RIETI Discussion Paper Series 19-J-067

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―

渡辺 翔太
株式会社野村総合研究所

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 19-J-067
2019 年 12 月

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[1]
―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―

渡辺 翔太（株式会社野村総合研究所）

要　旨

今日、サイバー空間に対す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。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の進める信頼ある自由なデータ流通(DFFT)との関係でも問題を生じ得る。

現状、EU や米国では、GA に対して一定の条件が満たされない限り個人データの国外移転を制限している。こうしたデータの越境移転制限について、GATS 上はデータの移転制限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ほか、CPTPP では制限そのものに規律を及ぼすが、両協定において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ことを明らかにした。

しかし、現状の通商協定の規律にはなお不明確な点が多く残されており、DFFT の推進に当たって GA を理由に移転制限が認められる条件に関して国際的な議論を推進すべきこと、そのために現在国連等で行われている議論を参照しつつ、通商分野を超えた分野横断的な議論が求められることを提言した。

キーワード: ガバメントアクセス、データ自由流通、プライバシー、国際通商法、WTO, GATS
JEL classification: F02, F13, F14, F52, F53

[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 IV 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頂いた。また、望月健太様（メルカリ）及び東京大学現代国際法研究会の同期である吉田咲耶弁護士（西村あさひ法律事務所）には本稿の草稿に対して有益なコメントを頂いた。本稿の執筆に必要な調査の一部や校閲を新谷里美様（東京大学大学院博士課程）にご協力頂いた。ここに記して感謝の意を表したい。ただし本稿にかかる誤りの責任は全て筆者に帰する。

I. 問題の所在

I-1. ガバメントアクセスとは何か

ガバメントアクセス（GA）とは、政府機関等の公的機関による、民間部門が保有する情報への強制力を持ったアクセスを意味する。これは典型的には令状に基づく差し押さえなど、刑事手続きにおける証拠収集等を思い浮かべていただければ想像がつきやすいと思われる。

刑事訴訟手続きを含むことから明らかなように、GA はかねてより一般的に実施されてきた。しかし、インターネットの時代に入ってあらゆる国民のデジタルデータを容易に取得できるようになり、また、テロリストなどが SNS を通じて募集され、インターネットを介して連絡を取り合うなどその国家による諜報活動上の重要性が増している。一方、大量のデータを容易に取得できるようになったため、後に見るスノーデン事件に見られるように、他国民を含めたプライバシー侵害の懸念や、特に国家機密に関わる諜報活動については秘匿性が高く、それゆえ安全保障とは無関係な目的、特に自国産業に有利な情報を GA を通じて取得する、いわゆる産業スパイ的な活動等の GA の濫用の懸念も指摘されている。

結果、外国の濫用的な GA から自国市民の個人情報を保護するといった理由から、当該国に対して自国からのデータ移転を制限するプラクティスが欧米等で生じている。また、わが国においても、個人情報保護委員会（PPC）が 2020 年の個人情報保護法改正に向けた中間整理において、「過度なガバメントアクセスは、個人の権利利益の保護の観点から看過しがたいリスクをもたらし、個人データのフリーフローを支える信頼を損なわせ得る」として、「このようなリスクをもたらし得る個人データの越境移転について、平成 27 年改正法で新たに規定された、外国にある第三者への提供の制限との関係で、どうとらえるべきか検討することが考えられる」と述べている [2]。

他方、こうしたデータの移転制限措置はデータの自由流通を阻害するものであることも事実である。安倍総理大臣は 2019 年 1 月、「信頼ある自由なデータ流通」（Data Free Flow with Trust; DFFT）概念を世界経済フォーラムにて提示した [3]。DFFT は、データが生み出す経済的・社会的な価値を最大限に引き出すには自由なデータ流通が重要であるが、他方で個人情報保護等、データを流通させることに対する信頼がなければ、自由流通そのものが成立しない。そこで、信頼性を担保しつつ、自由なデータ流通を達成するための枠組みが求められ、それを DFFT と命名していると考えられる [4]。

上記ダボス会議における演説の中で、安倍総理大臣は、上記の DFFT に関する交渉を大阪トラックと名づけ、WTO において開始することを宣言している。その後、DFFT は日本で開催された G20 においても言及されることとなり、茨城県つくば市で開催された G20 デジタル・貿易大臣会合 [5]、そして大阪で開催された G20 首脳宣言においても盛り込まれている [6]。先に引用した PPC の 2019 年中間整理が、GA についてフリーフローを支える信頼を損なわせ得る、と言及しているのもこの DFFT 概念に呼応していると考えられよう。

---

[2] 個人情報保護委員会事務局「個人情報保護法　いわゆる３年ごと見直しに係る検討の中間整理」（平成 31 年 4 月 25 日）、54 頁

[3] 外務省「安倍総理大臣による世界経済フォーラム年次総会演説『希望が生み出す経済』の新しい時代に向かって（2019 年 1 月 23 日）」（https://www.mofa.go.jp/mofaj/ecm/ec/page4_004675.html）

[4] DFFT の内実については、例えば G20 のコンセプトムービーを参照；https://g20-digital.go.jp/

[5] 経済産業省「Ｇ２０貿易・デジタル経済大臣会合閣僚声明（仮訳）」（https://www.meti.go.jp/press/2019/06/20190610010/20190610010-2.pdf）、パラグラフ 15-16

[6] 「G20 大阪首脳宣言（仮訳）」（https://www.g20.org/jp/documents/final_g20_osaka_leaders_declaration.html）、パラグラフ 10-12

こうした DFFT の考え方からは、データの越境流通を妨げる措置に対して一定の規律をかけることも重要であり、一般に行われる GA の存在を以って過度なデータの移転制限を行うこともまた避けなければならない。この点、現行の国際通商協定が過度な移転制限に対して何らかの規律をかけ得る可能性が指摘できるとともに、通商協定の規律が、本来的には国家安全保障等に必要とされる GA を理由とした移転制限に対してまでも規律を及ぼし（DFFT の文脈で言えば信頼の確保に必要不可欠な措置の導入をも阻害し）、個人情報保護法等の国内法上求められる GA からの保護義務と、国際通商協定上の義務の間で抵触を生じる可能性もある。

以上の背景の下、GA の関連したデータ移転制限措置が特に近年になって生じてきたことから、本稿では、まず各国における GA 制度を概観し（II）、それを背景とする各国の越境移転制限措置の現状を整理するとともに（III）、国際通商協定による当該措置の規律を検討することで、両者の抵触の可能性の有無、範囲を示し（IV）、今後のデジタル貿易の多国間ルール形成に向けた議論の土台を提供すること（V）を目的とする。

以上を DFFT 概念にひきつけるならば、本稿は DFF を支える“T”とは何か、を GA の文脈において明らかにする試みであるといえよう。越境移転制限を行い得る“T”がある限り、国際交渉において総論としての DFFT に反対する国は多くはないと想定される。しかし、データの越境移転を制限し得る事由となる具体的な“T”の内容をいかに策定するか、これがあまりに狭すぎれば国家に一般に必要とされる裁量が失われることで支持を失い、他方、あまりに広範にこれを認めるとすればデータの国際流通が阻害され、DFFT の本来の目的であるデータの収集と分析、それに基づく新たな価値の創出や社会課題の解決といった、わが国が DFFT 概念の先に見据える Society5.0 を実現できなくなってしまう [7]。

DFFT 概念の実現に向けては、GA に基づく越境移転措置を含め、具体的な各データ関連措置の文脈において、データの移転制限を行う正当な国家の権限と、データの自由流通の確保とのバランスをどのように取っていくかを考察し、その議論を積み重ねていく必要があり、本稿はそうした試みの最初の一歩となることを目指しているのである。

I-2. GA の類型化について

本論に入る前に、GA の体系化をしておくことが本稿の議論を進める上で有益である。というのも、国際通商協定は政策目的に応じて措置が許容される条件が異なるところ、GA からの保護を目的とした移転制限がいかなる政策目的から導入される措置であるかが決まらないと、適用される例外規定を特定できないためである。以下、きわめて試論的、暫定的な分類であるがこれを試みてみたい。

GA の類型は、その目的と開示を求めるデータの種類で分けることが可能であると考えられる。すなわち、EU での議論においては、個人データと非個人データ（個人データ以外のデータ）が明確に区別され [8]、前者は欧州基本権憲章に規定された基本権としての保障が及ぶ一方、後者については域内での自由流通が求められている。ただし個人データの定義には、国間の差異があり、例えば IP アドレスは EU では個人情報と扱われるが、日本では異なっている点に注意が必要である。

次に、GA の目的による区分が想定される。まず、GA の定義上含まれる犯罪捜査については、令

---

[7] Society 5.0 とは、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）を意味する（詳細については、次の内閣府資料を参照; https://www8.cao.go.jp/cstp/society5_0/index.html）。

[8] 例えば、EU の The Regulation on the free flow of non-personal data における、non-personal data の定義を参照されたい。

状主義の下、人権保障上も許容されるとされる場合がほとんどであるため、本稿の以降の議論ではこれが定義上含まれることは認識しつつも、基本的にその検討からは除外する。同様に、行政調査のうち強制力を伴うものについても、その目的は行政上の目的に応じて多様であり、GA の定義に含まれる得ることは認識しつつも、これを除外しておくこととしたい。

次に、国家が行う諜報活動についても、憲法上の人権保障が及ぶ。したがって基本的には令状主義が妥当し、それが一般的な犯罪捜査と異なることはない。しかし、このような令状主義に基づく諜報活動にも大きく分けると 2 つの類型がある。1 つは、刑事捜査における令状と同様、個人や対象となる情報が特定されている場合である。もう 1 つはそのような区分を実施せず、データを一括して収集した後で必要となるデータを抽出する場合である（いわゆるバルクアクセス）。このような区分はもちろん相対的なものであるが、国家実行や学説においてこの区分は一般的なものであり、例えば EU データ保護指令に基づいて設置された第 29 条作業部会（WP29）は個人データに対するバルクアクセスを" the massive and indiscriminate collection of personal data"と述べて、令状主義に基づくデータ収集と区別している [9]。

最後に以上とは異なった、産業政策としての GA、例えば民間企業に関する強制的な情報開示もあり得る。これは、例えば政府が介在しての外国企業に対する自国企業への技術情報の強制移転や、ソースコード開示義務のように、政府機関が直接情報を取得する場合等がある。近年では特に中国を念頭に、このような措置に関する懸念が生じている [10]。このような措置は基本的には非個人データである産業データを念頭に置いているが、その中に個人データが含まれる可能性も否定できない。

もちろん、これらの区分は今日の措置を演繹的に分類したものに過ぎず、これらに尽くされない GA が存在することは否定できないが、当面の議論を進める上での土台としてご理解いただきたい。

図表 1　GA の分類

分類	目的	個人データ	非個人データ
公共の安全 （国家安全保障）	犯罪捜査 （通常の刑事手続）	（本稿の検討外）	
	諜報活動 （バルクデータ）		
	諜報活動 （特定情報）		
産業政策	強制技術移転		

次に、以上の GA の分類に対応して、GA を理由とする越境データ移転制限についても、その政策目的が異なっている。諜報活動については、プライバシー保護の観点から越境移転に制限を課すことが一般的であり、他方、産業政策的な意図に対抗する場合には、営業秘密や知的財産の保護がその政策目的となると推測される。また、両者に共通して、大量の個人情報の移転や一部の情報については、国家安全保障の観点から移転制限を課す場合もあり得る。

---

[9] WP29, "Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data"

[10] JETRO「中国の技術移転関連の法令、政策、慣行を問題視」
（https://www.jetro.go.jp/biz/areareports/2018/576d6a1648358d2c.html）

II. GA をめぐる各国の制度

次に、議論の出発点として、各国のガバメントアクセスに関する現状を整理したい。刑事手続き上の GA については、各国とも憲法やそれに相当する規範（欧州基本権憲章など）において私生活の不可侵や令状主義が規定され、それに基づいて刑事訴訟手続きが定められている。I で述べた通り、ここでは、各国ごとの違いが大きく出る、諜報活動について各国がどのような制度を講じているかを論じていきたい。

本稿における II の位置づけは、未だ横断的に明らかにされているとは言いがたい各国の GA 法制の現状を概観するとともに、I で述べた濫用の危険がどのように引き起こされているか、濫用に対して人権保障等の観点から、各国が制度上どのような担保措置を講じているか（すなわち “T” の内容）を概観することにある。これによって III で概観する、講じられる移転制限が念頭に置く侵害類型が明らかにされることを目指している。

II-1. 米国

II-1-1. 米国における諜報法制

米国における諜報活動を目的とした政府のデータアクセス権限の中核は、対外諜報活動監視法（FISA)によって与えられている。FISA は、諜報機関による通信傍受の違法性を認めた米国内裁判所の判決への対応や、対外諜報の法整備を目的に 1978 年に成立した。

その後、2001 年の同時多発テロをきっかけにして成立した米国愛国者法や 2008 年の FISA 改正によって、諜報活動に関する政府権限の強化が図られることとなったが、これは同時に諜報機関の裁量の拡大をもたらし、法令が規定する第三者による監査等を骨抜きにすることとなった。その結果、おおよそ諜報活動とは無関係な一般市民の私生活や米国が国際交渉等を有利に運ぶための（必ずしも安全保障と関係しない）情報収集等が行われることなった。それが 2013 年のスノーデン事件で明らかになったのである[11]。結果、2015 年には米国自由法によって FISA の改正が行われ、政府機関の諜報活動に対する司法審査が強化された。

他方、後に見る通り、米国のこのような人権保障にもとる GA の存在を問題として、欧州司法裁判所は 2014 年の判決で EU-US セーフハーバー協定を無効とし、その後、2015 年にはセーフハーバー協定を改定した EU-US プライバシーシールドが締結された。

セーフハーバー協定やプライバシーシールドとは何か。EU のデータ保護指令上、EU との同等性を認められない国に対しては個人データの越境移転が禁止されるが、同等性が認められない場合でも、一定の規律を含む二国間協定で不足分を保管することで、その範囲で越境移転を可能とできる。そこで、米国と EU の間でこうした二国間協定を締結することとなったのがセーフハーバー協定とプライバシーシールドであり、商務省がこれを所管し、商務省に対して個別企業内での体制整備を以ってこれら協定に規定される水準を満たすことを届け出た事業者について、十分性が認められることとなっている。

なお、2017 年及び 2018 年にプライバシーシールドのレビューが実施されており、FISA を中心とした法令やその運用に関する EU 当局の監査が実施されている。

---

[11] スノーデン事件については本稿では詳述しないが、例えば次の文献を参照されたい；デイヴィッド・ライアン著、田島泰彦他訳『スノーデン・ショック――民主主義にひそむ監視の脅威』（岩波書店、2016 年）

時期	主なできごと
1978 年	対外諜報活動監視法（FISA)が成立
2001 年	愛国者法による権限強化
2008 年	法改正により米国民に対する権利保護強化と外国人に対する諜報活動の緩和
2013 年	スノーデン事件発生
2014 年	セーフハーバー協定無効判決（ECJ）
2015 年	米国自由法による FISA の改正
	EU-US プライバシーシールド成立
2017 年 11 月	EU-US プライバシーシールド第 1 回レビュー実施
2018 年 10 月	EU-US プライバシーシールド第 2 回レビュー実施

以上が、簡単な法令及びその関連事件の流れである。本稿では、以降、同改正を経た FISA やその関連法令を中心とした、米国における諜報法制の現在の概要を分析することとする。なお、FISA は合衆国法典（USC)第 50 編第 36 章に記載があるため、条文番号はそれによっている。

米国の現在の監視法制は、主に 3 段階から構成されている。第 1 段階は憲法上の令状主義であり、合衆国憲法第 4 修正がこれに当たる。第二段階は法令であり、FISA を中核としつつ、スノーデン事件後に当時のオバマ大統領が発出した大統領令（PPD-28）がこれを補完している。さらに、第三段階として、PPD-28 に基づいて諜報活動を行う政府機関、例えば中央情報局（CIA）や国家安全保障局（NSA）等が内規・ガイドライン等を策定している。

以下、この法制をさらに具体的に見ていくこととする。第一段階である合衆国憲法修正第 4 条は、政府による不当な捜索等に対する合衆国市民の権利保護を定めており、プライバシーの合理的な期待が認められる場合、原則として捜索等は令状を必要とし、令状は、捜索等に関する「相当な理由」に基づき、かつ、捜索等の対象となる場所や物を特定していなければならないとされる。

上記の権利保護のため、FISA では、司法長官及び対外諜報活動監視裁判所（FISC）という 2 段階の審査を経て、諜報機関の電子監視命令発令の申請が FISA 上の要件を充足しているか否かを審査することとしている。法文上、FISC は要件を満たした申請に対し、命令を「発令しなければならない」とされているため、要件を充足している場合、裁判所は当該命令を発する義務を負う。なお、FISA では政府機関による上訴手続きが定められており、FISC の後、FISCR、さらに最高裁という三審制をとっている。

FISA 上の令状取得に求められる要件については、同法第 1805 条が下記を規定している（下線は筆者）[12]；

1. 申請を行う連邦政府職員の身元
2. 可能であれば，電子的監視の対象者の身元

[12] 訳文は、鈴木滋「米国自由法―米国における通信監視活動と人権への配慮―」『外国の立法 267（2016. 3)』34-35 頁を引用している。

3. ①電子的監視の対象者が外国勢力ないし外国勢力のエージェントであると申請者が思料することを正当化するのに依拠した事実または状況、及び、②電子的監視が向けられる各施設や場所が外国勢力ないし外国勢力のエージェントによって使用されている、もしくは使用されようとしていると申請者が思料することを正当化するのに依拠した事実または状況についての説明
4. 提案する最小化手続についての説明
5. 求められる情報の性質と電子的監視の対象者の通信や活動の形態についての説明
6. 一定の連邦政府の職員による、①求められている情報が対外諜報情報であること、②電子的監視の目的が対外諜報情報を収集することに関連があること、③当該情報は合理的に考えて通常の捜査手法では入手できないこと、④その対外諜報情報が第 1801 条(e)項で規定される類型であること、⑤上記③及び④の内容であると証明できる根拠についての説明を含んだ証明
7. 電子的監視を実施するに当たっての方法及び物理的侵入が要されるかの説明
8. 以前の申請と、それらの申請につき取られた行動についての説明
9. 電子的監視が要される期間及びここで説明される情報を収集した際に自動的に電子的監視の承認命令が失効すべきではない場合には、さらに同種の情報が得られると思料することを支える事実についての説明

特に重要となるのが、最小化手続きである。これは第 1801 条(h)項で規定され、合衆国の必要性に反しない形で同意のない合衆国人に関する非公開情報の取得，保管を最小のものとすること、また、対外諜報の重要性を評価するのに必要な場合を除いては、非公開情報が合衆国人を特定することができないようにする手続きなどを指す。当初、外国に所在する外国人には合衆国憲法の保障が及ばないことから、この最小化手続きから外国人が除外されていた。

しかし、後述する 2014 年の大統領令が外国人に対しても等しく最小化手続を行うことを規定するに至り、2015 年に再度 FISA の改正が行われた。この改正によって外国にいる外国人への電子監視についても、米国人への電子監視と同様に、下記の事項を FISC が審査することとされており、内外差別的な状況が解消された（法第 1881a 条(g)項 [13]）。

⑴傍受は合衆国外にいると合理的に思料される個人を対象としており、送信者と受信者が傍受時に、合衆国内にいると判明しているあらゆる通信を意図的に傍受しないように合理的に企図されている手続があり、当該手続は FISC により承認された、承認のために提出された、もしくは提出されることとなっていること
⑵取られる最小化手続は第 1801 条(h)項の最小化手続の定義に採用される最小化手続に合致しており、FISC により承認された、もしくは承認のために提出された、もしくは提出されることとなっていること
⑶禁止事項の遵守及び傍受命令申請手続の遵守のためのガイドラインが採用されていること
⑷当該手続及びガイドラインが第４修正と合致していること
⑸傍受の目的が対外諜報情報を収集することに関係があること
⑹傍受が電子通信サーヴィスプロバイダーから、もしくはその援助により対外諜報情報を収集するものであること

[13] 同上

⑺傍受が冒頭に述べた禁止事項を遵守していることを証明しなければならない

次に、FISA と並んで重要なのが、2014 年、当時のオバマ大統領が策定した大統領令 28 号（Presidential Policy Directive – Signals Intelligence Activities; PPD-28）である[14]。

PPD-28 は、電子的な手段を用いて諜報活動上収集される情報（シギント情報）について第 1 条シギントの収集に関する統制の原則において、次の 4 つの原則を設定した。

第一に、シギント情報の収集は法令、行政命令、布告、または他の大統領令により認可され、憲法、適用可能な法令、行政命令、布告、及び大統領令に従って行われる。

第二に、米国のシギント活動の計画においては、プライバシー及び自由権についての考慮が不可欠である。合衆国は、批判や意見の相違に対して抑圧もしくは負担を与えるため、または民族、人種、性別、性的指向及び宗教に基づいて人に不利益を及ぼす目的でシギントを収集しない。シギントは専ら、国及び省の任務を支援するための外国諜報活動または対敵情報活動という目的がある場合にのみ収集され、その他のいかなる目的でも行われない。

第三に、海外の民間の商業的情報や企業秘密の収集は、合衆国、その協力国及び同盟国の国家安全保障の目的でのみ認可されない。米国企業及び米国の事業部門に商業的な競合優位性を与えるためにそのような情報を収集することは、認可された外国諜報活動または対敵情報活動の目的ではない。

第四に、シギント活動は現実に即して調整されない。シギントの収集を行うかどうかを決定する際、合衆国は、外交上の及び公開の情報源からのものを含む他の情報が利用可能かどうかを検討する。シギントに代わるそのようなふさわしくかつ実現可能な代替手段が優先される。

また、PPD-28 第 4 条は下記の通り、最小化手続きや政府各組織における内規の策定等を義務付けている。

(a) 政策及び手続き：国家情報長官は、司法長官と協力して、下記を確保する。
  i. 最小化（Minimization）
  ii. データセキュリティとアクセス（Data Security and Access）
  iii. データの品質（Data Quality）
  iv. 監督（Oversight）
(b) アップデートと公表：インテリジェンス・コミュニティ[15]の各機関は、1 年以内に、本条を履行するための手続きなどをアップデートする。
(c) プライバシー及び市民の自由に関する政府職員：国家安全保障担当大統領補佐官（APNSA）、行政管理予算局長、大統領科学顧問（科学技術政策局長）は当該職員を指名する。
(d) 国際外交に向けた調整：国務長官が本件に関する外国政府とのコンタクトポイントを指名する。

II-1-2.　米国の諜報以外の GA

米国では、上記の諜報活動以外にも、刑事捜査における特徴的な法令があるため、これを扱うこととしたい。米国が 2018 年に策定した Clarifying Lawful Overseas Use of Data 法（CLOUD 法）は

[14] The White House Office of the Press Secretary, “Presidential Policy Directive -- Signals Intelligence Activities” (https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities)
[15] 国家情報長官（DNI）、中央情報局（CIA）、国家安全保障局（NSA）、連邦捜査局（FBI）、国土安全保障省（DHS）、国防総省（DOD）等の政府諜報機関の集合体を指す。

その名の通り、米国企業が米国外のサーバーに保持している情報について、刑事手続き上米国当局による GA が許容されるか否かを規定したものである。

米国当局が米 IT 大手のマイクロソフト社がアイルランドに所在する自社サーバーに保有する証拠の提出を求めたことから問題となったことを発端として、CLOUD 法が策定された。この事件は最高裁まで判断がつかなかったが、結局立法による解決が図られて CLOUD 法が成立し、最高裁の審理は打ち切られた。

CLOUD 法は GA に関する問題について、①米国企業が海外に所在する情報に対する米国政府のアクセス権、②米国内に保存されている情報に対して外国政府の持つアクセス権、の 2 つを規律するものである。①の側面について、本法ではデータの開示がサーバー所在国などの国内法と抵触する場合について、データの開示を審査する裁判所に対して国際礼譲に基づく考慮を求め、その際の考慮要素について列挙している。

II-2. EU

EU では、越境収集を可能とする EU レベルでのルールが議論されているものの [16]、EU レベルで諜報活動上の GA を規定した法令はなく、各国別の立法措置が講じられている。

II-2-1. フランス [17]

フランスの諜報活動について規定しているのは、国内安全法（Internal Security Code）である。従来、同法は刑事手続きに比べて保護の水準が低く、特に第三者による監査が一部の諜報活動について及ばないという問題があったが、2015 年の法改正によって諜報活動法（Surveillance Law）が導入され、第三者監査のために諜報手段の監督に関する国家委員会（*Commission Nationale de Controle des Techniques de Renseignement*, CNCTR）が設立された。2015 年法の下では、諜報活動は首相の許可がある場合のみ許容され、許可は CNCTR が当該諜報活動が国内安全法の規定に沿っていると意見を出した後でのみ、発出される。テロ活動等が緊急に差し迫っている場合や、国際的な諜報活動については、CNCTR の意見は不要である [18]。ただし、フランス当局が国際的な諜報活動によって得たデータに対しても、CNCTR はアクセス権を有しており、監査は可能となっている。

フランス当局に諜報活動のターゲットとされていると考える個人は、CNCTR に対して救済を求めることができ、当局の活動が国内安全法に従っているか否かを CNCTR が調査できる。ただし、CNCTR は外国の当局から得た情報に対するアクセス権は持たず、これによって監査を回避できるとの批判もなされている。

また、フランス法に特に特徴的な活動形態がメタデータの収集と利用である。フランスのデータ保存政令（Data retention decree）に基づき、通信事業者は 1 年間位置情報やインターネットのログを含む通信記録を保存する義務を負う。また同じく、クラウドサービス事業者や SNS 事業者を含めたホスティング事業者もユーザーの氏名や住所、連絡先やコンテンツをアップロードした際の通信記

---

16 例えば、European Union, ”E-evidence - cross-border access to electronic evidence” (https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internaleurulesproposaloneevidence)

17 フランスの制度については次の文献を参照した； Winston J. Maxwell “Systematic Government Access to Private- Sector Data in France”, in Fred H. Cate and James X. Dempsy (ed.) *Bulk Collection; Systematic Government Access to Private-Sector Data*, (Oxford University Press, 2017)

18 *Ibid.*, pp. 52-53.

録などの各種データを保存する義務を負っている。これらのいわゆるメタデータは国内安全法に基づく GA の対象となっている。

次に、以上の GA について、どのようなセーフガードが施されているか見ていきたい。EU 法上はいわゆる比例性テストに基づいて、GA は政府の政策目的の達成に貢献し、かつより非侵害的な他の代替手段がないことが、過去の欧州司法裁判所等における司法判断で求められているが、先に挙げた GA に関するフランス法上、このような要求はない。しかし、行政訴訟の最高裁判所であるコンセイユ・デタは2016年の判決でフランス法は上記の比例性テストを満たすと示唆する判断を下している。

II-2-2. ドイツ [19]

1990 年以前は、個人情報の収集が基本権を制約するとは認識されず、諜報に明確な法的根拠はなかった。しかし、1983 年の連邦最高裁判決（BverfGE 65, 1）が国勢調査における個人情報の収集も、一般人格権（憲法第 2 条）から導かれる情報自己決定権を侵害すると判示して転機を迎えた。

以降、情報機関による諜報活動は、基本権に対する制約であるため法的根拠に基づかなければならず、情報機関の活動が民主主義国家で受け入れられるために透明性を確保する必要があるとの議論が主流となり、1990 年の MAD 法及び BND 法制定で明文化された。

さらに、国外の外国人に対する傍受（2016 年 BND 法改正）についても、法的根拠が整備された。

以前は、ドイツに対する武力攻撃のおそれがある場合、ドイツにおける国際的なテロ攻撃のおそれがある場合、薬物取引や資金洗浄等の組織犯罪のおそれがある場合等に限られてきたが、G-10 法改正により、情報機関（BND）は反テロ用のデータベースを構築・運用できるようになった。

安全保障上の諜報活動(strategic surveillance)の対象となる行為類型（改正法第 5～第 8 条）を限定しつつ、該当した場合には広範な情報の収集が可能となっている（第 10 条）。

光ファイバーなどへの物理接続、スマートフォンへのマルウェア埋め込みも可能であるが、国外との通信からの情報収集は、監視する通信網の容量の 20% 以下に制限されている。また、経済目的での偵察（経済スパイ）は禁止される（第 5 条）。また、通信偵察（外国での傍受）においては、個人のプライバシー情報は、いかなる場合でも収集が許されない（第 5a 条）。

BND は、収集した情報が目的に即して必要か自己検証し、不要な場合には直ちに消去する。通信偵察には、事前に連邦首相府が具体的に対象・期間等を指定する必要がある。

また、G-10 関連の情報収集活動は、連邦議会に設置された議会監視委員会と傘下の基本法第 10 条審査会が監査する。議会監視委員会は、連邦議会議員 9 名で構成され、年 4 回以上開催される。

II-3. 中国

中国における GA は様々な法律において、民間事業者が政府の治安維持活動に対して協力する義務を課されている点から生じているといえる。以下では、代表的な GA を定めるサイバーセキュリティ法と国家情報活動法を概観するが、中国は省レベルのルールや各政府機関の一般的な監督権限など様々な GA に関する手法を用意しているといわれている。

II-3-1. サイバーセキュリティ法

サイバーセキュリティ法は、義務の対象となる事業者として、ネットワーク運営者、重要インフラ

[19] ドイツの制度については、次の文献を参照した；Paul M. Schwartz, “Systematic Government Access to Private- Sector Data in Germany”, Fred H. Cate and James X. Dempsy, *ibid.*

運営者、ネットワーク製品及びサービス提供者、その他の 4 つを区分している[20]。ネットワーク運営者とはネットワークを用いている事業者を指し、例えば社内 LAN などもこれに該当するといわれる。他方、重要インフラ運営者とは、重要インフラを運営するものであり、重要インフラは主要な物理インフラのほか、国の安全、国民の経済・生活及び公共の利益に重大な危害を及ぼすおそれのある重要な情報インフラを指すとされ（第 31 条）、主要なウェブサイト、SNS 等もこれに該当する可能性が指摘される。

このうち、ネットワーク運営者については、ネットワーク運営ログの 6 ヶ月以上保存（第 21 条）、ネットワーク参加者の本人確認と国と NW 運営者間での本人確認の相互認証の促進（第 24 条）、及び国の監督検査への協力（第 49 条）などが規定されている。さらに、重要インフラ運営者には毎年 1 回以上の NW の安全リスクについて検査・評価の実施、担当機関への報告（第 38 条）があり、これらの規定を利用して GA が実施される可能性がある。また、以上の 2 つにネットワーク製品及びサービス提供者を含めた 3 類型については、提供するネットワーク製品・サービスについて、国の強制標準への適合性確保が求められており、この審査の過程でソースコードの開示等の GA が行われる可能性もある。

また、製造業に属する企業のデータベースまたは産業用制御システムにおいて保管され、または生成され、企業の生産運営状況及び業種の発展状況を反映する産業データは、国家標準「データ越境セキュリティ評価ガイドライン（意見募集稿）」における重要データに該当する可能性が指摘されている[21]。該当した場合にはローカライゼーションが定められており、このようなデータが GA の対象となる可能性も否定できない。

II-3-2. 国家情報活動法[22]

国家情報活動法はその第 14 条で企業に対して必要な支持、援助及び協力の提供を求めることができ、これに対して国家情報活動機構及びその活動要員が法に従って行う情報活動を妨害した場合は、拘留されることとなる（以下、条文を参照）。

第 14 条　国家情報活動機構は、法に従い情報活動を行うに当たり、関係する機関、組織及び国民に対し、必要な支持、援助及び協力の提供を求めることができる。

第 28 条　この法律の規定に違反して、国家情報活動機構及びその活動要員が法に従って行う情報活動を妨害した場合は、国家情報活動機構が関係機関に処分を求め、又は、国家安全機関若しくは公安機関が警告若しくは 15 日以下の拘留に処する。犯罪を構成するときは、法に従い刑事責任を追及する。

そして、これらの条文に規定される「国家活動情報」は、下記の同法第 2 条が規定する通り、いわゆる安全保障のほか、経済社会の持続可能な発展といった広い範囲を含んでいる。

第 2 条　国家情報活動は、総合的国家安全観を堅持し、国の重大な政策決定のために参考となる情報を提供し、国の安全に危害を及ぼすリスクを警戒及び除去するために情報面での支援を提供し、

---

[20] 同法については、JETRO「中国におけるサイバーセキュリティ法規制にかかわる対策マニュアル」（2018 年 2 月）を参照した。

[21] 同上

[22] 訳文について、岡村志嘉子「中国の国家情報法」『外国の立法 274（2017.12）』を参照している。

国の政権、主権、統一と領土保全、社会福祉、経済社会の持続可能な発展及び国のその他の重大利益を守るものとする。

さらに、上記法令においては、取得した情報の取り扱いに関する規律が含まれていない点にも留意する必要があろう。

II-3-3. 特定産業におけるデータの国内保管義務

中国は電気自動車など、自国の戦略的に重要な分野や、より一般的な外資企業と中国企業との合弁事業（Joint Venture）に関して、強制的な技術移転や自国内に特定の情報を保管する義務を定めている。

この点を問題視し、EU は中国の措置が TRIPs 協定や加盟議定書に反するとして、2018 年に中国に対して WTO 紛争手続きにおいて協議要請を行っている[23]。ここで本稿との関係で特に問題となるのが、中国が特定の情報を中国国内に保管するといった措置である。

EU 側のコンサルテーションによれば、中国の新エネルギー自動車規制（The New Energy Vehicle Production Enterprises and Product Admissions Regulations; NEV 規制）において、中国市場へのアクセスを認められるには、特定の製造設備や、製品開発に関する能力、特定のソフトウェアやハードウェア、マニュアル、パフォーマンスデータや技術及び設計上の使用を含めたデータベースを中国国内に設置することが求められている[24]。

なお、上記紛争は、米国、日本、台湾が参加表明をしているが、現在パネル設置などは行われていない。

以上をまとめると、国家情報活動法などに示される通り、中国においては非常に広範な情報について GA が認められているといえる。これは日本などで通常想定される安全保障の範囲を超えて、経済発展に必要な情報、例えば自国の産業政策上必要な技術情報等についても、法文上は排除されないような規定となっている。

そして、中国はサイバーセキュリティ法や、仮に EU の主張が正しい場合、中国製造 2025 のような産業政策上重要な特定産業では、NEV 規制等のより詳細な法令によって、自国内にデータの保管を義務づけているといえる。

これら広範な GA 権限とローカライゼーション義務が組み合わされた場合、中国に情報を移転してしまえば、当該情報に対して実質的にきわめて広範なアクセスを許容し、それら情報が産業上重要なものであった場合、中国の国有企業等に対して政府から再移転が行われる懸念も生じ得るのである。

II-4. 日本

日本においては、憲法上の令状主義に基づき、刑事訴訟法やその関連規則において GA とそれに対する制約が規定されている。

他方、米国や EU のような諜報活動について、後に III で述べる通り、日本政府は EU 側に対する

---

[23] 事件の経緯について；https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds549_e.htm

[24] “China – Certain Measures on the Transfer of Technology Request for Consultations by the European Union”, pp. 7-9.; https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157591.12.20%20-%20REV%20consultation%20request%20FINAL.pdf

返答において、日本の政府機関は諜報活動を実施しておらず関連する法制度は存在しないと返答している。

II-5. ASEAN 諸国：タイのサイバーセキュリティ法

中国のサイバーセキュリティ法策定に伴い、東南アジア諸国、例えばベトナムやタイといった国においても、サイバー空間の安全を確保する法令が制定されつつある。ここでは、タイのサイバーセキュリティ法を取り上げる。

タイのサイバーセキュリティ法は、2019 年 5 月に施行された。同法は、中国法と同様、重要インフラ（国の安全、国民の経済・生活及び公共の利益に重大な危害を及ぼすおそれのある重要な情報インフラ）を規定し、特にこれについて、国家安全保障や通信等の 8 つの分野を定めている。

また、特に注目されるのが、一定以上の危機的なサイバー脅威がある場合には、裁判所の令状を不要としてコンピュータ設備に対するアクセスが認められていることである。ただし、危機的なサイバー脅威に関する明確な定めがなく、その濫用の可能性をインターネット関連の業界団体が指摘している [25]。

II-6. 小括

GA が濫用される危険性については、I で指摘した通りである。各国のプラクティスで明らかになった通り、テロなどを未然に防ぎつつ十全な人権の保障を確保するため、各国で濫用的な GA に歯止めがかかるよう、創意工夫が積み重ねられている。しかし、これらは米国の制度の変遷を見れば分かる通り、国家安全保障上の問題、例えばテロ事件が起こるたびに手続き的な要件が緩和され、緩和された結果当局により濫用されるとまた厳しくなる、というサイクルを繰り返していることも事実である。なお、GA を受けた当事者である企業、特に主要な IT 大手である Google、Apple、Facebook、Microsoft 等においても、透明性レポートと呼ばれる統計を公開しており、どの国から、どのような GA が何件程度寄せられているか、といった情報を公表するようになっている [26]。

また、いわゆる産業スパイ的な濫用についての危険も懸念される。米国の大統領令 PPD-28 において明文で「海外の商業情報や企業秘密の収集は、合衆国、その協力国及び同盟国の国家安全保障の目的では認可されない。米国企業及び米国の事業部門に商業的な競合優位性を与えるためにそのような情報を収集することは、認可された外国諜報活動または対敵情報活動の目的ではない」と規定されているが、これは裏返せばそのような濫用の危険が常にあり得る（又は過去実際にそのような濫用が行われてきた）ことを物語っている。ドイツについても同様である。

他方、各国において、上記の GA の濫用懸念に対する制度的な対応には、大きな差異があることもまた事実である。例えば、米国や EU においては、基本権としての適正手続き（令状の司法審査等）の設定や、それを通じた人権保障が定められており、適正手続きは GA の実施を定める法令においても組み込まれている。他方、中国や ASEAN 諸国においては、そもそも安全保障概念自体が抽象的であり、濫用の危険性に対する十分な歯止めとなり得ない可能性が指摘される。

以上のような濫用の懸念が払拭されない場合には、当該国に対して自国からデータを移転した場

---

[25] “AIC Comment - Thailand Cybersecurity Law” (https://aicasia.org/wp-content/uploads/2019/03/AIC-Statement_Thailand-Cybersecurity-Law_28-Feb-2019.pdf)

[26] Google が透明性レポートを開示している企業を掲載している；
https://transparencyreport.google.com/?hl=ja
また、Google 等からなる次の団体が、GA に関して順守すべき原則を公表している；
https://www.reformgovernmentsurveillance.com/

合、濫用的な GA によって人権侵害や競争阻害的な行為、あるいは安全保障上の脅威となる可能性も否定できない。そこで、各国で GA を理由としたデータの越境移転制限措置が導入されつつあるのである。次の III ではこのような措置の内容について概観したい。

III. GA への懸念を理由としたデータの越境移転制限

II で述べた GA の濫用の危険性に対して、各国ではデータの移転制限が導入されつつある。ここで重要な点は、いかなる目的に基づいて、いかなるデータについて、どの程度の越境移転制限を導入しているか、である。ここからデータの越境移転措置の内容を分析し、IV での国際通商協定との整合性の分析に活用することが、ここでの目的である。

III-1. 米国

米国において、包括的なデータ移転を制限する法律はない。すなわち、米国は日本や EU のような、個人情報保護のために外国への個人データの移転を一律に制限するような法令は有していない。ただし、一部、パッチワーク的にではあるが種々の越境移転制限を課しているため、以下概観したい。

III-1-1. CLOUD 法

まず、II-1-2.で言及した米国 CLOUD 法は、米国企業が国外に持つデータへのアクセスを規定するのみならず、米国に所在するデータに対する海外政府からのアクセスをも規律している [27]。これが、同法がデータの移転制限を規定している点である。

外国政府から米国政府に対して、米国内のデータを提供する要請があった場合、行政協定（Executive Agreement）を当該外国政府と締結することとなる。

この締結には、司法長官が国務長官の賛同を経て、当該政府が下記を満たすことを議会に対して認証することしている。

1. 決定（認証）は信頼できる情報や専門家のインプットに基づく必要がある
2. 決定は下記を考慮要素に入れる
   (ア) 当該政府がサイバー犯罪や電子的な証拠に関する実体・手続規則を有していること、例えばサイバー犯罪条約への加盟など
   (イ) 当該政府が法の支配と無差別の原則を尊重していること
   (ウ) 当該政府が国際的な人権、特に下記を含むそれを尊重していること
      ① 私生活（privacy）への恣意的または不法な干渉からの保護
      ② 公正な裁判を受ける権利
      ③ 表現の自由、集会と平和的な行動の自由
      ④ 恣意的な逮捕や拘留からの保護
      ⑤ 拷問、非人道的または品位を傷つける取り扱いまたは罰則からの保護

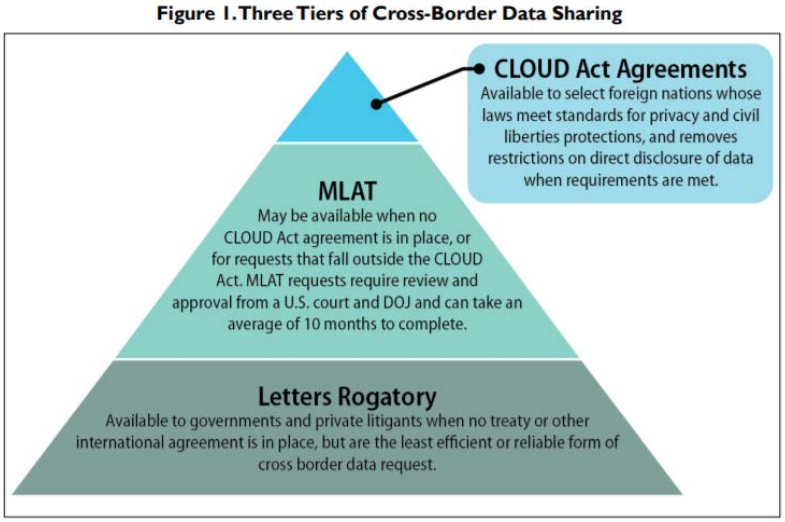
（以下略）

以上の通り、CLOUD 法に基づく米国からのデータの移転については、課される条件が多岐に渡る。ここでは、単なるプライバシー権だけではなく、表現の自由等の一般的な基本的人権保障があることを米国からの情報提供、すなわちデータの越境移転の条件としている。これは、本法が基本的には刑事訴訟における証拠の移転を定めたものであり、それゆえに GA のほか、データの移転に基づく刑事手続上の人権侵害などに対しても保護措置を要求しているものと解される。

[27] なお、連邦通信保存法（SCA）の下、原則として、米国拠点の事業者が外国政府に通信内容を開示することは禁止されていた。

以上の CLOUD 法に基づくデータ移転について、議会調査局の担当者によれば、これはもっとも厳しい条件のもと、直接米国の事業者に外国政府がデータ開示を命じることができる類型となることが予定されているといえる。米国では、従来からも刑事訴訟上の証拠に関する相互共有にかかる協定、日本でいう刑事共助にかかる協定は存在し、英語では Mutual Legal Assistance Treaties (MLATs)や強制力を持たない証人尋問請求書（letters rogatory）と呼ばれるものである [28]。

図表 2　CLOUD 法に基づく行政協定の位置づけ [29]



欧州議会資料によると、CLOUD 法における行政協定の締結権限は加盟国ではなく EU 委員会にあり、米国とは行政協定の締結交渉を進めている [30]。

III-1-2.　対内直接投資審査

第二に、間接的にではあるが、米国における対内直接投資への規制もデータの越境移転制限を課している。米国では、いわゆるエクソン・フロリオ条項に基づいて、米国に対する対内直接投資を、米・対米投資委員会が審査する枠組みを有している。2018 年には、外国投資リスク審査近代化法（FIRRMA）が成立し、米国への投資について審査が強化されている。

本項との関係で特に着目される傾向が、この審査基準として、個人情報の流出や機微情報の流出に関する項目が挙げられている点である。これは、従前の CFIUS の審査に関するプラクティスを明文化したものであり、具体的には以下のような事例があった。

例えば、位置情報やそれを分析する技術に関する事案として、米・HERE に対する中国企業（Tencent など）の出資事案がある。HERE は 2016 年 12 月 27 日、中国向け位置情報サービスの開発に向け、Tencent 及び NavInfo と戦略的パートナーシップを構築し、HERE と NavInfo は折半出資による合弁会社を中国に設立し、中国を含む世界の様々な産業を対象にした地図サービスの展開を図ると公表した。当該合弁会社を通じて HERE は中国向けサービスを拡大し、NavInfo の広範なデータを活用することとなっており、HERE と NavInfo は、自動運転車向けの高度な位置情報サー

---

[28] Stephen P. Mulligan, “Cross-Border Data Sharing Under the CLOUD Act” (Congressional Research Service 7-5700), p. 23

[29] *Ibid.*

[30] https://www.consilium.europa.eu/media/37476/st15252-en18-v2.pdf#page=17

ビスの構築と配備でも協力することとされ、他方、Tencent は HERE の地図サービスや位置情報ツールを、傘下の中国及び世界向けインターネットサービスで採用することとされていた。

また、上記の戦略的提携とは別に、Tencent と NavInfo 及び シンガポールの GIC が HERE 株式の合計 10%を取得することでも合意と発表されていた。しかし、CIFIUS の承認を得られないとして 2017 年 9 月、HERE は出資の受け入れを取りやめると発表した。

また、個人情報の流出を理由として買収の承認が得られなかった事案もある。2018 年 1 月、中国アリババ傘下の金融企業、Ant Financial は 12 億ドルで米・送金サービス大手のマネーグラムに買収を提案するも CIFISU の承認を得られなかった。

以上は投資に関する審査であってデータの越境移転を直接に規律するものではないが、買収後のデータの域外（具体的には両案件とも中国）への移転を懸念したものであり、間接的にはデータの越境移転規制といい得るであろう。GA の存在との関連は必ずしも明らかではないが、米議会・米中経済安全保障検討委員会は中国の強制技術移転と CFIUS 審査や輸出管理が必ずしも結びついていないことを警告しており [31]、今後こうした既存のデータの越境移転規制が外国における GA を理由としてさらに活用されていく可能性も否定できない。

III-2.　EU

EU においては、個人情報保護法制が越境移転制限の中核となるものであり、かつその審査基準も長年の議論の上で確立したものであるから、ここで取り上げたい。

III-2-1.　対米関係：プライバシーシールドのレビュー

III-2-1-1.　第 1 次レビュー（2017 年）

プライバシーシールド（PS）のレビューは、本文は簡易な結論のみを記載し、Staff Working Document において詳細な法令等の分析を行っているため、同文書を分析対象とした。特に、米国における GA については、4.2 において法令(4.2.1)、運用（4.2.2)、独立機関の審査（4.2.3)、個人の救済（4.2.4)、近時の発展（4.2.5）という 5 点を扱っている。これらの分析から、結論としてプライバシーシールドを以って、十分性認定を与える補完ができていると認定している。

[31] Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States", U.S.-China Economic and Security Review Commission Staff Report (https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf), p. 4.

図表 3　PS のレビューにおける評価項目とその内容

評価項目	評価の内容
法令(4.2.1)	法令として、FISA 及びそれに関連する大統領令（PPD-28）を検討
運用（4.2.2）	命令の発出状況の比較（件数の推移）について、米政府機関及び民間事業者の資料などを元に検討
独立機関の審査（4.2.3）	米政府機関内の監察官制度や、政府内に設置される委員会等の政府機関からの独立性、データへのアクセス権限について検討
個人の救済（4.2.4）	ＥＵ市民の不服申立について、裁判所による司法審査と、ＰＳで新設されたオンブズマン制度に基づく救済を検討
近時の発展（4.2.5）	近時の法令に関するアップデートや今後の法令の見直し等の見通しを検討

法令の検討

国家情報長官室（ODNI）が提出した情報、特に FISA 及び PPD-28 に基づいて、国家安全保障を目的としたパーソナルデータの収集及び利用について、審査を実施した。

PPD-28 によって、電子監視は諜報目的で、特定の人物に対して、他の手段がとれない場合にのみ行われること、したがって、バルクアクセスは例外的な状況でのみ起こり得ることが担保されていることなどから、PPD-28 は PS によって移転された EU 市民の個人情報を保護する中核であり、同命令が維持され続けることが重要であるが、ODNI はこの点を現政権下（すなわちトランプ政権下）でも保障した。また、PPD-28 に基づいて個別の諜報機関、例えば NSA や CIA が設定する施行令においても、これらの規定が担保されることとなる。さらに、ODNI はインテリジェンス・コミュニティ内で個人情報保護に係るレポートラインを設置し、PPD-28 に係る情報は全て情報長官に集約されることとなること、また NSA をはじめとする情報機関が職員の訓練を行っている点を強調する。

FISA については、米国自由法によってバルクアクセスへの歯止めがかかっており、第 702 条（USC 第 1881 条）に基づくものしか残されていない。しかし、法令上の要求として特定性、最小化措置等の歯止めがあり、一部公表された NSA の手続き（ターゲット手続き、最小化手続き）においてもこれが規定されている。

また、近年 FISC の審査結果も一部公表され、NSA の法令の不遵守が指摘されており、この点は懸念事項であるが、他方で米国政府自身が NSA の不遵守を FISC に通報している点にも留意する必要がある。

独立機関の審査

米国法上、連邦政府機関に設置される監察官（Inspector-General）に関しては、完全な独立性と当該政府機関の保有する機密情報を含めたあらゆる情報へのアクセスが認められている。監察官制度は 1978 年に連邦監察官法(Inspector General Act)により独立かつ客観的な監督機関として設立

され、各連邦政府機関の中に設置されている[32]。

もっとも、監察官の大統領による罷免、並びに司法長官が公共の安全を理由として情報へのアクセスを停止させることも可能であるが、両方の場合において議会への通知が必要となり、議会によるコントロールが及んでいる。

また、連邦プライバシー・市民自由監視委員会（PCLOB）が行政機関とは独立した監視機関として存在する。同委員会は超党派の 5 名の委員（定足数は 3 名）と事務局をもち、委員は上院の助言と同意に基づいて大統領が任命することとなっている。同委員会は、PPD-28 においても、同命令の履行状況を監視するよう推奨されている。2016 年の政権交代に伴って、現在のところ、1 名のみが残っているが、トランプ大統領は 2017 年に入って委員長を任命した。米司法省の説明によれば、現状でも委員会は委員と事務局を通じて機能している。

個人の救済

EU 市民に対して司法救済に利用可能な法令として、FISA や電子通信プライバシー法に加え、コンピュータ詐欺と濫用に関する法律等も利用可能である。

また、一般法である行政手続法（APA）並びに情報公開法（FOIA）も利用可能である。APA 等に基づく訴訟手続では原告適格の問題があり、実際には外国人が訴訟を行うことに障害がある旨指摘する NGO もあるが、実際の FISA に基づく監視活動に関して政府機関の行為の違法性を認めた判決もあり、これらの法令が機能している。

PS に基づくオンブズマン制度も導入されており、これを利用することで EU 市民はオンブズマンを通じて直接監視の有無を確認することができる。これに合わせて、データ保護指令に基づいて設置された WP29 も動いており、EU 市民の不服申立に関する手続規則を策定して、DPA と米国を結ぶ一元化されたチャネルとして WP29 を位置づけている。WP29 の手続規則によって、EU 市民の申請が具備すべき要件や、回答内容が機密区分されていた場合の手続等が詳細化された。

III-2-1-2. 対米関係：PS 第 2 次レビュー（2018 年）

欧州委員会は 2017 年 10 月の第 1 次レビュー結果公表の約 1 年後、2018 年 12 月には第 2 次レビューの結果を公表し、その認定を維持した。他方、2019 年 1 月には EDPB による評価レポートが公表され、そこでは欧州委員会よりも厳しい認定がなされているが、EDPB には認定権限がないため、ここでは欧州委員会の認定結果を概観したい。

第 2 次レビューでは、前回十分に評価できていなかった、法制度の実際の運用に焦点を当てた分析がなされており、これを民間セクター向け、政府機関向けの双方で実施している。

民間セクターでは、商務省により認証を初めて申請する事業者は認証を得るまでは PS への参加を広告できない規制が導入された。また、商務省による 100 を超えるランダムサンプリングに基づく実地調査、ウェブ上のプライバシーポリシー等の False Claim の監査が実施され、さらに FTC による執行（PS 関連の虚偽表示やケンブリッジアナリティカの調査）についても評価がなされている。

他方、政府機関向けについては、まず、トランプ政権にいてもオバマ政権下の法令（PPD28）が維持されている点を評価した。また、前回欠員となっていた Privacy and Civil Liberties Oversight Board の他の欠員メンバーの任命及び同委員会による PPD-28 の履行状況の監督報告の公開がなされている。

[32] https://www.mhlw.go.jp/shingi/2009/12/dl/s1203-6g.pdf

さらに、現時点でオンブズマンへの要求は無いが、クロアチアの DPA 経由で苦情が寄せられており、現在その調査中である。

以上の評価を元に、欧州委員会は第 2 次レビューにおいても十分性認定を維持している。他方、下記の 6 点を今後の改善に向け米国に対して提案している；

1. PS の特に実体的な原則について、商務省が認証を実施した後も、プロアクティブに監査を行う仕組みの構築
2. 商務省が第 1 次レビュー以来設定してきた虚偽表示に関する規制、特に一度も認証への申請を行っていない事業者へのそれについて、実効性を強化
3. FTC が PS の実体的な違反を調査するため、職権で召喚状（subpoenas）などを用いて行う調査を強化
4. HR データ等の更なるガイダンスが必要な情報に関して、商務省、FTC、EU の DPA が共同で追加的なガイダンスを発展
5. 恒久的（permanent）なオンブズマンの設置
6. オンブズマンによる実効的な苦情の取り扱いと解決

III-2-2.　対カナダ関係：PNR に関する欧州司法裁判所判決 [33]

テロ活動の防止等の安全保障を目的として、外国から自国を到着地とする航空便の乗客に関する情報を提示させることが国境管理活動の一環として実施されている。このような乗客に関する情報は PNR と呼ばれているが、カナダと EU が締結しようとした PNR のカナダへの移転及び処理に関する協定案が、欧州司法裁判所（ECJ）でその EU 法との適合性が審理された。ここで統治権の論点を除いて、協定案の実体面が審理されたのは同協定案と欧州基本権憲章第 7 条及び第 8 条の整合性である。2 つの条文は、下記の通りプライバシー権及びデータ保護に関する権利を規定している。

欧州基本権憲章 [34]（筆者訳 [35]）

第 7 条　私生活及び家族生活の尊重

全ての人は指摘並びに家族の、生活、住居及び通信を尊重される権利を持つ。

第 8 条　個人データの保護

1. 全ての人は、自らに関する個人データを保護される権利を持つ。
2. 個人データは、関係する人の同意に基づいて、もしくは法の定める正当な理由に基づいて、特定された目的のために公正に処理されなくてはならない。全ての人は自らに関する収集された情報を入手する権利を持ち、当該情報を修正させる権利を持つ。
3. 以上の規則の遵守は、独立機関による統制に服するものとする。

[33] 中西優美子「EU とカナダ間の乗客名簿（PNR データ）の移転および処理に関する協定案についての裁判所意見 1/15」、『国際商事法務』（2019 年 8 月）、1158-1165 頁を参照した。

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

[35] 次の資料を参考にした；衆議院憲法調査会事務局「欧州憲法条約　解説および翻訳」（http://www.shugiin.go.jp/internet/itdb_kenpou.nsf/html/kenpou/chosa/shukenshi056.pdf/$File/shukenshi056.pdf）

本調査との関係では、本件は外国における GA を理由とした越境移転の制限となり、その点で EU の GA を理由とした移転制限に関する審査基準を提供するものであるといえよう。他方、適用法規がデータ保護指令や GDPR ではなく、基本権憲章となっている点には留意が必要である。

裁判所はまず、本件協定案に基づくカナダへの PNR データの移転及びカナダ政府による取扱いに対しても、基本権憲章の条文が適用され得るとし[36]、個人データの保護に対する逸脱や制限は必要最小限にとどまらなければならないとする[37]。

次に、処理の根拠を基本権憲章第 8 条の「その他の法令」と認める一方で[38]、移転される情報が「頻繁な航空旅客及び特典情報」や「すべての利用可能な連絡先情報」など、十分特定されているとはいいがたい旨を指摘する[39]。また、機微データが含まれることや、危険な対象者の特定がアルゴリズムに基づいて自動的に実施されるがそれは誤判定を排除しないこと、さらに目的にも「その他」といった不明確なものが残されている点を指摘する。さらに、移転後にカナダ政府機関が PNR データを厳格に必要な範囲で保持・利用するよう規定していない点を問題視する。

さらに、個人データに対する個人の権利として、通知、アクセス権や訂正権などが確保されていない。

以上指摘した点を修正しない限り、同協定案は基本権憲章に合致しないと判断した。

III-2-3. 対日：十分性認定における審査[40]

EU は、公的機関による公益目的でのパーソナルデータの収集と利用を Government Access として定義し、特に刑事捜査と諜報活動の 2 つが問題になるとして、一般的な法的枠組みの検討に入る。まず、EU は一般的な法体系を確認し、憲法第 13 条を元にプライバシー権、特に第三者に対してみだりに個人情報を開示されない憲法上の権利保障や同第 35 条の令状主義の存在を指摘した。

それぞれ、最高裁の住基ネット判決（2008 年）や GPS 捜査判決（2017 年）に言及している。次いで、刑事訴訟法上の強制処分法定主義に言及し、憲法第 21 条 2 項及び電気通信事業法における通信の秘密の保護に言及する。

個人の権利保障について、裁判所へのアクセス（憲法第 32 条）、国家賠償（同第 17 条）に言及する。さらに、個人情報保護法第 3 条は、総則として政府機関に対しても個人の人格権保護のため個人情報の適正な取り扱いを定めている。ただし、公的機関の取り扱いは行政機関の保有する個人情報の保護に関する法律で規律され、義務の履行に必要な範囲での個人情報の利用や利用目的の制限等が規定されている。

以上の一般的な法体系を元に、①刑事捜査と②諜報活動という 2 つの場面について審査を行った。

---

[36] European Court of Justice, Opinion 1/15 of The Court (Grand Chamber), 26 July 2017, para. 134.
[37] *Ibid.*, paras. 140-141.
[38] *Ibid.*, paras. 142-147.
[39] *Ibid.*, paras. 155-163.
[40] European Commission, “Commission Implementing Decision (EU) 2019/419 of 23 January 2019, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information”(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC), paras 120-170.

（1）刑事捜査

①法的根拠と適用される制限/セーフガード（Legal basis and applicable limitations/safeguards）

憲法上の令状主義とそれを受けた刑事訴訟法上の強制処分法定主義に言及。特に、第 197 条が捜査に「必要な限り」で取調べを行える点を注目し、最高裁判例に従えば犯罪の重大性や証拠の価値といった一定の客観的な考慮要素を挙げている点を指摘している。

通信の傍受についても通信傍受法第 3 条に基づく令状主義があり、これは同法第 5 条に基づいて期間制限やその他の追加の制限が課される。

他方、行政機関は任意の情報提供を要請することができるが（例えば刑訴法第 197 条 2 項など）、捜査活動を担う警察の活動は、厳格に前項の責務の範囲に限られるべきものであることが警察法第 2 条で規定されている。最高裁判例によれば、捜査は比例性を満たすように実施されなくてはならない。また、捜査に協力する民間企業などについても、個人情報保護法に基づいて第三者提供が制限されている。

以上の過程を経て収集された個人情報は、行政機関の保有する個人情報の保護に関する法律に基づいて保存期間など一定の規律に服する。

②独立の監査（Independent Oversight）

刑事捜査を担う警察に対しては様々な独立の監査がある。まず、強制捜査については令状に対する事前の司法審査がなされる。また、任意捜査に対しては、企業等は不利益なくそれに協力しないことができ、また、警察職員は検察官と協働するため検察の監査も期待できる。

第二に、国会は憲法上の国政調査権を行使することで行政機関を監督することができる。さらに、警察組織は各都道府県の公安委員会の監査を受けることとなる。

以上に加え、警察庁長官は行政機関の保有する個人情報の保護に関する法律に基づいて総務大臣の監督を受けることとなる。具体的には総務大臣は情報提供を要請することができ、またこれは各県にある総務省の出先機関によって市民からの苦情を処理することで機能を補強できる。

③個人の救済（Individual redress）

各行政機関は、行政機関の保有する個人情報の保護に関する法律に基づいて、自らの個人情報の処理について苦情の処理等を行う義務がある（第 49 条）。さらに、警察法第 79 条に基づいて各県の公安委員会に対して苦情を申し立てることができる。これは警察庁通達などによって補強されている。

外国で外国語で救済を申し立てることの難しさに対応するため、PPC が独自に設定する仕組みがこれらを補完する。EU 市民は DPA を経由して PPC に対して苦情を申し立てることができ、PPC はその後、監督機関を含む各公的機関と連絡を取り、当該公的機関は PPC への情報提供を含む協力義務を負うこととなる（これは個人情報保護法第 80 条に基づく）。

以上に加え、司法審査を求めることができる。まず、令状の発出などについては刑事訴訟法が、また、一般的な国家賠償等については行政救済法が、それぞれ規定している。

（2）諜報活動

①法的根拠と適用される制限/セーフガード（Legal basis and applicable limitations/safeguards）

そもそも日本には刑事捜査以外の方法で行政機関が情報提供を求める法令は無い。したがって、公開情報または任意の提供のみに基づいて国家安全保障上の情報収集が行われている。

防衛省は防衛省の設置法に基づいて情報収集を実施しているが、任意の協力に基づくもののみを実

施している。
警察についても同様であり、警察法上の治安維持などの任務に基づいて任意で情報収集を行っている。
公安調査庁については、無差別大量殺人行為を行った団体の規制に関する法律や破壊活動防止法などに基づいて、公安審査委員会の決定に基づいて情報収集を行うが、これらも任意の捜査に基づいている。
以上の任意捜査については、最高裁判例における任意捜査に求められる必要性及び比例性の原則を遵守することが求められる。収集された個人情報は、行政機関の保有する個人情報の保護に関する法律に基づいて管理される。

先に述べた通り、国会には国政調査権に基づく一般的な監査権限がある。さらに、各行政機関内での独立した監査機構があり、防衛省では防衛大臣直轄の防衛監察本部があり、防衛省内の情報へのアクセス権限を有している。同本部は定期的及び特定の問題に対処する監察を行い、報告書を大臣に提出する。大臣はそれを元に改善を行うこととなる。
また、警察の独立監査については前述の通りであり、公安調査庁については、公安審査委員会の事前審査が行われる。
以上の独立監査と、PPC による補完が政府機関による権限の濫用を防止していると認定できる。

行政機関の保有する個人情報の保護に関する法律に基づいて、刑事捜査とは異なり、安全保障上の問題とならないなどの条件が満たされれば、個人は行政機関に対して開示、訂正、消去などを求めることができ、これが認められない場合には、さらに行政不服審査法に基づく審査請求を求めることができ、内閣総理大臣が国会の同意に基づいて任命する情報公開・個人情報保護審査会がこれを実施する。
さらに、上記で救済されない場合、個人は行政訴訟法に基づく行政訴訟が提起できる。損害が生じた場合には、国家賠償請求も利用できる。先に述べた PPC の救済メカニズムも利用できる。

III-3. 日本
日本においては、個人情報保護法がその第 24 条で個人データの域外移転に対して一定の制約を課している。すなわち、同条は国外にある第三者に対して個人データを移転する場合には、同意、十分性認定、又は組織単位での同等な保護措置の構築を義務づけ、これらいずれかが満たされない場合には越境移転を禁止している。このような越境移転と GA の関係について、EU に対する同条に基づく十分性認定を行うに際して、同法を所管する個人情報保護委員会は EU における GA を審査している。すなわち、同委員会は十分性認定における報告書において、「日本から EU 域内の事業者へ移転された個人データは、法執行（犯罪捜査等）及び国家安全保障の目的で、EU の当局が取得する（いわゆるガバメントアクセス）可能性があるが、犯罪予防目的での情報収集が認められるなど、範囲は我が国よりも広くなっている。したがって、捜査等に関する制度について確認を行った結果、EU 各国は、EU 警察指令に基づき措置した国内法に従い、適切に個人データが取り扱われることが確認された」と述べている [41]。具体的には、同委員会事務局は EU・WP29/EDPB の策定した文書 [42]に依拠

[41] 個人情報保護委員会事務局「個人情報の保護に関する法律第 24 条に基づく EU の指定に関する報告書」（平成 31 年 1 月 18 日）、8 頁
[42] Working Document 01/2016 on the justification of interferences with the fundamental rights

して、データ処理が、①明確、正確かつアクセス可能な規則に基づくこと（法的根拠）、②追求する正当な目的についての必要性と比例性を実証すること（制限）、③独立した監督機構が存在すること（監督）、④個人が効果的な救済を利用できること（救済）、の 4 要件から EU 警察指令を評価しこれらを満たすとした [43]。

また、同委員会は「過度なガバメントアクセスは、個人の権利利益の保護の観点から看過しがたいリスクをもたらし、個人データのフリーフローを支える信頼を損なわせ得る」として、「このようなリスクをもたらし得る個人データの越境移転について、平成 27 年改正法で新たに規定された、外国にある第三者への提供の制限との関係で、どうとらえるべきか検討することが考えられる。しかし、グローバルなデータフリーフローは、デジタルエコノミー時代のイノベーションの前提でもあることから、リスクを精査し、事業者等の実態をよく踏まえた上で、どのような措置が考えられるか見極める必要がある」と述べている [44]。

また、個人データ以外についても、外為法に基づく情報の移転制限や、投資審査を課している。これは必ずしも GA への懸念を念頭に置いたものではないが、米国同様、今後 GA の存在を理由としてこれらの既存の制度を活用していく方策も考えられる。実際、米国 FIRRMA の改正にあわせて、2019 年 5 月には、日本でもサイバーセキュリティの重要性が高まっていることを踏まえ、安全保障上重要な技術の流出を防ぐため等の目的から外為法が改正されている。ここでは、事前届出対象業種にソフトウェア関連や情報通信関連サービス業等の追加が行われている [45]。

III-4. 小括

各国の越境移転制限を分析すると、GA を理由としたデータの越境移転制限について、冒頭述べたいくつかの政策目的が存在していることが明らかになっている。例えば米国 CLOUD 法や、EU のデータ保護指令に基づく十分性認定などにおいては、個人情報の保護を追求したものであると評価できる。他方、米国や日本の近時の投資審査の強化については、必ずしも個人情報の保護を目的としたものではなく、むしろ米国のスタッフレポートにおいて CFIUS と強制技術移転の結びつきが弱いと指摘されている通り、強制技術移転を見越した防衛という面もあり得るように思われる。このように、必ずしも明示的に GA に言及したものではないものの、潜在的に GA を理由とした越境移転規制となり得る措置も生じてきていることが明らかとなっている。

さらに、措置の内容についても 2 つの類型、具体的には通商と投資に似た側面があることが指摘できる。前者はデータの流通を直接的に制限するものであり、EU のデータ保護指令や日本の個人情報保護法が該当する。他方、米国の CFIUS や日本の外為法については、投資後の投資元国へのデータの移転を見越してこれを未然に防ぐ措置ともみなし得るものである。

---

to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)

[43]個人情報保護委員会事務局「ガバメント・アクセスに係る『本質的保証』及び EU 警察指令における規定の例」（https://www.ppc.go.jp/files/pdf/310118_siryou1-1_betten5.pdf）

[44] 個人情報保護委員会事務局「個人情報保護法　いわゆる 3 年ごと見直しに係る検討の中間整理」（平成 31 年 4 月 25 日）、54 頁

[45] 経済産業省「対内直接投資等に係る事前届出対象業種の追加等を行います」（https://www.meti.go.jp/press/2019/05/20190527002/20190527002.html）

IV. GA を理由とした移転制限に対する国際通商協定の規律

II では GA の実体、III では GA を射程に含み得る越境移転制限措置の存在が明らかとなった。ここでは、GA の危険を理由として越境移転制限を行う場合、国際通商協定によって課される国家の義務、例えばサービスの自由化との関係で抵触を生じないのか、という分析を行う。この点、最も関連する国際通商協定は、WTO 諸協定のうちのサービスの貿易に関する一般協定（GATS）である。

また、CPTPP 協定は GATS の規律をさらに進めたものであり、電子商取引章においてデータの越境移転制限に対する規律を課している。また、TPP のデータの越境移転制限に対する規律を主導したといわれる米国は TPP 協定には加盟しなかったが、そのあと NAFTA を改良した USMCA においてデジタル省を新たに設け、そこでも CPTPP に類似する条項を規定している。

他方、EU は TPP や USMCA とは異なった条文案を提示しつつ、これを既に他国との FTA 交渉に組み入れつつある。

IV-1. 越境データ移転制限に関する GATS の規律

GATS が課すデータの移転制限に対する規律を分析した論考には枚挙に暇がなく、特に近年国際通商法の学術誌に対する投稿も増加を続けており、このテーマの関心の高さを示している[46]。とりわけそこに含まれる大半の分析は、個人情報保護に基づく越境移転制限と GATS の整合性をめぐるものであるが[47]、GA を正面から扱った研究は管見の限り見られない。ただし、国際通商協定に関する既存研究の蓄積は GA の分析においてもなお有用であり、本稿はこれら既存研究をレビューしつつ検討を進めたい。

まず、GATS の規範構造を明らかにすることから分析を始めると、大枠では、加盟国が負う GATS 上の実体義務、そして当該義務の違反に対する正当化、という 2 段階の構造で分析を行うことが適切であろう。ただし、実体義務について、GATS は GATT と異なりサービス区分に基づく複雑な義務の規定を持っている点に留意する必要がある。

IV-1-1. GATS 上の実体義務

最恵国待遇について、GATS はその第 II 条において関税及び貿易に関する一般協定（GATT）と同様に無条件でこの義務を課している。他方、内国民待遇（第 XVII 条）や市場アクセス（第 XVI 条）については、GATT とは異なり無条件で与えられるものではなく、締約国が約束表に記載したサービ

---

[46] 例えば 2018 年末～2019 年だけでも、次のような論考が発表されている（抜粋）; Neha Mishra, "Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?" *World Trade Review (2019)*; Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures", *World Trade Review* (First View); Susan Ariel Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?", *World Trade Review* (First View); Aaditya Mattoo and Joshua P Meltzer, "International Data Flows and Privacy: The Conflict and Its Resolution" *Journal of International Economic Law,* Vol. 21 (4) (December 2018); Andrew D Mitchell and Neha Mishra, "Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute", *Journal of International Economic Law* (Advanced Article).

[47] 上記のほか例えば、拙稿「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第 26 号』（2017 年）。その他、國見真理子「EU 個人データ保護指令/規則と WTO 協定との関係を中心とした個人情報保護制度に関する一考察」『InfoCom review (63)』（2014 年 7 月）（https://researchmap.jp/?action=cv_download_main&upload_id=214129）、同「国際経済法の観点からみた EU データ保護指令に関する検討」『消費者庁個人情報保護制度における国際的水準に関する検討委員会報告書』（2012 年）

スのみがその対象となる。なお、GATS はサービスの提供形態を 4 つに区分（モード）しており、約束はモード別になされている [48]。

外国における GA の存在を理由として当該国に対するデータの越境移転制限が、サービスについての市場アクセス又は内国民待遇違反を主張することが一般的であると考えられる。これは、データの越境移転制限（すなわちデータを国外の事業者に移転できない点）が自国事業者と外国事業者を差別的に扱っている点で内国民待遇に違反し、また、仮に全くデータの越境移転を認めない（例えば個人情報の国内保管義務がある場合）とすれば、それは越境的なサービス供給の禁止、すなわちサービスのゼロ割当てとなって、市場アクセスの制限に該当する可能性がある [49]。

GATS 違反を主張する申立国はまず、当該サービスの当該モード（越境移転の場合は基本的に越境的なサービス供給であるモード 1 になると考えられるが、国内拠点を設置してサービス提供を行うモード 3 も含み得る）について、これら義務の引き受けを約束表で約束していることを立証する必要がある。

しかし特に WTO 成立以降に生じたようなインターネット関連のサービスについて、過去の事案では約束表に含まれるか否かが問題となってきており、例えば約束表上の音楽配信サービスはインターネット経由のそれを含むのか、といった点が議論されている [50]。

また、そもそもサービスがどの区分に入るのかも定かではない。例えば、EU ではインターネット上でドライバーとユーザーをマッチングさせる Uber の提供するサービスが、運輸サービスに分類されるか、インターネット上のマッチングサービスとなるかが争われていた（両者は GATS 約束表上のサービス分類上も異なるものである）。欧州司法裁判所は Uber の提供するサービスを運輸サービスに区分すると結論づけている [51]。しかし、訴訟にまで発展したことから明らかなように、シェアリングエコノミーのようなサービスを従来の産業区分と見るかまとめてインターネット関連のサービスと見るかについては争いがあり、国によってこの判断が異なるとすれば、GATS 上の約束表の区分を決めることが非常に困難となるだろう。

このような約束表の解釈を経て、データの越境移転制限が当該サービスの供給の障害となり、当該障害が GATS 上の実体義務に対する違反となっていると認められた場合には、GATS 第 XIV 条における一般的例外、又は安全保障例外が援用されることとなる。

---

48 小寺彰「電気通信サービスに関する GATS の構造－米国・メキシコ電気通信紛争・WTO 小委員会報告のインパクトと問題点－」（RIETI Discussion Paper Series 05-J-001）、2-3 頁参照

49 Report of the Appellate Body, “United States – Measure Affecting the Cross-Border Supply of Gambling and Betting Services” (DS285), paras. 236-237. ただし、サーバーの国内設置とサービスの供給禁止の関係については異論もあり得るかもしれない。すなわち、サーバーを国内設置すれば当該サービスを提供しうる点で、なお市場アクセスへの制限と認められない余地もあるが、特にクラウドサービス等を念頭に置くと、サーバーの設置場所の指定は当該サービス提供への重大な制限となり得る。この点は、GATS 第 I 条の「サービス」の定義とも関係するところであるが、更なる分析が必要とされる。

50 Report of the Appellate Body “China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products” (DS363). 同事件については川島富士雄「中国－出版物等の貿易権及び流通サービスに関する措置(WT/DS363/R, WT/DS363/AB/R)―非 GATT 規定違反の GATT20 条正当化の可否を中心に―」（RIETI Policy Discussion Paper Series 11-P-013）を参照。

51 European Court of Justice, “The service provided by Uber connecting individuals with non-professional drivers is covered by services in the field of transport” (https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-12/cp170136en.pdf)

IV-1-2.　正当化事由

本稿ではI～IIIで取り上げた措置を踏まえて、①個人情報保護、②国家安全保障、③知的財産の保護、という3つの政策目的に対する越境移転制限のGATS整合性を検討したい。

IV-1-2-1.　個人情報保護

GAに基づく越境移転措置がGATS上の正当化を認められるか否かは、具体的な措置の内容次第ではある。一例として、先にIIIで検討したEUの個人情報保護を目的とした越境移転制限について検討してみたい。データ保護指令に基づき、EUは米国において濫用的なGAが存在することを理由として十分性を認めず、データの移転を制限した。これによって様々なサービスが影響を受けるであろう。ここでは、あるサービスのモード1（越境サービス提供）をEUがGATS上の約束表で約束しており、その内国民待遇違反が認定されたと仮定して検討を進める。

個人情報保護を目的とした移転制限については、GATS第XIV条において、明確に例外事由として認められている。すなわち、同条は「この協定のいかなる規定も、加盟国が次のいずれかの措置を採用すること又は実施することを妨げるものと解してはならない」として「この協定の規定に反しない法令の遵守を確保するために必要な措置」であって、「同様の条件の下にある国の間において恣意的若しくは不当な差別の手段となるような態様で又はサービスの貿易に対する偽装した制限となるような態様で適用しないことを条件」とする。そして、この「この協定の規定に反しない法令の遵守を確保するために必要な措置」の1つとして「個人の情報を処理し及び公表することに関連する私生活の保護又は個人の記録及び勘定の秘密の保護」がこれに含まれることを規定する（同条(c)(ii)）。

この条文から明らかなように、(i)個人情報保護という目的、(ii)（当該目的の達成に）必要であること、(iii)柱書への非該当、という3つの要件を充足する必要がある[52]。

EU措置が(i)を満たすことは明らかであり、これは1970年代以来のEU各国におけるデータ保護法の立法、1995年のデータ保護指令そして2016年のGDPRという一連の立法経緯から裏付けられるであろう[53]。

次に(ii)の検討に移る。これはGATT/GATSに共通する、いわゆる必要性テストの検討であるが[54]、この審査基準は過去のGATT第XX条における必要性の分析によって明らかにされている。そこでは、必要性の判断は、様々な要素を比較考慮して決せられるプロセス（比較衡量プロセス）であるとされ、具体的には、①当該措置の政策目的の重要性、 ②当該措置の貿易制限的効果、③政策目的実現への当該措置の寄与度、の三要素を総合考慮して行われる。

そして、暫定的な必要性が認定された場合に、申立国から「争われている措置と同等以上の寄与度を達成する、より貿易制限的でない代替措置」が提案された場合には、当該措置と代替措置の比較検討が行われ、暫定的に認定された必要性を再検証することになる。ここで申立国がかかる代替措置の存在を立証できなかった場合には必要性が確定し、争われている措置と同等以上の寄与度を達成する、より貿易制限的でない代替措置の存在が立証できた場合には必要性が否定される。なお、当該代替措置は、コストや技術的な観点から合理的に利用可能でなければならない[55]。

初めに、政策目的の重要性については、個人情報保護という目的自体の重要性はGATS上明文で規定され、また、国際連合で策定された市民的及び政治的権利に関する国際規約（International

---

52 経済産業省『不公正貿易報告書』（2019年版）、187頁

53 この経緯については、拙稿(前掲)を参照

54 必要性テストについては、内記香子『WTO法と国内規制措置』の第3章などを参照。

55 経済産業省『不公正貿易報告書』（2019年版）、191-192頁

Covenant on Civil and Political Rights; ICCPR）を初めとする国際人権条約においても認められているため、その重要性を争うことは困難であろう。

第二に、貿易制限性について、本措置によって米国からの越境サービスができなくなる可能性があるが、データ保護指令/GDPR 上は企業単位での体制構築（例えば SCC や BCR に基づく越境移転の可能性）が越境移転制限の例外として残されており、完全な禁輸に比べると制限性は高くないといえる。他方、移転後においても、移転前（すなわち EU 域内）と同様の個人情報保護水準を保つ、という目的への寄与度は肯定されよう。したがって、暫定的な正当化を認め得ると考えられる。

そこで、代替措置の検討に移るが、この点で参考になるのが OECD におけるプライバシーガイドラインである。同ガイドラインは、1970 年代の欧米対立を解消することを目的として 1980 年に策定され、2013 年に改訂されている [56]。本ガイドラインも下記の通り国単位又は組織単位での同等性が認められる場合をデータ移転制限の例外と位置づけている。

17. 加盟国は、自国と他の国との間における個人データの国際流通について、ガイドラインに一致する継続的な保護のレベルを保つために、(a) 他の国がガイドラインを実質的に遵守している場合、又は(b) 効果的な執行メカニズム及びデータ管理者により導入される適切な措置を含め、十分な保護措置がある場合、この流通を制限することを控えるべきである [57]。

前述の通り、EU 措置もまた国単位又は組織単位での同等性がある場合には越境移転を認める規制をとっているため、代替手段の立証は容易ではない。このように、一定の「相場」となるような国際基準が存在している場合には、代替手段の立証は容易ではないといえよう。

逆に、個人情報保護水準の同等性がある場合であっても移転を認めない、完全な越境移転の禁止（例えばロシアの個人情報保護法がこれを導入している [58]）を導入している場合には、上記の「相場」に照らして LRA を立証することが容易であり、必要性を認めるのが困難であるといえる。このように国際的に一定の合意がある場合には LRA の立証を行う上で、1 つの参照基準となり得る。こうした実体的な規制の収斂、例えばグローバルな基準策定を通じた相場感の形成の重要性に留意する必要があろう。

最後に、第 3 の要件である柱書に該当しないことを立証する必要があるが、この点については IV-1-2-4 で 3 つの目的をまとめて扱うこととしたい。

IV-1-2-2.　国家安全保障

ここでは、機微なデータ（軍事転用可能な機器、実験結果のデータや大量の個人情報等）を、濫用的な GA の存在を理由として特定国に対して持ち出しを禁じるような措置を仮定してみよう。GATS では下記の通り、第 XIV 条第 2 項において国家安全保障の例外が規定されている。

国家安全保障に基づくデータの移転制限については、既に輸出規制において一部の技術情報等の移転が制限されている。

しかし、こうした既存の輸出管理レジームと WTO 協定との整合性は、十分検討されてきたとはい

---

56 この経緯については、拙稿(前掲)を参照

57 JIPDEC による仮訳を参照した。

58 野村総合研究所「情報の自由な流通及びサイバー空間の公平と平等の確保に向けた調査」（https://www.meti.go.jp/policy/mono_info_service/connected_industries/pdf/gdpr02.pdf）、170-171 頁を参照

いがたい。両者は正面から検討すれば矛盾を生じさせるといわれ、例えば川瀬は「安全保障貿易管理の世界では、ワッセナー・アレンジメント・・・など、対象物資ごとに国家間レジームが形成されている。・・・各国はここで決まる、ある種の相場観に従って輸出管理を行い、その範囲を大きく逸脱する例外の濫用を慎んできた。他方で、この相場観に従って行動しているかぎり、他国の安全保障貿易管理措置が WTO 協定に整合しているかを問うことも自制してきた。前述のように、こうした措置は性質上、どうしても WTO 協定の原則と矛盾してしまう。とはいえ、国際社会の安定と平和のためには、安全保障貿易管理をやめることもできない。だからこそ、各国は輸出管理の WTO 協定整合性を厳密に問わず、例外の濫用も慎む大人の知恵を働かせ、本来緊張関係にある双方のレジームを注意深く共存させてきた。」と述べている [59]。

しかし、少なくとも情報の移転については、下記の通り(a)が明確に、自国の安全保障上の重大な利益に反すると当該加盟国が認める情報の提供という文言を用いて規定している。これは本来的には証拠の提出などに関するものであったと思われるが、WTO の文言重視の姿勢からすれば [60]、データの越境移転制限を正当化し得るであろう。

第 XIV 条の二 安全保障のための例外

1. この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。
   (a) 加盟国に対し、その開示が自国の安全保障上の重大な利益に反すると当該加盟国が認める情報の提供を要求すること。
   (b) 加盟国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを妨げること。
      i. 軍事施設のため直接又は間接に行われるサービスの提供に関する措置
      ii. 核分裂性物質若しくは核融合性物質又はこれらの生産原料である物質に関する措置
      iii. 戦時その他の国際関係の緊急時にとる措置
   (c) 加盟国が国際の平和及び安全の維持のため国際連合憲章に基づく義務に従って措置をとることを妨げること。
2. サービスの貿易に関する理事会は、1 の(b)及び(c)の規定に基づいてとられる措置並びにその終了について最大限に可能な範囲で通報を受ける。

本項は同様の文言を持つ GATT 第 XXI 条に基づくものであり、同条(a)や(b)については「加盟国が認める」との文言から、当事国の自己判断規定（Self-Judging Clause）であるとの理解もなされてきた。これは具体的には、そもそもパネルの審査権限の外にある、あるいは、パネルの審査は及ばない、といった主張であると解される [61]。そのような GATT 第 XXI 条の理解に基づけば、同様の文言を規定する本項についても、おおよそ本項に基づく措置については司法審査の余地がなく WTO 協定違反を問い得ない、という帰結となるであろう。例えば、米国やロシアなどがこのような立場を取っている [62]。

---

59 川瀬剛志「日本政府は韓国の輸出規制を再考すべきだ」（東洋経済オンライン；https://toyokeizai.net/articles/-/291562）

60 清水章雄「WTO 紛争解決における解釈手法の展開と問題点」、『日本国際経済法学会年報』（2009）参照

61 それぞれ、後掲ロシア・貨物通過事件におけるロシア、米国の主張である。

62 川瀬剛志「ロシア・貨物通過事件パネル報告書－米国・232 条紛争の行方と WTO 体制への影響－」（https://www.rieti.go.jp/jp/special/special_report/104.html）

しかし、上記の理解については、例えば(b)の(i)～(iii)については客観的な審査が及ぶとする学説[63]、そして2019年に公表されたロシア・貨物通過事件のパネル報告において、明確に否定されている[64]。同事件においては、(i)～(iii)に定められる状況が全て客観的に判断できる基準であることから、かかる条文の論理構造に鑑みて自己判断性はここまで及ばないと解釈され、パネルは条約の趣旨・目的、GATT1947 の起草過程を検討した上で、結論として(iii)の状況（「戦時その他の国際関係の緊急時」）の存否は客観的に評価されるとした[65]。

しかし、(a)は(b)の(i)-(iii)のような文言を欠くため、状況の存否という客観的な審査が及ばず、したがって、それに比べると緩やかな立証水準で足りることが考えられる。前述のロシア・貨物通過事件パネル報告書では、(b)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」という文言について、ウィーン条約法条約第 26 条、31 条等に基づいて信義誠実に条約解釈を行い、信義誠実に条約上の義務を履行する義務を負う以上、この文言についても完全な自由裁量ではなく、重大な利益を明示する義務を負い、この明示が求められる程度は(iii)の具体的な内容によるとされている[66]。しかし、(a)には(iii)に該当する文言がなく、仮に信義則に基づいて一定の説明義務が生じるとしても、その説明の程度は不明であるが、客観的な状況の存在による裁量統制が欠けている分、(b)よりもさらに緩やかになるといえるのではないか。この点、同事件ではロシアが自国の安全保障上の利益を明示していないにもかかわらず、クリミア危機への言及を以ってそれが満たされているとされた[67]。なお、この点については非常に低い審査密度であり、これで濫用の防止が実現できるのか、といった批判がある[68]。

他方、(b)の「必要と」という文言について、パネルは非常にかけ離れているか無関係（"so remote from, or unrelated to"）という基準を採用している[69]。この点については、(a)の「反する」についても異ならないといえるのではないかと考えられる。

それでは、具体的にどのような情報であればこのような証明が可能であるか。この点、(a)に関する先例は存在していないため、現時点では十分な分析を行うことは困難である。ただし、一般的に輸出規制上問題となる、高度な暗号や核開発、生物・化学兵器などに関する情報がこれに該当することはおそらく多くの論証を要しないであろう。他方、米国の投資審査項目にある、大量の個人情報についてはどうであろうか。個人情報、例えばメールアドレスはサイバー攻撃の手段となり、この中に政府職員や、政府から委託を受けた企業等が含まれていれば、その潜在的な脅威は無視できないものとなり得るかもしれない。また、同様に電力やガス、交通などのインフラへの攻撃手段ともなり得る可能性がある。

さらに、米国の 2016 年総選挙に対するロシア政府の介入も取り沙汰されてきた。仮に、大量の自国民の個人データが他国に移転され、他国の政府が GA によって移転された個人データを入手し、こ

---

63 中川淳司他『国際経済法』（第 3 版、2019 年）、124 頁
64 Report of the Panel, “Russia — Measures Concerning Traffic in Transit” (DS512)
65 *Ibid.*, paras 7.63-101
66 *Ibid.*, paras 7.130-134
67 *Ibid.*, paras 7.134-137
68 平見健太「国家安全保障を理由とした経済規制と WTO の安全保障例外」（国際法学会エキスパーコメント No. 2019-6）（https://jsil.jp/archives/expert/2019-6）。私見では、同事件はクリミア紛争というロシアーウクライナ間の重大な国際紛争について扱われたものであり、その点で立証水準を下げた点は是認できると考える。
69 Report of the Panel, “Russia — Measures Concerning Traffic in Transit” (DS512), paras 7.138-146

れを自国の選挙への介入（Facebook などの SNS での広告やフェイクニュースの流布など）に利用して当該他国にとって有利な候補者の当選を促す場合、これは安全保障上の重大な脅威といえないであろうか。少し前までであればこの様な可能性は風が吹けば桶屋が儲かる、といった形で一笑に付していたかもしれないが、上記の 2016 年米国大統領選挙に対するロシアの介入疑惑の捜査の進展につれて、こうした脅威も現実のものとなりつつあるように思われる。

このように、一定の具体的な国家安全保障上の利益を適切に説明することができれば、GATS 第 XIV 条 2 の(a)については、一定程度正当化する余地が残されていると考えられる。

IV-1-2-3. 知的財産の保護

最後に、強制技術移転が想定されるような国に対して、知的財産の保護を理由としてデータを移転させない、という措置はどうであろうか。GATS 第 XIV 条(b)号の文言は、GATT 第 XX 条(d)号と同様のものであるが、ここでいう「この協定の規定に反しない法令」には GATT の解釈では税関における模倣品の水際差し止めなど、知的財産の保護が含まれると解される。同様に GATS においても、仮に約束表で約束していたとしても、著作権を侵害する動画配信サイトのサービス提供を阻害することは、一般に許容されるであろう。

しかし、上記の場合は、知的財産を侵害していることが判明した後の措置であって、知的財産侵害の「おそれ」がある場合にまでサービス提供を制限し得るかという点はやはり未解明である。この点、移転されるデータがそもそも機微な情報であれば、IV-1-2-2 で述べた国家安全保障に基づく正当化の余地がある。しかし、その他の一般的な技術情報などにまで、これを拡張し得るかは定かではない。

IV-1-2-4. 柱書

以上、各号の内容を 3 つの政策目的に照らして検討してきたので、正当化事由の最後の要件の検討である、柱書の検討に移行したい。データの越境移転制限は内外差別又は市場アクセスの問題となると思われるが、柱書において適用段階における外国間の差別を問題とすることがあり得る。GATS 第 XIV 条の柱書は同様の条件下にある諸国の恣意的又は不当な差別を禁じており、これに該当する場合には措置が正当化できなくなる。

例えば個人情報保護に関する EU 措置を例にとると、先に見た EU-US プライバシーシールドは、米国を（成立時にはそうした枠組みを持たなかった）日本よりも優遇している、とはいい得ないであろうか[70]。この点は例外の作り方次第ではあるが、柱書によって運用に一定の制限を加えられる点には留意が必要である。

IV-1-3. 小括：GATS はインターネット時代に耐え得るか？

さて、以上を総括して、GATS の規律範囲に関する結論を述べたい。まず、GATS はデータの移転制限を WTO 違反として主張するには、きわめて使いにくいルールであることが明らかになった。

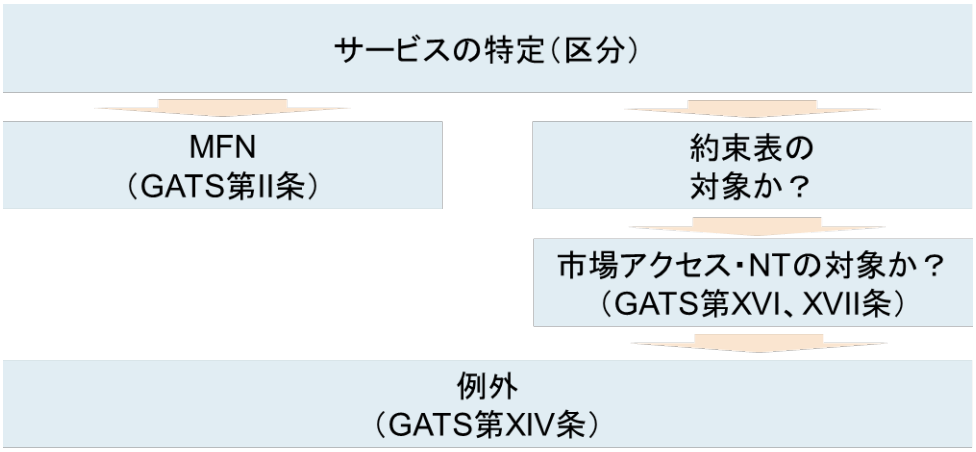
これは、越境移転規制は内外差別又は市場アクセスの問題であるから、GATS 違反を問うためには、約束表の約束内容を明らかにせねばならず、そのためには約束の内容に含まれるか否か、含まれるとしてどのサービス区分に含まれるか、をサービス別に立証する必要があるのである（下記図表を参照）。

---

[70] 私見では、過去のエビ・カメ事件上級委員会判断等における柱書解釈から、このような違反を問い得ると考えている（拙稿、前掲参照）。

もちろん、措置の構成によっては工夫できる余地はあるものの[71]、データの移転規制はあらゆるサービスに影響を与え得る一方で、個別サービスについて上記の立証を行うことはやはり労力がかかる。また、履行措置についても、違反が認められたサービスについてのみ是正すれば足りることとなってしまう。

図表 4　GATS の違反立証の構造



このように、GATS がデータという観点で構成されていない点を補い得るのが、次に見る近年締結された、CPTPP や USMCA 等の自由貿易協定における電子商取引章の規定である。

IV-2.　CPTPP 及び USMCA における越境データ移転制限に関する規律

GATS が正面からデータを扱うことなく、あくまでサービス貿易の自由化とそれに対する制限を規律していたのに対して、データという横串を通したのが TPP であり、その後継たる USMCA の電子商取引章・デジタル貿易章である。CPTPP のデータ移転に関する条項（第 14.11 条）と USMCA のデータ移転に関する条項（第 19.11 条）はほぼ同内容であるため[72]、ここでは CPTPP の条項を検討する。

CPTPP は第 14.11 条 1 で各締約国がデータの越境移転について、自国の規制上の要件を課すことを認めつつ、対象者の事業の実施のために行われる場合には、情報の電子的手段による国境を越える移転を許可する、とする。

他方、この例外として、締約国が公共政策の正当な目的を達成するために以上の規定に適合しない措置を採用し、または維持することを妨げるものではないとし、その条件として(a)恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと、(b)目的の達成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こと、の 2 点を挙げる。

CPTPP においては、事業上の必要な越境移転を原則として許可する、としている点に特徴がある。ここでいう公共政策の正当な目的に何が含まれるかは明らかではないが、先に述べた 3 つの目的は

[71] この点について、平見健太「WTO 紛争処理における measures 概念の展開―国際通商法に於ける『法の支配』の射程―」『日本国際経済法学会年報第 26 号』（2017 年）

[72] USMCA 第 19.11 条には、CPTPP 第 14.11 条 1 項の規制上の要件を課す権限を認める規定がない。

いずれも GATS 上も認められているものであるため、基本的には含まれ得るであろう。

次に、2 つの条件について。まず、(a)の必要性については WTO 協定のうち、TBT 協定の第 2.2 条類似の審査が実施される、とする説がある [73]。すると、過去の判断からは GATS 第 XIV 条類似の必要性審査が行われることとなる。また、もう 1 つの(b)についてもこれは GATS 第 XIV 条柱書と同様の文言であるから、実質的にはデータの越境移転制限の例外に関する審査は、GATS 第 XIV 条の審査と大きな差異がないということになる。

もっとも、ここでは個別のサービスが約束表に含まれるか否かを詳細に立証していく必要はない。CPTPP 第 14.11 条の適用対象となるのは CPTPP の「対象者」（第 14.1 条で定義される、投資財産、締約国投資家、サービス提供者）の事業の実施に必要なものであり、自国の企業や自然人がこの対象者に含まれている必要がある。越境移転が問題になる場合には、投資がなされていない場合も多く、そうするとやはりサービス提供者であることを立証する必要がある。

もっとも、CPTPP では GATS と異なってネガティブリスト方式を採用していることや、内国民待遇や市場アクセス違反に比べて、事業の実施のためのデータ移転への制限の方が一般には立証しやすい点をかんがみると、やはり GATS に比べて一定の進歩がなされているといえよう。

IV-3.　EU のデータフローと個人データ保護に関する共通条文案

欧州委員会が提案するデータフローに関する共通条文案は下記の通りであり、EU は、オーストラリアやニュージーランドなどと現在進行中の自由貿易交渉においても、この条文案を含むテキスト案を提案している [74]。

（EU モデル条文 [75]）

Article A Cross-border data flows

1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:

(i) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;

(ii) requiring the localisation of data in the Party's territory for storage or processing;

(iii) prohibiting storage or processing in the territory of the other Party;

(iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.

2. The Parties shall keep the implementation of this provision under review and assess its functioning in 3 years following the entry into force of this Agreement.

A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration.

---

[73] 河合優子、藤井康次郎「14 電子商取引」（Web 解説　TPP 協定　）
（https://www.rieti.go.jp/jp/projects/tpp/pdf/14_e-commerce_v2.pdf）

[74] https://www.jetro.go.jp/biznews/2019/05/1bc21a3f6b9c3bd3.html

[75] Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements)
(http://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf)

Article B 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.
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.
3. For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person.
4. For greater certainty, the Investment Court System does not apply to the provisions in Articles A and B.

まず、A 条においては、越境データ流通の促進にコミットすることが規定され、それを達成するためのローカライゼーション措置を中心とした禁止される行為類型が列挙されている。

他方、特に特徴的な規定は B 条である。ここでは、個人データの保護やプライバシーが基本権であることを確認し、これを保護する水準を加盟国は自由に定められるとともに、この協定によってこれらの保護が影響を受けないことを定めている。これは加盟国の権利（Each Party may）として構成されており、おそらく違反の余地なく措置が認められると解される。他方、CPTPP にあるような一般例外がなく、これは FTA 全体の一般例外に依拠すると思われるが、知的財産保護や安全保障に基づくデータの越境移転がどのような審査に服するかは不透明である。

EU 提案について、特に個人情報保護を正面から権利として認めている点は、CPTPP とは明確に異なっている。これは先に述べた通り、EU においてはデータ保護やプライバシーは EU 基本権憲章で規定されており、先に III のカナダとの PNR 協定に関する欧州司法裁判所意見で見た通り、欧州委員会がこれに反する対外協定、例えば自由貿易協定を結ぶことはできないことを反映している可能性がある。

また、基本権保護を欧州委員会の中で管轄するのは司法総局であって、通商総局ではない。このような EU 法上の位置づけや欧州委員会内における組織構造等から、基本権たる個人情報保護については通商交渉からの影響を避けたい、という思惑があって、EU はこのようなモデル条項を提案していると考えられる。

上記の様な理解を元にすると、日本が EU に対して CPTPP 型のデータ流通に関する条項を提案することは、EU の制度上の問題から非常に難しいといえよう。

IV-4. 小括

以上の通り、現在諸国で導入されている GA を理由とした越境移転規制について、その GATS 整合性には多くの不明な点が残されている。これはデータの移転制限について、GATS 第 XIV 条(b)などの GATS 特有の規定について、紛争解決手続で争われた先例がないことが理由の 1 つである。他方、安全保障例外のように GATT を含めて先例に乏しいものについては、現在係争中の案件の推移

も踏まえつつ、その射程を見極めていく必要がある[76]。

他方、FTA についてはその解釈がさらに乏しく、学説上も条文を超える深い議論はなされていない。ただし、FTA について、CPTPP は GATS と大きく変わらないものと推測され、したがって GATS の不明点がそのまま維持されることとなる。他方、EU 提案については個人情報保護の加盟国裁量を大幅に拡大しており、この点で GA を理由とした個人情報保護に基づく越境移転制限は、CPTPP や WTO に比べても認められやすくなっているだろう。他方、その他の理由に基づく正当化については、FTA 全体の例外として構成されることが考えられるが、その内容は不明確である。

このように、国際通商協定と越境移転規制については、それが抵触する可能性と、例外として認められて正当化される可能性の双方があり、結論は出ていない、というのが現状である。

[76] 現在複数の安全保障例外をめぐる紛争が WTO で係争中である。例えば、サウジアラビア、アラブ首長国連邦（UAE）、バーレーン、エジプトの 4 カ国は 2017 年 6 月に、カタールがテロ組織を支援していることを理由に陸路、海路、空路を遮断した。カタールはこれを WTO 違反として、WTO への提訴を行っている。また、米国の拡大通商法 232 条に関する WTO での係争もある。

V. 結論に代えて：今後のルール形成に向けた示唆

最後に、以上得た議論の土台をもとに、私なりに今後のルール形成、特に DFFT の実現に向けた展望を論じてみたい。私見では、DFFT は信頼（“T”）というマジックワードをつけることで、総論としては賛成をする国がほとんどであるが、他方で具体的に何を持って信頼を構成するか、例えば国家安全保障の範囲を議論し始めると、とたんにその同意を得にくくなるという概念であると認識している。その点で、この概念の下に何をルール化するのか、という具体策が不可欠である。

以下では、5W1H のうち、いつと誰を除く論点について、DFFT の具体化に向けて、GA に関するルール形成の展望を論じていきたい。

V-1. 何をルール化するか？

もっとも重要な論点は、何をルール化するかという点である。まずここで形成されるべきルールが、通商ルールなのか、あるいはより一般的なルールなのかという点が論点となる。濫用の危険があるにせよ、GA そのものを禁じることは、欧米を含めた大多数の国家が反対するものであり、その点では事の本質はいかにして GA の濫用を防止するかにある。

I で述べた GA の目的に立ち戻ると大きく国家安全保障と経済的な価値の追求があり、これらに応じて異なったルールを作成すべきである。本稿では I で述べた定義を採用したため両者をまとめて GA として論じてきたが、前者を諜報活動（Surveillance）、後者を強制技術移転（forced technology transfer）として全く異なった措置として取り扱うことも視野に入れるべきである。

前者の GA は必ずしも経済目的で行われるわけではなく、本来的に通商ルールとして形成するにはそぐわない主題であろう。したがって、まずは国家安全保障を目的とする GA について、経済的な目的を含めず、かつ、基本的人権を尊重する仕組みを持った一定の濫用防止に向けたルール作りが必要となる。難しいのが、GA によって引き起こされる影響範囲の広さである。IV で述べた選挙への介入などはその一例であるが、このように ICT の活用によって様々に広がっていく GA の濫用範囲をいかに適切に類型化しつつルールメイクしていくかが問われている。

他方、後者の GA については経済的な側面が主となるものであり、具体的には、その市場歪曲的な効果から、強制技術移転の原則禁止を軸に議論を組み立てるべきである。そして、このようなルールを持たない諸国については一定の制約、例えばデータの移転制限を課したとしてもやむを得ない仕組みとすべきであろう。制度設計として、強制技術移転については、その概要や導入目的等を通報するといった現行の補助金に類似する透明性ルールを設定した上で、透明性違反に対する制裁を含め、違反について争う制度を導入するといった形が考えられる。

以上議論を簡便にするために両者を区別して論じてきたが、ここで諜報活動と強制技術移転を本当に区別できるのか、という問題は残っている点に留意しなくてはならない。例えば米国の GA は本来的には技術移転を図るものではなかったが、やはり濫用的に、産業スパイ的な実行があったことは否定できないであろう。

また逆に、中国におけるソースコードの強制開示は一見すると強制技術移転にも見られるが、それだけにとどまるものではない。ソースコードの開示は、情報通信インフラを支配することでサイバー空間における言論統制、例えば一党独裁を批判する言動を押さえ込むこと（これもまた中国ではサイバーセキュリティとみなされる）につながっており、これはつまるところ国家安全保障（ここでの区分でいう諜報活動）に向けた措置ともいい得るのである。さらに敷衍すれば、欧米において、昨今問題となっている通信インフラの安全性の確保、例えば 5G インフラの調達において

Huawei 製品等にバックドアが仕掛けられていないことを証明するに当たって、ソースコードの開示を義務づける制度もでき得るかもしれない。

このように、今日では国家安全保障の内実が非常に多様化しており、一見すると強制技術移転に見える活動がその実国家安全保障につながり、その逆もまたあり得るということである[77]。

それでは、このような区別の曖昧さ、あるいは現代的な安全保障の多様化に対してはどう対処すべきであろうか。私見では客観的な「信頼」の担保がひとつのキーワードになり得ると考える。これはつまり、客観的な法制度的な担保と権利侵害の最小化、独立した第三者による監査、そして個人・企業に対する実効的な救済手段の確保によって信頼を担保することで、濫用の防止を図り、ルールの加盟国相互の信頼を確保していくということである。諜報活動については先に III で述べた EU 型の越境データ移転に関する評価基準を導入し、他方、強制技術移転についてもそれが安全保障目的であるならば同様の透明性を担保させ、それが難しいのであれば禁止される強制技術移転に該当する、というルールを形成していくというのが 1 つの姿であると考えられる。

V-2.　どこでどのようにルール化するか？

さて、では以上のルールをどのような場で交渉すべきであろうか。実は諜報活動については、スノーデン事件以降、国連の人権理事会において議論がなされてきている。スノーデン事件を受け、国連総会は 2013 年末、「デジタル時代のプライバシーに対する権利」と題する総会決議を発出した。その後、毎年のように類似の総会決議が出されて、最新のものは 2018 年である[78]。

2013 年の当初の総会決議において、人権高等弁務官事務所に対して特別報告者の選定と報告が依頼され、同事務所はこの問題を特に重大な問題であると位置づけ、マルタ大学のジョセフ・ケナタッチ教授を特別報告者として 2015 年に選定した。以降、同教授による報告書が毎年公表されており、最新版は 2019 年に公表された活動報告である[79]。ここではプライバシー権を規定する ICCPR 第 17 条を元にした、同条に基づく国家の監視活動からの個人の権利保護について議論が進められており、例えば 2018 年には国家の監視活動に関する「政府主導の監視とプライバシーに関する法文書草案」が提出されている[80]。同草案では、例えば前文において下記を規定しており、本稿の提言の方向性とも重なるものである；

(6)公共の安全に関する懸念がある種の機密情報の収集と保護を正当化する一方で、国家は国際人権法上の義務の完全な履行を確保しなければならない。通信の傍受を含む違法で恣意的な監視は、個人情報の違法で恣意的な収集と同様に、侵害の度合いがかなり高い活動であるので、プライバシーと表現の自由を侵害し、法の支配と人権の上に築かれた民主主義社会に反する。

(7)多くの国際的・地域的法システムにおいて、個人のプライバシー権を制限／限定／干渉するための措置は、個別の事前の承認と対象の限定が必要とされなければならないが、明示的に以下のよ

---

77 このように、経済問題と国家安全保障概念の再考を促す論考として；Heath, J. Benton, “The New National Security Challenge to the Economic Order”, *Yale Law Journal,* vol.119 (forthcoming), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3361107

78 U.N. Doc., A/RES/73/179

79 U.N. Doc., A/HRC/40/63 (https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/A_HRC_40_63.DOCX)

80 “Working Draft Legal Instrument on Government-led Surveillance and Privacy Including the Explanatory Memorandum” (https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf)

うに規定されている。(a)法に規定されていなければならない。(b)正当な目的を有さなければならない。(c)追求される目的に対し必要で均衡のとれたものでなければならない。(d)法により特定された適切な安全保護を提供しなければならない。(e)監視活動は独立した司法機関又は法によりその活動を規定された機関により承認されなければならない。(f)監視活動は正当な機関により監視されなければならない。

ただし、検討の特別報告者が EU 加盟国であるマルタ共和国から出され、年次報告においても EU が進める欧州評議会第 108 号条約の批准を推進する等[81]、かなり EU の影響が強い状況で検討がなされていることも事実である。EU の検討を下敷きとした本稿と方向性が重なるのは、そうした理由があり得よう。さらに、上記の政府主導の監視とプライバシーに関する法文書草案は ICCPR や世界人権宣言を下敷きにしたものであるが、果たしてそれらの実定法解釈の結果として上記の監視に対する権利を導き得るものか、疑問無しとしない。しかし、検討が開始されている会議があり、かつここでの共闘は EU の巻き込みにつながるものであるため、日本としても一考の余地のある選択肢といえるであろう。

例えば、非拘束的な指針を国連で合意しつつ、これを遵守しない場合には越境移転の規制を正当化する、といったルールのあり方が考えられる。また、プライバシー保護については、新たなプライバシーに関するガイドラインの策定を含め、OECD で継続的に議論が行われているが、国連の交渉結果をそこで活用する等も検討に値するのではないか。

他方、WTO という場については注意が必要である。ここでの交渉の担当者は通商担当者となるが、例えば EU についてはデータ保護を担当するのは司法総局（DG Justice）であり、通商総局（DG Trade）ではない。基本権と位置づけられる個人データ保護の問題を、基本的には経済的な考慮を基に議論を行う通商フォーラムで交渉することに関して、EU サイドが否定的となる可能性がある。先の OECD と同様、監視活動については国連で議論し、そこで得た結論を通商ルール、例えばサービスやデータの移転制限の例外として利用する、という形で通商フォーラムのルール形成に取り込んでいく、という姿勢が望ましいのではないか。

以上のように考えると、わが国は DFFT の実現に向け、GA というテーマだけをとっても、複数の価値観やステークホルダーが異なるフォーラムを横断的かつ戦略的に活用して交渉をリードしていくことが求められる。そこでは、わが国の交渉についても一元的な戦略を立案し、かつ総合司令塔的な役割を持った部署を作る、または官庁横断的な体制で取り掛かる必要がある。この点、日本経済団体連合会はデジタル省の設立を提言しているが[82]、これと類似した機能を短期的に作り上げていく必要がある。

V-3.　誰とルール化するか？

最後に、誰を巻き込むべきか、という論点の検討に移る。これはとりわけ難しい論点であるが、日本として既に交渉を開始している 3 極の相手方、米国と EU については巻き込みを図らざるを得ないであろう[83]。また、経済規模という点でもこれらのいずれを欠くことも難しいと思われる。

---

81 *op. cit.*, U.N. Doc., A/HRC/40/63

82 日本経済団体連合会「デジタルエコノミー推進に向けた統合的な国際戦略の確立を」（https://www.keidanren.or.jp/policy/2018/041.html）

83 日本経済新聞（2019 年 1 月 10 日）「日米欧貿易相、『データ流通圏』構築　交渉入りへ連携」（https://www.nikkei.com/article/DGXMZO39838980Q9A110C1000000/）

先に述べた通り、EU については、その複雑な機構や法体系が持つ各種制約を念頭に置きつつ交渉を行い、他方、米国については比較的に日本と近い立場であるため、EU と米国の間をいかにうまく調整できるかが、日本に問われているといえよう。

同時に、DFFT がグローバルな広がりを持つためには、中国やロシアといった新興国の巻き込みも重要になる。この点、例えば中国やロシアの言論統制を許容する代わりに、GA に関する透明性を確保させる、といった戦略もあり得るが、このような言論統制を許容することは欧米の価値観とそぐわない。他方で、これを認めない限りこれらの国が交渉に参加しない可能性もあり、予断を許さない状況である。

V-4. 残された課題

本稿は、冒頭で述べた通り、GA とそれに基づく越境データ移転規制の現状を整理するとともに、通商協定の DFFT の検討に向けた出発点、基礎資料となることを企図して執筆した。本稿がそれに応えるものとなっていれば望外の喜びである。

また、V では今後の交渉を見据え、若干の試論的な考察を行った。最終的なメッセージは、GA が安全保障という今日きわめて多義的に使われている概念にまつわるものであり、この概念については国際経済法全体としても認識を改めて取り組んでいかなければならず、したがって今後の交渉もその実態を踏まえたものとならざるを得ないこと、他方で監視活動の規律については特に人権保護の観点から国際的な議論が進みつつあり、ここでは EU が主導権を握りつつあること [84]、であった。

他方、残された課題もまだ多い。本稿は各国の監視活動についてその触りを論じたに過ぎない。例えば EU では EU 法秩序が形成され、その対外的な交渉が EU 法秩序の自立性に影響を与えるという観点から大幅な制約を受けている。このように日本が今後 DFFT に関する国際交渉を纏め上げるためには、各国の法システムに対する深い知見とそれに基づく落としどころを探る術が不可欠であるが、これにはわが国の各国法そして国際法の知見、政治や経済、産業、ICT をはじめとするテクノロジーの知見を総動員する必要があり、そのためには広く開かれた産官学の対話・連携のフォーラムが必要であろう。

また、本稿は、データに関する多国間ルール形成という観点から、GA に着目して、特に越境データに関連する論点を扱ったに過ぎない。しかし、GA への懸念に基づく措置には、半導体等の輸出規制や米国や豪州等における Huawei の 5G インフラからの排除など、政府調達や規格・基準、輸出管理のあり方などより通商秩序に影響を与える論点がある。これらの検討については他日を期したいが、いずれも DFFT の形成にとって不可欠な議論となるだろう。

最後に、日本として DFFT を通じてどのような世界を実現したいのか、という世界観を提示していくことも重要である。この点、安倍総理大臣のダボス会議演説にもあったように、DFFT によってデジタル経済の可能性を発揮し、社会課題の解決を図っていくということも重要な視点である。しかし、DFFT が支える価値とは、民主社会を支える言論の自由や、個人が自らの情報をコントロールとするという権利でもあるはずであり、必ずしも経済的な指標のみで図られるべきではない。

---

[84] V で取り上げた国連での議論のほか、本稿でも適宜参照しているが、近年、複数の”Surveillance Law”というタイトルの学術書が出版されている。例えば；David Grey and Stephan E. Henderson (ed.), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press, 2017). 及び II で挙げた参考文献を参照されたい。

この点、G20 に対して T20 が提言した自由なデータフローをアンカーとする政策体系の構築ではこれらの要素などを含んではいるが[85]、より積極的に打ち出すべき価値を日本として今一度考えていくべきではないか。

[85] 木村福成「自由なデータフローを支える政策体系の構築－T20 貿易・投資タスクフォースの政策提言より－」（https://www.rieti.go.jp/jp/columns/a01_0526.html）