けた有志国間連携の在り方

藤井 康次郎
西村あさひ法律事務所

室町 峻哉
西村あさひ法律事務所

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 24-J-018
2024 年 7 月

ガバメントアクセスに焦点を当てた DFFT の具体化に向けた有志国間連携の在り方[1]

藤井康次郎
（西村あさひ法律事務所・外国法共同事業　パートナー）

室町　峻哉
（西村あさひ法律事務所・外国法共同事業　アソシエイト）

要　　旨

日本政府が推進する DFFT の具体化においては、民間部門が保有するデータへのガバメントアクセスに対する規律をいかに図っていくかが重要である。例えば、EU の GDPR においては、第三国におけるガバメントアクセスからの保護をデータ越境移転の条件とする解釈・実務が発展しており、データ越境移転を促進するためには、ガバメントアクセスへの対応が必要となる。また、国際的には OECD において信頼性や適正性等の観点から個人データに対するガバメントアクセスに係る規律要素に関する議論が進んでいる。貿易協定においても、個人情報保護の水準を確保しつつ、データの自由な流通を促進するための規定が盛り込まれるようになっている。

他方で、データの自由な流通を促進する上では、法執行の実効性の観点から、自国の領域内のみならず、越境移転先に所在するデータの証拠収集をはじめとするガバメントアクセスの実効性が担保されていることも重要である。この点について、米国 CLOUD Act は、捜査目的での越境的なデータ提出要求のための行政協定の枠組みを規定しており、有志国間でかかる越境的なガバメントアクセスの実効性を確保しつつ、適正性の観点からこれを規律する手段となり得る。

本稿は、こうした動向を踏まえて、ガバメントアクセスに焦点を当てた DFFT の具体化に向けた有志国間連携の在り方を検討するものである。

キーワード：DFFT、ガバメントアクセス、GDPR、CPTPP、日 EU EPA、CLOUD Act
JEL classification: F13、F15、F53、F55、F68

[1] 本稿は、独立行政法人経済産業研究所（RIETI）におけるプロジェクト「現代国際通商・投資システムの総合的研究（第 VI 期）」の成果の一部である。本稿の原案は、経済産業研究所（RIETI）のディスカッション・ペーパー検討会で発表を行ったものである。検討会参加者からの有益なコメントに感謝したい。

1　はじめに

2024 年 4 月 30 日に G7 デジタル・技術閣僚会合において採択された閣僚宣言では、G7 各国が「信頼性のある自由なデータ流通」（Data Free Flow with Trust。以下「**DFFT**」という。）の具体化に向けた取り組みにコミットするとともに、DFFT を推進するための常設の事務局を伴う国際的な枠組み（Institutional Arrangement for Partnership。以下「**IAP**」という。）の設立が合意された。DFFT は、2019 年 1 月に開催された世界経済フォーラム年次総会において安倍晋三総理大臣（当時）が提唱したコンセプトであり、「プライバシーやセキュリティ、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」というものである[2]。

DFFT の具体化において重要とされている問題の一つとして、民間部門が保有するデータへの公的機関によるアクセス（以下「**ガバメントアクセス**」という。）に対する規律をいかに図っていくかという点がある。この点に関して、2022 年 12 月、OECD において、「民間部門が保有する個人データに対するガバメントアクセスに関する宣言」（Declaration on Government Access to Personal Data Held by Private Sector Entities。以下「**OECD ガバメントアクセス宣言**」という。）[3]が採択され、法執行及び国家安全保障の目的の個人データに対するガバメントアクセスに関して、7 つの原則が示された。同宣言は、特に個人データに対するガバメントアクセスに関する規律要素に関する初の国際的な合意として、極めて重要な意義を有し、上記 G7 デジタル・技術閣僚宣言の附属書 1 では、同宣言を歓迎するとともに他の国にも同原則への署名を奨める旨が記載されている。

こうした動向と並行して、筆者らが事務局を務める西村高等法務研究所「CLOUD Act 研究会」（座長：宍戸常寿東京大学大学院法学政治学研究科教授）では、2018 年 3 月に米国において成立した Clarifying Lawful Overseas Use of Data Act（以下「**CLOUD Act**」という。）への日本における対応を出発点に、捜査目的での企業が保有するデータに対するガバメントクラウドに関する法的課題等の検討を行い、2023 年 4 月に、検討結果を取りまとめた報告書の第 2 版（以下「**CLOUD Act 研究会報告書 Ver 2.0**」という。）[4]を公表した。

本稿は、筆者らが、CLOUD Act 研究会における検討結果やその後の取り組み、最新動向を踏まえて、特にガバメントアクセスの問題に焦点を当てて、DFFT の具体化に向けた有志国間連携の在り方について検討を行ったものである。まず、2 において、データ保護の水準を保ちつつデータ越境流通を促進するための仕組み作りの動向について概観する。次に、3 において、捜査当局による越境的なデータ提出要求のための仕組みの意義について述べた上で、CLOUD Act に基づく行政協定について説明する。そして、4 において、ガバメントアクセスに焦点を当てた DFFT の具体化に向けた有志国間連携の在り方について、本稿の結論を述べる。具体的には、「有志国間で、データ保護の水準を保ちつつデータ越境移転を促進するための仕組みを整備すると同時に、捜査当局による越境的なデータ提出要求のための仕組みを整備し、これらに対して適正性等の観点から適切な規律を及ぼすことで、自由なデータ流通と実効的かつ適切な法執行を両立させるデータ流通圏を構築する」という方向性を提示する。

2　デジタル庁ウェブサイト「DFFT」<https://www.digital.go.jp/policies/dfft>。

3　OECD, *Declaration on Government Access to Personal Data Held by Private Sector Entities*, OECD/LEGAL/0487, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

4　西村あさひ法律事務所・外国法共同事業「西村高等法務研究所（NIALS）CLOUD Act（クラウド法） 研究会報告書 Ver.2.0 - 企業が保有するデータと捜査を巡る法的課題の検討と提言 -」（2023 年 4 月）<https://www.nishimura.com/ja/knowledge/publications/92692>。

2　　データ保護の水準を保ちつつデータの越境流通を行うための仕組み

DFFT を具体化するにあたっては、データを越境流通させることにより、データ保護の水準が低下することがないよう、各国の国内法や各国間の協定等において、適切な仕組みを構築することが重要となる。こうした仕組み作りは、特に個人データ保護の分野において進んできている。以下では、こうした個人データ保護分野において進む仕組み作りの動向について、概観する[5,6]。

(1)　　OECD プライバシーガイドライン

OECD は、1980 年 9 月 23 日、各国におけるプライバシー保護法を調和させるとともに、プライバシーに関する個人の権利を保護しつつ、国際的なデータの流通を促進することを目的として、「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data。以下「**OECD プライバシーガイドライン**」という。）[7]を採択した。OECD プライバシーガイドラインは、個人データ保護に関する 8 つの基本原則（①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全確保の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則）を定めており、非拘束的なソフトローであるが、各国の個人データ保護法の基礎となっている。2013 年には、個人データの流通量の増加やリスクの変化、個人情報の取扱いに関するアプローチの変化を踏まえた改正がなされた。

データ越境流通に関して、OECD プライバシーガイドラインは、第 4 部において、以下の内容を定めている。

① データ管理者は、自らが管理する個人データに関して、当該データの所在場所にかかわらず責任を負う。
② 加盟国は、自国と他の国との間における個人データの越境流通について、本ガイドラインに適合する継続的な保護の水準を保つため、(a)他の国が本ガイドラインを実質的に遵守している場合、又は(b)実効的な執行の仕組み及び個人情報管理者により導入される適切な措置を含む、十分な保護措置が存在する場合、当該越境流通を制限することを控えるべきである。

5　　本稿で言及していないものを含め、データ保護の水準を保ちつつデータ越境流通を促進するための各種のアプローチをマッピングしたものとして、Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", OECD Trade Policy Papers, No. 248, OECD Publishing, Paris, https://doi.org/10.1787/ca9f974e-en 参照。本稿では言及しきれなかったが、例えば、APEC のプライバシーフレームワークに基づく越境プライバシールール（CBPR）システムは、個人データの越境移転を促進するための複数国間での認証枠組みとして、重要な意義を有する。

6　　非個人データについては、個人データと比較して仕組み作りが進んでいないものの、非個人データについても越境移転規制や国内保存義務を課す国も現れるようになっていることから、今後、IAP において、非個人データに関する仕組み作りの議論が進むことが期待される。

7　　OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.

③　個人データの越境流通に対するいかなる制限も、当該情報の機微性並びに域外移転の目的及び情況を考慮した、当該流通によって引き起こされるリスクに比例した制限でなければならない。

このように、OECD プライバシーガイドラインにおいては、個人の権利の保護と個人データの国際流通の促進のバランスをとるために、十分な保護の水準を保つことができる限りデータ越境流通を認めるという考え方がとられており、このような考え方は、バランスの取り方の具体的な反映方法には一定の幅があるものの、各国の個人データ保護法や APEC プライバシーフレームワーク（APEC Privacy Framework）等の複数国間枠組みにおいても採用されている。

(2)　GDPR

EU の一般データ保護規則（以下「**GDPR**」という。）においては、個人データの越境移転は原則として禁止されているが（GDPR 44 条）、①移転先の第三国が十分性認定を取得している場合（GDPR 45 条）、②標準契約条項（以下「**SCC**」という。）や拘束的企業準則等の適切な保護措置に従って行う場合（GDPR 46 条及び 47 条）又は③GDPR 49 条の例外規定に依拠する場合には、例外的に個人データの越境移転が可能となる。これらのうち、上記①及び②は、十分な保護の水準を保った上でデータ越境移転を認めるという、OECD プライバシーガイドラインに示された考え方に則ったものである。これに対し、上記③は、上記①及び②のいずれの方法にもよることができない場合に、例外的な特定の状況において越境移転を許容するものである[8]。

上記①（十分性認定）に関して、欧州委員会は、第三国の保護の十分性を評価するにあたり、GDPR 45 条 2 項において挙げられている事項を考慮することとされているが、そこでは、次の事項を評価することとされている。

(a)　法の支配、人権及び基本的自由の尊重、公安、国防、国家安全保障及び刑事法を含む、一般的又は分野別の関連法令、公的機関による個人データへのアクセス、並びにそのような法令の実施、他の第三国又は国際機関への個人データの再移転に関する規定であって、当該国、地域又は国際機関が遵守する法令を含む、データ保護規則、職業上の準則及び保護措置、判例法、並びに効果的かつ執行可能なデータ主体の権利、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

(b)　適切な執行権限を含む、データ保護法令の遵守の確保及び執行に関する機能、データ主体がその権利を行使する際に支援し助言することに関する機能、並びに EU 加盟国の監督機関との協力に関する機能を担う独立の監督機関が存在し、かつ効果的に機能していること

(c)　当該国、地域又は国際機関が加入している国際的な取決め、特に、個人データ保護に関する法的拘束力のある条約又は法律文書から生ずるその他の義務、及び多国間システム又は地域システムへの参加に基づく義務

そして、EU・米国間のプライバシーシールドが無効であると結論づけた Schrems II 事件判決[9]を踏まえて、欧州データ保護評議会は、2020 年 11 月、「監視措置に関する欧州市民

8　European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 May 2018, <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en>.

9　Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd &

の本質的保証のレコメンデーション 02/2020」[10]を採択した。同レコメンデーションでは、公的機関による監視措置に関して、第三国の法制度が EU 域内における保証されている保護のレベルと本質的に同等の保護のレベルを提供しているかどうかを評価するにあたり考慮すべき事項として、(A)処理は明確かつ正確で、利用しやすいルールに基づくべきであること、(B)追求される正当な目的に対する必要性と比例性が証明される必要があること、(C)独立した監督の仕組みが存在すべきこと、及び(D)個人に対して効果的な救済措置が提供される必要があることが挙げられている。

一方、上記②（適切な保護措置）に関して、欧州委員会は、2021 年 6 月 4 日、Schrems II 事件判決を踏まえた SCC の改定版[11]を公表した。改定版の SCC では、データ移転の具体的な状況等、移転先の第三国の法令と実務（公的機関へのデータの開示又は当該機関によるアクセスの許可を要求するものを含む）、補完的措置の内容を評価した上で、当局の要求に備えて文書で記録しておくという越境移転影響評価が明文化されている（改定版 SCC の Clause 14(b)(d)）。そして、同月 18 日には、欧州データ保護評議会が、補完的措置として必要される具体的内容を明らかにした「EU と同等の個人データの保護水準を確保するためのデータ移転方法を補完する措置に関するレコメンデーション」[12]を採択した。

このように、EU では、特に Schrems II 事件判決以降、第三国におけるガバメントアクセスからの保護を越境移転の条件とする解釈・実務が発展している。この点、Christakis

---

Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020), <https://curia.europa.eu/juris/document/document.jsf;jsessionid=BD731F5130B963C7072D2F6851E77B5E?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11046615>. 同判決が DFFT に与える示唆を検討した論考として、渡辺翔太「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）<https://www.rieti.go.jp/jp/publications/nts/21j035.html>も参照。

[10] European Data Protection Board, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10 November 2020, <https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en>.

[11] European Commission, *COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance)*, OJ L 199, 7.6.2021, p. 31–61, <https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj>. 概要について、石川智也・菅悠人・津田麻紀子・福島惇央「GDPR：欧州委員会による標準契約条項（SCC）改定版（最終版）の公表」（西村あさひ法律事務所・外国法共同事業　ヨーロッパニューズレター、2021 年 6 月 8 日号）<https://www.nishimura.com/ja/knowledge/newsletters/20210608-35066>も参照。

[12] European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, 18 June 2021, <https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en>. 概要について、石川智也・菅悠人・津田麻紀子・福島惇央「GDPR：越境データ移転に関する欧州データ保護評議会によるレコメンデーション（最終版）の公表」（西村あさひ法律事務所・外国法共同事業　ヨーロッパニューズレター、2021 年 6 月 23 日号）<https://www.nishimura.com/ja/knowledge/newsletters/20210623-35031>も参照。

（2024）[13]は、Schrems II 事件判決以降のデータ保護当局の実務は、「外国政府がデータにアクセスする理論上の可能性がある限り、データ越境移転を認めない」という、「ゼロリスクアプローチ」をとっていると指摘している。その上で、同稿は、ゼロリスクアプローチには限界があることから、①データの性質、②外国政府によるアクセスの可能性、及び③潜在的な損害の重大性を考慮した「リスクベースアプローチ」をとるべきであると主張している。

EU と日本は、それぞれ、EU の GDPR に基づく十分性認定と日本の個人情報保護法第 28 条に基づく指定により、互いのデータ保護法を同等とみなし、両者間で自由な個人データの流通を可能にしている[14]。日本政府は、2019 年に EU による十分性に認定を受けるにあたり、欧州委員会からの要請に応える形で、刑事捜査や安全保障の観点から行われる、EU 域内から日本に移転した個人データに対する日本の政府機関によるアクセスは、必要かつ相当な範囲に限定され、かつ独立機関による監督を受ける旨の説明を添えていた。2023 年 4 月には、日 EU 相互認証に係る共同レビューが完了し、自由な個人データの流通のための上記枠組みが維持されている。

(3) OECD ガバメントアクセス宣言

上記(2)に記載のとおり、GDPR では、第三国におけるガバメントアクセスからの保護を越境移転の条件とする解釈・実務が発展している一方、民主主義国家にとっても犯罪捜査等一定の場合にガバメントアクセスを行うことは必要不可欠である。そのため、必要と認められるガバメントアクセスを実施するための規律が重要となる。

2022 年 12 月に採択された OECD ガバメントアクセス宣言は、その適用対象となる「ガバメントアクセス」を「各国政府が、各国の法的枠組みに従って各国領域内で法執行及び国家安全保障の目的を追求しようとする場合に、民間部門が保有又は管理する個人データにアクセス及び処理すること（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、当該民間部門に対してデータ提供を義務付ける権限を各国法の下で有する場合も含む）」と定義している。その上で、ガバメントアクセスに関して、プライバシーその他の人権及び自由の保護のため、相互に補完し合う以下の 7 つの原則を提示している。

原則	概要
①法的根拠 （Legal basis）	ガバメントアクセスは各国の法的枠組みに根拠づけられ、規制される。かかる法的枠組みは、政府を拘束し、法の支配の下にある民主的に設立された機関によって運用され、濫用のリスクから個人を十分に保護するために目的、条件、制限及びセーフガードを定める。
②正当な目的 （Legitimate aims）	ガバメントアクセスは特定された正当な目的のためにのみ行われ、当該目的に照らして過剰な態様とならない。ガバメントアクセスは、批判を抑圧したり、民族、ジェンダー等の特性のみに基づいて個人に不利益を与えたりする目的で行われない。
③承認 （Approvals）	ガバメントアクセスが基準、規則及び手続に従って実施されることを確保するために事前承認要件が定められる。これらは、アクセスの結果として生じるプライバシー等の人権への干渉の程度に見合ったものであり、より深刻な干渉についてはより厳格な承

13 Christakis, Theodore, *The 'Zero Risk' Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach* (February 20, 2024). CIPL/CBDF Paper Series, <https://ssrn.com/abstract=4732294>.

14 個人情報保護委員会ウェブサイト「日 EU 間・日英間のデータ越境移転について」<https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/>。

	認要件が設けられる。
④ データの取扱い（Data handling）	取得された個人データの処理は権限を付与された者のみが行い、かかる処理は、プライバシー、セキュリティー、秘密性及び完全性を維持するための措置の実施を含む要件に従う。データの喪失や不正アクセスを防止するための内部統制が実施される。
⑤透明性（Transparency）	ガバメントアクセスに関する一般的な法的枠組みが明確で容易にアクセスできる。政府による法的要件の遵守に関して監督機関が行う公開の報告や、政府の記録へのアクセスを要求するための手続を含むガバメントアクセスに関する透明性を提供するメカニズムが存在する。
⑥監督（Oversight）	ガバメントアクセスの法適合性を確保するための効果的で公平な監督のメカニズムがある。監督システムは、関連する情報の入手、調査の実施、法的枠組みの違反への対処等の権限を持つ組織の活動を含む。
⑦救済（Redress）	国家安全保障と法執行活動の機密保持の必要性を考慮しつつ（これには、自分のデータに対するアクセスの有無等の個人への通知の制限が含まれ得る。）、法的枠組みに対する違反を特定し、是正するための効果的な司法的・非司法的救済を個人に対して提供する。

このように、OECD ガバメントアクセス宣言は、プライバシーその他の人権及び自由を保護しつつ、必要と認められる個人データに対するガバメントアクセスを行うための基本的な原則を示したものとして、極めて重要な意義を有する。ここで示された 7 原則は、データの越境移転先におけるデータ保護の水準を評価する上でも有益であると考えられる[15]ところ、今後、DFFT の下、有志国間でデータの自由な流通を進めていくにあたり、各国がガバメントアクセスに対して適正性等の観点から適切な規律を行っているかどうかを評価する際の指標にもなると考えられる。

(4) データの自由な流通に関する貿易協定（CPTPP 及び日 EU EPA 新条文）

近年では、貿易協定において、個人情報保護の水準を確保しつつ、データの自由な流通に関するコミットメントを設ける例が現れるようになっている。

例えば、「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」（以下「**CPTPP**」という。）は、第 14 章（電子商取引）の 14.11 条において、情報の電子的手段による国境を越える移転（データの越境移転）を原則として許可しなければならないとしつつ（CTPP 14.11 条 2）、公共政策の正当な目的を達成するために行われる措置については、一定の要件の下、これを許容している（同条 3）。また、個人情報保護に関しては、14.8 条において、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、又は維持すること、及び当該法的枠組みを作成するにあたり、関係国際機関の原則及び指針を考慮することが求められている（CTPP 14.11 条 2）。このように、CPTPP では、各締約国が個人情報の保護のための法的枠組みを採用・維持することを前提に、データの越境移転を（その越境移転先に関わらず）原則として許可することを締約国に求めつつ、公共政策の正当な目的を

15 個人情報保護委員会の「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（2016 年 11 月。2023 年 12 月一部改正）<https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/>では、越境移転先におけるガバメントアクセスに関する制度を評価するにあたり、参照することが考えられるものの具体例として、OECD ガバメントアクセス宣言が挙げられている。

達成するために行われる措置を一定の要件の下で許容することで、データの自由な流通と個人情報を含むデータの保護のバランスを図っている。

他方、2024 年 1 月 31 日、日本及び EU は、「経済上の連携に関する日本国と欧州連合との間の協定」（以下「**日 EU EPA**」という。）に新たな「データの自由な流通に関する規定」（以下「**日 EU EPA 新条文**」という。）を追加すること内容とする議定書に署名した[16]。日 EU EPA 新条文のうち、新 8.81 条は、締約国が「一方の締約国の領域への情報の移転を禁止すること」及び「他方の締約国の領域への情報の移転の前に一方の締約国の承認を要求すること」を禁止している（新 8.81 条 2(e)及び(f)）。その上で、CPTPP 14.11 条 3 と同様に公共政策の正当な目的を達成するために行われる措置を一定の要件の下で許容する条項（同条 3）とともに、別途、個人情報及びプライバシーの保護に関する措置が妨げられないことを規定した条項も設けられている（同条 4）。また、新 8.82 条は、個人情報保護について、CPTPP と同様に、個人情報保護のための法的枠組みを採用すべきこと、及び当該法的枠組みの策定にあたり関係国際機関の原則及び指針を考慮することを求めているが、これに加えて、「民間が保有する情報への政府のアクセスに関するプライバシー及び情報の保護の高い基準」がデジタル経済の信用に寄与することを確認し、かかる基準の具体例として、OECD ガバメント原則を挙げている（新 8.82 条 3）。

以上をまとめると下表のとおりとなる[17]。

	CPTPP	日 EU EPA 新条文
データの自由な流通	・ データの越境移転を（その越境移転先に関わらず）原則として許可することを要求 ・ 公共政策の正当な目的を達成するために行われる措置を一定の要件の下で許容	・ 「一方の締約国の領域への情報の移転を禁止すること」及び「他方の締約国の領域への情報の移転の前に一方の締約国の承認を要求すること」を禁止 ・ 公共政策の正当な目的を達成するために行われる措置を一定の要件の下で許容するとともに、個人情報及びプライバシーの保護に関する措置が妨げられないことを規定
個人情報の保護	・ 個人情報の保護について定める法的枠組みを採用・維持すること、及び当該法的枠組みを作成するにあたり、関係国際機関の原則及び指針を考慮することを	・ 個人情報の保護について定める法的枠組みを採用・維持すること、及び当該法的枠組みを作成するにあたり、関係国際機関の原則及び指針を考慮することを

16 外務省「日・EU 経済連携協定改正議定書の署名」（2024 年 1 月 31 日）<https://www.mofa.go.jp/mofaj/press/release/pressit_000001_00282.html>。

17 以上のほか、日 EU EPA 新条文と CPTPP の関連規定の比較について、藤井康次郎・室町峻哉「日 EU EPA における新たな『データの自由な流通に関する規定』」（西村あさひ法律事務所　独禁/通商・経済安全保障ニューズレター、2024 年 4 月 8 日号）<https://www.nishimura.com/ja/knowledge/newsletters/competition_law_international_trade_240408>も参照。

	要求 ・ ガバメントアクセスに関しては明示的な言及なし	要求 ・ 「民間が保有する情報への政府のアクセスに関するプライバシー及び情報の保護の高い基準」（OECD ガバメントアクセス宣言等）がデジタル経済の信用に寄与することを確認

このように、CPTPP 及び日 EU EPA 新条文は、いずれも、個人情報保護の水準を確保しつつ、データの自由な流通を促進する規定を含んでいるが、日 EU EPA 新条文は、締約国がガバメントアクセスに対する規律を含む高い水準の個人情報保護のための法的枠組みを有していることを確保しつつ、個人情報の保護についての信頼性が確保された締約国間におけるデータの越境移転の自由を確保する一方、必ずしも当該信頼性が確保されているとは限らない第三国へのデータ越境移転については制限する余地を残すような内容となっている。これは、GDPR が想定するような、「データの越境移転先において、（ガバメントアクセスに対する保護を含め、）個人データの十分な保護が確保される場合に限り、データの越境移転を認める」というアプローチをより厳格に採用した枠組みになっているといえる。

3 越境的なデータ提出要求のための仕組み

上記 2 でみたとおり、個人データ保護の分野では、ガバメントアクセスが個人データ保護に与える影響やガバメントアクセスの規律の在り方について、議論が進んでいるが、DFFT を具体化するにあたっては、各国の捜査当局等がデータの越境移転先に対しても必要に応じてデータの提出要求を行うことができるようにしつつ、これに対して適正性等の観点から適切な規律を及ぼせるような仕組み作りを行うことが重要と考えられる[18]。

(1) 越境的なデータ提出要求のための仕組みの意義

データが国境を越えて活発に移転するようになった昨今においては、捜査機関が必要とするデータが、国外に所在するサーバに保存されている[19]、又は保存されているサーバの所在地を特定することが困難であるようなケースが増えている。こうした国外に保存されたデータの捜査を目的とした取得については、他国の主権又は管轄権を侵害する違法な管轄権の行使に当たらないかが問題となるところ、CLOUD Act 研究会では、国外に保存されたデータの捜査を目的とした取得の国際法上の評価について、場面ごとに整理・検討を行った

18 この点に関連して、Christakis（2024）は、欧州データ保護評議会が唱道する「compliant European Economic Area (EEA)-sovereign cloud solutions」は、「外国政府によるアクセスのリスクは、非 EU クラウドサービスプロバイダを用いる場合にのみ生ずる」という考え方を前提としているように思われるが、そのような前提は越境的なガバメントアクセスの実態を適切に考慮できておらず、EU のクラウドサービスプロバイダを用いたからといって外国政府によるガバメントアクセスのリスクを完全にゼロにすることはできないと指摘する。

19 データを分割して国内外に所在する複数のサーバに分けて保存するようなケースも多い。

[20]。検討結果の概要は以下のとおりである。

場面		国際法上の評価
サーバ管理者等[21]にデータの提出を求める場合	サーバ管理者等が自国の領域内に所在する場合	実際のデータ又はその記録媒体の提出行為が国内で行われ、国外に所在するサーバへのアクセスは命令を受けた国内にいるサーバの管理者等が行うのであれば、国際法上許容されるべき（否定的に捉える見解もある）。
	サーバ管理者等が自国の領域外に所在する場合	捜査機関の所在国と他国に所在するサーバ管理者等との間に「正当な連結点」がある場合、捜査機関所在国の立法管轄権は及ぶと評価されるものの、執行管轄権については別途国際法上慎重な評価が必要。
捜査機関自らデータが保存された国外に所在するサーバにアクセスしてデータを取得する方法		他国領域に物理的に捜査機関が立ち入るものではないため、「他国領域内」における執行管轄権に基づく強制措置に当たらないとする立場もあるものの、議論は分かれている。

上記のとおり、自国の領域内に所在するサーバ管理者等に対してデータの提出を求める場合には国際法上違法と評価される可能性は低いものの、国外に保存されたデータの捜査を目的とした取得の国際法上の評価については、依然として、不明確な点も多い。また、特に自国の領域外に所在するサーバ管理者等に対してデータの提出を求める場面には、当該サーバ管理者等が所在する国の法令（個人データ保護法等）との抵触が生じ、事業者がデータの提出に応じない可能性がある[22]。こうした理由により、データに対する法執行への懸念が高まり、データ越境移転規制や国内保存義務を課すインセンティブとなる可能性がある[23]。そのため、データの越境移転を認めることの裏返しとして、越境移転先に対するデータ

20　CLOUD Act 研究会報告書 Ver 2.0 43-48 頁。

21　CLOUD Act 研究会報告書 Ver 2.0 では、企業が特定のサーバに対する所有権等に基づきこれを管理する権限を有する場合のほか、特定のサーバの記憶領域に対して利用権限を有する場合を包含して、「管理等」と表現し、また、サーバを管理等する企業等を指して「管理者等」という言葉を用いている（CLOUD Act 研究会報告書 Ver 2.0 17 頁）。

22　例えば、EU の GDPR は、管理者又は処理者に対して個人データの移転又は開示を命ずる第三国の裁判所又は裁定機関の判決又は決定、及び行政当局の決定は、当該第三国と EU との間で有効な相互の司法共助条約等の国際協定、又は、当該第三国と EU 加盟国の間の同様の協定に基づく場合に限り、承認され、又は執行可能になるとされている（GDPR 48 条）。

また、米国の Stored Communications Act は、電気通信サービス及びリモートコンピューティングサービスのプロバイダーが通信の内容を開示することを原則として禁止した上で（18 U.S.C. Sec. 2702）、連邦又は州の政府機関による保存された通信内容の開示要求の手続（18 U.S.C. Sec. 2703 以下）を定めているが、外国政府による開示要求はかかる手続の対象とならない。

23　藤井康次郎「Data Free Flow with Trust 構想とクラウド法－近時の経済連携協定デジタル貿易規律の概観と『クラウド法報告書』の紹介」日本国際経済法学会年報第 29 号 56 頁（2020）。御巫智洋「インターネットの利用に関する国際的なルールにおいて領域主権が果たす機能」国際法外交雑誌 121 巻第 1 号 1 頁、14 頁脚注 38（2022）も同旨（なお、同稿は、データの越境アクセスの問題について、国際法の観点から精緻な検討を行っており、意義深い）。

提出要求を行えるような仕組みを整えておくことは重要である。

その一方で、自国に所在するサーバ管理者等が、第三国の捜査機関からのデータ提出命令に応じてデータを提出することは、自国におけるデータ保護の水準を低下させることに繋がり得る[24]。この点への対処としては、①自国に所在するサーバ管理者等が第三国の捜査機関からのデータ提出命令に応じることを禁止するアプローチと、②当該第三国との間で、データ提出要求に係る適正手続について合意し、かかる適正手続を遵守する限りにおいて、データ提出命令に応じることを認めるアプローチがあり得る。上記のとおり、①のアプローチは国境を越える自由なデータ流通の阻害に繋がる可能性があることから、DFFT の具体化においては、②のアプローチを模索すべきであると考えられる。下記**(2)**においては、②のアプローチの具体例として、米国 CLOUD Act によって新設された行政協定の仕組みについて解説する[25]。

(2) CLOUD Act に基づく行政協定

米国 CLOUD Act は、プロバイダーが米国との間で行政協定を締結した外国政府からの直接の命令に応じてデータを開示しても、Stored Communications Act、Wiretap Act 及び Pen Register and Trap and Trace Statute といった国内法上、違法と評価されないことが明確化された（CLOUD Act 104 条、18 U.S.C. Sec. 2511(2)(j)、2520(d)(3)、2702(b)(9)、(c)(7)、2707(e)(3)、3121(a)、3124(d)）。外国政府が米国との間で行政協定を締結するためには、当該外国政府が、プライバシー及び人権（表現の自由等）に対して実質的かつ手続的に強固な保護を与えており、米国人に関する情報の取得、保持及び流布を最小限にする適切な手続を採用していること等が、米国の司法長官により承認される必要がある（CLOUD Act 105 条(a)、18 U.S.C. Sec. 2523(b)）。米国は、これまで以下の各国との間で CLOUD Act に基づく行政協定を締結し、又は締結に向けた交渉を開始している。

実際に、ベトナム等では、法執行の実効性を確保するために国内保存義務が課されている（廣澤太郎・村田知信・NGUYEN Tuan Anh「ベトナムのデータローカライゼーション義務を明確化する政令の制定」（西村あさひ法律事務所・外国法共同事業　アジア/個人情報保護・データ保護規制ニューズレター、2022 年 8 月 22 日号）<https://www.nishimura.com/ja/knowledge/newsletters/20220822-93281>参照）。ただし、上記のとおり、自国の領域内に所在するサーバ管理者等に対してデータの提出を求める場合には国際法上違法と評価される評価される可能性は低いことから、「自国の領域内にデータを保存させること」は、本来的には、データに対する法執行の実効性を確保する上で必須ではないとも考えられる。

[24] 自国のデータ保護の水準を維持することは、自国のデータ主体等の保護の観点から重要であることに加えて、EU の GDPR に基づく十分性認定等、別の第三国とのデータ流通の枠組みを維持する上でも重要である（CLOUD Act 研究会報告書 Ver 2.0 65 頁）。

[25] このほか、2021 年に採択されたサイバー犯罪条約の第二追加議定書も、他の締約国に所在する者との直接協力の手続を定めている。その概要については、CLOUD Act 研究会報告書 Ver 2.0 54-56 頁参照。

国	行政協定の締結・交渉状況
英国	2019 年 10 月に行政協定を締結、2022 年 10 月に発効[26]
オーストラリア	2021 年 12 月に行政協定を締結、2024 年 1 月に発効[27]
カナダ	2022 年 3 月から行政協定の締結に向けた交渉を開始[28]
EU	2019 年 9 月から電子証拠の収集を巡る取決めの締結に向けた交渉を実施（一次中断していたが、2023 年 3 月に再開）[29]

上記のとおり、米英間及び米豪間の行政協定については既に発効しており、協定文が公表されている[30]ところ、いずれにおいても、一方当事国の捜査機関が、他方当事国のプロバイダに対して直接データの開示命令を交付し、プロバイダがこれに応じてデータの開示を行うための手続が定められている。いずれの協定においても、かかる手続の対象となる犯罪は、捜査機関所在国の法令において拘禁刑 3 年以上の刑罰の対象となる重大犯罪に限定されている。

上記 **2(3)** に記載のとおり、OECD ガバメントアクセス宣言における「ガバメントアクセス」の定義には、「各国政府が、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、当該民間部門に対してデータ提供を義務付ける権限を各国法の下で有する場合」も含まれることから、同宣言で示された 7 原則は、越境的なデータ提出要求を規律する上でも参照に値すると考えられる。そこで、筆者らは、本稿末尾の**別紙**のとおり、米英行政協定及び米豪行政協定が、OECD ガバメントアクセス宣言の 7 原則に対応する規定を含むかどうかの整理・検討を行った。結論として、まず、米英行政協定は、「刑事犯罪の防止、調査、発見、起訴に関連する個人データの保護に関するアメリカ合衆国と欧州連合の間の協定」（以下「**2016 年米欧協定**」という。）を準用している（米英行政協定 9 条 1 項）こともあり、7 原則全てに対応する規定を含んでいるといえる。また、米豪行政協定についても、概ね、7 原則に対応する規定を含んでいるといえる。

このように、CLOUD Act が想定するような越境的なデータ提出要求に関する行政協定を締結することで、越境的なガバメントアクセスの実効性を確保すると同時に、そうした越境的なガバメントアクセスに対して適切な規律を及ぼし、データ保護の水準を維持することに資すると考えられる[31]。

---

26 U.S. Department of Justice, “Landmark U.S.-UK Data Access Agreement Enters into Force”, 3 October 2022, <https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force>.

27 U.S. Department of Justice, “Joint Statement by U.S. Attorney General Merrick B. Garland and Australia Attorney-General Mark Dreyfus KC Announcing Entry into Force of the United States and Australia’s Data Access Agreement to Support Investigations of Serious Crime”, 30 January 2024, <https://www.justice.gov/opa/pr/joint-statement-us-attorney-general-merrick-b-garland-and-australia-attorney-general-mark>.

28 U.S. Department of Justice, “United States and Canada Welcome Negotiations of a CLOUD Act Agreement”, 22 March 2022, <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>.

29 U.S. Department of Justice, “Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations”, 2 March 2023, <https://www.justice.gov/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations>.

30 U.S. Department of Justice, “CLOUD Act Resources”, <https://www.justice.gov/criminal/cloud-act-resources>.

31 ただし、CLOUD Act に基づく行政協定は、サーバ管理者等に対してデータ提出

4　ガバメントアクセスに焦点を当てたDFFTの具体化に向けた有志国間連携の在り方

上記2のとおり、GDPRのような個別の個人データ保護法や、CPTPPや日EU EPA新条文のような貿易協定といった複数国間の協定によって、個人データ保護の水準を保ちつつ、データの越境移転を行うための仕組み作りが進んでいる。これに加えて、上記3のとおり、こうした仕組み作りに加えて、各国の捜査当局等がデータの越境移転先に対しても必要に応じてデータの提出要求を行うことができるようにしつつ、これに対して適正性等の観点から適切な規律を及ぼせるような仕組み作りを行うことが重要であり、CLOUD Actが想定するような越境的なデータ提出要求に関する行政協定は、そのための手段となる。

これらを踏まえて、筆者らとしては、下図のとおり、「有志国間で、データ保護の水準を保ちつつデータ越境移転を促進するための仕組みを整備すると同時に、捜査当局による越境的なデータ提出要求のための仕組みを整備し、これらに対して適切な規律を及ぼすことで、自由なデータ流通と実効的かつ適切な法執行を両立させるデータ流通圏を構築する」という方向性で仕組み作りを行うことを提言する[32]。

具体的には、まず、有志国間で、自国の領域内におけるガバメントアクセス（自国の領域内の事業者に対するデータ提出要求）（下図の黄色の矢印）がOECDガバメントアクセス宣言で示された7つの原則に従い、適切になされていることを各国データ保護法に基づく相互の十分性認定や貿易協定におけるデータ保護に関する規律によりコミットし合う。

これに加えて、有志国間で、越境的なデータ提出要求（下図の赤色の矢印）を実施するための枠組みを構築することで、越境的なデータ提出要求の実効性を確保する。このとき、当該枠組みに基づく越境的なデータ提出要求により、各国の領域内におけるデータ保護の水準が低下することがないよう、当該枠組みに基づくデータ提出要求の手続や取得したデータの保管ルール、これらに対する監督・権利救済の仕組みを設けることが重要である。例えば、下図において日本と米国が越境的なデータ提出要求のための枠組みを構築することによって、日本国内におけるデータ保護の水準が低下してしまうと、EUから日本へのデータを越境移転する際の障壁となりかねないことから、日米間で適切な規律について合意しておくことが重要となる。

その上で、貿易協定において情報の電子的手段による国境を越える移転（データの越境移転）に関する規律を設けることで、有志国間でのデータの越境移転（下図の緑の矢印）がより自由かつ安定的なものとなる。

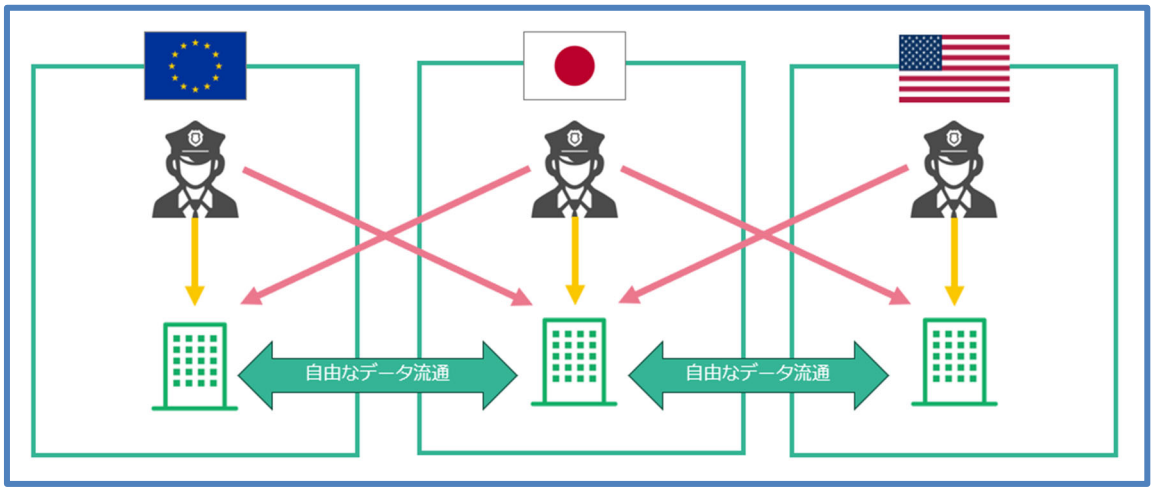
これらにより、有志国間では、データを自由に流通させつつ、データの所在に関わらず、OECDガバメントアクセス宣言等の国際的に合意された原則に従った適切なガバメントアクセスを実効的に行うことができ、自由なデータ流通と適切な法執行を両立することがで

を求める種類のガバメントアクセス（Compelled Access又はObliged Accessとも呼ばれる）の枠組みを作るものであり、データが保存されたサーバにアクセスしてデータを取得する種類のガバメントアクセス（Direct Accessとも呼ばれる）に対する規律の在り方については別途議論が必要である。

32　下図では、「有志国」の具体例として、日本のほか米国及びEUを挙げている。

前記2(2)に記載のとおり、EUでは、Schrems II事件判決以降、第三国におけるガバメントアクセスからの保護を越境移転の条件とする解釈・実務が発展しており、「ゼロリスクアプローチ」がとられているとの指摘もある。もっとも、EUにおいても2023年に電子証拠規則・電子証拠指令が制定され、EU域内でサービスを提供するEU域外の事業者に対しても電子証拠（データ）の提出を命ずることを可能とする制度が整備されつつある。また、前記3(2)に記載のとおり、EU・米国間では電子証拠の収集を巡る取決めの締結に向けた交渉が実施されている。これらの動向も踏まえると、本稿で提言するような仕組み作りにEUを巻き込むことも十分可能と考えられる。

きる[33]。



【図】自由なデータ流通と実効的かつ適切な法執行を両立させるデータ流通圏

以上

33　なお、こうした有志国間の枠組みの構築と併せて、又は別途、外国からの不適切なガバメントアクセスについては、ある種自衛的に対抗的な措置を講じたり、企業や市民に対してそうしたガバメントアクセスのリスクや対応策を啓蒙したりするなどして、これを抑制することも選択肢となると考えられるが、詳細な検討は他日を期したい。

別紙　　**米英行政協定・米豪行政協定と OECD ガバメントアクセス宣言 7 原則の対応関係**

	米英行政協定	米豪行政協定
①法的根拠 （Legal basis）	行政協定の対象となる命令の法的効果は、当事国の国内法にのみ由来する旨を規定（3 条 2 項）。	行政協定の対象となる命令の法的効果は、当事国の国内法にのみ由来する旨を規定（3 条 2 項）。
②正当な目的 （Legitimate aims）	行政協定の対象となる命令は、対象犯罪の予防、発見、捜査又は訴追に関連する情報を取得することを目的とするものでなければならず、言論の自由の侵害や人種や性別等に基づく不利益を与えるのために用いられてはならない旨を規定（4 条 1 項、2 項）。 また、取得の対象を対象犯罪の予防、探知、捜査又は訴追に関連する情報に限定するための標的化・最小化手続について規定（7 条）。	行政協定の対象となる命令は、対象犯罪の予防、発見、捜査又は訴追に関連する情報を取得することを目的とするものでなければならず、言論の自由の侵害や人種や性別等に基づく不利益を与えるのために用いられてはならない旨を規定（4 条 1 項、2 項）。 また、取得の対象を対象犯罪の予防、探知、捜査又は訴追に関連する情報に限定するための標的化・最小化手続について規定（7 条）。
③承認 （Approvals）	行政協定の対象となる命令は、当事国の国内法に基づく裁判所その他の独立機関による事前又は手続中の審査又は監督の対象となる旨を規定（5 条 2 項）。	行政協定の対象となる命令は、当事国の国内法に基づく裁判所その他の独立機関による事前又は手続中の審査又は監督の対象となる旨を規定（5 条 2 項）。
④ データの取扱い （Data handling）	行政協定の対象となる命令によって取得されたデータは、プライバシー等に関する国内法に従って取り扱われること、当該データを第三国に移転してはならない旨を規定（8 条 1 項、2 項）。 また、2016 年米欧協定の以下の規定が準用される（9 条 1 項）。 ・ 情報の質と完全性の維持（2016 年米欧協定 8 条） ・ 情報セキュリティ（2016 年米欧協定 9 条） ・ 情報セキュリティインシデントの通知（2016 年米欧協定 10 条） ・ 記録の維持（2016 年米欧協定 11 条） ・ 保存期間（2016 年米欧協定 12 条） ・ 特別の種類の個人情報（2016 年米欧協定 13 条） ・ アクセス（2016 年米欧協定 16 条）	行政協定の対象となる命令によって取得された個人データは、命令を発行した当事国の国内法枠組みに従って保護される旨、また、プライバシーの保護に以下の要素が含まれる旨を規定（3 条 4 項）。 a. 個人データの使用及び開示を、取得目的と両立しないわけではない（not incompatible with）目的に限定すること b. 個人データの保持を必要かつ適切な期間のみに制限すること c. 個人データの紛失、偶発的若しくは不正なアクセス、開示、改ざん、又は破壊から保護するための保護措置 d. 個人が自らに関する個人データへのアクセスを求め、取得し、不正確な個人データの訂正を求めるための枠組み e. 個人からの苦情に対応するための枠組み また、行政協定の対象となる命令によって取得されたデータは、プライバシー等に関する国内法に従って取り扱われること、当該デー

	・　訂正（2016 年米欧協定 17 条）	タを第三国に移転してはならない旨を規定（9 条 1 項、2 項）。
⑤透明性 （Transparency）	各当事国の指定官庁は、運用上又は国家安全保障上支障がない範囲で、行政協定の利用に関する集計データを反映した年次報告書を相手当事国の指定官庁に発行することとされている（12 条 4 項）。行政協定に基づく命令を受領したプロバイダが、受領した命令について、適用される法律に合致する統計情報を公表することは妨げられない（12 条 5 項）。 また、2016 年米欧協定の以下の規定が準用されれる（9 条 1 項）。 ・　説明責任（2016 年米欧協定 14 条） ・　透明性（2016 年米欧協定 20 条）	各当事国の指定官庁は、運用上又は国家安全保障上支障がない範囲で、行政協定の利用に関する集計データを反映した年次報告書を相手当事国の指定官庁に発行することとされている（11 条 3 項）。行政協定に基づく命令を受領したプロバイダが、受領した命令について、適用される法律に合致する統計情報を公表することは妨げられない（11 条 4 項）。
⑥監督 （Oversight）	両当事国は、毎年、行政協定の対象となる命令の発行・送達状況と命令に基づき取得されたデータの取り扱い状況について、相互にレビューを行うこととされている（12 条 1 項）。 また、2016 年米欧協定の以下の規定が準用されれる（9 条 1 項）。 ・　実効的な監督（2016 年米欧協定 21 条） ・　監督機関同士の協力（2016 年米欧協定 22 条） ・　共同レビュー（2016 年米欧協定 23 条）	両当事国は、毎年、行政協定の対象となる命令の発行・送達状況と命令に基づき取得されたデータの取り扱い状況について、相互にレビューを行うこととされている（11 条 1 項）。
⑦救済 （Redress）	2016 年米欧協定の以下の規定が準用されれる（9 条 1 項）。 ・　行政上の救済（2016 年米欧行政協定 18 条） ・　司法上の救済（2016 年米欧行政協定 19 条）	上記のとおり、各当事国の国内法に基づき、個人からの苦情に対応するための枠組みが設けられることが想定されている（3 条 4 項 e）。