RIETI Discussion Paper Series 21-J-035

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―

渡辺 翔太
野村総合研究所

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 21-J-035
2021 年 7 月

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―[1]

渡辺 翔太
（野村総合研究所主任研究員）

要　旨

欧州司法裁判所（CJEU）Schrems II 事件では、EU から米国へのデータ移転に関する法的根拠とされてきたプライバシーシールド（PS）と標準契約条項（SCC）の有効性が争われ、その帰結は日本の国際的なデータ流通政策にも影響を与える。

PS の前身セーフハーバー協定の無効を判決した CJEU の Schrems 事件で、CJEU は米国政府の監視活動が EU のデータ保護水準に適合しないとし、欧米間で PS を締結し米国の監視活動に対するデータ保護を強化したが、本判決は PS をもってしても米国のデータ保護は欧州の水準に達しないと判断した。ここでは GDPR 下でも従来の基準で外国の監視活動のデータ保護水準が評価された点が重要である。

本判決はさらに、十分性認定があるとしても、EU データ保護監督機関が苦情処理の中で越境移転の停止を命令できること、SCC は有効であるが相手先国のリスクに応じ追加的保護措置をとる必要があることを判断した。

本稿はその示唆として、日本政府は DFFT 構想等において政府による強制力を持った民間データへのアクセスの規律を検討しているが、EU の考えも方向性を同じくする点を明らかにした。また、EU 加盟国の監視が GDPR の適用外とされる中、外国にのみデータ保護を求めるのは内外差別とする批判の当否を検討した。

キーワード：DFFT、GDPR、ガバメントアクセス、データ保護、プライバシー
JEL classification: F02, F13, F15, F52

[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Ⅴ期）」の成果の一部である。本稿の原案に対して、経済産業研究所ディスカッション・ペーパー検討会の方々から多くの有益なコメントをいただいた。また、特に法律事務所 LAB-01 の望月様には詳細なコメントをいただいた。記して感謝の意を表したい。

１．はじめに

筆者はかつて、ガバメントアクセス（政府機関による民間保有データへの強制力を持ったアクセス。以下 GA）を理由とした越境移転制限の必要性やその通商協定との整合性について検討した[2]。

今日、サイバー空間に対する政府による諜報活動の重要性が増す一方、他国民を含むプライバシー侵害の懸念が生じていること、また、諜報活動は秘匿性が高く、それゆえ産業スパイ的な活動等の濫用の懸念もあることが指摘される。こうした懸念から近年、GA を理由として自国からのデータの越境移転制限が欧米等で生じているが、このような制限はデータの自由流通を阻害するため、既存の通商協定との抵触や、日本が進める信頼ある自由なデータ流通（Data Free flow with Trust; DFFT）構想との関係でも問題が生じ得ることを論じた。DFFT は、2019 年の世界経済フォーラム年次総会（ダボス会議）において、当時の安倍内閣総理大臣によって提唱され、同年の大阪サミットで参加国の支持を得た。この構想は、「プライバシー、データ保護、知的財産権及びセキュリティに関する課題に対処することでデータの自由な流通をさらに促進し、消費者及びビジネスの信頼を強化するという、「信頼」と「自由な流通」の相乗効果を提唱した概念である」と理解されている[3]。

また、現状、欧州連合（以下 EU）は、特に個人データについて、データの移転先国において GA に対して EU における保護と同等以上の保護が満たされない限り、国外移転を制限している。また、米国も投資審査等アドホックな措置を活用して外国の GA への対抗を行っている。こうしたデータの越境移転制限について、サービスの貿易に関する一般協定（GATS）上はデータの移転制限自体には規律が及ばないがサービス提供を阻害する措置として問題となり得る、また、環太平洋パートナーシップに関する包括的及び先進的な協定（CPTPP）ではデータの移転制限そのものに規律が及ぶが、両協定においてはプライバシー保護や安全保障を理由として措置が正当化される余地がある。筆者は、これらを前著で明らかにした。

以上の筆者の検討においては、特に外国での GA からのプライバシーの保護を理由とした EU による個人データの越境移転制限に関する議論が、GA の規律に関する重要な先例として位置づけられ、複数の欧州司法裁判所（CJEU）による司法判断を検討したところである。この論考において、筆者はとりわけ EU においては、1995 年に成立したデータ保護指

---

[2] 渡辺翔太「ガバメントアクセス（GA）を理由とするデータの越境移転制限―その現状と国際通商法による規律、そして DFFT に対する含意―」RIETI Discussion Paper Series 19-J-067（2019 年）（https://www.rieti.go.jp/jp/publications/dp/19j067.pdf, 2021 年 6 月 3 日最終閲覧）。

[3] デジタル・ガバメント閣僚会議決定「データ戦略タスクフォース第一次とりまとめ」（令和 2 年 12 月 21 日）（https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20201221/taskforce_torimatome1.pdf, 2021 年 6 月 30 日最終閲覧）、41 頁。

令に基づいて、海外における GA を理由として、当該国へのデータ移転を制限する措置が問題となってきたことを述べた。

この点、2020 年に入りさらにこの検討上注目すべき動きがあった。すなわち、2020 年 7 月には、米国政府機関の監視活動、換言すれば GA のリスクがあるにもかかわらず EU から米国へのデータ越境移転を認めるべきか否かが争われた、いわゆる Schrems II 事件において、CJEU が、一般データ保護規則（以下 GDPR）を適用法規として判決を下した。本稿はこの判決の内容を検討するとともに、同判決が我が国の推進する DFFT に与える示唆を検討するものである。

結論を一部先取りする形になるが、筆者の考えでは、本判決は次のような示唆を DFFT 構想に与えると思われる。第一に、GA 一般に関する議論への影響である。GA のリスクは、DFFT における信頼（Trust）の判断の中核的要素の 1 つであり、これは許容される/されない（すなわち信頼のある/ない）GA の審査基準の問題として立ち現れる。

第二に、仮にそのようにトラストの無い GA が外国に存在するとした場合、当該 GA に関する民間事業者の移転先国でのリスク調査義務や対応策に関する示唆を与えるものでもある。GA はその定義上、必然的に民間部門へのアクセスが問題となるが、この点で民間企業がどのように外国の GA のリスクに対応すべきか、あるいはできるのか、検討されることとなる。

第三に、欧米間のプライバシーに関する対立の再燃である。欧米間のプライバシー保護に関する対立は 40 年以上継続してきたが、それを一定程度緩和して妥協点を見出したのが欧米間のプライバシー・シールド（以下 PS）であった（後掲２．１．参照）。本件では、PS でいったん決着が図られた大西洋間のプライバシー・データ保護に関する欧米対立が再燃したといえるが、これをどう着地させるかは米国の政権交代の影響もあって不透明である。

最後に、この判決はその他にも、内国民待遇や事前通報義務等、今後の GA そしてデータの越境移転制限全般に関する国際的なルール形成への示唆を与える点でも重要な判例であると考えられる。

本稿は以上の問題意識に基づいて、次の構成をとる。すなわち、２．において Schrems II 事件に至る欧米対立を概観し、同事件の CJEU 判決を読み解く文脈を論じるとともに、その判決内容を概観する。また、それを踏まえた各論点に関して CJEU が下した結論に関する評価を行う。３．では本判決を受けた欧米、特に EU の欧州委員会などの行政サイドの動きを概観する。４．では２．と３．を踏まえた、DFFT 構想への示唆を論じる。

２．Schrems II 事件判決の概要と評価

２．１．Schrems II 事件判決前史

２．１．１．EU 成立以前の展開

まず、CJEU の Schrems II 判決に至るプライバシー保護をめぐる欧米の対立について述べていきたい。この点について、筆者はすでに別の論考でこれを取りまとめているため [4]、ここでは本判例を理解するために必要な限りでそれを要約することとする。

第二次世界大戦中、ナチスドイツが電子計算機に格納されたデータを用いてホロコーストを効率的に実行できた反省から、特に欧州では個人に関するデータが、それが公的部門であれ民間部門であれ、体系的に扱われる危険性について高い危機意識があった。

そして、1970 年代にスウェーデンのデータ保護法が世界で初めて個人データの越境移転制限を導入し、同法がドイツ・ジーメンス社職員の個人データについて、スウェーデンから西ドイツへの持ち出しを禁じたことから、越境データの移転制限という問題がビジネス阻害の 1 要因として認識されるきっかけとなった。

その後欧州でスウェーデンに類似した越境移転制限を規定するデータ保護に関する法令が導入されるに至ったものの、米国がこの動きを通商阻害と反発・非難したことから欧米の対立が発生した。いわゆる TDF（Transnational Data Flow）問題と呼ばれる事案である。

越境データに関する欧米対立の調整の場として OECD が活用され、1980 年には OECD で越境移転制限を含む個人データの取り扱いに関するガイドラインが策定された [5]。これはあくまでガイドラインであり、国際法上の拘束力を持つものではないが、2013 年の改訂を経て、今日に至るまで各国のプライバシー保護法制の基礎の 1 つとなっている。

越境データ関連では、とりわけパラグラフ 17 と 18 がこれを規定しており、個人データの越境移転制限は移転先国が本ガイドラインや国内のプライバシー保護法の迂回となる場合（すなわち、輸出先国が輸出元国と同等の保護水準にない場合）にのみ許されるとされている。また、保護に必要である以上に越境データ移転に制限を加える法制の制定を控えるべきである旨も規定されている。

> 17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain

[4] 渡辺翔太「個人情報の越境移転制限に対する規律―国際経済法の果たす役割の模索―」、『日本国際経済法学会年報』26 号（2017 年）188 頁以下。

[5] OECD, *Recommendation of The Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980, at https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (as of 30 June 2021).

categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

2．1．2．EU 成立に伴う 1995 年指令と「十分性認定」

1993 年の EU の発足に合わせて、EU ワイドでのデータ保護に関して定めるルールが必要とされ、1995 年にはデータ保護指令が策定され、これが EU 加盟国の国内法となる中で越境移転制限が EU 大に強化された[6]。

この中で導入された概念が「十分性認定」であり、これは国（およびその一部の地域や部門）を単位として EU における個人情報保護の水準と同等以上であると認めることで、EU から当該国への個人データ移転を可能とするものである。

包括的な個人情報保護法制を持たない米国は、EU との国単位での十分性認定を受けることは困難であったが、経済実態としてすでに大西洋間の個人データの越境移転は活発化しており、EU と米国は大西洋間の個人データの越境移転を効率的に実施する必要に迫られた。

これを実現するため、十分性認定の 1 つの形態である実装行為による補完としてセーフハーバー協定を締結した（実装行為による補完については後掲）。セーフハーバー協定では、米国の個人データを取り扱う事業者は自主規制としてセーフハーバー協定に規定された個人情報保護措置の内容を米国商務省に対してコミットし、商務省の監督に服する。セーフハーバー協定は、それにより、自主規制の登録事業者について EU 法との十分性を認めるものであった。これは大西洋間のデータ移転を可能ならしめる非常に重要な協定であったといえる。

2．1．3．スノーデン事件とセーフハーバー無効判決（Schrems 事件）

しかし、2013 年に米国国家安全保障局（NSA）の諜報活動員であったエドワード・スノーデンが NSA による様々な民間企業へのデータアクセスを含む諜報活動の実態を暴露した、いわゆるスノーデン事件が発生した。この中ではとりわけ、米国政府が PRISM と呼ばれる監視スキーム等を活用して、通信事業者や SNS 事業者等から多様なデータを、バルクデータ収集（事前の範囲指定なく一括でのデータ収集）を含めて、実施していたことが明らかにされた。

この事件を受けて、2013 年 6 月 25 日、オーストリア市民の Maximilian Schrems 氏は

[6] EU 法上、指令は加盟国の国内法として直接効力を持たず、加盟国が指令に基づく国内法化を行って初めて法的効力を持つ。

Facebook Ireland による米国への個人データの移転を禁止するようアイルランドデータ保護監督機関（DPA）に請求したが、アイルランド DPA は特にセーフハーバー協定に基づく欧州委員会による十分性認定（Decision 2000/520）に基づき、米国は適切な保護のレベルを確保しているとして請求を退けた。

Schrems 氏はこのアイルランド DPA による請求拒否について、アイルランド高等法院に不服審査を申し立てたが、高等法院はこの請求に関する判断を下すには EU 法に関する解釈が必要であるとして、CJEU に先決裁定（preliminary rulings）を依頼した。

結果、CJEU は 2015 年 10 月、CJEU は米国政府による諜報活動は EU の制度に比べて十分な保護を提供していない等として、セーフハーバー協定を無効とした(Schrems 判決（C-362/14, EU:C:2015:650)、2015 年 10 月 6 日)。

２．１．４． NSA の諜報活動の制限とプライバシーシールド（PS）の締結

スノーデン事件を受けて、当時のオバマ政権は大統領令（PPD-28 等）による諜報活動の制限等を実施して、米国の諜報活動の個人データの水準を高めるべく、一定の対応を実施した。

欧州委員会はこれを受けて米国とセーフハーバー協定の改正を交渉し、2016 年には新たに欧米間で PS が締結された。

その後 2017 年～19 年にかけて、PS に関して 3 回にわたる欧州委員会によるレビューが実施され、その実装行為による補完について欧州におけるデータ保護法制との同等性が確認されている。

他方、上記の複数回の欧州委員会によるレビューについて、EU における EU 加盟国の DPA の代表者および欧州データ保護監視官局からなる欧州データ保護会議 EDPB(European Data Protection Board)は PS が EU の制度と整合的でないと批判してきた。例えば、2019 年 1 月の文書においては、十分性を確認する欧州委員会と米国政府当局間のレビュー結果について、EDPB は自らのレビュー結果に基づき、PS について、「欧州委員会並びに米国当局双方が説明すべき深刻な懸念がいくつもある」と述べている [7]。

また、欧州議会も 2018 年にプライバシーシールドの停止決議を行う等、プライバシーシールドの欧州基準との整合性に批判的であった [8]。

---

[7] European Data Protection Board, *EU - U.S. Privacy Shield - Second Annual Joint Review*, adopted 22 January 2019, at https://edpb.europa.eu/sites/default/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf (as of 30 June 2021), para. 106.

[8] European Parliament, *European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP))*, at https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.html?redirect (as of 30 June 2021), para. 35.

２．２．Schrems II 事件判決の概要

２．１．で述べた通り、Schrems 氏はアイルランド国内で DPA への苦情申立、高等法院への提訴を行った。高等法院から先決裁定の要請を受けた CJEU は米国のセーフハーバー協定に基づく十分性認定が無効であることを決定した。

結果、請求がアイルランド DPA に差し戻されたため、アイルランド DPA は Schrems 氏に対し請求を再提出することを求めた。その後、Schrems 氏が請求を再提出したため、DPA は EU 域内の市民の個人データが米国において関連法令に違反する形で処理されている可能性があるという「暫定決定」を公表した。Schrems 氏が再請求において標準契約条項（以下 SCC）の有効性について問題を提起したため、DPA は高等法院に訴えを提起したが、高等法院は本件についても EU 法の解釈が関わるとして、CJEU に対して先決裁定を依頼した。この要請への回答が、本稿の主題となる CJEU による Schrems II 判決である。

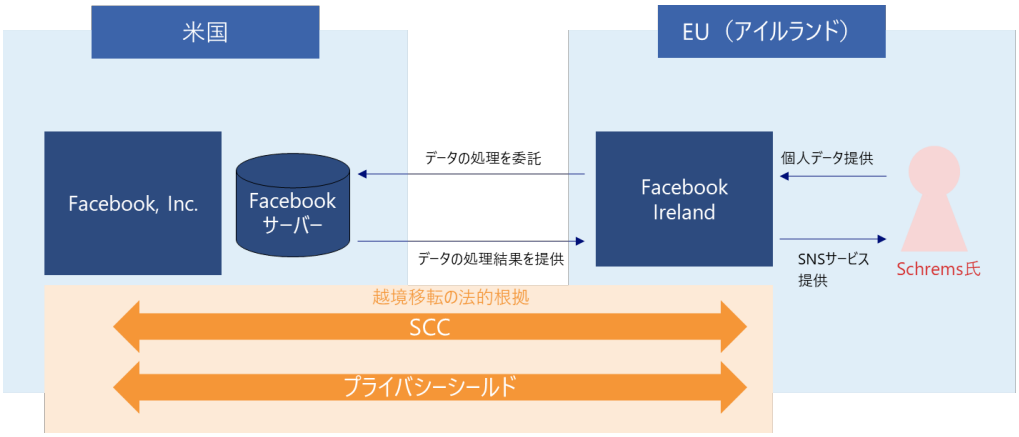
判決の内容に入る前に、分析の前提として、本事件における越境移転に関する事実関係を整理しておきたい。

オーストリア人である Schrems 氏を含む EU 市民は、Facebook のサービスを利用するにあたって、Facebook の欧州拠点であるアイルランド法人とサービス提供契約を締結する。Facebook 社アイルランド法人は、同社米国本社との間でデータ処理契約を締結している（アイルランド：管理者、米国：処理者）。Facebook 社のサーバーは物理的には米国に所在し、ここでは Facebook 社の米国本社とアイルランド法人という法人間でのデータ越境移転が成立している。

ここで、Facebook 社によるアイルランド法人から本社への越境移転の根拠は、①Facebook 本社・アイルランド法人間の SCC、②米 EU プライバシーシールド、の 2 つが考えられる。

以上を図に示すと、次の通りとなる。

図表 1　Schrems II 事件における契約関係と越境移転の法的根拠



また、ここで EU 法上の越境移転規制についても概観したい。データ保護指令やそれを引

き継いだ GDPR では原則として EU 域外への個人データの移転が禁止される。この原則の例外として越境が許容される場合が法令上規定されており、原則として EU 以上の保護水準をどのように確保しているのか、という観点から評価がなされていると理解すればよい[9]。

まず、国単位の十分性認定がある。この十分性認定は、例えばカナダのように民間部門のみ等の一定の制限がかかる可能性もあるが、国単位の認定が最も一般的であり、日本も 2019 年 1 月に個人情報保護法が適用される民間部門について十分性認定を受けている[10]。

そして、この国単位の十分性認定の中には、既存の国内法では EU 法上の保護と比べて不十分な部分について、二国間協定等の実装行為による補完を行ったうえでの十分性認定があり、これがまさにセーフハーバー協定や PS であった。

次に、移転先の組織が EU と同等の保護水準をとっている場合がある。これを担保するものとして、当事者間の SCC や拘束的企業準則（以下 BCR）によるものが一般的である。ここで、SCC は欧州委員会があらかじめ提示している契約のひな形に従って当事者間で契約を締結することとされ[11]、他方で BCR は企業グループ単位でのプライバシー保護制度について、DPA による認証を必要とする。実務的には SCC がより広く普及していると考えられる。

また、データ保護指令には規定がなく、GDPR で導入されたものの未だ十分に活用されていない越境移転の法的根拠として、認証や行動規範がある[12]。

さらに、上記の各根拠に依拠できない場合の例外として、同意や契約の履行等も存在するが、あくまで例外であり、反復継続が予定されない一時的なデータ移転が前提とされている点に留意する必要がある。

---

[9] この点について、例えば石井夏生利『EU データ保護法』（勁草書房、2019 年）、152-182 頁を参照。

[10] 日本では、公的部門については従来個人情報保護法の対象外となってきたが、法改正を踏まえて一元化が進められている。

[11] SCC の仮訳については次の URL を参照（ただし、本判決を受けて改訂される点に留意）；日本貿易振興機構「標準的契約条項（Standard contractual clauses：SCC）（欧州委員会資料の仮訳）（2018 年 3 月）」（2018 年 3 月 28 日）（https://www.jetro.go.jp/world/reports/2018/01/8d894f365ea5c3a7.html, 2021 年 6 月 30 日最終閲覧）。

[12] GDPR 上のこれらの規定については紙幅の関係上説明を省略する。邦語の解説書として、小向太郎・石井夏生利『概説 GDPR』（NTT 出版、2019 年）、西村あさひ法律事務所編『個人情報保護法制大全』（商事法務、2020 年）、森大樹他編『日米欧 個人情報保護・データプロテクションの国際実務』（商事法務、2017 年）等がある。

図表 2　Schrems II 事件における契約関係と越境移転の法的根拠

越境移転が許容される根拠		データ保護指令	GDPR
国単位の十分性認定（GDPR 第 45 条）	国単位の審査	○	○
	実装行為による補完	○	○
組織単位の十分性認定（同上第 46 条他）	標準契約条項（SCC）	○	○
	拘束的企業準則（BCR）	○	○
	認証	-	○
	行動規範	-	○
例外	同意	○	○
	契約の履行	○	○
	公共の利益	○	○
	その他	○	○

２．２．１　Schrems II 事件の諮問事項

本題の判決内容に戻ると、アイルランド高等法院から CJEU に先決裁定の中で特定された本件の諮問事項は合計 11 と多岐にわたっている[13]。これらについて筆者なりに整理を加えると、以下の図表の 4 点に集約されると思われる。

なお、以下のうち☆は判例評釈等において比較的触れられている事項である一方、★は筆者として、特に１．で掲げた DFFT への示唆という観点から重要であるものの、他の判例評釈等では必ずしも触れられていない点である。

[13] 個別の諮問事項については本稿の参考資料 1 を参照。

図表 3　Schrems II 事件の諮問事項

#	論点	論点の説明
1	★安全保障例外の該当性（諮問事項(1)）	• EU と加盟国の権限配分を定めるリスボン条約（以下 TEU）4 条 2 項は「国の安全保障は、各加盟国の排他的な責任のもとに留保される」と規定しており、そもそも第三国において安保を目的とした諜報活動は同条約に基づいて立法された GDPR の範囲外なのではないか？ • また、このような安全保障に関する例外として、米国の監視活動は GDPR2 条 2 項の例外規定にも含まれ得るのではないか？
2	☆SCC の有効性（諮問事項（2)、(3)、(6)、(7)、(11)）	• SCC の有効性を判断する EU 法上の保護水準（GDPR、EU 基本権憲章（以下基本権憲章））は何か？ • SCC は EU 法上の保護水準に照らして EU と同等の保護を提供しているか？
3	★DPA の権限(諮問事項(8))	• SCC が締結されている場合、当局は欧州委員会が決定した SCC についてデータの移転中止を命じることができるか？
4	☆PS の有効性(諮問事項質問(4)、(5)、(9)、(10))	• PS は EU 法上の保護水準（GDPR、基本権憲章）に照らして EU と同等の保護を提供しているか？

以下、上記図表の 1～4 の各論点について、Schrems II 事件判決の判断内容を概観する。なお、2018 年 5 月にデータ保護指令を置き換える一般データ保護規則（General Data Protection Regulation; GDPR）が施行されたため、CJEU による本判決はこれをもとに判断している点に留意いただきたい。

2．2．2．論点 1： 安全保障例外の該当性 [14]

上記から明らかなように、ここでの諮問事項は米国の監視活動が①EU 法のレベルでの適用除外、②データ保護指令/GDPR 上の適用除外に該当するか否か、である。①について、裁判所はまず加盟国と EU の権限配分を定めた TEU の第 4 条 2 項は、EU 内では、国家安全保障は加盟国の唯一の責任であり加盟国のみに関係すると定めており、この規則は現在の場合、GDPR の第 2 条（1）および第 2 条（2）(a)、(b)、(d）を解釈する目的には関係を持たない、とした。

次に②について、裁判所は、例外については GDPR の第 2 条(2)に規定されているが、本

[14] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559, paras. 80-89.

件では、法人間でのデータの移転が問題となっており、このような移転は自然人によるデータの処理を規定した GDPR 第 2 条(2)(c)の範囲に含まれないとした。また、第 2 条(2)の(a)、(b)、(d)に規定された活動にもあてはまらないため、これらの規定の範囲にも含まれないとした。

裁判所は、したがって、GDPR の第 2 条 (1) および (2) が、その移転時またはその後、公の秩序、防衛および国家安全保障の目的で EU から移転された個人データが当該第三国当局によって処理される責任があるかどうかに関係なく、加盟国で設立された経済運営者による第三国に設立された別の経済運営者への商業目的の個人データの移転にその規則が適用されることを意味するものとして解釈されなければならない、とした。

２．２．３．論点２：SCC の有効性 [15]

CJEU はまず、十分性を評価する法的枠組みについて次のように述べる。すなわち、CJEU は、EU 法の解釈と EU 立法の合法性の検討は、基本権憲章によって保障された基本的権利に照らして保障されなければならない、と判断してきた。また、CJEU は EU 法の規定の有効性と解釈は、明白に加盟国の国内法に言及されていない限り、国内法に照らして構成されてはならない、と一貫して判断してきた。

よって、本件のような商業目的での民間企業間の EU 加盟国から第三国への個人データの移転は、GDPR の適用範囲にある。この規制の目的は、EU 域内で自然人に対し一貫したハイレベルの保護を確保することにあり、その目的のために、GDPR 第 46 条(1)により求められる基本的権利の保護水準は、GDPR に照らして決定されなければならない。

GDPR 第 46 条の条文は考慮しなければならない要素を列挙していないが、同条(1)はデータ主体が適切なセーフガード、執行可能な権利、有効な法的救済を与えられなければならないと規定している。

したがって、GDPR の第 46 条(1)と (2)(c)は、データが第三国に移転されるデータ主体は GDPR によって EU 域内で保証されるのと同じレベルの保護を与えられなければならないという意味で解釈されなければならないというものである。

CJEU は以上のように述べた後、欧州委員会による SCC Decision の有効性の判断を行った。SCC Decision の第 4 条は、Implementing Decision 2016/2297 の前文 5 に照らして読めば、権限を有する監督機関が標準契約条項に従った第三国へのデータの移転を適切に一時停止または禁止することを妨げていないという見解を支持している。よって、DPA の権限への回答からも明らかなように（後掲２．２．４を参照)、欧州委員会の有効な十分性認定がない場合には、権限を有する監督機関は、標準契約条項が第三国で遵守されておらずまたは遵守不可能であり、他の手段によっても EU 法で求められる水準の保護を確保できな

[15] *Ibid.*, paras. 90-105, 122-149.

いと判断する場合には、管理者または処理者が自ら移転をやめない限り、当該移転を一時停止または禁止することが求められる。

よって、質問(7)、(11)への回答は、基本権憲章第 7 条、8 条、47 条に照らした SCC Decision の検証は、当該 Decision の有効性にいかなる影響も与えないということになる。

2．2．4．論点 3：DPA の権限[16]

論点 3 は、EU 加盟国の DPA が、欧州委員会による SCC 決定をどの程度尊重する必要があるか、という EU のデータ保護体制における権限配分に関する論点である。

CJEU は、欧州委員会による決定が裁判所により無効であると宣言されるまでは、加盟国とその当局は、拘束力を持つことを意図して第三国が適切なレベルの保護を保証していないと決定したり、その結果として第三国への個人データの移転を一時停止又は禁止したりする等の、決定に反する措置を採用することはできないと述べる。

ただし、GDPR 第 45 条(3)に従って採択された委員会の決定は、第三国に個人データが移転された個人が国内の権限ある当局（すなわち DPA）に対し、GDPR 第 77 条(1)に基づく請求を申し立てることを妨げることはできない。同様に、委員会による決定は基本権憲章第 8 条(3)と GDPR の第 51 条(1)、57 条(1)(a)によって国内監督機関に与えられた権限を削除または縮減することはできない。

したがって、もし委員会による決定が採択されていたとしても、加盟国の DPA は苦情処理の中で、当該決定とは完全に独立して、データの移転が GDPR に反するものであるか否かを検討することができる。

よって、GDPR 第 58 条(2)（f）と(j)は、有効な欧州委員会による決定がない場合には、権限を有する監督機関（DPA）は、当該移転の状況に照らして、これらの条項が第三国において遵守されておらず、EU 法、特に GDPR の第 45 条と 46 条と基本権憲章によって求められる保護が SCC への追加的保護措置（ additional safeguards ）によって確保されていないと判断した場合には、委員会によって採択された準契約条項に基づいた第三国へのデータの移転を一時停止、又は禁止することを求める。

SCC については、移転が違法な場合には DPA が差し止めできるため、SCC の規定自体が GDPR に反するものではない。

2．2．5. 論点 4：PS の有効性[17]

アイルランド高等法院での訴訟においては PS の有効性も検討されているため、本件においても PS の有効性の検討が必要とされる。

CJEU は、個人データの民間企業から政府当局等の第三者への提供は基本権憲章の第 7 条

---

[16] *Ibid.,* paras. 106-121.

[17] *Ibid.,* paras. 150-202.

と 8 条に規定される基本的権利への干渉を構成すると判断してきたが、第 7 条および 8 条に規定される権利は絶対的なものではなく、社会における機能との関係で検討されなければならない。

これに関連して、基本権憲章の第 8 条（2）に基づいて、個人データは、特に、「特定の目的のために、そして関係者の同意またはその他の法律で定められた正当な根拠に基づいて」処理されなければならないことにも注意する必要がある。

基本的権利の行使に対する制限が法律によって提供されなければならないという要件は、それらの権利の干渉を許可する法的根拠自体が、関連する権利の行使に対する制限の範囲を定義しなければならないということを示している。

本件では、米国が GDPR によって EU で保証されているものと本質的に同等の個人データの適切なレベルの保護を保証するという Privacy Shield Decision における欧州委員会の決定は、とりわけ、米国の外国情報監視法（FISA）の第 702 条と合衆国大統領令 12333 号（EO12333）に基づく監視プログラムから生じる干渉が、比例原則に従い、基本権憲章第 52 条 (1) の 2 文によって保証されるレベルと本質的に同等の保護のレベルを保証する要件によってカバーされていないのではないか、という疑問を提起する。したがって、これらの監視プログラムの実施がそのような要件の対象であるかどうかを調べる必要がある。

欧州委員会の決定によれば、FISA702 条は、米国の PRISM 等の監視プログラムについて、司法長官と国家情報長官の認証に基づき、個別の事案ではなく概括的に外国情報監視裁判所が審査するに過ぎない。CJEU の先例に基づくと、基本権への干渉を許容する法的根拠は比例性の原則を満たし、権利行使への制限に関する範囲を規定し、審査される措置の範囲や適用を規定する明確かつ適切な規則を定め、最低限の保護を課すものである必要がある。米国の上記制度はこのような要求に合致していない。

また、上記の米国監視プログラムは大統領政策指令 PPD-28 の要件に従うが、PPD-28 はデータ主体に米国当局に対して訴訟を提起できる権利を付与していない。したがって、Privacy Shield Decision は基本権憲章と本質的に同等の保護のレベルを保証していない。EO12333 に基づく監視プログラムも米国当局を訴えることができる実行可能な権利を付与していないことは明らかである。

また、基本権憲章第 47 条は EU 法に基づき権利と自由を保証された者は皆、違反に対し裁判所における有効な救済を得る権利を有していることを定めており、同条第 2 パラグラフでは独立した裁判所による審査の権利を有していることを定めている。

本件に関し、Privacy Shield Decision が言及するオンブズパーソン制度は、個人データが米国に移転された個人に対し基本権憲章 47 条で保証されるのと本質的に同等の保護を保証する機関への訴因を挙げていない。

よって、米国が十分なレベルの保護を与えているとした Privacy Shield Decision 第 1 条における委員会の決定は、GDPR の第 45 条(1)の要件を欠いており、Privacy Shield Decision 第 1 条は、GDPR の第 45 条(1)に反している。

Privacy Shield Decision の第 1 条は第 2 条と第 6 条、附属書と不可分であるから、第 1 条の無効性は、Privacy Shield Decision 全体の有効性に関わる。

以上から、CJEU は Privacy Shield Decision は無効であると結論づけた。

２．２．６　諮問事項に関する結論

以上、4 点に関する諮問事項の本判決における結論をまとめると、次の図表の通りとなる。

図表 4　Schrems II 事件の諮問事項とその判決における結論

#	論点	概要	判決における結論
1	★ 安全保障例外の該当性	• EU と加盟国の権限配分を定める TEU4 条 2 項において「国の安全保障は、各加盟国の排他的な責任のもとに留保される」と規定しており、そもそも第三国において安保を目的とした諜報活動は同条約に基づいて立法された GDPR の範囲外なのではないか？	• TEU における権限配分は EU 加盟国を念頭に置いたものであり、第三国には該当しない。 • GDPR 第 2 条 2 項は GDPR の適用除外を定めるが、本件データ移転は私企業によるビジネス上の個人データ移転であり、いずれにも該当しない。 • 以上より、GDPR が米国へのデータ移転とその後の米国政府による移転データの取り扱い（監視活動等）がなされる可能性があるものにも適用される。
2	☆ SCC の有効性	• SCC の有効性を判断する EU 法上の保護水準（GDPR、基本権憲章）は何か？ • SCC は EU 法上の保護水準に照らして EU と同等の保護を提供しているか？	• 求められる保護水準は EU と同等なものである。 • SCC については、移転が違法な場合には DPA が差し止めできるため、SCC の規定自体が GDPR に反するものではない。 • 移転先のリスクに応じて EU 法上の保護との十分性を確保する適切な体制構築が求められ、必要に応じて追加的保護措置（Additional safeguard）が求められる。
3	★ DPA の権	• SCC が締結されている場合、当局は欧州委員会が決定した SCC についてなお	• DPA は SCC に従っている場合であっても、具体的な事案において、個別の苦情処理の権限に基づいて、デ

	限	データの移転中止を命じることができるか？	ータ管理者へのデータ処理(SCC に基づく越境移転を含む）に関する執行を行うことができる。
4	☆ PS の有効性	• PS は EU 法上の保護水準（GDPR、基本権憲章）に照らして EU と同等の保護を提供しているか？	• PS は比例性、救済等の点で EU と同等ではなく、PS は EU 法に反しているため、無効である。

２．３．Schrems II 事件の評価

ここでは、以上取りまとめた判決の内容について、筆者の評価を加えることとする。

２．３．１．論点１： 安全保障例外の該当性

論点１は CJEU の判断内容が若干わかりづらいが、判示をまとめると、次のようになろう。

まず、TEU における権限配分は EU 加盟国を念頭に置いたものであり、第三国には該当しない。次に、GDPR 第２条２項は次の通り GDPR の適用除外を定めるが、本件データ移転は Facebook 社の米国本社とアイルランド法人という私企業によるグループ会社間のビジネス上の個人データ移転であり、もちろん公共の安全を目的とした取り扱いではないから、下記のいずれの例外にも該当しない。

> 本規則は、以下の個人データの取扱いには適用されない：
> (a) EU 法の適用範囲外にある活動の過程で行われる場合。
> (b) 加盟国によって EU 条約第 5 款第 2 章の適用範囲内にある活動が行われる場合。
> (c) 自然人によって純粋に私的な行為又は家庭内の行為の過程において行われる場合。
> (d) 公共の安全への脅威からの保護及びその脅威の防止を含め、所管官庁によって犯罪行為の防止、捜査、 検知若しくは訴追又は刑罰の執行のために行われる場合。

したがって、Facebook のアイルランド子会社から本社への移転には GDPR が適用される、というものである。

以上の通り、この判決自体は TEU や GDPR の解釈にとって特に目新しいものはないであろう。TEU はあくまで EU 加盟国間の条約であって、その適用対象や除外の対象に第三国が入ることはおよそ想定しづらい。また、GDPR も同様に EU 加盟国を名宛人としたものであり、その適用除外に第三国が入るとは想定できない。

しかし、仮に Facebook が本社も EU 域内に置く企業であり、アイルランド子会社から別の EU 加盟国にある本社にデータを移転しており、当該本社のある EU 加盟国が監視活動の

ために Facebook 社に個人データの提供を依頼した場合、この事件の帰結はどうなるか。この場合、TEU 第 4 条 2 項や、それを踏まえた GDPR 第 2 条 2 項(d)の例外事由に当たりそうである。

この両者の間には、データの移転やサービスの提供という経済実態の側面では大きな差異はないが、EU 法上の枠組みにおいては大きな差異がある。それによって米国のみが過度な負担を負わされているととらえられるのではないか。

この点、まさに米国からは、本判決について、EU 加盟国には広範な安全保障上の裁量が与えられているが、EU 域外国に対してはそのような裁量が認められず、不公平であるとの指摘もなされている [18]。すなわち、Joshua Meltzer によれば、「実際各 EU 加盟国はデータ保護の権利と国家の安全保障に関する均衡点を設定する裁量を与えられている。しかし、EU はこのような裁量を第三国には与えない。実態として、GDPR は EU の個人データへのアクセスを認めない脅威を、他国の安全保障機関に対して CJEU が定める比例性等の改革を求めるツールとして利用しているが、EU 加盟国の政府に対しては同様の期待や脅威を除外している。そして、このような安全保障分野における GDPR の第三国と EU 加盟国への適用の違いが、諜報当局の活動実態と EU の要求がさらに乖離するリスクを増大させている。米国では安全保障と米国憲法を反映したプライバシー保護の均衡が目指されるが、EU にはこのような均衡はなく、(中略) 結果として、第三国の国家安全保障機関に対して、EU が EU 加盟国の同様の機関に対しては要求せず、またすることもできない要求を行っているといえる」と述べている [19]。

しかし、このような批判については、必ずしも当たらない部分もあるのではないかと筆者は考えている。EU 加盟国においては、国際連合による市民的及び政治的権利に関する国際規約（ICCPR）や欧州人権条約（ECHR）等の国際人権条約、そして何より国内法の憲法上の人権保障によって諜報活動に関して市民のプライバシー等の人権保障に一定の制約、あるいは Meltzer の言葉を借りれば均衡が担保されているのである。上記の批判において Meltzer は本判決の言明をもとに、すなわち EU 法のみを念頭に置いているが、EU においては EU 加盟国の国内法上の権限でこのような人権保障と安全保障の均衡を独自に設定できるのであり、Meltzer の批判はこのような国際法、EU 法、国内法という人権保障法制の多重性を見落としているといえよう [20]。

---

[18] Joshua P. Meltzer, "The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security," *Brookings Report* (5 August 2020), at https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/ (as of 30 June 2021).

[19] *Ibid.*

[20] なお、このような保護の重層性は後掲の 2020 年 10 月の CJEU の判決においても触れられている。Joined Cases C-511/18, La Quadrature du Net and Others v. Premier ministre and

ただし、上記の筆者による再批判を踏まえたとしても、EU における個別の加盟国が実施する監視活動における市民の個人データ保護の水準が、EU が GDPR に基づいて米国に求めるそれと同等かという検証はさらに必要となる。

この点の検証は本稿の射程を超えるものであるが、筆者は各国の諜報活動の根拠法の概略を調査しており、例えばフランスの諜報法制が比例原則を充足しておらず、EU 法上の人権保障を備えているか疑問を感じる点も指摘してきた[21]。また、例えば ECHR に基づく欧州人権裁判所での英国の諜報活動法制に関する ECHR との整合性に関する判決等[22]、国際裁判においてもこの点が議論されてきたところである。

そして、2020 年 10 月には 4 件の注目すべき CJEU の判決が公表されるに至っている[23]。これらはいずれも政府の諜報活動に対して GDPR や ePrivacy 指令の保護が適用されるかが争われたものである。

これらの判例では、まさに Schrems II 事件で問題となった TEU 第 4 条による除外は、民間企業には妥当せず、民間企業が諜報機関に対して情報提供を行うことは当然に個人データの取り扱いとなり、GDPR の適用範囲となることが示された。これはまさに、民間データに対する政府機関のアクセスという、GA の構造を逆手にとって EU 法上の保護範囲を実質的に拡大するものであり[24]、いわば上記の法的保護の重層性にさらに公的/私的の区分を加えたものといえる。

また、同判決は下記の通り、加盟国政府によって権利侵害を伴う措置が安全保障上の目的で実施されたという主張だけで当然に EU 法の適用対象外となるというわけではない、との判断も示しており、安全保障の適用除外は、少なくとも CJEU の解釈においてはかなり限定的に解釈されていると考えられる[25]。

Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Other, ECLI:EU:C:2020:791 [hereinafter La Quadrature du Net and Others v. Premier ministre and Others], para. 103.

[21] 拙稿「前掲論文」(注 2)、9-10 頁。

[22] Case of Big Brother Watch and Others v. The United Kingdom, Judgement of 13 September 2018, European Court of Human Rights.

[23] La Quadrature du Net and Others v. Premier ministre and Others , *supra* note 20; Case C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, ECLI:EU:C:2020:790. これらの判決について、研究発表の場において経済産業省通商戦略室の皆様から貴重な示唆を得た。ここに記して謝意を表したい。

[24] Juraj Sajfert, "Bulk Data Interception/Retention Judgments of the CJEU – A Victory and a Defeat for Privacy," *European Law Blog: News and Comments on EU Law* (26 October 2020), at https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/ (as of 30 June 2021).

[25] La Quadrature du Net and Others v. Premier ministre and Others , *supra* note 20, para. 99

99 Article 4(2) TEU, to which the governments listed in paragraph 89 of the present judgment have made reference, cannot invalidate that conclusion. Indeed, according to the Court's settled case-law, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law

上記判例は本判決より後に公表されたものであるが、以上を踏まえれば、本判決の内容は妥当なものであったといえよう。この論点に関する CJEU の判断は、TEU 第 4 条は第三国を含まない民間企業間の経済的な移転であるから GDPR の適用除外には含まれない、といった一見すると形式的な判断を行っているように見えるが、実際には上記のように一連の判例の中で、本件事案の解決に必要な限りでの判示を行ったものであったということができるかもしれない。

そして、本判決を踏まえて、上記の GA に対する多層的な市民への法的保護が EU 加盟国の法制で具体的にどのように構成されているか、さらなる検討を継続する必要があるだろう。

２．３．２　SCC の有効性に関する判断/ DPA の権限に関する判断

第二に、SCC の有効性に関する判断については、かねてより SCC は民間企業間のデータ取り扱いに関する契約であり、第三国の政府機関等を拘束できないがゆえに無効になる恐れがある、と指摘されていた[26]。

この点、筆者は、本件における CJEU の判断は、DPA の権限に関する判断と組み合わせることで、巧みにバランスをとったといえると考える。すなわち、SCC はあくまで民間企業間の契約であるが、その内容として移転先国におけるリスクに応じた適切な対応を求めることは（民間企業が諜報機関の活動に実際どの程度対処可能かという疑問をおくとして）理論上は可能である。他方で、このような追加的な保護措置がなされない場合であっても SCC の存在をもって常に移転が許可されるというのは妥当でなく、どこかで DPA の関与する余地を残す必要があり、そのいわばとっかかりを苦情処理の権限に求めたといえる。

他方で、上記の通り、民間企業がどのように第三国のリスクを特定し、どのように対処できるのかについてはなお定まっておらず、この点で企業実務に対してのガイダンスとしては十分ではないが、それは司法機関に求めるものでないといえよう。この点についてはすでに欧州委員会が対応を開始している（後掲３．２．を参照）。

[26] Christopher Kuner, "Schrems II Re-Examined," *Verfassugsblog on Matters Constitutional* (25 August 2020), at https://verfassungsblog.de/schrems-ii-re-examined/ (as of 30 June 2021).

２．３．３．PS の有効性に関する判断

最後に、PS の EU 法との同等性に関する判断枠組は Schrems 事件を踏襲したものであって、それ自体には新味がない。本件判決の意義は、適用法規が 95 年指令から GDPR にかわっても、同一の基準が用いられることを確認した点にあるといえよう。

３．判決を受けた欧米の動向

Schrems II 判決を受け、欧米間における PS の改訂、欧州における DPA の執行や SCC の改訂、追加的な保護措置に関する勧告等が発出されている。

３．１．　欧米間の動向

判決を受け、2020 年 8 月 10 日には、米国のウィルバー・ロス商務長官（当時）と EU 欧州委員会の司法担当委員による共同声明が発出された。この中で、商務省と欧州委員会は PS の改訂に関する可能性の検証を行うための議論を開始した、と非常に迂遠な表現で PS の改訂を示唆したが、この表現にある通り、具体的な進展は見られていない[27]（下線は筆者）。

> The U.S. Department of Commerce and the European Commission have initiated discussions to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to comply with the July 16 judgment of the Court of Justice of the European Union in the Schrems II case. This judgment declared that this framework is no longer a valid mechanism to transfer personal data from the European Union to the United States.
> The European Union and the United States recognize the vital importance of data protection and the significance of cross-border data transfers to our citizens and economies. We share a commitment to privacy and the rule of law, and to further deepening our economic relationship, and have collaborated on these matters for several decades.　（以下略）

なお、2021 年 3 月には欧州委員会の司法担当 Reynders 委員と米商務長官 Raimondo 氏の連名で、上記の交渉を加速させるとのプレスリリースが発出されているが、やはり具体的な動きは見られない[28]。

３．２．欧州の動向

３．２．１　EU における DPA の執行

---

[27] U.S. Department of Commerce, *Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders*, 10 August 2020, at https://2017-2021.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european.html (as of 30 June 2021).

[28] European Commission, *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo*, 5 March 2021, at https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443 (as of 30 June 2021).

上述の Schrems II 判決を受けて、PS が無効になるとともに、SCC にも追加的な保護措置が求められる等、企業に求められる対応事項が多数生じた。

この点、報道等では判決直後からアイルランド当局が判決以降 2020 年 9 月には Facebook 等の PS に依拠する事業者の移転停止に向けた執行を検討すると発表、ドイツでも DPA が独自にガイドラインを策定する動きを見せる等積極的な動きを見せる DPA があったものの、具体的な執行活動に至るケースはなかったと見られる。

しかし、2021 年 2 月には、ドイツの DPA 会議において、ハンブルク州 DPA とベルリン DPA が中心となって Schrems II 事件に係る執行活動を行う旨が決定された[29]。ハンブルク州 DPA が無作為に企業に対して Schrems II 対応の調査を実施し、同判決で対応が求められる事項を履行しているか否か判断するとしている[30]。

３．２．２．追加的保護措置に関する勧告と SCC の改訂[31]

Schrems II 事件判決のより本質的な課題は SCC に求められる民間企業による追加的保護措置の内容であったが、2020 年 11 月 10 日に EDPB が追加的保護措置に関する勧告案を公表しパブリックコンサルテーションにかけている[32]。

この中で、EDPB はデータの出し手に対して、データの移転先国の GA に関するリスクを適切に評価するとともに、それに対して追加的な保護措置を検討、履行するよう求めている。EDPB は特に、GA に対しては契約や組織的な保護措置では限界があることを指摘し、技術的な保護措置の重要性を指摘しており、契約や組織的保護措置は技術的保護措置を補

---

[29] Datenschutzaufsichtsbehörden des Bundes und der Länder, Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Videokonferenz am 25. und 26. November 2020 - Protokoll -, 14 January 2021, at https://www.datenschutzkonferenz-online.de/media/pr/20210203_%2020201030_protokoll_100_100.pdf (as of 30 June 2021), Top8a.

[30] Gary LaFever, "Schrems II: DPAs in Germany Begin Compliance Checks - Other Jurisdictions Soon to Follow," *Linkedin* (20 February 2021), at https://www.linkedin.com/pulse/schrems-ii-dpas-germany-begin-compliance-checks-other-gary-lafever/ (as of 30 June 2021).

[31] この点に関する日本語の論稿として、板倉陽一郎・寺田麻佑「Schrems II 決定（CJEU Case C-311/18）を受けた『追加的な措置』（Supplement Measures）及び新たな標準契約約款（Standard Contractual Clauses）の動向」『情報処理学会研究報告』（Vol.2021-EIP-91 No.7）がある。

[32] 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*, adopted 10 November 2020, at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (as of 30 June 2021).

完することを指摘している[33]。

そして、このような技術的保護措置として、必要に応じてデータの受け手と連携しつつ、次の 4 点を考慮に入れて必要な追加的保護措置を決定すべきとしている[34]。

1. データフォーマット（平文か仮名化、暗号化など）
2. データの性質
3. データ処理のワークフローの長さや関与する主体の数、それらの関係性
4. データのさらなる移転の可能性（移転先国やさらに別の国）

また、上記の技術的保護措置について、Annex II でユースケースを挙げて解説している点も注目される。この中で、追加的保護措置が有効なユースケースとして、①強力な暗号化がなされている場合の第三国におけるバックアップ、②適切な仮名化がなされている場合の移転、③エンドツーエンド暗号化がなされている場合の第三国の通過、④暗号化がなされている場合の特に保護された輸入者への移転、⑤秘密計算の利用が挙げられている。

他方、無効なユースケースとして、⑥クラウドサービスの利用において当該サービスに GA が行われる場合，⑦ビジネス目的でリモートアクセスを行うが GA が行われる場合、が挙げられている。

さらに欧州委員会は、2020 年 11 月に改訂版の SCC 草案を公表し、同年 12 月までこれがパブリックコンサルテーションにかけられていた。この草案は、①条項をモジュール化して 4 つのシナリオ（管理者/処理者の組み合わせ）を想定して必要な条項を選択性にしている点、②これによって処理者を起点とするデータフローが設定された点、③3 者以上での契約が可能となっている点、等が挙げられる[35]。

---

[33] *Ibid.,* para. 48.

[34] *Ibid.,* para. 49.

[35] Caitlin Fennessy “New EU SCCs: A modernized approach,” *IAPP* (13 November 2020), at https://iapp.org/news/a/new-eu-standard-contractual-clauses-a-modernized-approach/ (as of 30 June 2021).

４．Schrems II 事件が DFFT の議論に与える影響

以上を踏まえて、本稿の目的である DFFT 構想への示唆を、特にルール形成という観点から導出したい。筆者は、本判決から下記の 5 点の示唆を得ることができると考える。

区分	論点	本件での判示事項	日本のルール形成への示唆
GA に関するグローバルなルール形成への示唆	①越境移転制限が許容される GA の審査基準	• 基本的にはかねてからの CJEU の本質的同等性に関する基準を踏襲している。	• GA が具備すべき条件に関するルール形成に対して一定の指針を与えるが、大枠で変化はない。
	②民間企業側での GA のリスク審査と越境移転制限	• SCC を締結したとしても、移転もとは移転先の GA のリスク等を踏まえて、適切な追加的保護措置を導入する必要がある。	• 改正個人情報保護法も同様のリスク確認を事業者に求めており、本判決の立場を先取りしていたといえる。 • グローバルな GA リスクの議論の土壌はある？
	③内国民待遇	• TEU や GDPR における安全保障の除外は米国政府の行為には適用されない。	• 国内に比べてより高い基準を外国に対して課すことは基本的に正当化できないため、何等かのルールを設けるべきである。
	④越境移転制限に関する透明性や移行期間の設定	• PS は即座に効力を停止され、SCC は追加的保護措置が即時に求められる。	• 予測可能性や移行期間を欠いたままでの越境移転制限は極めて困難となる。 • 貿易の技術的障害に関する協定（以下 TBT 協定）にあるような、事前通告による移行期間の設定等のルール策定が望ましい。
EU のプライバシーに関する対外交渉	⑤欧州委員会の国際交渉における余地の縮減	• DPA はいつでも苦情処理に基づいて欧州委員会の十分性認定を覆せる。	• 十分性だけに頼ることの不安定性が顕在化した。トラストをどのように担保するか、プロセス論にも示唆を与える。

４．１．越境移転制限が許容される個人データへの GA

２．で述べた通り、本判決における個人データへの GA の審査枠組自体はデータ保護指令を踏襲したものであり、この点、EU においてはその審査基準は一貫したものであるといえよう。

実際、EDPB が Schrems および Schrems II 事件やその後の CJEU の事案を踏まえて 2020 年 11 月に公表した監視措置に対する欧州の本質的保護（European Essential Guarantee for surveillance measures; EEG）に関する勧告において、下記の A～D が EEG の構成要素として記載されている [36]；

A. 取り扱いが明確、正確かつアクセス可能であること
（Processing should be based on clear, precise and accessible rules）

B. 正当な目的に対する必要性および比例性が示されること（Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated）

C. 独立した監査機構が存在すること
（An independent oversight mechanism should exist）

D. 個人にとって利用可能な実効的救済が存在すること
（Effective remedies need to be available to the individual）

EDPB は、上記はあくまで個人データに対する監視に関する基準であり、EU 法上の本質的同等性を判断する 1 つの部分集合に過ぎない点を注意喚起している [37]。

上記の A～D が意味するところはおおむね明らかであるが、特に B における必要性と比例性について付言すると、まず比例性とは（権利制限の）干渉度合い（seriousness of interference）と公益上の目的の重要性（importance of public interest objective）が均衡しているか否かで判断される [38]。他方、必要性は、この EDPB の文書からでは一般的な内容としては明らかではないが、客観的な指標に基づいて監視の対象となる個人やデータが十分特定されていること、逆に一般的な指標をもとにバルクでのデータ収集を認めないことを指しているものと考えられる [39]。

筆者はこの EU の基準を参考に、最低限 GA が具備すべき最低限の要素を規定した審査基準として次を想定している。

---

[36] European Data Protection Board, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, adopted 10 November 2020, at https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (as of 30 June 2021), para. 24

[37] *Ibid.*, para. 9

[38] *Ibid.*, para. 33

[39] *Ibid.*, para. 37-8

図表 5　筆者の考える GA の（最低限の）審査基準

審査基準	内容
法的根拠	• GA（民間保有のデータに対する政府機関の強制力を持った開示要求）が明確、正確かつアクセス可能な規則に基づくこと 例）公開された刑事訴訟手続関連の法令
制限	• GA について、正当な目的ととられる措置の関係について、必要性と比例性を実証すること（ここでいう必要性とは措置が目的の達成に貢献しより市民の権利侵害の少ない代替手段が存在しないこと、比例性とは権利侵害と得られる利益の均衡である[40]）。 例）上記代替措置の有無等に関して、令状等に対する事前の司法審査を行なうこと
監督	• GA に対して独立した監督機構が存在すること。 例）GA の実施機関に対して保有するあらゆるデータへのアクセス権限を有する第三者委員会やオンブズマン制度
救済	• 個人が実効的な救済を利用できること 例）行政不服審査、行政訴訟（取消訴訟、国家賠償請求）

先に挙げた拙稿でも指摘した通り、外国における GA リスクへの対処として、リスク所在国への自国からのデータ越境移転制限が考えられるものの、そのような制限は当然にデータ流通を阻害するため、客観的にそれが許される基準を明らかにすべきであると考えられる。

この点、上記の筆者の基準は客観的かつ EU や日本等の合意が得られやすいと思われるため、これを満たさない個人データへの GA を許容する制度が存在する他国に対しては、越境移転制限が許される、等の国際ルールを策定すべきであると思われる。ただし、目的をどこまで明示すべきか、制限をどこまで厳密に規定すべきか等、国家安全保障との関係で十分に詰め切れない可能性も容易に想定され、特に米国の立場を踏まえると、上記の審査基準をどこまで精緻に規定できるか、なお隔たりがある可能性も否定できない。

以上の問題意識に照らして注目すべき動向が、OECD の動きである。OECD デジタル経済データガバナンス・プライバシー作業部会（Working Party on Data Governance and Privacy in the Digital Economy：DGP）においては、日本政府の主導の下、プライバシーガイドラインの改訂作業に合わせて、GA に関する議論も”Trusted Government Access（TGA）”

[40] 筆者の概念する必要性は、先に述べた EU の EEG における理解と異なっている点に注意されたい。

との議題の下活発化している[41]。

DGP は個人データに対する無制限かつ比例的でないガバメントアクセス（unconstrained and disproportionate government access）をデータガバナンスとプライバシー上の重要な課題、信頼ある自由なデータ流通の潜在的障壁（a potential barrier to enabling the free flow of data with trust）と位置づけた。

また DGP は、デジタル経済のグローバルに相互依存的性質にかんがみて、無制限、非合理的または比例的でない政府による強制力を持った民間保有の個人データに関するアクセスは、信頼を損なうものと懸念し、データフローの制限やそれに伴う経済的な影響を与え得るとしている。

DGP は対応として、まずは現状の OECD 諸国の TGA に関するプラクティスを理解し、そこからハイレベルな原則や政策上のガイダンスを探るアプローチをとっている。

ここでは、安全保障と権利保障の調和が目指されており、特に次の事項に関するセーフガードが議論されているが、これらは先に述べた筆者の基準を敷衍したものといえよう[42]。

法的根拠、正当な根拠、必要性や比例性、透明性、事前の許可や制限、取得された個人データの取り扱いに対する制限（秘密性、完全性、利用可能性の制限を含む）、独立した監査、および実効性のある救済措置

上記の目的のため、デジタル経済政策委員会（Committee on Digital Economy Policy; CDEP）は法執行機関や情報機関を含む政府代表や専門家からなる起草委員会を立ち上げることを合意した。起草委員会は 2021 年初頭から活動を開始し、他の OECD の関連委員会と連携をとりつつ、CDEP に対する提言をまとめることとされている。

このような動向は GA の国際的なルール形成に向けた重要な動きであるとともに、特に盛り込むべきルールの内容は筆者がかねて主張してきたものとも軌を一にするものであり、日本政府としても引き続き議論を主導し、積極的な関与を継続すべきものと考える。

---

[41] OECD, *Government Access to Personal Data Held by the Private Sector : Statement by the OECD Committee on Digital Economy Policy*, 22 December 2020, at http://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm (as of 30 June 2021)． なお、当初の日本政府提案では Unlimited Government Access(UGA)であったが、途中でこのようにタイトルが変更された。

[42] 特に Schrems II 判決を受けて EU 側の審査基準等が OECD での TGA の議論に影響を与えた可能性が大きく、筆者の基準も EU の基準をもとにしているためこのような類似が生じていると考えられる。

４．２．民間企業側での GA のリスク審査と越境移転制限

二点目は、EU においても、民間企業に対して、自らの越境データ移転のリスクを認識する重要性を制度の中で義務づける方向に動いてきたことである。今後、SCC の補完措置を検討する中で、民間企業は必然的に移転先国の GA のリスクを評価することとなる。

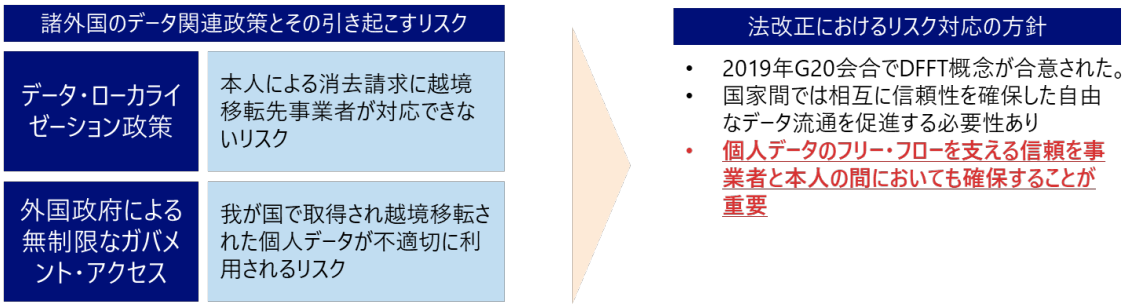
この点で先駆者となっているのが日本であり、特に令和 2 年度に成立した改正個人情報保護法は次の内容を規定している。

（1）越境移転の同意取得に際して、下記の情報提供が義務化（第 24 条第 2 項）
移転先国の個人情報保護制度
移転先組織の個人情報保護措置、等
以上の追加的な情報提供義務については、施行日より適用され、遡及しない（附則第 4 条）

（2）本法上事業者が講ずべき措置に相当する措置（相当措置）に基づく移転の場合には、相当措置に関する情報提供が義務化（第 24 条第 3 項）

このような情報開示の強化は、法案成立時は GDPR 水準を超え国際的に前例がないものであったが、データ・ローカライゼーションや無制限な GA 等、移転先国の政策によって個人データに関する権利が制限されたり、不適切に利用されたりするリスクを本人に明示し、本人の関与を拡大することがこの改正法の立法趣旨である。

図表 6　個人情報保護法改正の背後にある
諸外国のデータ関連政策が引き起こすリスクと対応方針 [43]



したがって、上記の改正法による規律強化に対応する日本企業には、DFFT との関係を意識して、特にローカライゼーションや GA 等に関する情報提供が求められることとなると考えられる。

[43] 個人情報保護委員会「個人情報保護法　いわゆる 3 年ごと見直し　制度改正大綱」（令和元年 12 月 13 日）（https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf, 2021 年 6 月 30 日最終閲覧）より筆者作成。

この点、個人情報保護委員会から、令和２年改正個人情報保護法関係の政令・規則が公布されている。上記（１）越境移転の同意取得時における情報提供については、同意取得時に本人に提供すべき情報として、①移転先の所在国名、②適切かつ合理的な方法で確認された当該国の個人情報保護制度、③移転先が講ずる措置について情報提供を求めることとしている[44]。

また、2021 年 5 月には上記規則を踏まえた個人情報保護法に関するガイドライン案が公表され、パブリックコメントにかけられている[45]。特にガバメントアクセスに関連するところでは、「個人情報保護法ガイドライン（外国にある第三者への提供編）の一部を改正する告示（案)」において、特に②について、「(ア）当該外国における個人情報の保護に関する制度の有無、(イ）当該外国の個人情報の保護に関する制度についての指標となり得る情報の存在、(ウ）OECD プライバシーガイドライン 8 原則に対応する事業者の義務又は本人の権利の不存在、(エ）その他本人の権利利益に重大な影響を及ぼす可能性のある制度の存在」が定められることとされている[46]。

とりわけ、(エ）については、ガイドライン案では下記の２事例が例として挙げられており、まさに先に挙げたデータ・ローカライゼーションと GA が定められているといえる[47]。

【本人の権利利益に重大な影響を及ぼす可能性のある制度に該当する事例】
事例 1) 事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度
事例 2) 事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義務に係る制度

---

44 個人情報保護委員会「令和２年改正個人情報保護法 政令・規則の概要」（令和 3 年 3 月 24 日）（https://www.ppc.go.jp/files/pdf/210324_seirei_kisoku_gaiyou.pdf, 2021 年 6 月 3 日最終閲覧)。

45 個人情報保護委員会「「個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）の一部を改正する告示」等に関する意見募集について」（2021 年 5 月 19 日）（https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=240000069&Mode=0, 2021 年 6 月 30 日最終閲覧)。

46 個人情報保護委員会「個人情報保護法ガイドライン（外国にある第三者への提供編）の一部を改正する告示（案)」（2021 年 5 月 19 日）（https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000219181, 2021 年 6 月 30 日最終閲覧)、56-60 頁。

47 同上、59-60 頁。

なお、現時点の提供すべき情報として、移転先国名、個人情報保護制度等が想定され、後者の個人情報保護制度については、事業者が移転先の環境を認識するために企業独自の取り組みが望まれるが、個人情報保護委員会も参考情報を提供予定である[48]。

以上のように、我が国の改正個人情報保護法における越境移転における透明性強化は世界的に珍しい立法であったが、本判決の議論を先取りしていたといえ、本判決を経て EU も同じ立場に立ったといえる。したがって、OECD での議論を踏まえつつ、EU と協働して GA に関するリスクの国際舞台での啓発や、個別国のリスク特定、無制限な GA の是正等、様々な取り組みを実施していく土壌が整っているといえる。

４．３．内国民待遇

２．で述べた通り、米国からの本件判決への批判は必ずしも的を射たものではないが、仮に越境移転に際して自国/地域内での移転よりも厳しい制限を行うとすれば、それは許容されない、すなわち過度な越境データの移転制限となることに異論はないであろう。この原則は、２．で述べた 1980 年のプライバシーガイドライン以来連綿と続くものであり、国際通商法の内国民待遇に通じるものといえよう。

したがって、このようなルールをデジタル貿易に関連したルールとして取り込むことが考えられる。他方、ルールとしては、仮に外国にのみ高い保護水準を課すとすれば、それはデータの自由移転を定めた条項においても必要でない制限とみなされる可能性が高く[49]、どのようなルールを策定すべきか、既存のルールのカバー範囲を含めてさらなる検討が必要なように思われる。

４．４．越境移転制限に関する透明性や移行期間の設定

４．３．の議論に関連して、将来的な DFFT 構想に関するルール形成という観点では、今回企業実務として非常に困難を抱えた点の 1 つが、判決によって突然に越境移転の実施根拠が失われてしまった点である。

仮にこれに基づいて、各国の DPA から GDPR の制裁金（全世界売上高の 2〜4%）が課されるとすれば、企業にとっては非常に事業上の予測可能性がなく、またリスクが高いものとなってしまう。

この点、例えば強制規格の制定に関する WTO・TBT 協定 2.12 条のように、越境データ

---

[48] 国立国会図書館「第 201 回国会　参議院　内閣委員会　第 13 号　令和 2 年 6 月 4 日」〔其田真理個人情報保護委員会事務局長発言〕（令和 2 年 6 月 4 日）（https://kokkai.ndl.go.jp/simple/detail?minId=120114889X01320200604&spkNum=0#s0, 2021 年 6 月 30 日最終閲覧）。

[49] 例えば CPTPP 第 14.11 条における、越境移転制限が「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るものではない」という要件にもかかるように思われる。

移転スキームの無効化から実際の移転停止等の執行活動の開始までは一定の合理的な期間をとる、といった規定を設けることも一案ではないかと考えられる。

2.12　加盟国は、2.10 に規定する緊急事態の場合を除くほか、輸出加盟国、特に開発途上加盟国の生産者がその産品又は生産方法を輸入加盟国の要件に適合させるための期間を与えるため、強制規格の公表と実施との間に適当な期間を置く。

ここにいう「適当な期間（reasonable interval)」は過去の上級委員会（以下 AB）の判断によると少なくとも 6 カ月と解釈されているため、このような期間を設定することが一案かと思われる。すなわち、米国クローブタバコ事件 AB 判断によれば、ドーハ閣僚会議の「実施に関する決定」のパラグラフ 5.2 によれば、妥当な期間は少なくとも 6 か月だとされている。AB は同事件で、同会議の決定を、ウィーン条約法条約第 31 条 3(a)「条約の解釈又は適用につき当事国の間で後にされた合意」に当たるとした[50]。

ただし、EU としては個人データの保護は基本的人権であって、TBT2.10 条類似の緊急性のある案件に当たると主張する可能性が高いかもしれない。また、そもそも新たに制度が設けられる場合と、すでにある制度（こちらの方が予見可能性は高い）の例外を認めないと決定する場合では、妥当な期間も異なる可能性もある点には留意が必要である。

４．５．EU のプライバシーに関する対外交渉

欧州委員会は、従来から CJEU に条約審査を実施されることで対外交渉に圧力を加えられ、例えば EU・カナダ 包括的貿易協定 （通称 CETA）の投資章等に顕著であるが、EU 法との整合性に腐心してきた。

この流れに連なるものとして、EU が公表している通商・投資協定における越境データ流通とプライバシー保護に関する水平的モデル条項がある[51]。この中で、プライバシーに関して基本的人権と認めるとともに、締約国が適切と認める措置を導入する権利を持つと定められている。

Protection of personal data and privacy 1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

[50] Appellate Body Report, *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, WT/DS406/AB/R , adopted 24 April 2012, paras. 257-268.

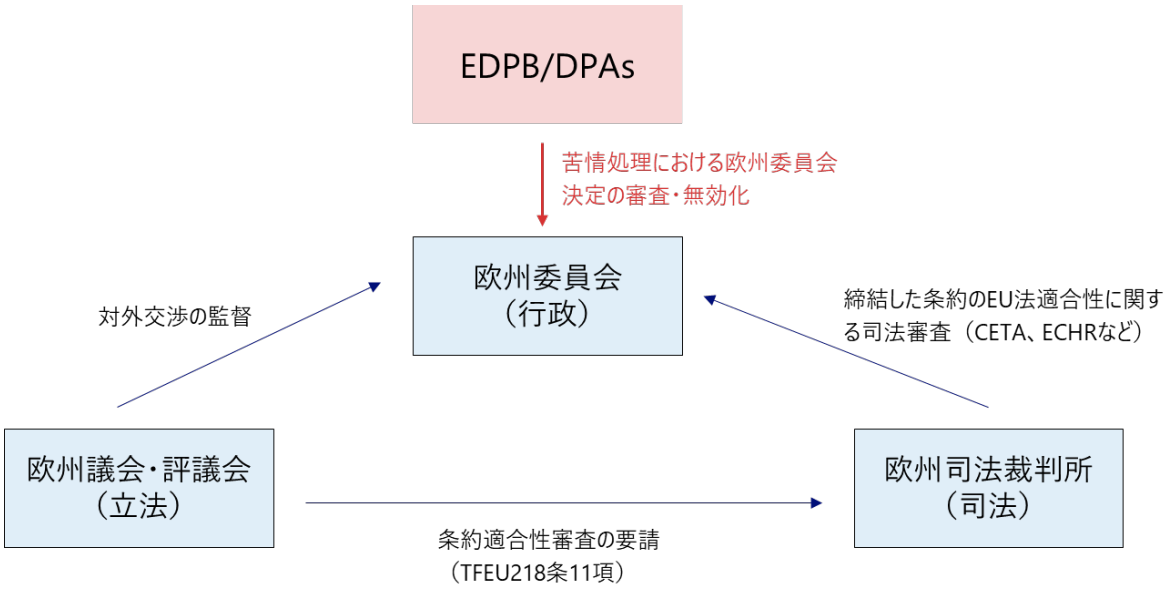
[51] European Commission, *Horizontal provisions for cross-border data flows and for personal data protection*, at https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf (as of 30 June 2021).

2. Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.
（以下略）

この条項は、EU 法上基本的人権として保護されるデータ保護に関して、欧州委員会がまとめる対外交渉による制限を避ける趣旨であると考えられる。このように、欧州委員会は対外交渉の結果が EU 法上の基本権の侵害とならないよう腐心してきたところであるが、今回 DPA が欧州委員会の十分性認定があるとしても、それをいつでも苦情処理の中で覆せることが明らかにされた。

すなわち、新たに DPA による欧州委員会による決定の審査が加わるため、さらに対外交渉の幅を狭められる（よりリスクをとりにくくなる）こととなると思われる。

図表 7　Schrems II 事件判決後欧州委員会が対外交渉で受ける圧力



これは日本政府としての対岸の火事ではなく、今後の OECD や WTO の電子商取引交渉における EU 側の交渉余地がある範囲がさらに狭まり、交渉が難航する可能性があるといえよう。

５．終わりに

以上、本稿では Schrems II 事件判決の概要とともにその評価を論じた。本判決は今後の GA に関する議論を行うリーディングケースであるとともに、日 EU が GA のリスクに関して非常に多くの要素を共有していることを示す判断でもあった。これは、例えば日本が推進する OECD における TGA の議論に、特に本判決の後、従来にも増して EU サイドも積極的に参加していることに表れているように思われる。日本政府は、こうした EU 側の巻き込みをさらに継続していく必要があるだろう。

また、米国の動向も注視していく必要がある。従来、米国では連邦レベルのプライバシー保護に関する立法に消極的であったが、カリフォルニア州等、州法レベルでの法律制定の動きもあり、このままではパッチワーク的な州法が乱立するため、連邦レベルでのプライバシー保護に関する法令の制定に前向きになる可能性もある。この点、いわゆる GAFAM をはじめとする主要な米国企業はすでに GDPR 対応を完了しており、連邦レベルのプライバシー保護法が制定されたとしても、追加の対応コストが限定されるため、立法に必ずしも反対ではない。仮に米国においてそのような立法がなされた場合、日 EU 間の個人データの相互流通をどのように促進していくかという議論が求められることになろう。この点、2021 年 3 月には下院議員の Suzan DelBene 氏が連邦プライバシー法案の素案（名称は Information Transparency and Personal Data Control Act）を提出している [52]。同議員は、本法が GDPR にグローバルなデータ保護に関する規制の主導権を握られないことを目的としていると、その概要説明で述べている [53]。

最後に、日本に目を向けると、本判決は同時に、越境移転におけるリスク確認や追加的な保護措置等、企業実務に負荷を与える内容も多く含まれていた。GA は民間部門の保有するデータへのアクセスであるため、必然的に民間企業にも影響を与えることとなる。

この点、我が国の検討では GA の民間での対抗をめぐっては、移転リスクに関して改正個人情報保護法における透明性の向上が議論されてきたが、今後は日本としても EU の事例も参考にしつつ、暗号化等の GA への対抗手段も検討を加えていく必要があるだろう。

（校了後、本稿の３．２．２．追加的保護措置に関する勧告に関して、パブリックコンサルテーションを踏まえた EDPB 勧告に接した [54]）

---

[52] U.S. Congresswoman Suzan Delbene: Representing Washington's 1st District, "Press Release: Delbene Introduces National Consumer Data Privacy Legislation," (10 March 2021), at https://delbene.house.gov/news/documentsingle.aspx?DocumentID=2740 (as of 30 June 2021).

[53] U.S. Congresswoman Suzan Delbene: Representing Washington's 1st District, "Information Transparency and Personal Data Control Act," (10 March 2021), at https://delbene.house.gov/uploadedfiles/delbene_consumer_data_privacy_bill_fact_sheet.pdf (as of 30 June 2021).

[54] European Data Protection Board, *Recommendations 01/2020 on measures that supplement*

参考資料　Schrems II 事件の諮問事項

(1)　個人情報が民間企業によってEU加盟国から第三国の民間企業に対してSCC Decisionに従った商業目的に基づいて移転され、さらに第三国の当局において国家安全保障、法執行、第三国外交実践の目的で処理されている状況において、(基本権憲章を含む) EU 法は、国家安全保障に関してTEU第4条2項と、公的安全と防衛、国家安全保障に関してDirective 95/46の第3条2項の第1インデントの条項に関わらず適用されるか。

(2)
(a) SCC Decision に基づく EU から第三国へのデータの移転を通じて個人の権利の侵害があるかどうかを判断する際に、国家安全保障の目的でさらに処理される可能性がある場合は、以下はDirective 95/46の目的に関連する比較基準となるか。
(i) 基本権憲章、EU 条約、FEU 条約、Directive 95/46、人権と基本的自由の保護に関する欧州条約、(またはEU法の他の規定)
(ii) 1つ以上の加盟国の国内法
(b) 関連する比較基準が (ii) である場合、1つ以上の加盟国における国家安全保障の状況における慣行も比較基準に含まれるべきか。

(3)　Directive 95/46の第26条の目的に照らして、第三国がその国に移転された個人データに対して EU 法で要求される保護レベルを保証しているかどうかを評価する場合、以下を参照して第三国の保護レベルを評価する必要があるか。
(a) 国内法または国際的義務に起因する第三国で適用される規則、および第三国で遵守される専門的規則とセキュリティ対策を含めるためにそれらの規則の遵守を確実にするように設計された慣行;
(b) 第三国で実施されている行政、規制、コンプライアンスの実践、ポリシーの保護、手順、プロトコル、監視メカニズム、および非司法的救済策と合わせて、(a) で言及されている規則

(4) 米国法に関連して高等法院が認定した事実を踏まえ、個人データがSCC Decisionに基づいてEUから米国に移転されると、これは基本権憲章第7条または第8条に基づく個人の権利を侵害するか。

---

transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, Adopted on 18 June 2021, at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (as of 30 June 2021).

（5）米国法に関して高等法院が認定した事実を踏まえ、個人データが SCC Decision に基づいて EU から米国に転送された場合：
（a）アメリカ合衆国によって提供される保護のレベルは、基本権憲章の第 47 条によって保証された個人のデータプライバシー権の侵害に対する司法的救済に対する個人の権利の本質を尊重しているか。
5（a）の答えが肯定的である場合：(b) 基本権憲章第 52 条の意味の範囲内で比例する米国の国家安全保障の文脈における司法的救済に対する個人の権利に米国法によって課される制限であり、国家安全保障の目的で民主主義社会で必要なものを超えないか。

（6）
（a) Directive 95/46 の第 26 条 4 項に基づく委員会の決定に従って採択された SCC に従って、第三国に移転された個人データに与えられる必要のある保護のレベルは、Decision 95/46 の規定と、特に基本権憲章第 25 条および 26 条に照らしてどのくらいか。
（b）SCC Decision の下で第三国に移転されたデータに与えられた保護レベルが Directive 95/46 および基本権憲章の要件を満たしているかどうかを評価する際に考慮すべき事項は何か。

（7) SCC がデータエクスポーターとデータインポーターの間に適用され、データインポーターに対し、SCC Decision に従って移転された個人情報のさらなる処理のためにそのセキュリティサービスを利用できるよう要求する可能性がある第三国の当局を拘束しないという事実は、Directive 95/46 の第 26 条 2 項で想定されているように、条項が適切なセーフガードを導入することを妨げるか？

（8）第三国のデータエクスポーターがデータ保護機関の観点から、SCC または Directive 95/46 の第 25 条と 26 条かつ/または基本権憲章と矛盾する監視法の対象である場合、データ保護機関は、Directive 95/46 の第 28 条 3 項に基づく執行力を行使してデータフローを一時停止する必要があるか、この権限の行使は SCC Decision の備考 11 に照らして例外的なケースのみに限定されるか、データ保護機関はデータフローを中断しないようにその裁量を使用できるか。

（9）
（a）Directive 95/46 の第 25 条 6 項の目的に照らして、Privacy Shield Decision は、アメリカ合衆国は、国内法または米国が締結した国際的な約束の理由により Directive 95/46 の第 25 条 2 項の意味の範囲内で適切なレベルの保護を保証するという限りにおいて、データ保護当局および加盟国の裁判所に対する拘束力のある一般的な敵用の認定を構成するか。
（b）そうでない場合、Privacy Shield Decision は、SCC Decision に従って米国に移転され

るデータに提供されるセーフガードの適切性に対して行われる評価に関連性があるか、もしあれば、それはどのような関連性か。

（10）米国法に関連する高等法院の認定を踏まえ、米国の既存の制度と合わせて採用した場合、Privacy Shield Decision の附属書 A から附属書 III に基づくプライバシーシールドオンブズパーソンの規定は、基本権憲章第 47 条と互換性のある SCC Decision に基づいて個人データが米国に移転されるデータ主体に救済策を提供するか。

（11）SCC Decision は基本権憲章の第 7 条、8 条、47 条に違反しているか。