平和研　研究ノート

NPI

経済安全保障研究会 研究報告(No.4)　2020年12月24日

GAのリスク拡大とその経済安全保障への影響

渡辺翔太(株式会社野村総合研究所　主任研究員)[1]

1. 問題の所在

1.1. GAとは

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指す[2]。この定義から明らかなように、通常の刑事捜査における証拠収集等、GAは日常的に国家の作用として行使されているといえる。

他方、本稿で問題とするのは、このような刑事捜査にとどまらない、民間の様々なデータに対する政府機関の強制力を持ったアクセスである。例えば、ある外国政府が自らに批判的な言論の弾圧を目的とて発信者の情報提供を要求したり、あるいは自国産業の発展を意図して自国に所在する外国企業が持つ産業政策上有用な技術データの取得を目的して当該データの収集を求める(いわゆる産業スパイ)など、様々な類型が考えられる。

図表 1 GAの類型とその実施例

GA活用類型	実施例
犯罪捜査	• サーバーへのリモートアクセス • 海外に所在するデータの提出命令、等
諜報活動	• 防衛機密の入手 • 政治家に関する情報を入手して外交交渉を有利にする、等
外国での世論操作	• 選挙介入(ケンブリッジ・アナリティカ事件等) • 自国に有利な情報の発信 • フェイクニュースによる社会分断、等
自国の情報統制	• 為政者に不利な批判などの削除 • 反政府言論の抑圧(投稿者の個人情報提出など)、等
産業スパイ	• 産業政策上重要な機密データの入手、等

1.2. GA拡大の背景

[1] 本稿は中曽根康弘世界平和研究所・経済安全保障研究会における筆者の報告とその後の参加者との議論をもとにしており、参加者各位に謝意を表したい。ただし本稿に存する誤りはすべて筆者に帰責されるものである。また、本稿はあくまで筆者の個人的見解であり、筆者の所属する組織を代表するものではない。

[2] GAの詳細については、拙稿「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)を参照。

このように GA が懸念されるに至った背景として、特に指摘できるのが情報の流通経路としてのインターネットの発達である。今日の社会は、サイバー/フィジカル空間が融合され、多様なデータが AI によって解析・活用される世界＝Society5.0 が到来するといわれている。他方で、このような Society5.0 の情報流通の基盤、すなわちインターネット、プラットフォーム（SNS 等）、クラウドサービス等はすべて民間企業が主体となって管理している。具体的には、インターネットは通信キャリアや ISP、プラットフォームやクラウドサービスは GAFA 等のいずれも民間企業が、それぞれ管理・運営しているのである。これに IoT 等のリアル世界のデータ収集が加わったとしても、その運営主体はやはり民間企業が多くを占めるであろう。

すなわち、かつてに比べ民間部門（その多くは経済部門でもある）が管理するデータが莫大に増加し、政府は民間部門が保有するデータを活用した各種の活動が実施できるようになった点が、GA に特に着目され、それゆえリスクが高まっている背景であるといえよう。

1．3．問題の所在

以上のような情勢のもと、今後のわが国の経済安全保障、特にデータに関するそれを検討するにあたっては、GA のリスクを勘案することは不可避であると考えられる。

他方、のちに3．で述べる通り、GA への対抗策として、データの自国内から自国外へのデータ越境移転制限を導入する国が多い。

しかし、このようなデータの越境移転規制は、日本企業にとっても適用されるものであり、自由なデータの流通をもとにした Society5.0 の実現に向けても大きな障壁となりうる。すなわち、外国における GA にいかに対抗するかという観点に加え、データに関する越境移転規律が強化される中、過度な越境移転規制を抑制し、日本企業の海外展開をいかに円滑にしていくかの観点も重要なのである。

このように GA への対抗策に関して、わが国が政策的にデータの自由流通と GA への対抗措置としての越境移転制限のバランスをいかに取っていくか、さらに例えば通商協定等の既存の国際/国内ルールとの整合性をどう考えるかという問いが投げかけられているといえる。

これは中長期の検討を要するテーマであり、本稿でそのすべてを明らかにすることは、紙幅の関係でも、また現時点での筆者の考察の到達点という観点でも難しい。そこで本稿では、特にデータをめぐる経済安全保障について GA という重要な問題が存在する、また、それが具体的にどのように問題になるのか、という点を明らかにすることにフォーカスしたい。そして、日本が進める国際的なデータ政策の中でいかに位置付けていくべきか、その方向性を明らかにすることを本稿の目標としたい。

2．GA の実例

1．の問題意識をもとに、2．ではより具体的に、いかなる国のいかなる措置が GA として日本の経済安全保障上の問題となるのかを見ていく。ここでは、欧米でも検討が進んでいる中国とロシアの措置に注目することとしたい。もっとも本稿の情報ソースが欧米、特に米国の分析に偏っている点は否めず、この点は引き続き検討が必要であるが、他方で、特に情報活動の分野は透明性がなく、外形的な情報では得られる資料に限界があるのも事実である。まず、我が

国としても GA のリスクを適切に判断する調査手法の確立も併せて検討されなければならないことは、ここで付言しておきたい。

2．1．中国:国家情報法

中国では、様々な法令によって、広範な目的を理由として、民間部門の保有する個人/非個人データの政府による開示要求権限が違反に対する刑事罰と共に規定されている。このうちでも、最も問題をはらんだものが国家情報法である。

同法はまず、非常に広範な情報活動の範囲を規定する。すなわち、同法にいう「国家情報活動」には、国の重大な政策決定の参考となる情報を提供すること、国家安全に危害を及ぼすリスクを除去するため情報面での支援を提供すること、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が包含されており、非常に広範である。

例えばここにいう経済社会の持続可能な発展については、自国の産業政策上必要な情報の取得に利用される可能性もある。また、国の安全や政権、主権の保全等については、言論統制等に利用される可能性も指摘できるだろう。

さらに、同法においては情報活動の実施についても広範な権限が当局に与えられている。すなわち、同法第 14 条は情報機関が関係する機関、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と規定し、第 28 条は拘留を含む措置を認めているほか、刑事罰にも言及している。

中国　国家情報活動法[3]

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。

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、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。

このような広範な民間事業者への協力義務を定めた法令は各国の懸念を引き起こしている。例えば、米国は中国 TikTok 社に関する大統領令において、同社が中国共産党に対して、TikTok ユーザーとなった政府職員やその契約者の位置情報等を提供しており、これによって政府職員への脅迫や諜報活動等が可能になっていると指摘している。

[3] 訳文は岡村志嘉子「中国の国家情報法」『外国の立法』274(2017.12)を引用している。

また同じ大統領令において、同社は香港やウイグル族等ムスリム少数派をめぐる中国共産党の言論統制に協力しており、また、例えば 2019 年のコロナウィルスの発生起源に関する陰謀論など、共産党に有利になる世論誘導に用いられる可能性があると指摘している[4]。

もちろんこのような懸念を否定する見解もあり、例えば同じく米国の制裁の対象とされている Huawei 社は自社のウェブサイトにて、ここで取り上げた国家情報法は上記のように理解されるべきものではなく、「通信機器メーカーにバックドアの埋め込みまたは顧客ネットワークの無効化を要請することを国家情報機関に許可するような中国の法律はありません。中国政府が当社のビジネスや製品のセキュリティに干渉することはありません。さらに、いかなる国や組織から、そのようなことを強要するような試みが行われた場合、当社は断固として拒否します」と述べている[5]。

筆者にはもちろんこれら見解の事実的な当否を判断する能力はないが、一つ指摘しうるのは、国家情報法だけが問題なのではなく、適正手続きや法の支配など、実効性を持った基本的人権の保障が十分になされているか疑義を持たざるを得ない事案が発生していることが、同法の理解についても懸念を引き起こしている点である。

2．2．ロシア：主権インターネット法

ロシアでは、個人情報保護法の改正において、ロシア国民の個人データを国内に保管することを義務づけた（いわゆるローカライゼーション措置。ただし、国外のサーバーにも並行して保管することは可能である）[6]。そして、このような義務違反に対しては、違反者のロシアのインターネットからの遮断を含む制裁措置が規定された。

2019 年 11 月には主権インターネット法が制定された。同法に基づいて、ロシア国内にあっては、ISP などに対して政府の検閲を手助けする機材の導入が義務化され、すべてのパケットが政府による監視、すなわち GA の対象となっている。

同法では、インターネットの安全を保護するため、すべてのロシア国内の ISP 等に対して、政府によるインターネット上のトラヒック監視のため、パケットの内容を含めて情報を取得しうる DPI（Deep Packet Inspection）を可能とするための機材の導入を義務付けている。

また、同法は、ロシアの ISP が国際的なインターネットに接続するポイントを政府が制限する権限を認めており、（その実効性には疑義があるものの）ロシア国内のインターネットをグローバルなインターネットから遮断しうる。

（同法成立以前の事案ではあるが）先に述べたロシアの個人情報保護法のローカライゼーション義務に対しては、インターネット接続の遮断が罰則として盛り込まれており、実際に米国の SNS サイト Linked In が同義務違反を理由としてウェブサイトを遮断されている[7]。

---

[4] Whitehouse, “Executive Order on Addressing the Threat Posed by TikTok” (https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/)

[5] Huawei 社ウェブサイト「当社について」（https://www.huawei.com/jp/trust-center/trustworthy/we-are）

[6] 同法については、例えば拙稿「EU はじめ世界に広がる越境移転規制・ 域外適用と日本企業の対策」『知的資産創造』（2018 年 9 月号）を参照。

[7] ロイター「ロシアのリンクトイン遮断　米政府が深い懸念を表明」

ロシア政府は、DPI で入手したすべてのインターネット上の情報にアクセスできるとともに、インターネットが危険にさらされている場合には、ロシア国内のインターネットを外国から遮断しうる、としている。

このように、ロシア国内での情報活動に向けた基盤として、同法が機能しうる可能性があることは指摘できよう。同法を介してインターネットトラヒックの解析が行われ、これが1．で挙げた多様な GA の実施に活用される可能性がある。

3．各国の GA への対抗策

2．で欧米の議論を中心に概観した通り、GA のリスクはその国内法上の根拠とともに、一定の合理性をもって提示されてきたといえよう。それでは、このようなリスクに対して、各国はどのように対処しているのか、ここでもやはり欧米の対抗策を中心に概観したい。結論を先取りすれば、欧米とも、GA への対抗措置として、データを自国外に移転しないという措置をとっているといえる。これは、当該国内においてはあくまで当該国の法制度を尊重すべきであり、まずは自国の管轄権の及ぶ範囲内に情報を留めるというのが最も有効な対抗策であるという考え方が背景にあると考えられる。

まず、米国においては、GA への対抗策はパッチワーク的に、様々な法令に規定された大統領の権限を活用したものが多い。例えば、国際緊急経済権限法（IEEPA）を活用して、米国人に関する個人データの取り扱いを特定企業に中止させるための売却命令が発令されている。また、外国投資リスク審査近代化法（FIRRMA）も重要であり、この改正に合わせて個人データに関するリスクが明確に対内投資審査の考慮要素として組み込まれている。また、ここでは買収後の技術情報等に関する GA のリスク（例えば外国企業が米国企業を買収し、当該企業の技術情報を本国の本社に移転するが、当該情報に対して GA が行われるような場合）についても審査されうる可能性がある。

他方、EU においては、個人データに関する保護が伝統的に継続されている。一般データ保護規則（GDPR）の前身となる 1995 年に策定されたデータ保護指令においても、すでに個人データの越境移転制限が規定されていた。これをそのまま GA にも活用する形で EU の法制度が形作られており、その中核となるのはやはり GDPR やデータ保護を含め EU 市民の基本的人権の保障を定める、EU 基本権憲章である。

GDPR を中心とする EU の個人情報保護法制においては、原則として外国への個人データの移転は禁止される。そして、移転先国の GA のリスクをも判断して、当該国の個人情報保護水準が EU と同等以上の水準にあるか否かを審査して、それを認めて欧州委員会がその旨の決定を行う場合（いわゆる十分性認定）には、この一般的な禁止が解除される、という枠組みとなっている。

過去、特に米国の GA に対して欧州司法裁判所は 2 回欧州委員会による十分性認定を覆しており、この司法判断の中で、外国の GA に関しては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）、②独立の監査（Independent

（https://jp.reuters.com/article/linkedin-sns-idJPKBN13G06C）

Oversight)、③個人の救済(Individual redress)が審査基準になる旨を確認しており、判例上確立したものとなっている。

他方、このような十分性認定が存在しない場合には、企業・組織単位で EU と同等な保護水準を確保することで移転が許容されることとなる。これは具体的には拘束的企業準則(BCR)や標準契約条項(SCC)等の契約関係を移転元と移転先で結ぶこととなっている。特に SCC はすでに欧州委員会の用意したひな形に基づいて契約関係を設ければよく、有用な越境移転の手段となっていた。

しかし、2020 年 7 月のいわゆる Schrems II 事件においては、SCC を締結した場合であっても、個別企業は移転先組織の所在する国における GA のリスクを個別に判断して、必要な追加的措置を取らなければならないことが判示された[8]。したがって、個別の企業が外国における GA のリスクを判断する必要が生じ、実務上どのように対応すべきか、議論が重ねられている。

また、EU は非個人データについても、その越境移転規制に関する法制化を進めている。一般的な対内投資規制に関する枠組み等もその一例であるが、直近の動向で特に着目すべきは現在欧州委員会から提案されている、Data Governance Act における非個人データの関連規定であると思われる。

すなわち、EU 加盟国の公的主体が保有するデータの再利用を定める同法案第 5 条は、第 9 項で知的財産や営業秘密で保護された再利用されるデータが EU 域外国に移転される場合、当該移転先国の保護水準を審査する同法案の施行規則を定めること、そこでは知的財産権や営業秘密の保護水準が EU と同等であること、当該水準が効果的に適用・執行されていること、実効的な司法救済が存在していること、等が基準とされることが規定されている。これは一見して明らかなとおり、EU が個人データの十分性認定について適用している審査基準とかなり近いものとなっている(非個人データについては監査に関する事項がない点に留意)。

今回の法案は公的機関の保有する非個人データかつ一定の法的保護(知的財産、営業秘密)があるものを対象としているためこのような検討は早計かもしれないが、この兆候が、EU が個人/非個人データを問わず信頼がおける他国を審査する基準を策定しつつある、とみること可能であるようにも思われ、本法案のデータの越境移転関連施策についてさらなる注視が求められるといえよう。

[8] Court of Justice of the European Union (CJEU), Case C‑311/18, Judgement of the Court(16 July 2020), paras. 132-134.

Article 5 Conditions for re-use[9] (9) The Commission may adopt implementing acts declaring that the legal, supervisory and enforcement arrangements of a third country: (a) ensure protection of intellectual property and trade secrets in a way that is essentially equivalent to the protection ensured under Union law; (b) are being effectively applied and enforced; and (c) provide effective judicial redress.

図表 2 米国と EU の GA に対する対抗策の比較

国/地域	米国		EU[10]
根拠法令	国際緊急経済権限法（IEEPA）	外国投資リスク審査近代化法（FIRRMA）	EU 基本権憲章、データ保護指令/GDPR
対象データ	個人/非個人データ	個人/非個人データ（技術情報含）	個人データ
対象となる GA	アドホックに決定される （例：共産党の中国民間企業データへの GA）	投資後の個人情報や重要な産業データへの本国への移転（および移転後の GA）	個人データへのアクセス （米 FISA 等）
取られる措置	アドホックに決定 （TikTok の例では、同社との取引停止（後、売却命令）	買収の禁止・出資の引き上げ	越境移転制限
GA が許容される条件	（アドホックに判断）		①法的根拠と適用される制限/セーフガード ②独立の監査 ③個人の救済

以上の通り、米国、EU とも GA への対抗策としては越境データ移転制限が選択されていること、ただしその法的な実装は既存の法体系との関係もあって、米国と EU でかなり異なっていることが明らかになった。それでは、諸外国のこのような動向を踏まえて、日本の立ち位置はどのように映るであろうか。

[9] European Commission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)”
[10] 本文で触れた通り、法案レベルでは非個人データの規律も導入されつつある。

4. 我が国の GA への対応

4．1．日本の立ち位置

3. の分析を踏まえ、あえて大胆な GA に関する日欧米のアプローチの比較を行うと、次の表のように整理されると思われる。

図表 3 日米欧の GA に対する対抗策の比較

国/地域	米国	EU	日本
規制に関するアプローチ	対症療法（EU に比べ、守るべき価値が見えない）	演繹的（基本的人権である個人情報の保護を基軸として考える）	バランス志向？
根拠法令	国際緊急経済権限法（IEEPA）他	個人情報については、EU 基本権憲章や GDPR	個人情報保護法（後述）、外為法
概要	大統領令や投資審査等、問題が生じている部分をアドホック、パッチワーク的に対応している。	特に CJEU の判例法理を通じて、EU 基本権憲章や GDPR 等をベースに解釈の積み重ねで演繹的に対処している。	DFFT 概念を提唱したものの、それ以前には主だった議論なし。
グローバルな GA に関するルール形成への意向	明示的なルール形成には言及がなく、自国法令に基づく一方的措置を志向	あり（GA に関する国連での条約化、各国への GDPR 輸出等）	あり（DFFT 構想：WTO の EC 交渉、OECD における GA の議論、等）

先に3. で述べた欧米の動向を比較したとき、米国は対中政策の文脈の中で GA をとらえている部分もあり、必ずしも価値観を前面に押し出したアプローチを志向していないといえる。ここではあくまで中国による自国内での影響を削ぐことに眼目があり、個人情報の保護がどの程度重視されているかは必ずしも明らかではない。例えば、TikTok をめぐる大統領令であれば、個人情報それ自体ではなく、それによって政府職員が監視されていることを問題視している。USMCA や日米デジタル協定の電子商取引関連規定を踏まえるとデータの自由流通を志向しているとも読み取れうるが、これが特に対中国との関係では定かではない部分がある。

他方、米国に比べると EU はより演繹的なアプローチをとっており、基本的人権としてのデータ保護の権利に基づく体系を構築している。これはある種一貫しているが、結果として EU はデータの自由流通よりも個人データの保護をより上位に置くアプローチをとっている。

これに対して、日本は米国ほどアドホック的でもなく、かといって EU ほどに基本的人権としてのデータ保護を上位概念と規定せずに演繹的なアプローチをとっていないという点で、ある種のバランス感覚を持ったアプローチを志向しており、これを体現した政策が日本が推進する

DFFT（Data Free Flow with Trust）構想である。筆者は、すくなくとも当初の DFFT 構想は、データの自由流通を志向しつつもそれを信頼できる諸国との間で行う構想であったと理解しているが[11]、今日ではこれはより多義的な意味を持ち、信頼を持ったデータが流通する状態や、データへの信頼性等論者によって様々な意味を含意するようになっていると思われる。

そして、ここで DFFT に関して実質的な検討を進めるには、ここにいう"Trust"の意味するところを明らかにしていくことが不可欠と思われるが、これを考えるうえで 1 つの核となる概念が GA のリスクであることは、本稿の事例から明らかであろう。日本のデータ関連政策はバランス志向であるものの、その具体的な取り組みについてはいまだ十分明らかにされていない。

4．2．日本における GA 対策の具体例：改正個人情報保護法

他方で、我が国においても全く GA に対する対抗策がないというわけではなく、その萌芽は出始めている。特に着目されるべきは、本年改正法が成立した個人情報保護法であろう。

同法第 24 条では、EU と同様に越境移転を原則として禁止し、越境移転に係る本人同意や相当措置等を定めているが[12]、この同意の所得に際して、移転先国や移転先組織の個人情報保護制度を開示することが求められる。具体的な開示内容は委員会規則で定められることとされているが、現時点で公表されている委員会規則の方向性においては、開示すべき要素の 1 つとして、GA の有無が規定されている[13]。これは、個人が外国における GA のリスクを踏まえて自らのデータを越境移転させるかどうかを選択させる機会を提供するものであり、GA に対する有益な対抗策の一つといえよう。

今回形となった改正法の方向性自体は昨年度から検討されており、このような GA のリスクの提示は、Schrems II 事件を受けた欧州にも先行していたといえる。また、OECD のプライバシーガイドライン改訂の議論においても、GA を盛り込むことが検討されている点も注目される。

5．終わりに

以上、本稿では GA の実例を検討することで、特に欧米において GA のリスクがどのように理解され、それに対してどのように対抗しているのかを明らかにした。これらの実例をもって、まずはデータに関連する経済安全保障にとって、GA のリスクが大きな意味を持っている点をご理解いただけていれば幸いである。

次に、日本に目を転じて、日本が国際的なデータ政策の中核とする DFFT 構想に関して、GA のリスクがその"Trust"を担保するうえで重大な脅威となることや、その具体的な施策として今年度改正された個人情報保護法の規定を参照し、GA のリスクが政策レベルでも認知されつつあることを分析した。

---

[11] これは DFFT の交渉の場として WTO という国家間交渉のフォーラムが選択されていたことからも明らかであろう。

[12] 詳細については、個人情報保護委員会事務局「改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）」（令和 2 年 11 月 4 日）（https://www.ppc.go.jp/files/pdf/201104_ekkyouiten.pdf）を参照。

[13] 同上、7 頁

最後に、経済安全保障に関して GA のリスクにいかに対抗するか、その方向性を提言して本稿の結びとしたい。国際的なルール形成に関する提言はすでに他の論考にまとめているため[14]、ここでは特に国内的な政策について述べていきたい。

まず、国内的には、議論の土台となるガバメントアクセスのリスクの分析が十分になされていない、という問題がある。今回取り上げた事例の多くは欧米の調査に負うところが大きく、我が国としてガバメントアクセスのリスクを自らの手で十分に分析できているわけではない。各国の法制度や様々な GA の手法についてさらなる調査必要とされる。ただし、部分的は改正個人情報保護法におけるリスクの特定の過程において実施されるであろう。

第二に、リスクへの対抗手段の整備である。欧米のアプローチを踏まえると、おそらく短期的には、国際ルールの欠如からデータの越境移転制限という一方的措置を取らざるを得ないであろう。この際活用できる、いわば GA への武器となる制度を日本は十二分に用意しているとはいいがたい。現時点では、個人情報保護法のほか、外為法における指定業種の拡大[15]、リモートセンシング法や各種の輸出規制（これは例えば武器に転用されうる製品のデータを含んでいる）などが存在する。

米国のように、広範かつ強力な規制権限を行政府（例えば内閣総理大臣等）に付与するということも考えられるが、我が国はより制度的に予測可能性を持ったアプローチを志向すると思われ、その点でより参考になるのは EU 型のアプローチであると筆者は考えている。

他方、EU においては、Data Governance Act のように一部のデータについてはより強固に、個人データと同様の仕組みで信頼を担保する枠組みを構築しつつある。我が国においても、このように、特に重要なデータを特定し、これについては相手先国の信頼を担保する等の制度を検討する余地もあるように思われる。

最後に、より根源的な問題として、すでに拙稿において指摘している点でもあるが、中長期的な GA に関するルール形成において重要と思われる点を二点、指摘しておきたい。

第一に、個人の自由と GA を理由とするデータ越境移転規制との関係である。個人データについては、自己情報コントロール権との関係からも明らかなように、仮に外国に GA のリスクがあるとしても、リスクを認識したうえでなお移転したいと本人が望む場合、それを否定することは理論的に困難かもしれない。しかし、例えばそのようなデータが移転先国で解析され、SNS 等を通じて日本の選挙への介入やフェイクニュースの拡散に用いられたりするとしたら、仮に本人が望んでいたとしても、特に高度なリスクを有する国への移転はなお制限されることを認めるべき、という議論もあり得るように思われる。今回の改正個人情報保護法においてはまずリスクの透明化に力点が置かれこのような検討にまでは踏み込まれなかったが、やがては射程に入れるべき議論であるように思われる。

---

[14] 脚注（2）の拙稿を参照。
[15] 総務省他「対内直接投資等に係る事前届出対象業種の追加」
（https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000105.html）

第二に、DFFT を実現することはあくまで手段であり、これを通じて実現すべき価値に関する、いわば哲学的な議論である。筆者の見解としては、特にガバメントアクセスは思想統制的な意味合いや不公正な競争につながるリスクが高く、民主主義や法の支配といった今日の基本的価値を維持・発展しつつ、公正な競争による経済発展をいかに志向していくか、という点が重要であると考えており、DFFT もこのような思想のもとに実現されるべきであると考えている。その 1 つの基盤は近時日本が推進する「自由で開かれたインド太平洋」構想に求めることもできるかもしれないが[16]、いずれにせよ、DFFT の先にある、実現すべき価値という本質的な議論もまた必要とされていると考えている。本稿が当初の目的を達成していれば幸いである。

以上

[16] 外務省資料（https://www.mofa.go.jp/mofaj/files/000430631.pdf）を参照。この点は藤井康次郎弁護士（西村あさひ法律事務所）との議論から示唆を得た。