CFIEC
Center for International Economic Collaboration

ガバメントアクセスのルール形成：
個人データ・非個人データの国際流通の適正化に向けて

ガバメントアクセスと貿易ルールに関する検討会

報告書

（要約版）

2022 年 5 月 20 日

一般財団法人国際経済連携推進センター

概要

民間部門が保有するデータを政府が利用すること（ガバメントアクセス）が不適切に行われた場合、国際間のデータ流通の直接的な阻害要因となるとともに、データの利活用を支える個人や企業の信頼を損なうことになる。必要かつ有益なガバメントアクセスは否定されてはならないものの、その判断基準を明確にし、必要なルールを共有することが求められる。不十分、不明確、不適切なルール形成は、データに関連する事業の開発や維持拡大に悪影響を与える。

例えば、政府が民間部門のデータの管理方針に不適切に強制的な介入をすると、他の法的義務や契約、運用方針などの事由からくる安全管理措置や秘匿義務と相容れない対応を強いられることも想定される。また、ガバメントアクセスに正当性がある程度認められていても、民間部門の自発的なデータ提供の限度を超える過剰な要求が行われると、健全な事業活動や適切なデータの管理が困難になりかねない。国際間ではガバメントアクセスの適正範囲に関する判断基準や執行基準が国や地域間で異なることにより、民間部門におけるデータの取り扱いが分断化され、管理コストとリスクを共に増加させる。

日本の進める DFFT（信頼性のある自由なデータ流通）の概念は G7、G20、OECD などでの国際議論に良い影響を与えつつあり、その重要な要素としてガバメントアクセスについても言及が始まっている。国や地域の間で、適切なガバメントアクセスの範囲と条件について立場の違いから生じる国際間の摩擦を低減するために、準備段階として将来の適切な規律形成議論に資する要素（以下「規律要素」と記す）に従って、必要かつ正当なガバメントアクセスと不適切なものとの間の判断基準を共有するための議論を始めるべきである。

本報告書は、国際経済連携推進センター（CFIEC）内に設置された検討会での議論を取りまとめたものであるが、直接ガバメントアクセスのルール自体を提言するものではない。今後、議論が進むにつれて明らかになる規律要素の意義と必要性について、現時点での事実関係と考え方の整理を行うことを主眼とする。また、現在先行するガバメントアクセスの議論は個人データを対象としたものが中心であるが、個人データと非個人データの区別は絶対的なものではない。個人情報保護以外の観点、例えば、デジタル分野の通商面や経済を含む安全保障面、知財保護やデータ駆動型イノベーションなどへの配慮も同様に重要である。国際的なデータ流通を支えるという観点からは、個人非個人どちらか一方に限定しない包括的な視点が必要となる。また、複雑化する国際情勢の中では多様な観点が共存することを想定し、特定のイデオロギーや政体の違いを一方的に排除しない整理の仕方を取ることにも留意した。

ガバメントアクセスの実態は広範にわたる形態をとり、その中には個人情報保護法制の違いからくる正当性の認識議論、データの維持管理に関する国家主権のあり方の違いからくる懸念などが含まれる。既存の議論の対象を拡大し、個人情報だけではないより広い範囲での民間部門保有データに対するガバメントアクセスの分類については、議論の結果以下のような分類軸を想定することで、課題の抽出や規律要素の議論においてなるべく偏りが生じないように配慮できる。

ガバメントアクセスの分類

1. データの種類による分類：データの対象（個人か非個人か：一義的に決まらないことも含めて）、データの性質（例えば 3V、volume：量、variety：多様性、velocity：更新頻度）、データの価値（知的財産等）
2. 強制性による分類：罰則等を伴うかどうかにかかわらず強制によるものか、民間側からの任意、自主的な提供によるものか
3. データのライフサイクルによる分類：生じる課題がデータ取得時の行為に起因するものか、取得後の利用や該当する政府以外への提供、改変や削除の要求を想定したものか
4. データの流れによる分類：データ提供の流れが政府部門への直接の提供か、政府部門が指定する組織（特定の民間部門も含む）への提供を想定したものか
5. 課題の越境性による分類：該当する国・地域の内部に閉じた課題か、二箇所以上の国・地域をまたぐ要求からくる課題か
6. ガバメントアクセスの目的による分類：犯罪捜査、安全保障、国内産業振興、自国民の個人情報保護など、ガバメントアクセスにどのような目的が想定されるか

これらの 6 つの分類軸により、想定されるガバメントアクセスの課題の広がりについて認識が得られたが、特に、1. データの種類、2. 強制性、5. 越境性の 3 つの軸により、ガバメントアクセスの性質を特徴付けることができる。

この分類軸をもとに広範な事例を分析[1]し、既存のガバメントアクセスに関する議論を参考にしながらその範囲を拡大し、将来の適切なルール形成に求められる要素（規律要素）として

[1] 別添 1　ガバメントアクセスの事例集

14 項目[2]を示した。このうちの前半の 7 つは、既存の議論[3][4]を元に改めてその意味について議論を加えたもので、8 番目以降は今回の検討から追加されたものである。全項目を通じて意味の重複や包含を恐れず、将来の規律議論に資するために多くの論点を提示した。これらの規律要素は、無条件で議論の対象とされるべきではなく、目的に応じて対象候補あるいは網羅性の確認のためにのみ必要に応じて参照されることを想定している。

非個人データを含むガバメントアクセスで検討されるべき拡大された規律要素の例

1. 法的根拠（legal basis）：ガバメントアクセスが行われる国（要求する政府、要求される民間部門の保有データ所在国など）において、有効な法律上の拠り所があるべき
2. 目的の正当性と手段の必要性・比例性（meet legitimate aims and be carried out in a necessary and proportionate manner）：ガバメントアクセスの目的が正当であり、そのために取られた手段が必要かつその必要性に比例したものであるべき
3. 透明性（transparency）：特にデータを提供する民間部門側にとって、そのガバメントアクセスの内容とプロセスが明示的であるべき
4. 承認及び制約（approvals for and constraints）：ガバメントアクセスは承認を経たものであり範囲の制約を受けるべき
5. 制限（limitations）：データの最小限の取り扱いと維持について明確な制限を持つべき
6. 独立した監督（independent oversight）：独立した機関による監督及び承認を前提とすべき
7. 実効的な救済（effective redress）：違法または不適切なガバメントアクセスに異議を唱え救済を求めるための明確なメカニズムを持つべき
8. 公平性（impartiality）・無差別性（non-discrimination）：ガバメントアクセスの対象となる民間部門の選定に不公平や差別的な取り扱いは排除されているべき

---

[2] 別添２　個人・非個人データによらないガバメントアクセス規律要素

[3] OECD “Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy” (2020 December) https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm（2022 年 5 月 20 日閲覧）

[4] Global Privacy Assembly (GPA), “Adopted resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes”, 2021 October, https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf（2022 年 5 月 20 日閲覧）その他の既存議論については詳細版を参照。

9. 運用の一律性（uniformity）：ガバメントアクセスにかかる法制度の運用が恣意的にならず、一律な基準と方法で行われるべき
10. 公正性（fair and equitable treatment）：恣意的で不公正、不正義または特異なものでなく、人種、民族、文化、宗教、拠点・居住地、ジェンダーなど偏見や差別によらないものであるべき
11. 経済的合理性（economic rationality）：ガバメントアクセスの対象とされる民間部門あるいは社会全体に過度なコストや負担を強いるものではないこと
12. 補償（compensation）：ガバメントアクセスを受ける企業や経済的な影響を被った個人について、求めに応じて相当な補償が行われるべき
13. 責任制限（limitation of liability）：民間部門がガバメントアクセスに応じたことにより生じうるさまざまな責任について、該当する民間部門の責任は不問あるいは限定されるべき
14. 法の抵触（conflicts of law）：ガバメントアクセスの根拠となる法律に抵触する別の法制度が該当する国内外にあり、それらが矛盾・対立する場合は事前事後を問わず政府が調整の主体となるべき

報告書の中では、これら 14 項目の規律要素について一つ一つ分析を行い、判断基準を提示している。各規律要素の判断基準とは、該当するガバメントアクセスに理解が得られるための条件として、政府側に得られる何らかの保護法益と、いずれかの主体（個人や民間部門あるいは社会）の逸失利益を考えるための指標について考察したものである。また、該当する規律要素を組み込むことの意義、他の規律要素との関係、他の国際ルールとの関係についての分析を記している。

本報告は、政策立案者や企業実務者を想定読者として、国際的な議論の場において活用されることが期待される。「アクセス」の語の意味する範囲にも注意が必要で、単なる政府あるいは政府機関にだけ利用可能なデータの取得形態のみが問題となるのではなく、他者のアクセスの恣意的な制限や、データそのものの改変、改ざん要求や削除、隠蔽なども広い意味の「アクセス」の中に含めて議論する必要性も指摘された。

今後引き継がれるであろう、国際ルール形成の活動と並行して、WTO・知的所有権の貿易関連の側面に関する協定（TRIPS 協定）などの既存の国際ルールによる対処や、アクセスの

生じた国・地域の国内法に基づいて不当なガバメントアクセスに対処することも重要である。更に、ルール形成議論の基礎となるエビデンス収集として、ガバメントアクセスのもたらす経済的な負の影響等を定量的に調査分析することも求められる。

ガバメントアクセスが無制限に行き過ぎた場合、民間部門が保有するデータが政府及び政府機関により実効的に支配されることとなる。データの利活用と自由な流通に重要なことは、データガバナンスの主語が誰として考えるべきかである。ここでもマルチステークホルダーの理念を尊重し、政府、民間、データ主体のそれぞれの役割と権限を整理し、分担の明確化を通じて普遍的な理解として共有することが必要である。報告書に示した 14 項目の「規律要素」を参考にしながら、ガバメントアクセスがデジタル経済とイノベーションの健全な発展、社会的課題の解決に悪影響を及ぼさないようにしなければならない。

2022 年 5 月 20 日

一般財団法人国際経済連携推進センター

ガバメントアクセスと貿易ルールに関する検討会

委員　（所属は検討会開始当時のもの）

生貝　直人　一橋大学
石井夏生利　中央大学
板倉陽一郎　弁護士（ひかり総合法律事務所）
高倉　成男　明治大学
中谷　淳　　富士通・ＪＥＩＴＡ通商委員会委員長
根本　拓　　ＯＥＣＤ貿易・農業局
平見　健太　早稲田大学
山田　佑　　経済団体連合会
渡邉真理子　学習院大学

座長・進行役

横澤　誠　　国際経済連携推進センター

オブザーバー

経済産業省

別添 1（要約版）

ガバメントアクセスの事例集

将来の適切な規律形成議論に資する要素（規律要素）を抽出するために事例を収集し分析を行った。特徴的な事例について、主要な分類軸上の評価とともに以下に示す。記述については情報が提供された当時のものを基準としており、その後、法制度自体が改訂され、運用が変更となり問題が解消あるいは軽減された可能性のある事例を含む。また参照した報告者の観測に基づくものもあり、状況によって異なる観測も否定しない点もあるが、できる限り柔軟な視点で記述を加えている。

事例 1　中国：行政承認と引き換えの機密技術情報の開示要求
事例 2　中国：自動車収集データの越境移転の禁止
事例 3　中国：政府による国家安全保障目的の音声データ取得
事例 4　インド：非個人データ共有の義務化（高価値データセット作成と利用の枠組み）
事例 5　米 EU 間：ＥＵからの移転データに対する米国政府の監視等を目的としたアクセス（Schrems I/II 事件）
事例 6　米 EU 間：犯罪捜査に係る国外のデータ開示要求（Microsoft 事件・CLOUD 法）
事例 7　中国：国家情報法による政府の無制限のデータ取得の懸念
事例 8　シンガポール：COVID-19 感染対策アプリデータの犯罪捜査等への利用。

事例１　中国：行政承認と引き換えの機密技術情報の開示要求

中国政府が、国内市場へのアクセスと引き換えに、直接的または間接的に海外企業（特にハイテク産業）に技術移転を迫っていた事案である。

2018 年 3 月、米通商代表部（USTR）は、中国政府が海外企業の技術や知的財産を獲得することにより自国産業の高度化を図る目的のため、不公正・非合理・市場歪曲的な法令や慣行があることを調査した調査報告書[5]を公表した。これに基づき米国政府は関税の政策措置を発動した。

報告書では、中国政府が用いていた技術移転メカニズムの一つとして、必要な行政承認と引き換えの機密技術情報の開示要求を指摘している。ICT、製薬、化学、農業食品（特に遺伝子組み換え作物）、機械、金融サービスなど様々な業界の外国企業は、工場建設や工場建設や製品販売などの認可を得るために、政府機関に詳細な情報を提供しなくてはならなかった。こうした企業情報が現地産業に提供され、類似の産業活動に利用されたケースもあるという。また情報開示は政府だけでなく、当該外国企業と競合する利害関係者を含む可能性のある専門家パネル（政府、産業界、学界等で構成）による審査を通じて、第三者に提供される懸念があった。この専門家パネルによる審査要求は、企業が中国で事業を行うどの段階でも様々な業種で発生する可能性があった。USTR の改訂版報告書では、特に航空宇宙企業や化学企業などのハイテク産業は、技術移転の強い圧力に直面したと報告されている[6]。

米国政府は中国政府による差別的な取り扱いについて WTO の紛争処理機関に提訴している[7]。こうした諸外国の動きを受けて、中国では法改正を行い、2019 年の「外商投資法」では強制的な技術移転が禁止された。また 2021 年制定の「データ安全法」では、中国国内でのデータ処理活動を規範づけ、データ安全の保障、個人および組織の保護義務、罰則等を規定している[8]。

---

[5] The Office of the United States Trade Representative （USTR）, “Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974”, 2018 March.

[6] The Office of the United States Trade Representative （USTR）, ”Update Concerning China’s Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation”, 2018 November, p.23.

[7] *Ibid.*, p.5.

[8] 湯野基生「中国　データ安全法の制定」（『外国の立法』No.289-1，2021 年 10 月版）
https://dl.ndl.go.jp/view/download/digidepo_11767245_po_02890113.pdf?contentNo=1
（2022 年 3 月 24 日閲覧）

事例２　中国：自動車取集データの越境移動の禁止

中国政府が自動車収集データの越境移動を禁止している事案である。

中国では、2017 年にサイバーセキュリティ法、2021 年には、中国データ安全法と中国個人情報保護法が成立し、中国のデータ保護３法による体系が整った[9]。

これらを受けた関連細則が次々と制定される中で、自動車産業に対しては、2021 年 8 月に「自動車データのセキュリティ管理に関する一定の規定（試行）[10]」、10 月には「情報セキュリティ技術 自動車収集データに関するセキュリティ要件[11]」が公表された。この双方において、自動車データの越境移動が原則として禁止されており、データを越境する必要がある場合は、国家ネットワーク情報部門が実施するデータ越境セキュリティ評価に合格しなければならないとされている[12]。ここで該当する「自動車データと自動車データ処理者」が広範であり[13]、中国政府のデータ取得の範囲は、目的に反して広く設定され過ぎているといえる。また、日系自動車メーカーの生産や開発活動には支障が生じている。一方で、「自動車データのセキュリティ管理に関する一定の規定（試行）」（第 11 条）では、「中国が締約国である国際条約又は協定に異なる規定がある場合には、中国が留保すると宣言した規定を除き、当該国際条約又は協定が適用されるものとする。」としており、国際的な協定の有無によって、異なる取り扱いを行う可能性も示唆されている。

---

[9] データ保護３法の中国名称は記載順に次のとおりである。
「中华人民共和国网络安全法」「中华人民共和国数据安全法」「中华人民共和国个人信息保护法」

[10] 国家互联网信息办公室『汽车数据安全管理若干规定（试行）』（2021 年 8 月 16 日発表）
http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm
（日本語訳参考サイト：http://maruyama-mitsuhiko.cocolog-nifty.com/security/2021/08/post-fefed0.html?fbclid=IwAR1iu43oAGFGt8-MSFQ6A5JdgmbC2KS_vJLiCIBtaA1b1qiB05dTN3i51LE）（2022 年 3 月 24 日閲覧）

[11] 全国信息安全标准化技术委员会『信息安全技术 汽车采集数据的安全要求』（2021 年 10 月）
https://www.tc260.org.cn/file/2021-10-19/e5a87bcd-770f-4035-83dd-610e15a34096.pdf
（日本語訳参考サイト：http://maruyama-mitsuhiko.cocolog-nifty.com/security/2021/10/post-69a493.html）
（2022 年 3 月 24 日閲覧）

[12] 前掲註（9）（第 11 条）および、前掲註（10）（第 7 条）参照。

[13] 前掲註（9）「（第３条）本規定でいう自動車データには、個人情報に関わるデータ及び自動車の設計、生産、販売、使用、運用及び保守の過程における重要なデータが含まれる。……自動車データ処理者とは、自動車メーカー、部品・ソフトウェアサプライヤー、ディーラー、整備工場、旅行サービス会社など、自動車データ処理活動を行う組織を指す。……重要データとは、改ざん、破壊、漏洩、不正アクセス、不正利用された時点で、国家安全保障、公共の利益、個人または組織の正当な権利や利益を脅かす可能性があるデータを指す。」

事例３　中国：政府による国家安全保障目的の音声データ取得

中国が国家安全保障を目的として、国家規模の音声認証データベースを構築している事案である。

中国では、トップダウン的にデジタル戦略が推進されていると同時に、政府が資金面、政策面等、全面的に重点産業の民間企業を支援することで、官民一体型のイノベーションの創出を行っている[14][15]。2017 年 7 月、中国科学技術部等は「次世代人口知能（AI）発展計画」を策定。AI を活用したイノベーションの実現に向けて、４つの重点分野（①自動運転、②スマートシティ、③医療分野、④音声認識）を定め、分野ごとにけん引企業を選定した。

中国政府は政府の支援で大きく発展した AI 技術を活用し、テロ対策・治安維持等を目的とした国家規模の音声認証データベースを構築するために、個人の音声認証データ（生体認証データ）を収集している[16]。音声認識分野のけん引企業は、公安部の国家音声パターンデータベースの構築に協力し、通話から対象となる「声」を自動的に特定できる監視システムのパイロット版を開発しているという。また、新疆ウイグル自治区や安徽省の警察局が購入する音声パターン収集システムの指定サプライヤーでもある。中国の携帯電話向けの商用の音声合成および音声認識アプリを提供しているが、アプリから得られる大規模な音声データセットは、監視にも使われる可能性を含んでいる。企業が商業目的で収集した個人情報を公安部とどの程度共有しているかは不明であるが、関連する政府部門の要求に応じて、個人情報を開示することもあるとしている。

ヒューマン・ライツ・ウォッチの中国担当者は、2017 年のレポートにおいて、「中国政府は何万人もの人々の音声パターンを収集しているが、そのプログラムや、対象となる人々やその情報がどのように使用されるかを規制する法律については、ほとんど透明性がない」として、歯止めなき監視と政府批判者に対する報復行為が続く中国で、当局が簡単に収集したデータを悪用する可能性を指摘している。ただし、現在では、2021 年に「データ安全法」が制定され、ガバメントアクセスにかかるデータの取り扱いについて整備が進められている。

---

[14] 李　智慧「中国のデジタル強国戦略の形成と発展」（『海外投融資』2021 年 9 月号） pp.20-26. https://www.joi.or.jp/modules/news/index.php?page=article&storyid=462（2022 年 3 月 25 日閲覧）

[15] 株式会社三菱総合研究所「中国における人工知能の社会実装に向けた動向について」 https://www.soumu.go.jp/main_content/000483136.pdf（2022 年 4 月 4 日閲覧）
音声認識分野では、企業が国の蓄積する膨大かつ良質なデータを学習データとして活用し、音声認識技術を向上させてきたという。

[16] Human Rights Watch『中国：音声認証データの収集 プライバシーへの脅威　法のグレーゾーンで警察と AI 大手が協力』（2017 年 10 月）https://www.hrw.org/ja/news/2017/10/23/310343 （2022 年 3 月 25 日閲覧）

事例４　インド：非個人データ共有の義務化（高価値データセット作成と利用の枠組み）

インド政府より非個人データの共有を義務化する報告書が提出された事案である。

2020 年 12 月、インドの専門家委員会より、非個人データガバナンスの枠組みに関する報告書が提出された[17]。これは、非個人データを公共財とみなし、データが共有されることによってインド社会が最大の価値（特に経済的利益）を得られるようにする構想である。報告書では、データ保有団体に対して、非個人データの共有を義務化するという新しい枠組みが提示されている。

具体的には、非個人データに関するルールを統括する非個人データ機関（Non-personal Data Authority：NPDA）を設立する。その規制の中で、データトラスティは、データカストディアンからデータを収集し、高価値データセット（HVD）を作成・管理する。インドで登録した全ての組織は、データトラスティに HVD データを要求することができる。データトラスティはデータ処理等にかかる費用を賄うための手数料を徴収することができる。インド政府は、非個人データの共有と利用によって、データへのアクセスが制限されている新興企業等におけるイノベーションが促進されることを期待している。

一方、データ共有の義務化については、研究者や民間企業など関係者から批判も寄せられている[18]。第一の批判は、企業はデータ取集にコストがかかる一方で、何のインセンティブもなく無償でデータセットの共有が義務付けられる点である。第三者が使用するためのデータを準備することに対する補償や、データの価値に対する補償を検討する必要がある。また、第三者のデータ使用に起因する責任からの保護も必要である。第二に、匿名化されたデータは、非個人データになるのかという問題である[19]。データカストディアンは匿名化処理を施した上で、データトラスティにデータを提供するが、個人から収集されたデータソースが急増している現在では、匿名性の高いデータであっても個人を識別することが容易になってきている。第三に、大規模なデータセットを社会で共有することが、イノベーションの促進につながるということが既存の研究で証明されているわけではないということである。

---

[17] Ministry of Electronics and Information Technology-Government of India, “Report by the Committee of Experts on Non-Personal Data Governance Framework”, 2020.

[18] Jain, R., Pingali, V., “India’s non-personal data framework: a critique”, *CSI Transactions on ICT* 9, 2021, pp.171–183.

[19] NPD 報告書の提案された法令の範囲は、Personal Data Protection Bill,2019（PDP 法案 2019）で「個人データ」としてカバーされていないすべてのデータを対象としている。

こうした理由から、インドのNPDA設立は検討に値する新しいアイディアであるが、実行に移すには時期尚早であり、まず個人データ保護等への法整備や投資が必要という意見も出ている[20]。

事例５　米国：ＥＵからの移転データに対する米国政府の監視等を目的としたアクセス（Schrems Ⅰ/Ⅱ事件）

EUから米国へ移転された個人データが、米国政府機関による監視の対象となる懸念に関する事案である。

EUでは、1995年に「EUデータ保護指令[21]」が採択され、EU域外への個人情報のデータ移転について、基本的には欧州委員会がデータ移転先国について「十分性認定（adequacy decision）」をした場合にのみ認めていた。米国との間には「十分性認定」がなかったが、2000年に同等の保護を得るための枠組み「セーフハーバー協定」に合意し、米国商務省が認証した企業にのみ個人情報の移転が認められていた[22]。

しかし、2013年の「スノーデン事件」によって、米国家安全保障局（NSA）が米国内のIT企業が保有するデータを監視・収集していたことが発覚したのをきっかけに、オーストリア在住のSchrems氏は、米国へ移転された自らのFacebook上の個人データに対する保護が不十分だとして申立てを行った（Schrems I事件[23]）。2015年10月、EU司法裁判所は、米国への個人データ移転を特例として認める「セーフハーバー協定」を無効とする判断を下した[24]。その理由は、EUから移転されたデータが、国家安全保障、公益、法執行のために厳格に必要かつ比例原則に即した範囲を超えて米国政府機関によってアクセスされてしまう恐れがあると判

---

[20] Kapoor, A., Nanda, A., “Non-personal data sharing: Potential, pathways and problems”, *CSI Transactions on ICT* 9, 2021, pp. 165–169.

[21] Directive 95/46/EC of the European Paliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX：31995L0046（2022年3月24日閲覧）

[22] EU MAG「EU･米国間の新たな個人情報移転枠組みスタート」（Vol.54、2016年10月号）https://eumag.jp/behind/d1016/（2022年3月17日閲覧）

[23] Judgment of the Court （Grand Chamber） of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362（2022年3月17日確認）
解説は、宮下紘「EU-USプライバシーシールド」（『慶應法学』No.36、2016年12月）pp. 145-179. 参照。

[24] ICR - 情報通信総合研究所「欧州司法裁判所によるセーフハーバー協定無効判決について」（『InfoCom Law Report』2015年）https://www.icr.co.jp/newsletter/law20151008-fujii.html（2022年3月24日閲覧）

断されたからである。また、米国監視プログラムの下で行われる個人のデータの収集と追加処理に関して、自己データへのアクセス、修正、消去や、行政・司法上の救済を受ける機会がないとされた。

米国企業はセーフハーバー協定に基づくデータ移転ができなくなったため、標準契約条項（Standard Contractual Clauses（SCC））と拘束的企業準則（Binding Corporate Rules）が当面のデータ移転の根拠となったが、2016 年 7 月に新たな移転枠組みとして「プライバシー・シールド [25]」が欧州員会によって採択された。「プライバシー・シールド」では、EU 市民のデータを保護するより強力な措置を講じることが義務付けられ、米国の公的機関によるアクセスに対して制限と保護規定が設けられた。

しかし、このプライバシー・シールドや SCC に依拠してデータ移転する場合であっても、米国において十分に保護されない懸念があるとして、Schrems 氏は再び申立てを行った。その結果、2020 年 7 月、欧州司法裁判所はプライバシー・シールドの枠組みを無効とする判決を出した（Schrem II 事件 [26]）。この判断の理由として、（1）セーフハーバー協定と同様に、米国の国家安全保障、公益、法執行の必要性が、ＥＵ基本権憲章上保障されるデータ主体の基本権に優先することを認めるものであること [27]、（2）米国の諜報活動の根拠となる外国情報監視法（FISA）702 条と大統領令（E.O.12333）が、EU 法に基づく比例原則から生じる必要最小限の範囲に制限されていないこと [28]、（3）権利侵害時の苦情申し立て制度が十分でなく、データ主体に対して法的救済が保障されていないこと [29]などを挙げている [30]。一方、EU の一般データ保護規則（GDPR[31]）の枠組みにおける欧州委員会の標準契約条項（SCC）に関する

[25] Commission Implementing Decision （EU） 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield （notified under document C（2016） 4176）
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG（2022 年 3 月 17 日閲覧）

[26] Commissioner v. Facebook Ireland and Maximillian Schrems, Case C-311/18
https://curia.europa.eu/juris/document/document.jsf;jsessionid=48D66A2471F8C7EE1646CCD64E8CF7A2?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9718457（2022 年 3 月 17 日閲覧）

[27] *Ibid.*, pp.164-165.

[28] *Ibid.*, p.184.

[29] *Ibid.*, pp.191-192.

[30] 解説は、企業法務ナビ「プライバシーシールド（米国への十分性認定）無効判決の概要と影響 ～ EU 司法裁判所 Schrems II 事件判決 ～」（2020 年） https://www.corporate-legal.jp/news/3604（2022 年 3 月 24 日閲覧）参照。

[31] 日本貿易振興機構（JETRO）「EU 一般データ保護規則（GDPR）について」
https://www.jetro.go.jp/world/europe/eu/gdpr/（2022 年 3 月 17 日閲覧）

決定[32]は有効とした。SCC とは欧州委員会が認めたひな形条項による契約の締結であり、導入までのハードルが著しく高かったが、欧州委員会はプライバシー・シールドの無効判決を受けて、2021 年 6 月に SCC の改定[33]を行った。新たな SCC は、データ移転の幅広いシナリオに対応するものとなっており、データ処理の複雑なプロセスにも対応している。また、個人データの保護については、ＥＵ内と同等の保護を実現するための安全確保条項の規定を置き、データ移転国の政府によるデータアクセス要請を受けた場合などには、データ輸入者からデータ輸出者への通知などが必要となるなど、ガバメントアクセスによる個人データ侵害リスクにも備えている。

2020 年末の調査において、SCC は国際的なデータ転送の仕組みとして最も利用されており、特に欧州のあらゆるビジネスにとって重要なものとなっている[34]。

事例 6　米国：犯罪捜査にかかる国外のデータ開示要求（Microsoft 事件・CLOUD 法）

米国政府による国外に保存されたデータに対しての開示要求に関する事案である。

米国において、2018 年に Clarifying Lawful Overseas Use of Data Act（CLOUD 法）が制定される前は、電気通信サービスの等のプロバイダーに対するデータの開示手続き等を定めた Stored Communications Act（「SCA」18 U.S.C. § 2703）[35]等の法令上、米国の政府機関が、国外に保存されたデータの開示を明示的に認める規定はなかった。

2013 年、米国の捜査機関が Microsoft 社に電子メールの情報を提出するように求めたが、Microsoft 社は保存サーバがアイルランドにあることを理由に、海外に保管されている資料の開示を要求することは、SCA の違法な域外適用にあたると主張し、令状無効判決の申立てを行った。連邦地方裁判所はこの申立てを棄却したが、Microsoft 社が控訴すると、第 2 巡回区

[32] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council（notified under document C（2010） 593）
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087（2022 年 3 月 17 日閲覧）
[33] European Commission “European Commission adopts new tools for safe exchanges of personal data”, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847（2022 年 3 月 24 日閲覧）
[34] DIGITALEUROPE “Schrems II Impact Survey Report”, 2020.
[35] 18 U.S. Code Chapter 121 - Stored Wire And Electronic Communications And Transactional Records Access, https://www.law.cornell.edu/uscode/text/18/2703（2022 年 3 月 18 日確認）

連邦控訴裁判所は、SCA 法は米国国内に保管されているデータに対しての効力を有するとして、同社の主張を認めた（Microsoft 事件）[36]。

このような中、米国連邦議会は CLOUD 法[37]を制定して、SCA 法による令状が領土外に効力を有することを明確に規定し、Microsoft 事件は争訟性を喪失した。CLOUD 法は、米国政府が米国の司法権にあるプロバイダーに対して、国内外に保有しているデータの保存、バックアップ、開示を強制できることを明確化している[38]。

グローバルに事業を展開する通信サービスプロバイダー（CSP）は、複数の国の法令の適用を受ける可能性があり、ある政府によるデータ開示要求と、別の政府によるデータ開示制限の法的義務に矛盾が生じる可能性がある[39]。このような法の抵触問題は、「相互法的支援条約（MLAT）」という協定制度を利用して解決できる場合もあるが、データの取得に他国の裁判所や政府を介するため、手続きが複雑で長期間かかることが課題であった。CLOUD 法では、米国が法の支配の尊重など一定の基準を満たす他国と行政協定（executive agreement）を締結することを想定しており、両国は相手の政府を介さず直接的に CSP に電子データ提出の命令を出すことができるようになる。その際、米国法上の制限を解除し、法的対立をなくすことができる。

ただし、CLOUD 法による協定は、米国および外国の CSP に対して、相手国の政府の命令に応じる義務を課すものではなく、相手国の CSP に対して司法権を有することにもならない[40]。また、データの開示はテロを含む重大犯罪の防止、捜査等に関連する目的のみに限られ、法執行機関が電子データの開示を要求する前に、既存の米国法上の高い基準を満たす必要がある。さらに、データの開示を求められたプロバイダーは、開示に応じることで、協定締結国の法律に違反する重大なリスクを伴うと合理的に信じる場合、米国裁判所に 14 日以内に申立てを行うことができ、開示命令の修正または取消しを求めることが可能となっている[41]

---

[36] United States v. Microsoft Corp., 829 F.3d 197 （2nd Cir. 2018）

[37] 2018 年 3 月 23 日、2018 年連邦歳出法（Consolidated Appropriations Act 2018）の一部（DIVISION V）として制定された。

[38] CLOUD Act Sec.103（a）（1）, 18 U.S.C. Sec. 2713.

[39] U.S. Department of Justice “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act”, April 2019, pp.2-6.

[40] *Ibid.*, p5. 加えて、協定はどちらの政府に対しても、他方の政府が発した命令に企業が従うことを強制する義務を課すものではない。

[41] CLOUD Act Sec.103（b）, 18 U.S.C. Sec. 2703（h）.

CLOUD 法によって米国政府が日本企業にデータの開示を求める場合、日本国憲法やその他国内法（電気通信事業法、個人情報保護法等）に整合しないおそれがある。また、今後、日本が米国と行政協定を締結する場合には、捜査目的での越境データ取得が円滑になる反面、日本が締結している他の国際協定への影響について留意する必要がある。信頼性のある自由なデータ流通（DFFT）のコンセプトを実現し、データ主体を保護しつつ捜査への適切な協力を可能にしていく上で、様々な法的論点の検討が必要とされている[42]。

事例 7　中国：国家情報法に基づく政府の無制限のデータ取得の懸念

2017 年 6 月、中国で国家情報法が施行された[43]。同法の下で、国家情報機関が国内外で情報活動を行う際に、関係する機関・組織・個人に対して事実上無制限のガバメントアクセスを行う懸念が指摘された事案である。

国家情報法の第 7 条は、いかなる組織及び個人も法律に従って国家の情報活動に協力し、国の情報活動の秘密を守る義務を有し、国は情報活動に協力した組織及び個人を保護することを規定している[44]。

中国では 2015 年に国家安全法が施行されたが、同法第 2 条は、「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」の安全な状態を持続する能力を国家安全保障として捉えている[45]。

ここで定義される国家の安全が、一般的な経済の発展等を含む広範なものであることを前提とした上で国家情報法を考えると、例えば、諸外国にて通信機器を提供している中国企業は、法に基づいて情報提供義務を負い、同社製通信機器から取得されたデータについても中国政府に対する無制限の提供が義務付けられる可能性がある。そのため、国家情報法は自国民だけでなく、中国企業の製品を利用している諸外国の市民等に対しても個人／非個人データの取得が

---

[42] 西村高等法務研究所『「CLOUD Act（クラウド法）研究会」報告書―企業が保有するデータと捜査を巡る法的課題の検討と提言―』（2019 年 12 月）

[43] 岡村志嘉子（2017）「中国　国家情報法の制定」（『外国の立法』No.272-2，2017 年 8 月版）
https://dl.ndl.go.jp/view/download/digidepo_10404463_po_02720209.pdf?contentNo=1（2022 年 3 月 1 日閲覧）

[44] 全国人民代表大会「中华人民共和国国家情报法」（2018 年）
http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml（2022 年 3 月 1 日確認）

[45] 岡村志嘉子「中国　国家安全法の制定」（『外国の立法』No.264-2，2015 年 8 月版）
https://dl.ndl.go.jp/view/download/digidepo_9480563_po_02640209.pdf?contentNo=1（2022 年 3 月 1 日確認）

事実上可能となっている。米国では、国家安全保障上の懸念から、中国通信機器メーカーの認証を禁じる法案を成立させ、国内市場からの排除を強めている[46]。

事例８　シンガポール：COVID-19 接触追跡アプリデータの犯罪捜査への利用

シンガポール政府が、COVID-19 接触追跡アプリのデータを犯罪捜査に利用できると公表した事案である。

2020 年 3 月、シンガポールでは COVID-19 感染対策として、政府主導で開発した接触追跡アプリ「トレーストゥギャザー（TraceTogether）」の利用を開始した。2022 年 3 月現在、90%以上の人々がこのアプリをダウンロードしており[47]、ホテルや飲食店、ショッピングモール、オフィスビル、イベント会場など、多くの場所でアプリを使用した入場が義務付けられている[48]。

TraceTogether の仕組みは、Bluetooth を利用して匿名 ID を近接者と交換する方法である[49]。利用開始時には、ユーザー情報として携帯番号、身分証明情報を登録し、ランダムに生成される ID とともに安全なサーバに保管される。個人の位置情報が収集されることはなく、Bluetooth によって、一定時間ごとに更新される仮 ID を近距離のアプリを入れている端末同士で交換する。この匿名 ID データは各自の端末に保存されており、25 日間経過後に自動的に削除される。COVID-19 陽性になった場合にのみ保健省からデータ共有の要請があり、手動でアップロードを行う必要があるが、保健省のサーバにデータがアップロードされている場合を除いて、アプリ利用者は自身の識別データを削除するよう要求することができる。

アプリ運用を開始した当初のプライバシーポリシーは「保健省と共有される全ての Bluetooth データは COVID-19 の接触追跡にのみ使用される」としていた。しかし、2021 年 1 月にシンガポール政府高官が、「シンガポール警察は犯罪捜査のために TraceTogether を含むあらゆるデータを入手できる権限がある」ことを発表すると、接触追跡への参加が実質的に強制である

[46] 鳳山太成「米、中国製通信機器の排除法が成立　ファーウェイなど」『日本経済新聞』（2021 年 11 月 12 日）https://www.nikkei.com/article/DGXZQOGN120MP0S1A111C2000000/（2022 年 2 月 16 日確認）

[47] アプリのダウンロード以外に、TraceTogether のトークン（小型端末）を利用する方法もある。

[48] 在シンガポール日本国大使館『新型コロナウイルスの発生に関する注意喚起（その 43）』（2021 年 4 月）https://www.sg.emb-japan.go.jp/files/100182789.pdf（2022 年 3 月 23 日閲覧）

[49] TraceTogether Privacy Safeguards, https://www.tracetogether.gov.sg/common/privacystatement/index.html（2022 年 3 月 23 日閲覧）

こともふまえて、プライバシーの懸念から批判が寄せられた[50]。この公表後に TraceTogether のプライバシーポリシーは変更され、「COVID-19（臨時措置）法[51]に規定された重大な犯罪に関する捜査または刑事手続きにデータが必要な場合のみ例外となる」と追記されている。

シンガポール以外の国でも接触追跡アプリが運用されている国では、以前からプライバシーに関する懸念が指摘されている。

[50] MIT Technology Review『シンガポールの接触追跡アプリが方針転換、犯罪捜査でも利用可に』（2021 年 1 月）https://www.technologyreview.jp/s/230403/singapores-police-now-have-access-to-contact-tracing-data/（2022 年 3 月 23 日閲覧）

[51] COVID-19 （Temporary Measures） Act 2020 （No. 14 of 2020）, https://sso.agc.gov.sg/Act/COVID19TMA2020?ProvIds=P111-#P111-（2022 年 3 月 23 日閲覧）

別添２（要約版）

個人・非個人データによらないガバメントアクセス規律要素の検討

適切なガバメントアクセスの範囲の判断に求められる「規律要素」（将来の適切な規律形成議論に資する要素）について議論を行った。個人情報保護に関連する規律要素ついては先行する議論で公表された範囲の内容を踏まえつつ、新たな独自の解釈を加えて分析を行った結果を示している（項目１から７まで）。

また項目８以降は、個人データと非個人データの区別を意識せず、データ全般について対象となるガバメントアクセスの規律要素として議論しうるものとして追加された。

１．法的根拠（legal basis）

判断基準：個人データへのガバメントアクセスを強制する法的根拠が、アクセスを行う政府の側に存在すること。単にアクセスの根拠となる法令等が存在するだけではなく、その内容として実体的なデータ取扱いの根拠となる規定や、アクセスに向けた手続きが定められている必要がある。

意義と役割：政府側のデータの取り扱いに係る実体的な法的根拠を明確化することで、政府による恣意的な権限行使を抑止し、また手続きを規定することでアクセスを受ける企業や個人に対して予見可能性を向上させる。政府側のセーフガードが存在しない場合は委縮効果が生じる可能性があり、データ流通を阻害し得る。

他の規律要素との関係：実体的な内容については「必要性や比例性」が、手続的内容は「承認及び制約」（いずれも後述）の要素において規律されることが予定され、これらは本要素と一定の重複が生じうる。しかし、単に内容を問わず法令を整備することでガバメントアクセスが許容されると認識されることを避けるべきとの観点から、本要素においても内容に関するルールを入れ込んでいる。また、ともに予見可能性を担保するルールのため「透明性」との重複も生じることになるが、ここでは政府側の法的根拠を明示することで恣意的な権限行使の抑制に重点がおかれ、「透明性」はアクセスを受けるデータ主体の権利保障により重点が置かれている。

他の国際ルールとの関係性：強制処分について手続き等を法定すべきとの考え方については、例えば、市民的及び政治的権利に関する国際規約（ICCPR）第 9 条がそれを定めている。

２．目的の正当性と手段の必要性・比例性（meet legitimate aims and be carried out in a necessary and proportionate manner）

判断基準：目的の正当性については、ガバメントアクセスの目的が正当であること（正当性の判断基準は政治体制に依存しないものであるべき点は合意）。手段の必要性に関しては、ガバメントアクセスが政策目的の達成に対して貢献すること。かつ当該ガバメントアクセス以外による非侵害的な取り得る手段がないこと。目的と手段の比例性に関しては、ガバメントアクセスの目的と手段が均衡しており、達成される目的に比して結果（ないし権利利益の侵害の程度）が著しく不釣り合いでないこと。

意義と役割：本要素はガバメントアクセスが適切になされるための中核的な規定であり、目的が不当なものでないことを確保するとともに、仮に正当な目的であったとしても不必要に企業・個人の法的に保護された利益が侵害されることが無いように、その目的を達成するのに必要かつ合理的な範囲に企業・個人の権利侵害を留めるために必要とされる。

他の要素との関係：当初、「データ取得とガバメントアクセスの目的の実現の関係性が厳密に精査され合理的であること」を経済合理性として独立した要素としていたが、このような経済的合理性は、本要素に内包されうるとして統合した。

他の国際ルールとの関係性：目的の正当性・必要性は、通商ルールにおいて原則からの逸脱を審査する中核的な要素である（関税および貿易に関する一般協定（GATT）第 20 条、サービスの貿易に関する一般協定（GATS）第 14 条等の一般例外における議論を参照）。他方、比例性については WTO 協定では求められていない。

３．透明性（transparency）

判断基準：法的根拠となる法令等が公表されアクセス対象にとって利用可能であり、かつその内容が本ルールの諸要素が充足されているか否かを判断できる程度に詳細であるかどうかが判断となる。また、ガバメントアクセスに関する運用状況等（件数や増加減少傾向、内容の内訳）の政府による公表の積極性や、ガバメントアクセスの目的を妨げない範囲で、ガバメントアクセスがあったことがデータ主体等に通知されることも判断対象である。

意義と役割：アクセスされる企業・個人にとって、法令が公開され、その内容が、本ルールの諸要素が充足されているか否かを判断できる程度に詳細であることは、自らに対してどの程度のデータの公開が求められるか、どのような救済を受けられるかなどの重要な情報を知る機会を担保する不可欠の要素である。また、国家によるアクセス情報の公開は、その濫用の防止に向けた市民による監督等を提供する。データ主体等への通知は、データ主体が自らのデータに対するアクセスを知り、当該アクセスのガバメントアクセス諸要素への適合性や権利救済に向かう機会を保障するものである。

他の要素との関係：「法的根拠」との重複が指摘されたが、両者に重複があることを認めつつ、その差異について述べたため、4．1．1．の記載を参照されたい。
また、当初独立した要素としていた予見可能性とのすみわけについて議論があったが、本要素に統合された。ここでは、ルールの公表やそれに基づいてアクセスを受ける主体が、諸要素が充足されているか否かを判断できる程度に詳細にルールが定められ・公表されることが、予見可能性を担保していると整理している。

他の国際ルールとの関係性：GATT 第 10 条 1 項が、法令及び行政決定等について、「諸政府及び貿易業者が知ることができるような方法により、直ちに公表しなければならない」と定めている。

４．承認及び制約（approvals for and constraints）

判断基準：ガバメントアクセスを行うときの手続的要件が確立しており、その手続的要件の内容が個人の権利に対する侵害/介入の程度に見合うものであること。特に権利侵害の度合いが大きいときは独立の司法機関または行政機関による承認を得なければならないこと。

意義と役割：アクセスを実施する政府機関と独立した機関による承認があることなど適正手続きを規定することで、要素を充足しないガバメントアクセスによる企業・個人の権利利益の侵害を未然に防止する意義がある。
適正手続の担保によって権利利益の侵害から保護されることが明らかとなることで信頼を担保し、企業・個人にデータ流通を躊躇する不安を払しょくすることができる。

他の国際ルールとの関係性：適正手続きは自由権規約第 9 条が規定している。

５．制限（limitation）

判断基準：アクセスされたデータが特定され、当該目的内で取り扱われること（目的内利用）が必要。また、アクセスされたデータの保管について、機密性、完全性、利用可能性の保護措置があるかどうかが判断基準となる。

意義と役割：ガバメントアクセスによって収集されたデータが、承認及び制約によって特定された目的に沿って利用され、また適切な保護措置の元で保管されることを担保する意義がある。自らのデータが提供後も当初想定した範囲の中で適切に取り扱われることを担保することで、公的機関による恣意的なデータ利用を防止し、企業・個人の不安を払しょくすることでデータ流通を促す趣旨である。

他の国際ルールとの関係性：OECD プライバシーガイドラインの原則 4（利用制限）、5（安全保護）等が関連事項を規定している。

６．独立した監督（independent oversight）

判断基準：データのアクセス、利用、保管等について事後に独立した組織による監督がなされていること。

意義と役割：アクセスを実施する政府機関と独立した機関によってガバメントアクセスに関する諸要素が満たされているかが事後に監督され、要素を充足しない不当なガバメントアクセスによる企業・個人の権利侵害を事後的に発見して救済につなげる意義がある。権利利益侵害への事後的な保護を規定することで信頼を担保し、企業・個人の不安を払しょくし、データ流通の確保に貢献する。

他の国際ルールとの関係性：GDPR 等が独立した監督機関（データ保護監督機関（DPA）等）による監督を規定している。

７．実効的な救済（effective redress）

判断基準：上記のアクセス・利用・保管等の規律について、政府がそれに違反した場合にデータのアクセス対象・データ主体が実質的に利用できる、法的に拘束力のある救済があることが必要。救済としては権利利益に対する損害賠償も含まれうる。

意義と役割：不適切なガバメントアクセスを受けた企業・個人が、処分の取り消し等の適切な救済や補償を受けられる権利を確保できる。

他の要素との関係：「補償」との関係性について議論があった。詳細は後掲「補償」を参照。

他の国際ルールとの関係性：GATT 第 10 条 3 項は「各締約国は、特に、関税事項に関する行政上の措置をすみやかに審査し、及び是正するため、司法裁判所、調停裁判所若しくは行政裁判所又はそれらの訴訟手続を維持し、又はできる限りすみやかに設定しなければならない」と規定。また、自由権規約第 14 条も裁判を受ける権利を規定する。

８．公平性（impartial）・無差別性（non-discrimination）

判断基準：ガバメントアクセスが実施されることで、アクセス対象者に競争上の不利な影響（競争歪曲性）が生じないこと。

意義と役割：ガバメントアクセスが措置の内容（措置の構造・デザイン）や、その結果として競争歪曲を生じさせないことで、市場における内外国企業間又は外国企業間の競争条件の平等を確保する意義がある。競争歪曲が存在する場合、企業・個人がデータ収集のインセンティブを削がれる（自社データが競合他社に不当に流れることを恐れてデータ収集や移転を控える等）可能性があるため、それを防止する意義がある。

他の要素との関係：検討会では「運用の一律性」との重なりを含む関係が指摘された。本要素は、「ガバメントアクセスの制度や結果」つまり、措置の構造・デザイン自体がもたらす競争歪曲効果の防止、あるいは当該措置の適用される結果として生じる競争歪曲効果の防止に着目している一方、「運用の一律性」は、措置の運用過程の適切性に着目している。

他の国際ルールとの関係性：GATT をはじめとする国際通商法は無差別原則を規定する（GATT 第 1 条、第 3 条他）。

９．運用の一律性（uniformity）

判断基準：ガバメントアクセスの運用（過程）における一律性が担保されていること。GATT 第 10 条 3 項を念頭に置いたもので、法制度の運用の仕方が、ガバメントアクセスの判断基準となり得る。

意義と役割：ガバメントアクセスが競争歪曲効果をもたらすか否かとは別に、ガバメントアクセスにかかる法制度の運用の仕方が恣意的である場合（法制度の解釈適用が一律でない、公平でない等）、こうした不安定な法制度運用は、企業にとっての予測可能性を著しく害し、その結果、企業の経済活動を萎縮させかねない。とりわけ、外国市場においてかかるリスクが存在する場合、企業は当該市場へのデータ共有や移転を躊躇することとなり、国際的なデータフロー確保にも悪影響を及ぼす。こうした問題に対処すべく、ガバメントアクセスのもたらす競争歪曲効果とは別に、ガバメントアクセスの運用過程の適切性を規律するルールの必要性が指摘された。

他の要素との関係：前掲「公平性・無差別性」を参照。なお、ガバメントアクセスにかかる法制度の運用に関して、対象企業間でそれぞれ異なる解釈適用がなされているものの、競争歪曲効果が発生しているとまでは言えない事案の場合には、「公平性・無差別性」の要素ではなく、本要素において対処することが可能である。

他の国際ルールとの関係性：GATT 第 10 条 3 項（a）は「各締約国は、1 に掲げる種類のすべての法令、判決及び決定を一律の公平かつ合理的な方法で実施しなければならない。」と規定する。また、GATT 第 20 条柱書も同様の趣旨を規定する。

１０．公正性（fair and equitable treatment）

判断基準： 恣意的で不公正、不正義または特異なものでなく、人種、民族、文化、宗教、拠点・居住地、ジェンダーなど偏見や差別によらないものであるべき。

意義と役割：競争阻害性のみならず、偏見や不公正等、より幅広い要素を規律している。より広範な要素が規律されることで、データの取り扱いに係る信頼を担保し、データの流通を促進する意義がある。

他の要素との関係：「公平性・無差別性」との重なりについて、前者が競争阻害性に着目しているのに対して、本要素は不公正や偏見といったより広範な要素を規律している点で両者が区別される。

他の国際ルールとの関係性：公正衡平待遇（fair and equitable treatment）については、大半の投資保護協定において規定されている（NAFTA 第 1105 条）。

１１．経済的合理性（economic rationality）

判断基準：企業・個人にデータ提供に係る過度なコスト・負担を強いないこと。

意義と役割：アクセスを受ける企業・個人に対してデータ提供に関して過度なコスト・負担を強いないことで、当該企業・個人の事業の阻害や権利侵害等を防止する。また過度なコスト・負担を強いられるリスクを低減することで、当該リスクによって生じるデータの収集や移転に関する委縮効果を緩和し、データの流通を促進する意義がある。

他の要素との関係：検討会では「補償」との関係性が指摘された。「補償」と「経済的合理性」は、ガバメントアクセスは適法的である場合においても、企業や個人に過度な負担を課して経済的な損失を生じさせている場合には政府による手当を行うという点で、類似の要素内容であることが指摘された。

１２．補償（compensation）

判断基準：データの経済的価値の対価として、データ提供元の企業・個人に対して相当な補償を行うこと。ただし、補償により他の規律要素により制限される不適切なガバメントアクセスが認められる訳ではない。

意義と役割：財産的価値を持ったデータに対して、政府にその利用に対する対価を支払わせることで、財産権に対する補償と同様、企業や個人の利益への補填を行う趣旨である。このような補償がなされない場合、当該国におけるデータ収集のインセンティブが低下するとともに、内資企業にデータが共有される場合には安価にデータの利用が可能になるため競争阻害も生じる。結果として、事業者の事業展開が困難になり、データの流通自体が阻害されることとなるため、これを防止する意義がある。また、事業者の経済的利益が損なわれる（本来有償で売れるようなデータを無償で提供しなければいけなくなる）懸念を防止する意義もある。加えて、「相当な補償」の内容については議論があり、例えば常に補償を行う必要があるか（補償が不要となる場合もあるのではないか）といった要否の判断や、あるとしてどの程度の水準か（例えば、市場価格、要したコスト等）といった点についてはこの文言の解釈に委ねられている。

他の要素との関係：「実効的な救済」との関係性について以下の通りである。
「補償」は、適法的なガバメントアクセスであったとしても相当の補償がなされることを規定している一方、「実効的な救済」は、違法行為に対する損害の補填が想定されている、という指摘がなされた。

他の国際ルールとの関係性：国際慣習法上、企業・個人の財産等に対する政府による収用については、公共政策上の目的があり、無差別であり、かつ十分・実効的かつ迅速な補償を行うことが義務づけられている。また、EU ではデータ法の改正の中でも B2G データ共有の論点の 1 つとして補償が議論されている。

１３．責任制限（limitation of liability）

判断基準：データ提供者及び提出されたデータ内容に対する法的根拠による責任制限（提出データの信頼性・品質と、データ主体の権利侵害に対する責任制限）が存在すること。ただし、ガバメントアクセスの目的が責任を問わないと達成できない場合（課税のための適切な財務関連情報の提供など）についてはこの限りではない。

意義と役割：データの提供を行った企業・個人が政府のアクセスによって不当な責任を負わされることを回避する意義がある。
仮に上記の不当な責任を負わされるとすれば、事業者はデータを仲介（媒介）しない、あるいはデータを移転させないといった選択肢をとることとなり、データ流通が阻害されるため、このような事態を防止する意義が認められる。

他の国際ルールとの関係性：EU の B2G データシェアリング要素では、免責について「提出データの信頼性、品質に対する免責だけでなく、データ主体の権利を政府要求によって損なう形で提出することに対する免責（プロバイダ責任制限）が規定されている。

１４．法の抵触（conflicts of law）

判断基準：ガバメントアクセスから生じる法の抵触（他の法制度との矛盾）に対処するため、ガバメントアクセス実施国での法令遵守が、その国あるいは他国での法令違反とならないように、国内外法制度の矛盾・対立について問題提起し解決するメカニズムを構築すること。

意義と役割： ガバメントアクセスの根拠法に基づくデータ提供義務と自国他国の法令上のデータの第三者提供の禁止義務等が抵触する場合、その調整を企業・個人が行う負荷をあらかじめ軽減する意義がある。
仮にこのような法の抵触の問題を生じさせる法制度が存在する場合、企業が進出を躊躇する、抵触の結果事業展開が阻害されるなどの事業上の制約が生じ、それを回避するためにサーバー

の所在地を変更する、事業展開を断念する等の事態が生じうる。結果、データ流通を阻害することとなるため、それを回避する意義がある。

他の国際ルールとの関係性：EU のデータガバナンス法案は第 30 条国際アクセスにて、公的機関や企業・個人は、自らの保有するデータの越境移転が EU 法やその加盟国法との抵触が生じる場合、それを回避すべく可能なあらゆる技術的、法的並びに組織的な措置を取るべきことを規定している。この際、刑事共助条約に基づく場合や外国で適切な保護がなされる場合など、一定の条件が満たされる例外的な場合には、外国政府等の要請に基づいてデータを移転し得ることを規定している。