国境を越えるデータ
～グローバルとローカルのせめぎ合い～

目　次

フェロー　隅山　正敏

要　約

Ⅰ．はじめに

国境の概念のない「データの行き来」において国境を人為的に設ける動きがある。

Ⅱ．データ移転を意識させた LINE 問題

LINE 事案は「外国にデータを移すこと」と「国内データに外国アクセスを許すこと」に対する懸念を明らかにした。特にガバメントアクセス（現地政府のデータ入手）が危惧された。

Ⅲ．国境を越えるデータの現状

個人ではネット利用者が発信側に回り、企業では製造業のサービス化やデジタル・トランスフォーメーションがデータの行き来を増やす。個人・企業のみならずモノ（IoT）もデータを生み出す。これらがもたらす経済成長や社会的課題の解決を最大化するためには「自由な行き来」が重要である。

Ⅳ．欧米のデータを巡る対立

欧米間では個人データを欧州から米国に移すプラットフォームが問題となった。個人データが国境を越えるとプライバシーを保護できないため、切れ目なく政策目的（プライバシー保護）を実現するためにデータに「国境」を設ける必要があるが、それは「貿易摩擦」をもたらすことにもなる。

Ⅴ．米中のデータを巡る対立

米中間では企業データ（企業秘密）を米国から中国に移すことが問題になった。矢面に立たされたのは政府との一体化を疑われた中国企業である。米国は中国へのデータ流出を阻止する（自国企業防衛）ために、中国は国内秩序を維持する（国家安全保障）ために、データに「国境」を設ける。

Ⅵ．国際間のデータを巡る対立

デジタル貿易を阻害する各国規制の撤廃や最小化を図る貿易交渉が行われている。データの移転や処理において「国境」を設ける規制の外に、デジタル商材の取扱いが争点になっている。

Ⅶ．おわりに

データを最大限に活用するためには「国境を越えた自由な行き来」が望ましい。他方で、データの行き来が国内規制に穴を開ける場合に、各国は「国境」を設ける。「国境」をなくすことは困難であり、それを「低くする」努力が、国にとっても企業にとっても現実的な対応となる。

Ⅰ．はじめに

インターネットが世界の隅々にまで張り巡らされ、その上を「データ」が自由に行き来している。物品やサービスが自由に行き来する「グローバリゼーション[1]」は、貿易交渉という人為的な努力を通じて初めて実現されたが、これら 2 者に比べて「データ」はそもそも国境のない、本来的に「グローバル」な存在である。かつ「データ」のもたらす付加価値を最大化する上では「国境を越える自由な行き来」を確保する必要がある。ところが、世界中を行き来する「データ」に「国境」を人為的に設ける動き（データ・ローカライゼーション）が生じている。欧州が「個人データの行き来」に国境を設けて欧米対立を引き起こし、米国が「企業データの行き来」に国境を設けて米中対立に繋がった。「データ」の活用を犠牲にしてまで「国境」を設けるのは何故か、どのような解決が志向されているのかという疑問を中心に置いて、データの行き来を巡るグローバルとローカルのせめぎ合いを概観する。

Ⅱ．データ移転を意識させた LINE 問題

インターネットを利用する際に、その上を「データ」が行き来することを考える機会は殆どない。しかし、2021 年 3 月に発覚した LINE 問題は、改めて「データの行き先」を考える契機となった。最初に、LINE 問題を通じて「国境を越えるデータ」の何が問題なのかを概観する。

１．個人情報保護法の改正

LINE 問題は、同社が改正個人情報保護法への対応を進める中で発覚した。事案の中身に入る前に、個人情報保護法改正の経緯を概観する。

個人情報保護法は、2003 年に制定された当初、データの移転を「第三者への提供」と位置付け、その第三者が国内に居るのか海外に居るのかを区別しないで、一律に規制していた（同意の取付け又はオプトアウト手続の設定)。しかし、欧州とのデータのやり取りを円滑に進める必要が生じた（下記「コラム１」参照）ことから、2015 年改正[2]において「外国にある第三者への提供」に関する独立した条文を設けた。そこでは、本人の同意を取り付ける際に「外国にある第三者への提供」であることを説明することを求めた。なお、わが国と同等の保護水準にある「国」又は所要の社内体制を整えている「事業者」に提供する場合に、個別同意の取付けを免除した。これらの要件を満たさない「国境を越えるデータ移転」は許容されないので、データ・ローカライゼーション措置の一種となる。LINE 社に話を戻すと、この改正への対応として利用規約を改定し、「自国と同等のデータ保護法制を持たない国に個人データを移転することがある」旨を追加した。

その後、データ保護に懸念をもたらす海外法制（下記３参照）が出現したことから、2020 年改正[3]では、本人同意を取り付ける際に「移転先の国の名称」や「移転先の国の個人情報保護制度に関する情報」などを提供することを義務付けた。

---

[1] グローバリゼーションは、国内市場の開放や国内企業の海外進出を指すことが多い。日本経済新聞での初出は 1986/06/21 付「新産業論(50)：成熟産業の新展開」である。

[2] 2015 年改正法は同年 9 月に成立し、2017 年 5 月に施行された。

[3] 2020 年改正法は同年 6 月に成立し、2022 年 4 月に施行された。

２．問題の発覚とその所在

2020 年改正法の施行（2022 年 4 月）に向けて LINE 社が準備を進める途上の 2021 年 3 月、個人情報管理の不備を指摘する報道[4]がなされた。報道自体は、中国所在の関連会社（業務委託先）の技術者が国内に保存された個人情報にアクセスできる状況にあったことを問題視したが、同社は、これに加えて、国内に保存された個人情報の一部を韓国に移転していたことも認めた[5]。問題になったのは、「外国から国内データにアクセスできること」と「外国に国内データを移転したこと」の 2 点であり、いずれも利用者説明が不十分であった点に問題がある（法令違反があった訳ではない）。これらの問題は、2020 年改正に向けて個人情報保護委員会が 2019 年 12 月に発表した「いわゆる 3 年ごと見直し制度改正大綱」において既に取り上げられていた。外国からのアクセスについては「外国政府による無制限なガバメントアクセスによって、我が国で取得され越境移転された個人データが不適切に利用されるおそれ」が、外国へのデータ移転については「データ・ローカライゼーション政策との関係から、本人による個人データの消去の請求に越境移転先の事業者が対応することができないおそれ」があるとする。

３．データ・ローカライゼーションとガバメントアクセス

わが国が個人情報保護法 2015 年改正において導入した「データ・ローカライゼーション措置」は、個人情報の保護を目的とするが、異なる目的で導入する国もある。例えば、中国は、近年整備したデータ 3 法[6]、すなわちサイバーセキュリティ法（ネット利用の規制、2016 年 11 月成立、翌年 6 月施行）、データセキュリティ法（データ利用企業の規制、2021 年 6 月成立、同年 9 月施行）及び個人情報保護法（2021 年 8 月成立、同年 11 月施行）においてデータ・ローカライゼーションに関する定めを置くが、その理由として「国家安全保障（国内秩序の維持）」が加わっている（詳細は下記Ⅴ－４参照）。

上記２に紹介する「最終報告書」は、データの行き来がもたらすリスクとして「ガバメントアクセス」を指摘する。ガバメントアクセスとは、外国政府が、自国の事業者に命令して、その取り扱うデータ（自国民以外の個人情報など）に自らアクセスすることである。政府命令に犯罪捜査などの正当な理由があり、かつ、裁判所の令状の取得など適正な手続を踏んでいるのであれば、それを受け入れざるを得ない。しかし、外国政府が権限を濫用する可能性も払拭できない。

例えば、中国は、ガバメントアクセスを広範に認める法制を整備している。国家安全保障の基本法である国家安全法[7]（2015 年 7 月成立・施行）77 条は、全ての国民・団体に対して「国家の安全に危害を及ぼす活動の手掛かりを報告すること」「国家安全機関等に協力すること」などを定める。国家情報活動（スパイ活動）の基本法である国家情報法[8]（2017 年 6 月成立・施行）7 条は、全ての国民・団体に対して当該活動への協力を義務付けている。サイバーセキュリティ法やデータセキュリティ法も、ガバメントアクセスに関する定めを置いている。なお、データ・ローカライゼーション措置は、自国内に留め置くデータを増やしてガバメントアクセスを拡張する意味合いを持つ。

---

[4] 朝日新聞「LINE の個人情報管理に不備、中国の委託先が接続可能」2021/03/17
[5] LINE「ユーザーの個人情報に関する一部報道について」2021/03/17
[6] データ 3 法の概要は経済産業省「2022 年版不公正貿易報告書」（2022/06）に詳しい。
[7] 国家安全法の和訳は岡村志嘉子「中国の新たな国家安全法制」国会図書館外国の立法 267 号（2016/03）。
[8] 国家情報法の和訳は岡村志嘉子「中国の国家情報法」国会図書館外国の立法 274 号（2017/12）。

Ⅲ．国境を越えるデータの現状

わが国政府が決定した成長戦略のうち「未来投資戦略 2018」（2018 年 6 月）は「データ駆動型社会」を副題に選んだ。そこでは「データ」を「デジタル新時代の価値の源泉」と位置付け、「経済社会システムの健全な発展」を図るために「一部の企業や国がデータの囲い込みや独占を図る『データ覇権主義』」を避けるべきだとする。本章では「データ」が価値創造に繋がっている現状を概観する。

１．個人が生み出すデータ

我々がインターネットを利用する都度、様々なデータが生まれる。例えば、検索エンジンを利用すれば、表示されたホームページに転移して「閲覧履歴」が生まれ、電子商取引を利用すれば、「閲覧履歴」に加えて注文データや決済データが生まれる。これらは第一世代のネット利用（Web 1.0）とされ、データの流れが一方向に止まり、利用者がデータ生成を意識することは少ない。これに対して第二世代のネット利用（Web 2.0[9]）は「双方向性」に特徴があり、利用者自らがメッセージを発信し、動画を投稿する。利用者が自己表現の欲求を満たし、場合により収入を得るという形で「付加価値」が生じている。一方、デジタル・プラットフォームの運営者は、世界中からこうした「データ」を収集・分析し、収入源となる事業（ターゲティング広告など）に投入し、「付加価値」を生み出す。

行き来する「データ」量が多くなればなるほど、創出される「付加価値」が大きくなるので、「個人が生み出すデータ」にとり「自由に行き来する」状態が望ましい。

２．企業が生み出すデータ

企業活動が国際化すると、経営資源（ヒト・モノ・カネ）も国境を越えて行き来するようになる。例えば、部品（モノ）を輸出して完成品を組み立て、要員（ヒト）を派遣して海外市場を開拓し、資金（カネ）を送金して現地工場を建設するといった具合である。近年は、行き来する経営資源の中で「データ」の重みが増している。また、製造業が製品を売り切るビジネスモデルから製品関連のサービスを提供するビジネスモデルに脱皮する（サービス化）局面でも、サービスに付加価値をもたらす要素として「データ」が重要になっている。投入する経営資源としても、収入を生み出す「付加価値の源泉」としても重要になった「企業が生み出すデータ」にとっても「自由に行き来する」状態が望ましい。

（１）企業活動の国際化

企業活動の国際化は、製造業を例にとると、①自国で製造した製品を外国で販売する（輸出）、②外国で製造した製品を外国で販売する（現地生産）、③部品調達・製造・販売の全てを外国で行う（サプライチェーン構築）といった段階を踏んで進められる。各段階において、日本から外国に製造データを送り、外国から日本に販売データを送るという形で「データの行き来」が生じる。また、社内で完結していた「データの行き来」が親子間のやり取り、更には現地企業とのやり取りに広がっていく。国境を越えて行き来する「データ」が、組織（供給網）全体の一体運営を支えている。

---

[9] Web 3.0 はプラットフォーム（中央一括処理）依存から脱却したネット利用であり、ブロックチェーンを用いて個人と個人が繋がり、取引するネット利用を言う。DeFi（分散型金融）が代表例である。

近年は、商品設計や市場調査など、幅広い業務をグローバルに展開する動き（バリューチェーン構築）も生じており、国境を越えて行き来する「データ」の幅も広がっている。これらのいずれにおいても、「データ」は収益を得るためのインプット（経営資源の投入）として用いられる。

（２）製造業のサービス化

製造業のサービス化の代表例は、2015 年頃に注目を集めた「MaaS: Mobility as a Service[10]」である。それまで「製品の売り切り」で終わらせていた製造業が「製品に関連するサービス」を提供して、販売後も収入を得るという動き（サービス化）は古くから観察される（売った製品の保守・修理サービス）。

2000 年代に入りサービスの多様化が進んでいる。これらを類型化[11]すると、第 1 に製品から得られる「便益」を切り離して提供する類型（便益分離型）がある。自動車メーカーが特定の「車」でなく乗換自由な「移動手段」を提供するサブスクリプションサービスなどである。支払う対価も「製品」に対するものでなく「サービス」に対するもの（定額課金）となる。第 2 に製品の「利用」の幅を広げる類型（利用拡張型）がある。情報端末メーカーがアプリストアを営むケースなどである。端末が普及すればアプリが売れ、売れるアプリが端末販売を後押しするという相乗効果に特徴がある。第 3 に製品を販売する際に「保守サービス」まで一括受託する類型（サービス一体型）がある。社内システムを構築する場合などに良く見られる。

サービスだけを切り出すと競合企業は多いが、製品と一体で提供できる「製造業」ならではの強みがある。製品に取り付けたセンサーから収集する「製品の使用状況に関するデータ」である。これを用いれば、サービス利用者が必要とする「便益」を予測し、その好みを予測して最適な「利用ソフト」を売り込み、実際の利用状況を分析して最適な「価格プラン」を提示し、製品の不具合を予測して稼働を止めることなく「保守」作業を終えることができる。これらのケースにおいて「データ」は付加価値の源泉として用いられる。

（３）デジタル・トランスフォーメーション

今やあらゆる企業の課題とされる「デジタル・トランスフォーメーション：DX」も、データの生成・利用の両面で「企業発のデータ」を急増させる。DX を理解する上では、国連開発計画によるデジタル化の分類（進化）[12]が参考になる。それによると、第 1 段階を Digitization（物質的な情報をデジタル化すること）、第 2 段階を Digitalization（デジタル化を通じたビジネスモデルの刷新）に区分する。その延長線上に DX を置くと、第 3 段階は「ビジネスモデル刷新に適合的な組織・文化の変革」と言えそうである。イノベーションの原動力として重視される「個人のアイデア」について考えてみると、全員が同じ目標に向かって突き進むのに適した「ヒエラルヒー」型の組織・文化を維持したままでイノベーションに取り組んでも、「個人のアイデア」をイノベーションの起爆剤に成長させ、更にビジネスモデルの

10 複数の交通手段を組み合わせて旅行者等に「移動サービス」を提供するものだが、本稿では、輸送機器メーカーから見た「MaaS」を取り上げる。

11 みずほコーポレート銀行・みずほ銀行産業調査部「サービス化の視点での企業の競争力強化に関する考察」（2013/05）は、課金サービス、アフターサービス、サービスプラットフォームの提供、サービスのクロスセルという 4 類型に分けるなど、他の分類方法も存在する。

12 DX については総務省「令和 3 年版情報通信白書」（2021/07）が詳しい。

刷新に繋げていくというプロセスの「途中」でいくつもの「障壁」に遭遇してしまう[13]。例えば「フラット」型の組織・文化に転換して「個人のアイデア」から「ビジネスモデル刷新」までの道筋を短縮するという取組みは、DX の一部を構成することになる。

３．モノが生み出すデータ

製造業が「製品の生み出すデータ」を自社のサービスに利用する事例は、あらゆる「モノ」がインターネットに繋がる「IoT: Internet of Things[14]」の一類型である。通信機器の小型化・低廉化とデータ処理技術（人工知能など）の進化がもたらした「IoT」は、近年、生み出されたデータを製品単体で利用するだけでなく、「製品群」の連携に用いるようになっている。居宅内の設備機器を連携して「快適な生活」を実現する「スマートハウス」が代表例である。そこでは、メーカー1 社が提供する設備機器を連携するだけでは不十分であり、企業間の連携やデータの開放性が重要になる[15]。なお、複数の製品の結節点となる「プラットフォーム」が寡占をもたらす[16]ことも懸念されている。

IoT の活用を産業政策に取り込んだのはドイツが最初である。ドイツ連邦政府は 2011 年 11 月に、IoT がもたらす生産性の向上を「第 4 次産業革命[17]（Industrie 4.0）」と名付け、中身の具体化と個別施策の展開を図っている。わが国でも「日本再興戦略 2016」（2016 年 6 月）の副題に用いられた。わが国では更に、IoT のもたらすインパクトは製造業に止まらず、社会全体の変容に繋がるという見方を採用し、「未来投資戦略 2018」（2018 年 6 月）の副題を「第 5 段階の社会[18]（Society 5.0）」に変えた。

いずれも「モノが生み出すデータ」を経済成長や社会変容に有用であると位置づけ、「自由に行き来する状態」を望ましいものとする。

４．小括

本章では「個人が生み出すデータ」、「企業が生み出すデータ」、「モノが生み出すデータ」に分けて、生成される「データ」量の増加傾向が続いており、それに比例して生み出される「付加価値」が大きくなっていることを概観した。データの活用においては「国境を越えて自由に行き来する状態」が最も望ましい。しかし、「自由に行き来するデータ」が副作用をもたらすこともある。次章以降で「自由な行き来」に対する規制の動向を概観する。

---

13 柳川範之「経済全体に DX を」（2021/03/16 付け日本経済新聞）は、伝統的な大企業が「意思決定の階層構造」や「社内の人事制度」を変える必要があるとする。

14 日本経済新聞での初出は 2013/03/28 付「人との境界溶ける、久多良木健氏に聞く」である。

15 越塚登「IoT の動向と今後の課題」（計測と制御 55 巻 12 号、2016/12）は「これまでのユビキタスの時代と近年の IoT の最大の違いは、得られたデータの開放性（オープン性）ではないか」（1025 頁）とする。

16 境野哲「IoT への期待と課題」（情報の科学と技術 67 巻 11 号、2017/11）は「モノの生産から流通・使用・修理・リサイクルまでの過程を（略）1 社で一元的に行えるようになる」（561 頁）とする。

17 蒸気機関の発明を受けた産業の勃興（第 1 次、18 世紀）、流れ作業による大量生産方式の確立（第 2 次、19 世紀初頭）、ICT を用いた生産の自動化（第 3 次、1990 年代）に続く生産性の革命が起きているとする。

18 技術による社会変容を狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に分け、IoT が新たな社会変容をもたらすとする。

Ⅳ．欧米のデータを巡る対立

欧州は、域内住民のプライバシーを保護することを目的として、個人データの行き来に「国境」を設けた。移転先の国が「欧州と同等の保護水準」にあれば「自由な行き来」を許容するという「緩やかな規制」であったにも拘わらず、米国がテロ対策として導入した「ガバメントアクセス」が障壁となり、2013 年から現在に至るまで「対立」が続いている。ただ、政府間の対立というより欧州内の対立（欧州委員会 vs 司法裁判所）に特徴がある。

１．プライバシーを重視する欧州

プライバシーを権利として捉える考え方は米国発祥[19]である。欧州は、第二次世界大戦中の蛮行を教訓として人権保障に注力してきたが、プライバシーに関する法的制度にあっては、コンピュータによるデータの大量処理が進んだ 1970 年代まで待つ必要があった。1970 年に独ヘッセン州で、1973 年にスウェーデンでデータ保護法が制定され[20]、各国もこれに追随した。1993 年 11 月に発足した欧州連合は、各国でばらばらに整備されたプライバシー保護法制を調整する必要に迫られ、1995 年 10 月に「データ保護指令[21]」を採択した（1998 年 10 月発効）。この指令は、各国法制の標準化だけでなく、域内から域外へのデータ移転に関する規定も含んでおり、欧米対立の起点となった。

（１）プライバシー保護と国境を越えるデータ

最初に、国境を越えるデータ移転がプライバシー保護に与える影響を概観する。各国法制は領土外に適用されないというのが原則であるので、個人データは、国境を越えた途端、自国内にあった場合と同じ保護を受けられるとは限らなくなる。自国民保護（プライバシー保護）を移転先でも確保しようとすると、自国の法律を外国でも適用する（域外適用）か、データ移転に国境を設ける（越境移転規制）かのいずれかを選ぶことになる。域外適用は、自国がいくら適用を主張しても、相手国での執行力を伴わないため、越境移転規制を基本としつつ域外適用で補足する国が多い。

（２）欧州データ保護指令

欧州委員会は、移転先の「国」が保護制度を有しているか、移転を受ける「企業」が保護体制を整備しているかのいずれかが満たされれば、自国民保護（プライバシー保護）を図ることができると考えた。そこで、外国企業への個人データの移転の禁止を原則としつつ、移転先の「国」が「十分な保護水準」にあるときは、その「国」に所在する全ての事業者に対する移転を包括的に許容し、そうでないときは、移転先の「企業」が「十分な社内体制」を約束したときに限って移転を個別に許容するという枠組みを整備した。企業の約束には、グループ企業間で用いられる「拘束的企業準則」やグループ外でも利用可能な「標準契約条項」などがあり、いずれも欧州委員会が認めたものを使用する。

---

[19] S. D. Warren and L. D. Brandeis, *"The Right to Privacy,"* Harvard Law Review Vol. 4 No. 5, 1890/12

[20] 宮下紘「プライバシーをめぐるアメリカとヨーロッパの衝突(1)」駿河台大学比較法文化 18 号（2010/03）134 頁

[21] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995/10/24)

この枠組みは、指令の後継である「一般データ保護規則（GDPR）[22]」（2016 年 4 月制定、2018 年 5 月発効）にも受け継がれた。

（３）セーフハーバー枠組み

データ保護指令制定当時、欧米間で既に大量のデータが行き交っていた。欧米の外交当局は、この現実を重く受け止めた上で交渉を開始した。両者は、米国当局（国務省）がセーフハーバー原則を定め、米国企業が原則遵守を宣言し、米国当局が宣言企業を公表するという米国サイドの枠組み（セーフハーバー枠組み）に基づいて、欧州当局（欧州委員会）が「十分な保護水準」を認定することを 2000 年 3 月に合意した。なお、欧州委員会による十分性の認定は同年 7 月に行われた。

ただ、「妥協」が垣間見られるセーフハーバー枠組みには当初から批判があったようである[23]。

２．テロ対策を強化する米国

米国の法制の整備は、欧州と同じく 1970 年代に入ってからで、1974 年プライバシー法（公的部門に対する規制）や分野毎の個別立法を順次整備していった。これらのプライバシーを「保護する制度」に問題はなかったが、プライバシーを「侵害する制度」（テロ捜査の強化）が、世界同時多発テロ（2001 年 9 月）を機に強化され、欧米対立の火種となった。

最初の「対立」は、米国が同年 11 月に自国を離発着する全ての航空会社に対して旅客情報（氏名、住所、性別、座席番号、決済記録など）の提供を義務付けたことが起点になった[24]。欧州の航空会社は、米国企業向けのセーフハーバー枠組みを利用できないことから、情報を提供すれば欧州法令に抵触し、提供しなければ米国規制に抵触するという「板挟み」状態に陥った。第 2 の「対立」は、米国がベルギーに本拠を置く国際銀行間通信協会（SWIFT）に対してテロ関係者の送金データの提供を依頼していたこと（2006 年 6 月発覚）から生じた[25]。欧州各国当局の連合体である 29 条作業部会は同年 11 月、SWIFT による提供がデータ保護指令違反になると指摘した[26]。いくつかの火種が燻る中で、スノーデン事件（2013 年 6 月）が新たな「対立」をもたらすことになる。

３．欧米の個人データを巡る対立

米国政府（国家安全保障局 : NSA）の契約社員であったスノーデン氏は、NSA がテロ対策として極秘に大量の個人データを収集していたことを 2013 年 6 月に暴露した。その中に大手ネット企業の保有する個人データにアクセスしてテロ情報を収集するプログラム（PRISM）が含まれていた。これを受けて、米国ネット企業が欧州域内の個人のデータを米国に移している現状に対する警戒が強まり、争いが司法の場に持ち込まれた。そして、行政（欧州委員会）がデータ移転を容認する決定を下し、これを司法（欧州司法裁判所）が無効とするという事態が繰り返されることになった。

---

[22] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2016/04/27)
[23] 宮下(2010)150 頁。識者は「アンセーフ・ハーバー」（安全でない避難港）と批判した。
[24] 宮下(2010)144 頁。両政府が協定を締結することで解決した。
[25] 宮下(2010)142 頁。欧州連合の批判は SWIFT に向けられ、欧米間の対立には至らなかった。
[26] Article 29 Data Protection Working Party, *"Press Release on Swift Case,"* 2006/11/23

（1）第 1 次シュレムス訴訟

オーストリア在住のシュレムス氏は、PRISM の監視対象とされた 5 社（Apple、Facebook、Skype、Microsoft、Yahoo）を相手取り、その拠点国（アイルランド、ルクセンブルク、ドイツ）の当局にデータ移転の停止を求める申立てを 2013 年 6 月に行った。そのうち Facebook を相手とするアイルランド当局への申立てが欧州司法裁判所に持ち込まれた。因みに、欧州の利用者は Facebook のアイルランド法人とサービス提供契約を、アイルランド法人は米国本社とデータ処理契約をそれぞれ締結しており、契約関係の上では、利用者データがアイルランドから米国に移転していることになる。

司法裁判所は 2015 年 10 月、セーフハーバー枠組みが無効であるとの決定[27]を下した。その理由として、①枠組みが米国当局に対する拘束力を持たない、②米国当局の介入に対して被害者が救済を求める手段がないという 2 点を指摘し、米国当局のアクセスを認めるにしても、その可否や範囲を決める客観的基準が必要であるとした。判決を受けて、29 条作業部会は同月、セーフハーバー枠組みに基づく移転の実務を 2016 年 1 月末までに是正するよう要求した。対象企業は約 4,500 社[28]であったとされる。

セーフハーバー枠組みに係る交渉（1998-2000 年）の時点でガバメントアクセス（特に犯罪捜査）の問題が顕在化しておらず、その点を交渉していなかった欧州委員会を責めるのは酷である。しかし、問題の発端がガバメントアクセスにある以上､裁判所としては交渉の不備を指摘するしかなかった｡ただ、米国においてガバメントアクセスに対する歯止めが不十分であるということになると、米国企業がいくら「プライバシー保護」を約束しても、移転を認めるべきでないことになる。この問題が第 2 次訴訟に繋がった。

（2）第 2 次シュレムス訴訟

第 1 次判決を受けて、Facebook はプライバシー保護を約束する「標準契約条項」方式に基づく移転に切り替え、原告（シュレムス氏）はそれに応じて申立書を差し替えた。申立てを受理したアイルランド当局は、標準契約条項方式の有効性に疑義を持った。一方、欧米両政府は、セーフハーバーに代わる枠組みを模索し、2016 年 2 月にプライバシーシールドという枠組み[29]に合意した。なお、欧州委員会による十分性の認定は同年 7 月に行われた。こうして、標準契約条項方式とプライバシーシールド枠組みという 2 つの有効性が再び司法の場に持ち込まれた。

司法裁判所は 2020 年 7 月、標準契約条項方式を有効とし、プライバシーシールド枠組みを無効とする決定[30]を下した。プライバシーシールド枠組みについては、米国の政府利用を制限していることを評価しつつも、①政府利用の必要性と基本権保護の必要性のバランス（比例原則）が分析されていない、②過剰な政府利用を抑止するオンブズパーソン制度に実効性がない、などの理由を挙げて無効とした。標準契約条項方式については、同方式に基づくデータ移転を有効としつつ、加盟国当局が移転先の国で十分な保護を受けられないと判断したときは移転の停止・禁止を命じることができるとした[31]。

---

[27] CJEU, *"The Court declares that the Commission's US Safe Harbour Decision is invalid,"* 2015/10/06
[28] 宮下紘「EU-US プライバシーシールド」慶應法学 36 号（2016/12）159 頁
[29] 宮下(2016)162 頁
[30] CJEU, *"The Court invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield,"* 2020/07/16
[31] 結局、有無効の判断を加盟国当局に委ねており、法的安定性に課題を残した。

第 2 次判決を受けて、アイルランド当局は 2020 年 8 月にデータ移転停止の暫定命令を発し[32]、対立は、現在に至るまで解決されていない。なお、欧州委員会は 2022 年 3 月に新たなプライバシー枠組みで米国と合意した旨[33]を発表している。

（３）欧米間の対立か欧州内の対立か

外形だけを見ると、欧州司法裁判所が米国プラットフォームによるデータ移転に「NO」を突き付けている。しかし、「NO」の理由付けを見ると、政府間合意に問題があったとするのでなく、欧州外交当局（欧州委員会）に検討不足があった点を指摘する。判決を見る限り、欧米間の対立というより欧州内の対立と捉える方が実態に即すことになる。他方で、ドイツやフランスにおける偽情報対策立法の制定過程[34]を見ると、政府の規制権限よりプライバシーを重視する姿勢が窺え、欧米間の「文化の違い」に遠因を求めることもできる。

本稿の主題との関係では、データの越境移転が「プライバシー保護」に穴を開けること、そのために越境移転規制が正当化され得ること、規制の要否の判断材料として「ガバメントアクセス」問題があることを指摘しておく。

《コラム１》日欧間の個人データ移転

わが国では、取材の自由を束縛するというメディアの反発を受けて、規制色を薄めた個人情報保護法が 2003 年に制定された。そうした生い立ちを受けて長年にわたり改正機運が盛り上がることはなかった。ところが、マイナンバー法制定（2013 年 5 月）を受けてその活用が課題となり、かつ、SUICA 情報販売問題[35]（同年 6 月）を受けてデータを活用するための条件を明確にする必要が生じたことから、最初は「データの利活用」の観点から改正作業が始まった。同時期に、欧州が一般データ保護規則（GDPR）制定に向けて議論を進めていたことから、欧州から十分性の認定を受けることが検討課題に加わった。10 年ぶりとなる 2015 年改正（2015 年 9 月成立、2017 年 5 月施行）は、様々な背景を受けて改正が多岐にわたる。その中には、欧州による認定を意識して、越境移転規制の導入のみならず、要配慮個人情報の導入、開示等請求の裁判上の行使の解禁、個人情報保護委員会の設置などが盛り込まれた。

法制の整備を受けて、個人情報保護委員会は 2016 年 7 月に EU との定期会合の開催を決定し、2017 年 7 月に対 EU の越境移転を可能とする手続を開始することを表明し、2018 年 7 月に欧州委員会と相互認定で合意した。相互認定は 2019 年 1 月に発効した。なお、日本企業のニーズは、従業員データに集中しており、グローバルな人事データベースの構築[36]に利用している。

---

[32] Wall Street Journal, *"Ireland to order Facebook to stop sending user data to US,"* 2020/09/09 など

[33] European Commission, *"Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework,"* 2022/03/25

[34] 2016 年米国大統領選で顕在化した偽情報問題について、ドイツはネットワーク執行法（2017 年 6 月）を、フランスは情報操作との闘いに関する法律（2018 年 12 月）を制定したが、プライバシーの観点から政府権限の面で譲歩を強いられた。

[35] 日立製作所が 2013 年 6 月に交通系 IC カード「SUICA」の利用履歴を用いたサービスについて公表したところ、匿名処理を実施しているにも拘らず、批判が殺到し、提供元である JR 東日本はデータ提供取り止めに追い込まれた。

[36] 個人情報保護委員会「日米欧における個人データの越境移転に関する実態調査報告書」2022/01/27

４．非個人データを巡る状況

非個人データの越境移転については、欧米共に産業振興の観点から肯定的に捉えている。ただ、欧州は、IoT 機器の製造者と利用者（欧州中小企業など）との較差の是正も重視し、法制面では「推進」を標榜しながら「制限」の方が目立っている。この構図は、個人データにおいてデータ主体（個人）を保護するために米国プラットフォーマーのデータ利用に制限を課している状況とパラレルである。

（１）非個人データ自由流通枠組み規則

欧州委員会は、加盟国の採用するデータ・ローカライゼーション措置が非個人データの利用の妨げになると考え、その撤廃を最初のターゲットとした。先ず、政策文書「デジタル単一市場戦略[37]」（2015 年 5 月）において、デジタル経済の振興を目標に掲げた上で、データ活用に係る技術的・法的障害を取り除く方針を打ち出した。続いて政策文書「データ経済の構築[38]」（2017 年 1 月）において、データの自由流通の阻害要因としてローカライゼーション措置の存在を指摘し、対応を進めることを表明した。それを受けた「非個人データ自由流通枠組み規則[39]」（2017 年 9 月提案、2018 年 11 月成立）は、加盟国に当該措置の撤廃を求めるものである。

（２）データガバナンス法

非個人データ利用の障壁を除去した欧州委員会は、利用推進に舵を切った。先ず、政策文書「欧州のデジタルの未来を形成する[40]」（2020 年 2 月）において、商品・サービスの開発に向けてデータを容易に利用し、簡単に処理することのできる「単一データ市場（欧州データ空間）」を構築することを表明した。その第 1 弾が「データガバナンス法[41]」（2020 年 11 月提案、未成立）である。同法は、公的データの開放とデータ共有サービスの推進を定める。公的データの開放では、個人情報の匿名化や企業秘密の削除などの措置を講じた上で、加盟各国に設ける 1 か所の窓口でデータを提供するという枠組みを定める（5 条）。また、公的データの域外移転について、知的財産権・機密保護の観点で「十分性」の認定を受けた外国への移転などを許容する。データ共有サービスについては、「推進」を標榜しながら「規制」の色合いが濃い。具体的には、サービス提供主体が他の事業を営むことを禁止し、データの用途にも制限（データ販売の禁止、自社製品への活用の禁止など）を加える（11 条）。サービス提供主体が外国法人である場合には、法定代理人の域内設置を義務付ける（10 条）。

（３）データ法

欧州委員会は 2022 年 2 月、「データ法[42]」を提案した（未成立）。データガバナンス法を補完するもの

---

37 European Commission, *"A Digital Single Market Strategy for Europe,"* 2015/05/06
38 European Commission, *"Building a European Data Economy,"* 2017/01/10
39 Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union
40 European Commission, *"Shaping Europe's Digital Future,"* 2020/02/19
41 European Commission, *"Data Governance Act: Commission proposes measures to boost data sharing and support European data spaces,"* 2020/11/25。データガバナンス法の解説は JETRO「欧州委、官民のデータ共有促進を目指すデータガバナンス法案発表」2020/12/01 に詳しい。
42 European Commission, *"Data Act: Commission proposes measures for a fair and innovative data economy,"* 2022/02/23。データ法の解説は JETRO「欧州委、産業データへのアクセスの包括的ルール定めたデータ法案発表」2022/02/28 に詳しい。

と位置付けられた同法は、「IoT」で用いられるネット接続機器とクラウドサービス（データ処理）を対象として弱者保護を図るものである。ネット接続機器については、データ利用における製造者優位を是正するために、機器の利用により生成されたデータについて機器利用者にアクセス権やデータ共有を決定する権利を付与する（4-5 条)。データの利用・アクセスに関する契約については、弱者保護のために不公正な条項を無効とする（13 条)。クラウドなどのデータ処理サービスについては、サービス提供者が市場を寡占する現状に鑑みて、他のサービスへの乗換えを阻害する技術的・法的な障害の除去を事業者に義務付ける（23 条)。事業者がデータ処理業務を他社から容易に引き継げるように「相互運用性」に関する定め（28 条）も設ける。現在規制のない「非個人データの越境移転」について、移転後のデータの取扱いが欧州法（知的財産権保護など）に抵触しないように、合理的措置の実施をデータ処理事業者に義務付ける（27 条)。

５．小括

個人データの移転を巡る「欧米間の対立」は、欧州が域内住民のプライバシー保護を「移転先」でも確保するために「移転規制」を導入したことから始まった。外国企業が勝手に個人データを持ち出して「国内規制」を反故にすることを許さないという意味で「正当な規制」である。他方で、米国がテロ対策のために導入した「ガバメントアクセス」も、米国にとっては「正当な規制」である。一方の規制が正しく、他方が誤りであるというシンプルな構図ではなく、両者の「均衡点」を見つけるしか解決方法はない。本稿の関係では、「正当な理由」に基づくデータ・ローカライゼーション措置があるという点を押さえる必要がある。

他方で、非個人データについては、公的データの海外移転（データガバナンス法 5 条）及びデータ処理事業者による海外移転（データ法 27 条）を規制する動きがある。こちらは、知的財産権保護や機密保護を目的とするものだが、やはり「データ・ローカライゼーション措置」に位置づけられよう。

Ⅴ．米中のデータを巡る対立

現在も続く米中対立の発端は、2018 年に遡る。米中対立の特徴は、政府と一体化した企業をターゲットとする点、当該企業が不当な活動を行う「リスク」を制裁理由とする点にある。想定されている「不当な活動」は、技術情報の窃取、中国製通信機器を入口としたサイバー攻撃や偽情報を用いた世論操作など「データ」を巡るものである。ただ、実際の活動内容を「実証」した上で制裁を発動している訳でない。制裁手段は、従来からある関税に止まらず、企業活動全般を「封じ込める」措置を講じている。

１．米国の危機意識

米国の対中政策は、国交樹立（1979 年）以降、「建設的関与」を基本としていたと言われる。中国の経済成長を手助けすれば、中国自身がその果実を増やそうとして、政治面での民主化・経済面での自由化を推し進めるという期待が背景にあった。しかし、対中貿易赤字の拡大、中国企業の台頭、軍事力の強化などを背景として、関与路線から対立路線に転換した。路線転換の背景には「米国企業の対中投資が中国を経済大国に押し上げたにも拘わらず、技術移転の強要、知的財産権の窃取などの形で米国企業

をいじめて中国の製造業の基盤を整え、軍事力を強化している[43]」という認識が存在する。こうした認識は、政権内部よりも米国議会に強いと言われる。

（1）下院インテリジェンス特別委員会報告書

米国議会の危機意識は、下院インテリジェンス委員会が 2012 年 10 月にとりまとめた「中国通信機器企業がもたらす国家安全保障問題に関する報告書[44]」に典型的に現れる。米国政府が中国の華為技術（Huawei）に対して米国企業から購入した資産を「自主的に」売却するよう勧告し、これを不服とした華為が調査を求め、米国議会が 2011 年 11 月に調査を乗り出した。報告書は、米国の通信システムを中国の政府系企業に過度に依存すると、スパイ活動に利用される懸念が高まるだけでなく、通信システムに繋がる重要インフラシステムに影響を与え、社会全体の破壊的混乱を引き起こすことが可能になることを指摘する。調査は、対象とする中国企業 2 社に質問を投げかけ、その回答を精査する形で進められた。中国企業が調査を要求したにも拘わらず、協力的な態度で臨まなかったこともあり、報告書は、「反証」がなかったことをもって「実証」されたものと取り扱い、一方的な断罪を行っている印象を受ける。

（2）USTR 知的財産権侵害報告書

米国通商代表部（USTR）は、大統領令（2017 年 8 月）を受けて調査を開始し、2018 年 3 月に「技術移転等に関する中国の法令・政策・慣行に関する報告書[45]」をまとめた。報告書は、中国政府が、①米国企業に対して技術・知的財産権を中国企業に移転するよう圧力をかける、②中国企業とのライセンス交渉等における交渉力を米国企業から奪う、③技術移転を目的とする中国企業による米国企業への投資・買収を指揮し介入する、④サイバー攻撃等による機密情報の窃取を支援するといった様々な「米国企業いじめ」を指摘した。議会が中国企業に対する聞き取りを行ったのに対し、USTR は中国に進出する米国企業に対する聞き取りを行って、報告書に仕立てた。報告書は、米国企業が中国政府に不信感を抱きながら中国進出を図っている様子を浮かび上がらせる。

2．米国における企業制裁の枠組み

米国議会は、多岐にわたる企業制裁手段を用意し、時の政権にその積極的な行使を求めている。政権が交代しても対中政策にぶれが生じない要因となっている。ただ、制裁手段の多様性は、制裁対象企業の拡大と相俟って、中国企業制裁の全体像を分かり難いものにしている。そこで、最初に制裁手段を整理しておく[46]。制裁手段は、企業の資金繰りを支える 3 つの活動、すなわち営業活動（製造と販売）、投資活動（企業買収と資産購入）、財務活動（資金調達）の全てを網羅しており、資金繰りを通じて企業の成長の阻止を狙っている。

---

[43] ペンス副大統領が 2018 年 10 月にハドソン研究所で行った演説。Hudson Institute, *"Vice President Mike Pence's Remarks on the Administration's Policy towards China,"* 2018/10/04。

[44] House Committee on Intelligence, *"Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZT,"* 2012/10/08

[45] USTR, *"Findings of Investigation into China's Acts, Policies and Practices related to Technology Transfer, Intellectual Property and Innovation,"* 2018/03/22

[46] 米国による中国企業制裁の詳細は CISTEC 事務局の一連のレポート（巻末）に詳しい。

（１）製品販売に関する制裁

中国企業がその製品を米国市場で販売することを制限する制裁がある。その第 1 は従来から存在する「関税」である。対中追加関税は 2018 年 7 月に開始された。第 2 は「政府調達からの排除」であり、2019 年国防権限法（2018 年 8 月成立）は中国製通信機器の政府機関による購入を禁止する。第 3 は「民間取引からの排除」であり、情報通信技術サービスの供給網の確保に関する大統領令（2019 年 5 月）は「敵対国」製の対象機器を一定の民間企業が購入することを禁止する。第 4 は「免許・認証の拒否」であり、事業免許の付与を拒否し、または国内販売に必要となる製品認証を停止することを通じて米国市場から締め出す。免許拒否は 2019 年 5 月に、認証停止は 2021 年 8 月にそれぞれ開始された。その他にも「中国産品輸入の禁止」などが行われている。

（２）製品製造に関する制裁

部品を海外から調達して製造した完成品を米国に輸出する中国企業に対し、部品調達に制限を加えることで「製造」を困難にしている。安全保障の観点から軍事転用が可能な民生品の輸出を規制する制度は、諸外国でも一般的だが、米国は、2019 年輸出管理改革法（国防権限法の一部として 2018 年 8 月成立）を通じて、この枠組みを企業制裁に転用した。その際、輸出管理の対象を定める「エンティティリスト」に中国企業の製品を追加する（2019 年 5 月開始）だけでなく、外国企業が「米国の技術を用いて米国外で製造した部品」を製造地から輸出することにまで米国制度を適用している（2020 年 5 月開始）。

（３）事業拡大（企業買収）に関する制裁

企業買収は、一般的には事業領域の拡大に用いられるが、中国が最先端の技術・知的財産権を自国に移転する手段として用いているというのが米国の見方である。そこで企業買収審査制度を技術移転の阻止に転用している。2019 年外国投資リスク審査現代化法（国防権限法の一部として 2018 年 8 月成立）は、出資先企業の支配権を握る「支配的な投資」だけでなく、機密情報へのアクセスを可能にする「非支配的な投資」までを政府による審査の対象に加え、また、重要技術への投資に事前届出を義務付けた。なお、買収審査は、審査機関である対米外国投資委員会（CFIUS）が買収承認の可否を勧告し、それを受けて大統領が買収禁止命令の要否を判断する仕組みになっている。トランプ政権は 2017 年 9 月以降、買収禁止命令・売却命令を積極的に出している[47]。

（４）資金調達に関する制裁

中国企業が米国証券市場を利用して成長資金を調達していることに着目し、「資金調達」を制限して企業成長を抑制している。当初は「中国軍に所有・管理されている中国企業」をリスト化して注意喚起を図る（2020 年 6 月）に留まったが、大統領令に基づく株式売買の禁止（2020 年 11 月）や株式保有の禁止（保有株式の売却の義務付け、2021 年 1 月）に広がっている。また、2020 年 12 月に外国企業説明責任法を成立させ、米国上場の外国企業に対して「外国政府の支配・管理下にないこと」を証明するこ

[47] 中国キャニオンブリッジ（投資ファンド）に対して半導体ラティス買収を禁止（2017/09）、ブロードコムに対して半導体クアルコム買収を禁止（2018/03）、北京中長石基信息に対して IT ステインタッチの売却を命令（2020/03）など。

とを義務付けた。同法は、元々は中国企業に頻発した不正会計に対処することを目的としていたが、「政府の手先となっている企業」を炙り出す道具として転用されている。従来、米国政府は企業制裁を正当化するために「企業と本国政府との関係」を立証する必要があったが、この立証責任を上場企業に転嫁するものでもある。

（５）小括

企業制裁手段の多様化の端緒になったのが 2018 年 8 月に成立した国防権限法である。同法は、政府調達の制限のみならず、従来から存在した輸出管理制度や企業買収審査制度を強化して、強力な制裁手段を政権に提供する役割を果たしている。外国企業説明責任法も、立証責任の転換を通じて企業制裁を容易にする。米国議会が時の政権（行政）に対して、立法を通じて企業制裁の手段を提供するという構図である。対中強硬姿勢は、トランプ政権が始めたと言われることが多いが、議会主導の面もあることを認識する必要がある。なお、本稿とは無関係だが、企業制裁を徹底するために「米国外での活動」にも規制を及ぼしており、わが国企業も対応を迫られている。

３．中国企業制裁の状況

米国が最初のターゲットに選んだのは、下院報告書で取り上げた「通信機器企業」である。米国の通信ネットワークに中国製機器を使用すると、そこを裏口（バックドア）としてネットワークに侵入し、サイバー攻撃や偽情報の拡散を通じて米国社会を混乱させることが可能になると懸念された。企業制裁を通じて「自国の通信ネットワーク」から中国を切り離すもので、その上を行き来する「データ」に「国境」を設ける効果も有する。なお、バイデン政権に交代した後も、対中強硬姿勢に変化は見られない。

（１）米国通信ネットワークからの排除

初期の企業制裁のターゲットは通信機器企業である。対イラン経済制裁への違反を理由に、中興通訊（ZTE）に対する輸出規制（2016 年 3 月）や華為技術（Huawei）に対する刑事責任追及（2019 年 1 月）と輸出規制（同年 5 月）が行われた。2019 年後半には無線機器の海能達通信（Hytera）、防犯カメラの杭州海康威視（HikVision）と浙江大華（Dahua）が制裁対象に加わり、5 社を対象とした制裁は、政府調達からの排除（2019 年 8 月）、輸出規制（同年 10 月）、民間取引からの排除（同年 11 月）、米国発の投資の注意喚起（2020 年 8 月）、製品認証の停止（2021 年 8 月）と続いた。

また、通信サービス企業については、中国移動による免許申請を却下した（2019 年 5 月）ことを皮切りに、既に下した免許を取り消す動き（2021 年 10 月中国電信、2022 年 1 月中国聯通、同年 3 月中国系 2 社）に繋がり、更に、製品認証の停止（2022 年 3 月）にまで及んでいる。

（２）個人データの移転の阻止

これらの企業制裁は「企業データ」の流出（窃取）を阻止するものだが、「個人データ」の流出を阻止するタイプの企業制裁が出現している。トランプ大統領は 2020 年 8 月、WeChat アプリの使用の禁止と、TikTok アプリの使用を含むバイトダンス社との取引の禁止を命じる大統領令を発した。中国政府が

民間企業の保有するデータに広範にアクセスできることから、こうしたアプリで収集された米国国民の個人データを利用してスパイ活動や偽情報キャンペーンを展開し、また、米国を訪問した中国国民の個人データを利用して米国での監視活動を展開するリスクがあるというのである。なお、米国が懸念する「中国のガバメントアクセス」について上記Ⅱ－３を参照されたい。

《コラム２》米中対立の多元性

近年の米中対立の起点は、USTR 知的財産権侵害報告書（上記１（２）参照）である。トランプ大統領（当時）は、報告書発表と同日（2018/03/22）に対中制裁の発動を決定し、追加関税の賦課に繋がった。起点となった USTR 報告書は、中国の軍民融合政策に焦点を当て、①産業振興が軍事力強化の目的をも持つ、②産業振興で外国技術を重視する、③それが「技術の窃取」などの行き過ぎを生むと分析する。ここに、軍事力抑止のために中国民間企業を制裁するという構図が生まれた。

制裁企業の拡大を「製品製造に関する制裁」で見ると、スーパーコンピュータ企業（2018 年 6 月）、原子力発電企業（同年 8 月）、監視機器企業（同年 10 月）、セキュリティソフト企業と人工知能技術企業（2020 年 5 月）、遺伝子解析企業（同年 7 月）、半導体製造受託企業とドローン製造企業（同年 12 月）、量子コンピューティング企業（2021 年 11 月）と続く。制裁企業の拡大は、軍事力の抑止と産業振興の阻止との境界を曖昧にし、米国が中国の産業政策である「中国製造 2025[48]」を狙い撃ちしているという見方をもたらした。また、監視機器企業と遺伝子解析企業に関する制裁理由は「新疆ウイグル自治区における人権侵害への加担」であり、軍事力と無関係な人権外交の要素も企業制裁に持ち込まれた。

企業制裁から離れても、中国の「一帯一路[49]」構想について、独自の経済圏を構築するものだと捉えて、インド太平洋構想で対抗する（経済安全保障）、自国の統治モデルを周辺国に輸出するものだと捉えて、中国共産党による中国支配を批判する（統治体制批判）という動きも生じている。このように、通商を巡る対立、価値観（人権など）を巡る対立、安全保障を巡る対立、統治モデルを巡る対立という様々な局面[50]で米中が対立しており、「多元的対立」と称される。

４．データを囲い込む中国

中国の国家統制は「データ」の世界に及んでいる。例えば、データ３法（上記Ⅱ－３参照）は、いずれもデータ・ローカライゼーションに関する定めを置いている。サイバーセキュリティ法（2016 年 11 月成立）は、重要情報インフラ運営者に対して、個人データと重要データを国内で保存すること及び国外移転時に安全評価を受けることを義務付け（37 条）、データセキュリティ法（2021 年 6 月成立）は、サイバーセキュリティ法 37 条に準拠することを明らかにする（31 条）。個人情報保護法（2021 年 8 月成立）は、国内保存義務と安全評価受検義務の対象に大規模個人情報処理者を加え（40 条）、それ以外の主体が国外に移転する際には安全評価の受検、公的認証の取得、標準契約の締結などを義務付ける（38

[48] 中国政府が 2015 年 5 月に発表した産業政策で、10 分野・23 品目に重点を置いて「世界の製造強国の仲間入り」を目指す。
[49] 習近平総書記が 2013 年 9 月に提唱した「シルクロード経済ベルト（一帯）」と同年 10 月に提唱した「21 世紀海上シルクロード（一路）」を統合した構想で、習総書記は 2014 年 11 月の APEC 首脳会談で統合後の構想を披露した。
[50] 舟津奈緒子「アメリカの対中政策からみる米中対立」日本国際問題研究所（2021/06）56 頁

条)。インターネットサービスにも監視の目を光らせており、水面下でソースコード開示を要求している。IBM が開示に応じる[51]一方で、Apple が拒否した[52]という報道が 2015 年前後になされている。

近年は、中国企業が海外で上場して現地の開示規制に服することを「データ流出」の観点から懸念するようになっている。例えば、配車サービスの滴滴出行が 2021 年 6 月、ニューヨーク証券取引所に上場したのに対し、中国政府は翌月に新規ユーザー登録の停止やアプリストアでの販売の禁止を命じ、米国上場廃止に追い込んだ[53]。また、2021 年 7 月に海外上場前にサイバーセキュリティ審査を義務付ける規制案を発表した。こうした動きについて「IPO 資料を通じた情報流出や外国企業説明責任法による監査情報・政府との関係に係る情報の流出を懸念したという指摘がある[54]」と紹介されている。

５．小括

米国は、「自国の通信ネットワーク」から中国を排除し、米国発の「データ」（技術情報など）と中国発の「データ」（サイバー攻撃、偽情報など）に「国境」を設ける。この「自国ネットワークの防衛」の動きは、米国以外にも広がっている[55]。一方、中国は、個人情報の保護や国家安全保障の確保など様々な理由からデータ・ローカライゼーション措置を講じ、こちらも「データ」に「国境」を設ける。米中対立が「民主体制 vs 強権体制」という根深い対立から発しているのだとすれば、「データの自由な行き来」への復帰を望むことは難しい。

Ⅵ．国際間のデータを巡る対立

多国間や二国間の貿易交渉においても「国境を越えるデータ」が議論されている。「国境を越えるデータ」が「デジタル貿易」を支えている[56]からである。デジタル貿易の定義は、世界的に確立されてはいないが、商取引における注文・発送・決済というプロセスのいずれかでデジタル処理が用いられていることに着目し、OECD 作業ペーパー[57]は「物品・サービスの貿易のうちデジタル化が可能にした処理を伴うもの」と定義し、「デジタル貿易は国境を越えるデータの行き来によって支えられている」とする。

１．デジタル貿易の制約要因

「デジタル貿易」は、物品を物理的に移動させる「配送」を除けば、「注文データ」や「決済データ」、更には取引対象である「デジタル商材（アプリ、音楽など）」が国境を行き来することにより貿易として成り立っている。冒頭で述べたとおり、「データ」の行き来に国境がないにも拘わらず、人為的に「障壁」を作る動きがあり、貿易拡大を阻害している。

---

51 PIIE, *"Should US Tech Companies Share Their Source Code with China?"* 2015/10/28
52 Reuters, *"Apple refused China request for source code in last two years,"* 2016/04/20
53 ペトロチャイナ、中国人寿保険など 5 社は 2022/08/12 に米国上場廃止を申請すると発表した。
54 CISTEC 事務局「中国ビジネスの安定性・前提を揺るがす米中の諸規制の一層の先鋭化」CISTEC Journal 195 号（2021/09）
55 次世代通信規格「5G」から華為（Huawei）製品を排除する動きは、オーストラリア（2018 年 8 月）とイギリス（2020 年 7 月）が公式に表明し、フランス・欧州連合（2020 年 7 月）も非公式に追随している。
56 貿易交渉は商取引を対象とし、データ移転（私人間のメール交換などが含まれる）そのものを取り上げることはない。
57 J. L. Gonzalez and M. Jouanjean, *"Digital Trade,"* OECD Trade Policy Papers No. 205, 2017/07

（１）データ移転に対する制約

第１の制約は、「データ移転」に国境を設ける「データ・ローカライゼーション」である。自国民の個人情報の保護を国外でも確保することを目的とする国があれば、自国の安全保障（国内秩序維持）の確保を目的とする国もある。経済産業省「2022 年版不公正貿易報告書」は、中国、インド、ベトナム、インドネシア、ロシア、欧州連合における措置の内容を紹介している。外国企業が「越境移転」を禁じられた場合、当該企業は関連データを「現地」に留め置くためにデータ保存用サーバーを現地に設置する必要が生じる。また、国境による「データの分断」はビッグデータの分析・利用を困難にする。該当する企業はビジネスモデルの見直しを余儀なくされる[58]。

（２）データ処理に対する制約

第２の制約は、「データ処理」を規制する動きで、①国内処理を義務付けるもの（コンピュータ関連設備の国内設置の義務付け）と、②処理内容の開示を義務付けるもの（ソースコード・アルゴリズムの開示の義務付け）とがある。なお、①は、国内で処理した後のデータの移転を制限するものではないが、移転制限とセットで扱われることが多い。①と②の制約は、移転規制と異なり、外国企業が国内市場に参入する際の要件として設定されることが多い。他方で、規制理由（自国民の保護や国家安全保障の確保など）は移転規制と共通である。

（３）デジタル商材の取扱い

貿易で取り扱われる「商材」は、従来から存在する物品・サービスに加えて、デジタル商材のウェイトが高まっている。アプリ・ゲーム・音楽・動画などである。デジタル商材に対してどの貿易原則を適用するのかも問題になっている。

世界各国が合意する貿易原則は、大きく物品の貿易に関するもの（関税と貿易に関する一般協定：GATT）とサービスの貿易に関するもの（サービス貿易に関する一般協定：GATS）とに分かれており、デジタル商材にいずれを適用するのか（モノを買ったのか、サービスを買ったのか）という問題である。

２．WTO 交渉

世界貿易機関（WTO）は、1998 年 5 月にグローバルな電子商取引に関する検討を開始してから今日に至るまで、デジタル貿易に関する議論を継続している[59]。加盟国の利害が対立して議論が行き詰まる中、2017 年 12 月から有志国で議論を牽引する動きが生じている。わが国は、2019 年 1 月の非公式閣僚会合で「信頼できる自由なデータ流通（Data Free Flow with Trust: DFFT）」を提唱し、データ移転とデータ処理の自由化を目指している。なお、DFFT は「プライバシーやセキュリティ・知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す、というコンセプト[60]」だとされる。

残るデジタル商品（例えば音楽配信サービス）に係る交渉では、これまでの取扱いと同じにすべきで

[58] WIRED「LinkedIn の中国撤退」2021/10/18、NHK「米ヤフー　中国からサービス撤退」2021/11/03 など。
[59] 経済産業省「2022 年版不公正貿易報告書」492 頁など
[60] IT 総合戦略本部「デジタル時代の新たな IT 政策大綱」（2019/06）

あるという点で一致するものの、これまでの取扱い（音楽 CD＝物品の提供と見るのか、放送＝サービスの提供と見るのか）に関する理解が異なっており、決着に至っていない。

３．EPA/FTA における取扱い

WTO を場とする多国間交渉の議論が行き詰まる中、二国間又は地域内の貿易協定（EPA/FTA）を締結する事例が世界的に広がっており、そうした協定の中でデータ移転・データ処理に係る規制の最小化を図る動きがある[61]。

例えば、アジア太平洋経済協力（APEC）は、企業に対して個人情報保護を求める「APEC プライバシーフレームワーク」を有しており、国境を越えてデータを行き来させる企業がフレームワークに準拠していることを認証する「越境プライバシールールシステム」を 2011 年 11 月に導入している。日米間の個人データの移転は、この認証システムを活用して行われている[62]。

もう一歩進んで、データ移転、コンピュータ関連設備の設置、ソースコード等の開示に関する定めを置く事例も出てきている。例えば、環太平洋パートナーシップ協定（TPP）は、データ移転（14･11 条）、設備設置（14･13 条）、ソースコード（14･17 条）に関する定めを置く。データ移転については、第 1 項で各国が規制上の要件を課すことを認め、第 2 項で事業を実施するための移転を原則として許可すると定める。ところが、第 3 項で公共政策目的に基づく第 2 項に適合しない措置を容認する。濫用の歯止めとして目的の正当性、差別的適用の禁止、過剰規制の排除を定めるものの、自由なデータ移転を完全に確保する訳ではない。他の条文もほぼ同様の構成をとる。

４．小括

貿易交渉においては、国内規制（各国の主権の行使）が貿易の障壁となる場合に、規制の撤廃もしくは最小化に向けて議論を進める。データの越境移転については、多国間においても二国間においても、公共目的に基づく規制を容認する。各国とも経済的には「国境を越えた自由な行き来」に期待を寄せつつ、「行き来を規制する権限（主権）」を手放すことはしない。したがって、交渉上の現実的な選択肢は「規制の最小化」となる。わが国の提唱する DFFT も、同様であろう。最小化に向けては、データ移転を規制する公共目的とは何か、その目的に照らして過剰な規制となってないかといった議論を深めて、「許容される最小限の規制」を明らかにする必要がある。

Ⅶ．おわりに

経済成長の推進や社会的課題の解決において存在感を増す「データ」は、本来的には世界の隅々にまで「自由に行き来する」ものである。ところが、その「性質」が国内規制に「穴」を開けるケースが生じる。「国境を越える自由な行き来」と「国内規制の徹底」という 2 つの価値が対立する局面において、データに「国境」が作られる。データの越境移転を規制する動きを一概に否定することはできない。

他方で、「国内規制の徹底」を常に優先する必要もない。例えば、自国産業の振興を目的とする規制で

[61] 城山英明「自由な越境データ流通と多様な公共政策目的の調整」日本国際問題研究所（2022/03）など
[62] 個人情報保護委員会と米商務省幹部との面談（2016/09/05）において APEC 越境プライバシールールシステムへの参加を促進することを確認した。

あれば、産業の成長度合いに応じて低減していくことが、その産業の国際的競争力に繋がっていく。したがって、データの越境移転を規制する場合であっても、規制目的が正当なものか、目的に照らして過剰に規制してないかなど、「規制の最小化」に努める余地はある。第Ⅵ章で概観した「貿易交渉における取組み」は、未だその途上にあるが、その「成果」がもたらす果実（経済成長・課題解決）は、加速度的に大きくなっている。

各国は、データの活用（グローバリゼーション）と国内規制の徹底（ローカライゼーション）という「矛盾」に挟まれながら揺れ動いている。データの「国境」を受け入れつつ「低い垣根」を目指すというのが現実的なスタンスである。企業も、データ利用者として「自由な行き来」を待ち望む立場にあるが、当面は現実的な「対応」を求められる。

注目度が高いとは言えない「データの越境移転」問題が経済・社会にもたらす「重み」を改めて認識したい。

＜参考文献等＞

第Ⅲ章
・JETRO「世界貿易投資報告 2020 年版」2020/08
・経済産業省「2022 年版通商白書」2022/06
・産業構造審議会情報経済小委員会「CPS によるデータ駆動型社会の到来を見据えた変革」2015/05
・永野博「インダストリー4.0 は何の革命か」情報管理 59 巻 3 号、2016/06
・増田貴司「なぜ製造業のサービス化が進んでいるのか」東レ経営研究所、2017/09
第Ⅳ章
・JETRO「ASEAN 主要国における個人情報保護規程」2021/07
・JETRO「EU デジタル政策の最新概要」2021/10
・経済産業省「データの越境移転に関する研究会報告書」2022/02
・島村智子「EU：非個人データの域内自由流通枠組みに関する規則」国会図書館外国の立法、2019/04
・鈴木將文「情報・データの法的保護を巡る諸問題」別冊パテント 23 号、2020/07
・須田祐子「データプライバシーを巡る米 EU 関係」成蹊大学一般研究報告 43 号、2010/03
・藤井昭夫「個人情報保護法制定過程に関する考察」日本大学政経研究 50 巻 2 号、2013/09
第Ⅴ章
・小野亮「FIRRMA・ECRA の成立と変容する米国の対中観」みずほレポート、2018/11
・関志雄「米中貿易摩擦の拡大化と長期化」RIETI 中国経済新論、2019/06
・安全保障貿易情報センター（CISTEC）一般サービス「米中の新輸出規制等の動向」の各記事
「米中の貿易関連等の諸規制の動向について」2019/09
「米中間の緊張に伴う諸規制の動向と留意点」2020/03
「米中関係等の緊迫化と諸規制の動向について」2020/06
「米中緊迫下における米国諸規制についての QA 風解説」2020/09
「米国の中国通信企業・中国企業製アプリへの規制・制裁に関する QA 風解説」2020/09

「中国企業製通信・監視関連機器等の米国政府調達禁止に関する QA 風解説」2020/09
「最近の米国の対中諸規制に関する QA 風解説」2020/11
「米国大統領選後に打ち出された米議会・政府による対中規制・政策について」2021/01
「米国新政権下における対中政策・規制をめぐる動向」2021/03
「バイデン政権発足後の米中の規制動向及び留意点に関する QA 風解説」2021/04
「先鋭度を増す米中の諸規制の動向と留意点」2021/07
「中国ビジネスの安定性・前提を揺るがす米中の諸規制の一層の先鋭化」2021/08
「米国・中国の経済安全保障関連規制の諸動向」2021/10
「米国・中国の経済安全保障関連規制の諸動向(2)」2021/12
「最近の米国・中国の経済安全保障関連規制の諸動向(3)」2022/07
・CISTEC「米国国防権限法 2019 の概要」2018/09