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

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データ主体や民間事業者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、政府が民間事業者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、民間事業者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、民間部事業者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、一般財団法人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：リアルタイム性）、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、民間事業者側からの任意、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への直接の提供か、政府が指定する組織（特定の民間事業者も含む）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 14 項目を示した。このうちの前半の 7 つは、2020 年 12 月の OECD の公開資料を基礎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、要求される民間事業者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事業者側にとって、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事業者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
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事業者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民間事業者や経済的な影響を被ったデータ主体について、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）
    民間事業者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、該当する民間事業者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（個人や民間事業者あるいは社会）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。

ガバメントアクセスに関する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、データ主体や民間事業者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、民間事業者、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[1]

[1] 本報告書は、2022年11月にCFIECが出版した『ガバメントアクセスと通商ルール：民間データへのアクセスの在り方』を元に改訂した。

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	ＪＥＩＴＡ通商委員会
根本　　拓	ＯＥＣＤ貿易・農業局
平見　健太	早稲田大学
山田　　佑	日本経済団体連合会
渡邉真理子	学習院大学

進行役

横澤　　誠	一般財団法人国際経済連携推進センター

オブザーバー

経済産業省

1. 検討会の問題意識と目的・検討方針

1. 1　検討会の問題意識

日本政府が提唱する Society 5.0 等の概念に明らかなように、データを活用したビジネスは今後の経済発展や社会課題の解決に不可欠である。その根幹であるデータ流通が阻害されると、デジタルトランスフォーメーションによって多くの産業が依拠するデータに基づくビジネスの実施が困難となり、幅広い産業に対して悪影響を与えうる。

上記の悪影響に対処する観点から、データ流通を促進する我が国の基本政策である「信頼性のある自由なデータ流通（DFFT）」は、プライバシー、知的財産権及びセキュリティに関する課題に対処することでデータの自由な流通を更に促進し、消費者及びビジネスの信頼を強化するという、「信頼」と「自由な流通」の相乗効果を提唱した概念である[2]。

民間保有データに対する公的機関からの不適切なアクセス（ガバメントアクセス）はプライバシー、知的財産権を侵害する危険性をはらみ、データ流通に対する「トラスト（信頼）」を損なうことでデータの自由流通を阻害する可能性があり、負の循環を発生させる。

現在のところ個人データと非個人データの双方を含むガバメントアクセスに関する国際的に合意されたルールはなく、経済協力開発機構（OECD）のデジタル経済政策委員会（CDEP）等において個人データに関する規律要素の検討が、報告書公表時においても進められている[3]。

しかし、個人データの性質はそもそも流動的で、完全に個人データ／非個人データを切り分けることはできない。個人データの定義自体も各国の個人情報保護制度によって異なりうるもので、企業にとってその区別は容易でない。例えば EU の一般データ保護規則（GDPR）では、ほとんどの情報をそれ単体として個人データとして扱わざるを得ないとの指摘もあるが、別の国では、個人データは匿名化によって非個人データとして扱われる。したがって、個人データだけでなく、非個人データへのガバメントアクセスも重要な課題である。

---

[2] 総務省「包括的データ戦略」（2021 年 6 月）p.50
https://www.soumu.go.jp/main_content/000756398.pdf（2022 年 8 月 22 日閲覧）

[3] OECD, “Government Access to Personal Data Held by the Private Sector: Statement by the OECD Committee on Digital Economy Policy”, December 2020, https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm, accessed 2022/08/22.

インドの非個人データガバナンス枠組みや、EU のデータガバナンス法（Data Governance Act）及びデータ法案（Data Act）、中国のデータ関連法（サイバーセキュリティ法、データ安全法）など、国家が非個人データを管理する法制度の動きも加速しており、非個人データに対するガバメントアクセスが国際的な合意のないままに進もうとしている。この点も上記の非個人データへのガバメントアクセスルールを議論する重要性を高めている。

現行の国際ルールの形成状況をみると、個人・非個人データ双方を含むガバメントアクセスルールを通商ルールとして定める事が有益と考えられる。上記の通りガバメントアクセスは国境を越えたビジネスに大きな影響を及ぼしうるが、国境を越えたモノやサービスの提供は世界貿易機関（WTO）諸協定が規律しており、DFFT 実現に向けた動きの 1 つとして WTO において電子商取引交渉が進展している。近時は自由貿易協定ないし経済連携協定（FTA/EPA）の電子商取引章等において、データの取り扱いルール（データの自由流通、サーバーの国内設置義務＜データローカライゼーション＞の禁止等）を含むデジタル貿易に関する規律が発展し、DFFT を促進するものとして位置づけられている。

したがって、国境を越えたビジネスに影響を及ぼしうるデータに関する国家行為の規律という観点に着目し、ガバメントアクセスについてもデジタル貿易規律の一環として、通商ルールの中に取り込む必要がある。

1．2　検討会の目的と検討の指針

本報告書は、一般財団法人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を基礎としているが、将来の通商ルール化に向けた基礎的検討として、自由なデータ流通を確保する、個人・非個人データ双方を対象としたガバメントアクセスの規律要素に関する考え方の提示を目的とした。また、その規律が民間事業者に対して意味を持つことがデータ主体の保護のためにも重要と考えた。

そのため、検討会では、①ガバメントアクセスの実態把握、②個人データと非個人データに求められる規律の乖離分析、③規律要素の判断基準議論、④非個人データ対象規律要素の過不足検討（追加・削除すべき要素の特定）、という 4 つのステップを踏み、ガバメントアクセスの規律要素に関する考え方を提示した。

検討の方針として、グローバルなルール形成を目指す観点から、特定の国家（例えば特定の政治体制を持つ国等）を一律に排除することがないようなルール形成を図ることとした。ま

た、通商ルール化を目指す観点から、特にビジネス上の支障を除去するための規律要素を盛り込むこととした。

2. ガバメントアクセスルール検討に向けた事例収集と分析

2. 1　分析対象とする事例の選定基準

規律要素の検討においては、個人や民間事業者の権利利益の保護と越境データ流通への悪影響の防止が重要となる。そのため、特にこれらに影響があると考えられたデータの種類、強制性、課題の越境性の 3 つを念頭に置くのが適切である。

- **データの種類**

  非個人データを含む規律要素を検討するという問題意識から、非個人データの検討が重要である。また、一般にデータの特性として言われる 3 つの V[4]もデータの特性を考える上で指針となる。つまり、データの量（Volume）、多様性（Variety）、リアルタイム性（Velocity）の性質が、アクセスを受ける個人や民間事業者の権利利益の侵害に異なる影響を与えうる。

  この観点からは、医薬品の試験データのような知財的価値の高い情報から、リアルタイムの自動車の走行情報、健康や売り上げ等の販売情報等などリアルタイム性を持つデータへのガバメントアクセス事例と、反対に定点観測的なデータに対するガバメントアクセス事例を探索することができた。

- **強制性**

  任意提供の場合は、権利利益の処分に個人やデータを提出する民間事業者の同意があるため侵害が問題となりにくいため、権利利益の侵害が問題となるのは、その強制・任意の区分が一様でないためである。ただし、強制の内実が多様であること、例えば法的な義務付けのほか、許認可と引き換えにしたデータ提供、任意でありつつその背後に強制処分が控えているものなどがあることに留意する必要がある。

[4] Marbella International University Centre, “The V’s of Big Data”, May 2020, https://miuc.org/vs-big-data/, accessed 2020/08/22.

後述の事例研究においては、法的な義務付けがあるもののほか、応じなかった場合に不利益が生じるなど事実上の強制力が生じている懸念があるもの、懸念が極めて弱い又はないもの（政府から任意の提出要請があったもの）等を選定した。

- **課題の越境性**

一つの国や地域に閉じた課題が生じることも多いが、越境データの自由な流通への影響を議論することが重要である。事実上、データ流通の制限が、超法規的に実施されているとの報道もある、海外における外国人を対象にした諜報活動について、その信頼性のある実態把握が困難であることも少なくない。

この基準により選定された事例の中には、外国からの移転データに対するアクセスがあるもののほか、その懸念が生じうるものが含まれる。さらに、ガバメントアクセスを行った国の所在も地政学的な特徴である。ビジネス促進につなげる観点から、ビジネスへの悪影響が指摘される新興国が行った事例と、国際的な議論では必ず言及される先進国（米国、EU）の事例を分析対象となりうる。

2．2　ガバメントアクセスの事例

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。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】国家情報法に基づく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 接触追跡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で、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付け、データ安全の保障、個人及び組織の保護義務、罰則等を規定している[8]。

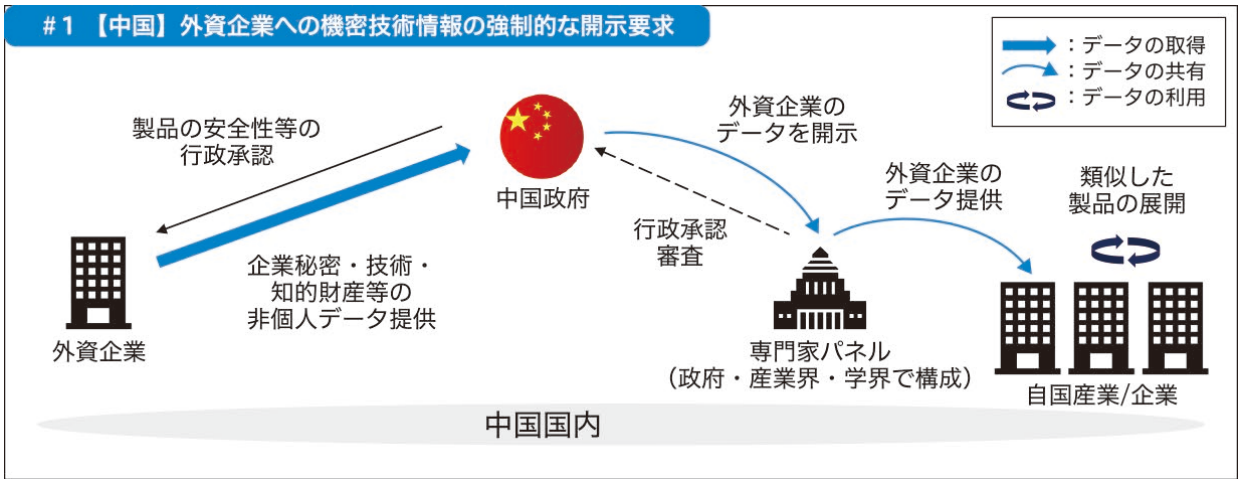
---

[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”, March 2018.

[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”, November 2018, 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 8 月 22 日閲覧）



出典：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," March 2018. を元に作成。

事例 2【中国】自動車収集データの越境移転の原則禁止

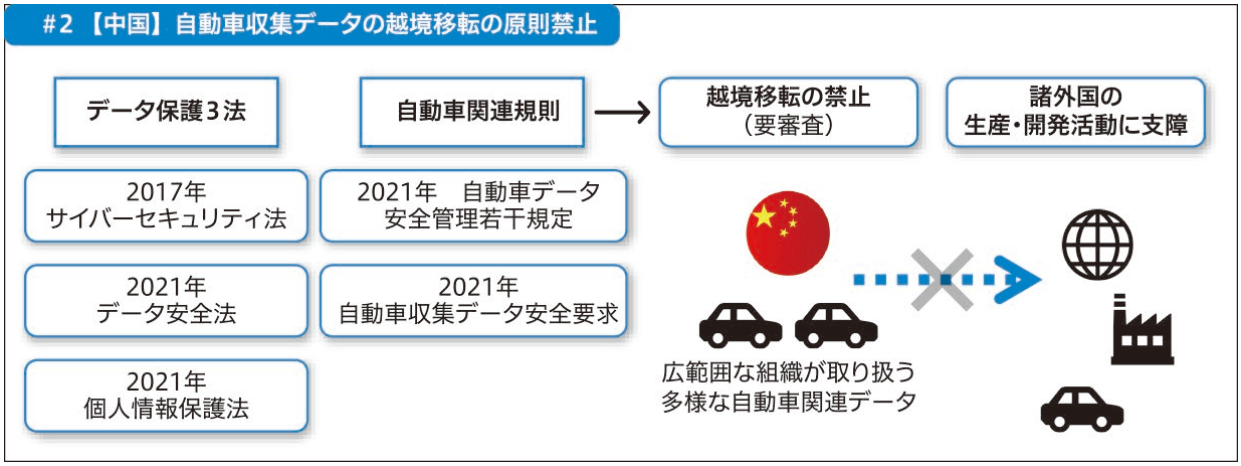
中国政府が自動車収集データの越境移転を禁止している事案である。

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転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

[9] データ保護 3 法の中国名称は記載順に次の通りである。
「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 8 月 22 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 8 月 22 日閲覧）

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。



出典：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）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)を元に作成。

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

[12] 前掲註（10）（第 11 条）及び、前掲註（11）（第 7 条）参照。

[13] 前掲註（10）「（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。」

行っている[14]。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。

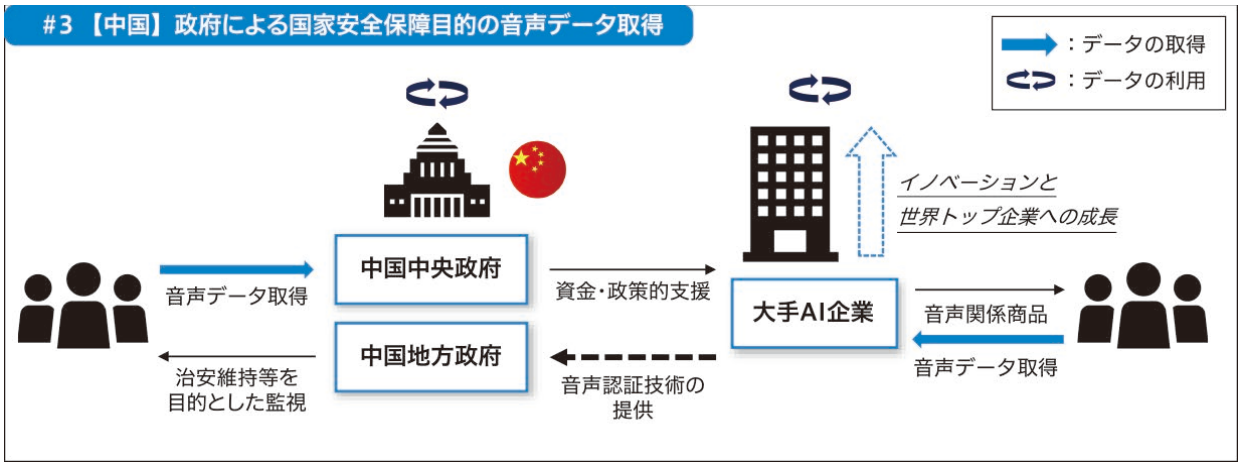
中国政府は政府の支援で大きく発展した AI 技術を活用し、テロ対策・治安維持等を目的とした国家規模の音声認証データベースを構築するために、個人の音声認証データ（生体認証データ）を収集していた[15]。音声認識分野のけん引企業は、公安部の国家音声パターンデータベースの構築に協力し、通話から対象となる「声」を自動的に特定できる監視システムのパイロット版を開発していたという。また、新疆ウイグル自治区や安徽省の警察局が購入する音声パターン収集システムの指定サプライヤーでもあった。中国の携帯電話向けの商用の音声合成および音声認識アプリを提供しているが、アプリから得られる大規模な音声データセットは、監視にも使われる可能性を含んでいた。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係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.；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 8 月 22 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。

[15] 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 8 月 22 日閲覧）



出典：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.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 8 月 22 日閲覧）を元に作成。

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。

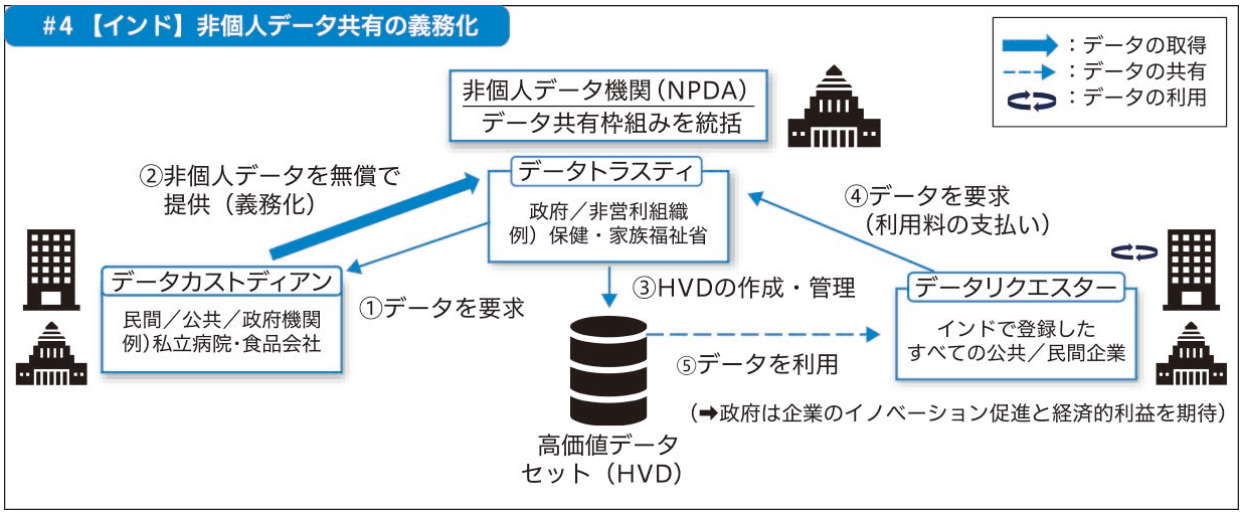
2020 年 12 月、インドの専門家委員会より、非個人データガバナンスの枠組みに関する報告書が提出された[16]。これは、非個人データを公共財とみなし、データが共有されることによってインド社会が最大の価値（特に経済的利益）を得られるようにする構想である。報告書では、データ保有団体に対して、非個人データの共有を義務化するという新しい枠組みが提示されている。

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。NPDA の管理下で、データトラスティ（Data trustee／データを信託される組織）は、データカストディアン（Data custodian／民間・公共・政府機関などデータを保有・管理する組織）が保有しているデータを収集し、高価値データセット（HVD）を作成・管理する。インドで登録したすべての組織は、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

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

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[17]。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がある[18]。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。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[19]。



出典：MEITY-Government of India, “Report by the Committee of Experts on Non-Personal Data Governance Framework”, 2020. を元に作成。

[17] Jain, R., Pingali, V., “India’s Non-Personal Data Framework: A Critique”, *CSI Transactions on ICT* 9, 2021, pp.171–183.

[18] 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。

[19] Kapoor, A., Nanda, A., “Non-Personal Data Sharing: Potential, Pathways and Problems”, *CSI Transactions on ICT* 9, 2021, pp. 165–169.

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[20]」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[21]。

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[22]）。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[23]。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・

---

[20] Directive 95/46/EC of the European Parliament 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.）

[21] 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 8 月 22 日閲覧）

[22] CJEU, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, 2015.
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。

[23] 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 8 月 22 日閲覧）

シールド[24]」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[25]）。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[26]、（2）米国の諜報活動の根拠となる外国情報監視法（FISA）第 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[27]、（3）権利侵害時の苦情申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などを挙げている[28]。一方、EU の一般データ保護規則（GDPR[29]）の枠組みにおける欧州委員会の標準契約条項（SCC）に関する決定[30]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[31]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

---

[24] 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）

[25] CJEU, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Case C-311/18, 2020.

[26] Ibid., pp.164,165.

[27] Ibid., p.184.

[28] Ibid., pp.191,192. 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 8 月 22 日閲覧）参照。

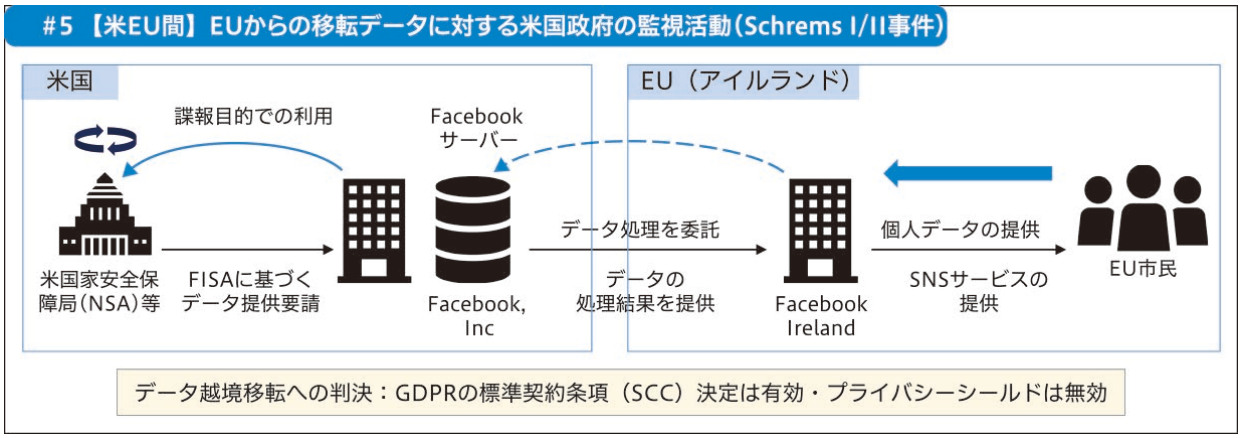
[29] 日本貿易振興機構（JETRO）「EU 一般データ保護規則（GDPR）について」 https://www.jetro.go.jp/world/europe/eu/gdpr/（2022 年 8 月 22 日閲覧）

[30] 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）

[31] European Commission, “European Commission Adopts New Tools for Safe Exchanges of Personal Data”, 2021,

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 は国際的なデータ移転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 [32]。



出典：CJEU, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Case C-311/18, 2020. を元に作成。

事例 6【米国】犯罪捜査に係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）[33]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 社は保存サーバー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

[32] DIGITALEUROPE, “Schrems II Impact Survey Report”, 2020.

[33] 18 U.S. Code Chapter 121 §2703 - Required Disclosure of Customer Communications or Records.

区連邦控訴裁判所は、SCA 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）[34]。

このような中、米国連邦議会は CLOUD 法[35]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[36]。

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[37]。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、米国及び外国の 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[38]。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、開示命令の修正又は取消しを求めることが可能となっている[39]

---

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

[35] 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。

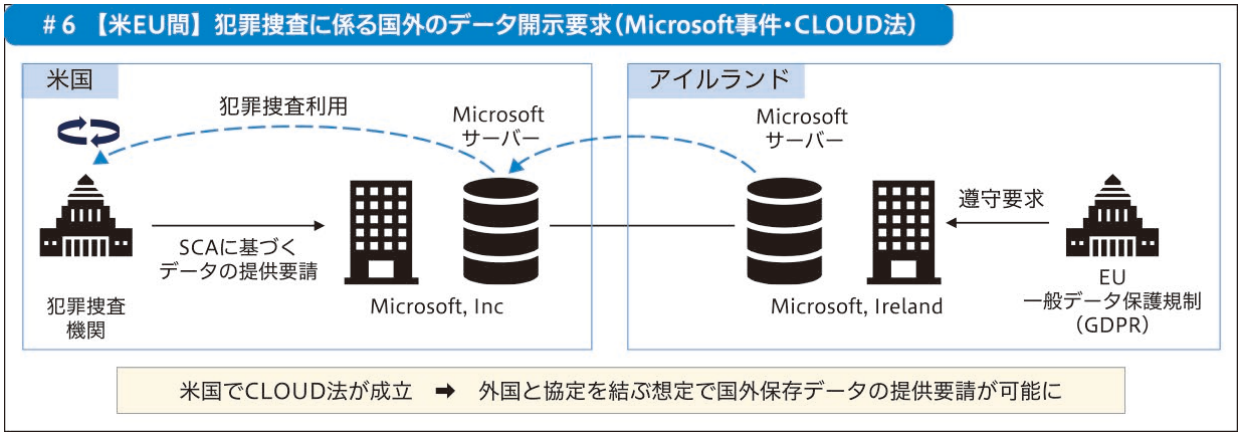
[36] CLOUD Act Sec.3(a)(1), 18 U.S.C. Sec. 2713.

[37] 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.

[38] 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。

[39] CLOUD Act Sec.3(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[40]。



出典：United States v. Microsoft Corp., 829 F.3d 197 (2nd Cir. 2018). 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”, 2019. を元に作成。

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[41]。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[42]。

---

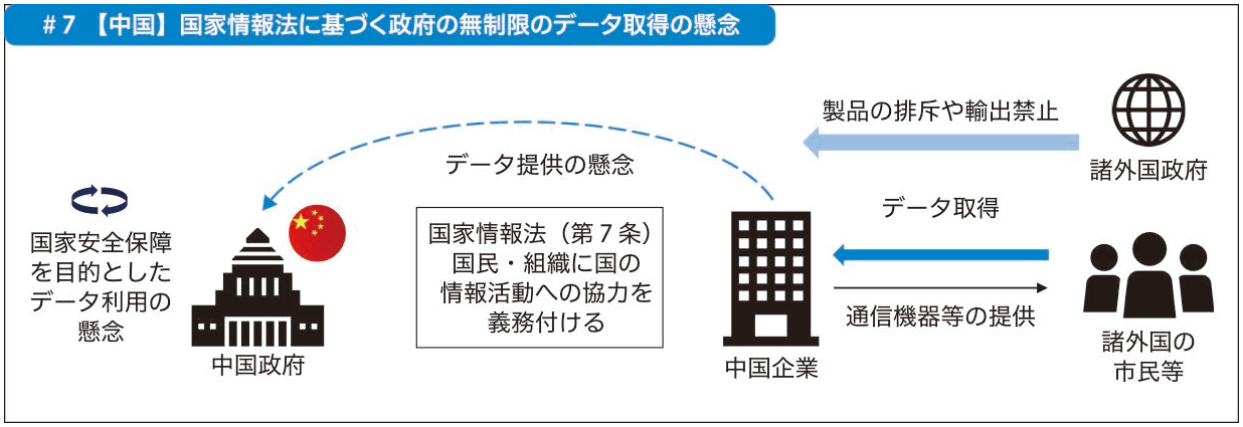
[40] 西村高等法務研究所『「CLOUD Act（クラウド法）研究会」報告書―企業が保有するデータと捜査を巡る法的課題の検討と提言―』（2019 年 12 月）

[41] 岡村志嘉子「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 8 月 22 日閲覧）

[42] 全国人民代表大会「中华人民共和国国家情报法」（2018 年）

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 [43]。

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 [44]。



出典：岡村志嘉子「中国　国家情報法の制定」（『外国の立法』No.272-2，2017 年 8 月版）、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）を元に作成。

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、

[43] 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 8 月 22 日閲覧）
[44] 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 8 月 22 日閲覧）

90%以上の人々がこのアプリをダウンロードしており[45]、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[46]。

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[47]。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ーに保管される。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、保健省のサーバー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すべての 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、接触追跡アプリへの参加が実質的に強制であることも踏まえて、プライバシーの懸念から批判が寄せられた[48]。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[49]に規定された重大な犯罪に関する捜査又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。

---

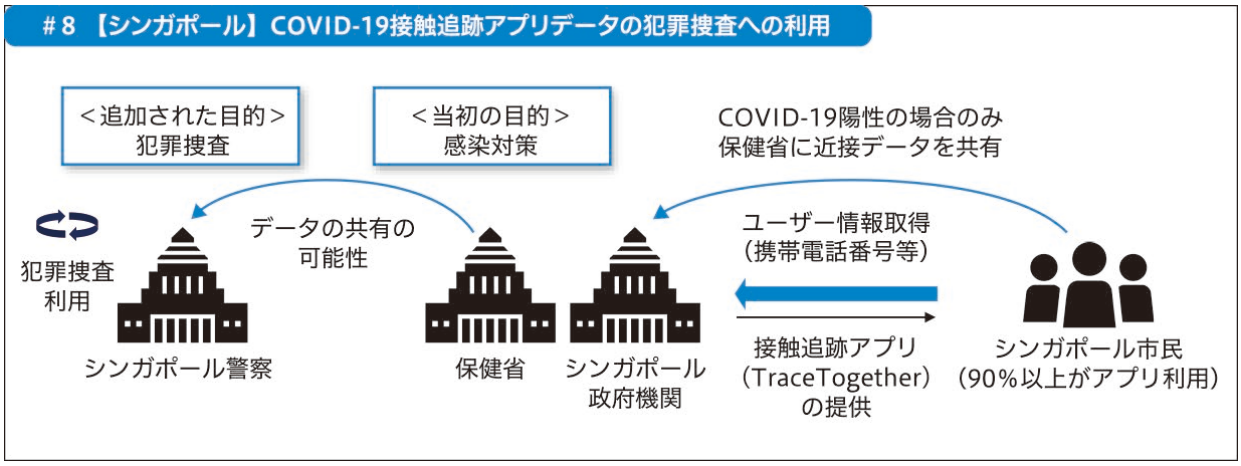
[45] アプリのダウンロード以外に、TraceTogether のトークン（小型端末）を利用する方法もある。

[46] 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 8 月 22 日閲覧）

[47] TraceTogether Privacy Safeguards, https://www.tracetogether.gov.sg/common/privacystatement/index.html, accessed 2022/08/22.

[48] 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 8 月 22 日閲覧）

[49] COVID-19（Temporary Measures）Act 2020（No. 14 of 2020）, https://sso.agc.gov.sg/Act/COVID19TMA2020?ProvIds=P111-#P111, accessed 2022/08/22.



出典：TraceTogether Privacy Safeguards, https://www.tracetogether.gov.sg/common/privacystatement/index.html, accessed 2022/08/22. 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）を元に作成。

2．3　事例から見るガバメントアクセス目的の多様性

前節の事例をもとに、ガバメントアクセスの影響を分析するにあたり、多様な分析軸を想定することとした。それにより、政府がどのような目的でガバメントアクセスを実施するか、そこからアクセスを受けるデータ主体や民間事業者がどのような権利利益の侵害を受けるかを分析の観点として、ガバメントアクセスの実態を把握することができる。

個人・非個人データ双方を含むガバメントアクセスには、個人データのみを対象としたアクセスよりも広い目的がある点が明らかになった。一般にガバメントアクセスとして議論の中心となってきた法執行や安全保障に加え、公衆衛生（コロナ対策や肥満の予防など）や都市計画、製品安全などその他「公益」目的を持ったガバメントアクセスの実例が複数あることがわかる。

事例収集から得られたガバメントアクセスの目的

大分類	小分類	該当する事例（ケーススタディ対象ケース）
法執行	犯罪捜査	・米国：政府による Microsoft 社への犯罪捜査に係るデータ開示要求（米国法・EU 法〈GDPR 等〉の抵触問題）（事例 6）
安全保障	諜報活動・安保活動	・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）（事例 5）
	自国における思想・言論統制	・ベトナム：外資 SNS サービスに対する政府によるコンテンツの検閲・削除（サイバーセキュリティ法）
国内産業育成	強制技術移転	・中国：ハイテク産業等における外資企業への行政承認と引き換えの機密情報の開示要求（米国 301 条調査事例）（事例 1）
	政府を介したデータ共有による自国企業の競争力強化	・政府による民間企業支援と国家規模の音声認証データベースの構築（事例 3）
その他「公益」目的※	公衆衛生	・インド：企業検診データの取得とその公衆衛生対策への利用及びインド企業での活用（非個人データ共有枠組み）（事例 4） ・シンガポール：政府による COVID-19 接触追跡アプリデータの取得と、その犯罪捜査への利用（事例 8）
	都市計画	・中国：新エネルギー車データのリアルタイム収集及び国家プロジェクトでの利用
	補助金の不正防止	
	製品安全	
	交通安全	・中国：地方政府による自動運転関連技術テストを通じた走行データの取得・利用 ・EU：交通安全を目的とした自動車走行データの官民データ共有プラットフォームの構築（PPP）

※広義には上記大分類すべてが公益目的となるため、その他「公益」と記載

ガバメントアクセスの目的により、政府とデータ主体や民間事業者の権利や利益に与える影響も多様となる。例えば、個人データを中心としたガバメントアクセスの議論においては、個人のプライバシー保護と、公的機関の法執行や安全保障という利益の調整が規律要素に関する議論のポイントとなっていた。つまり、規律要素の内容を、政府の行為に対する制限として強

化すれば、個人のプライバシー保護は増進するが、その分政府側が本来必要とするアクセス（政府側の利益）が制限される可能性もある。両者のバランスをいかに調整するかが鍵となるのである。

他方で、個人データのほか非個人データを対象に含むガバメントアクセスの規律要素は、上の表でまとめたアクセスを行う政府側の多様な利益と、それによって侵害されうるデータ主体や民間事業者の権利利益の調整を行う制度と位置付けられ（例えば、その他「公益」とデータ主体や民間事業者のデータの管理権や経済的利益の調整等）、個人データを前提に検討が進んでいるガバメントアクセスの規律要素に、何らかの要素が加わる可能性があることが確認された。

また、政府側のアクセス目的が多様となるため、侵害を受けうるデータ主体や民間事業者の権利利益の種類も増え、典型的なプライバシー権のほか、特許権等の知的財産権や営業秘密等が確認された。さらに、知的財産権として保護されないデータへのガバメントアクセスでも、データ主体や民間事業者にはデータの管理権や財産的価値といった権利利益が存在すると考えられる。このような権利利益は、通例著作権や特許等で保護されないローデータの集合体であるビッグデータ特有の議論であり、ガバメントアクセスから保護すべき権利利益としてこの類型も考慮に入れる必要がある。このようなデータの集合には国際ルールでの保障根拠として、WTO 協定のうち TRIPS 協定第 39 条があるが 、同条の適用範囲については定かでなく、さらなる検討が必要である。

3. 先行するガバメントアクセスに関連する規律議論の例

既に紹介した OECD における検討以外にも、世界的なガバメントアクセスの規律議論の高まりが見てとれる。ここではいくつかの先行する議論について、検討会における議論の元としたものを紹介する。

また、詳細は省略したが、検討会の開催中に ICC（International Chamber of Commerce、国際商業会議所）の「ガバメントアクセス白書」[50] が作成されており、2022 年 4 月に公開された白書の内容には、本検討会の議論の内容についても盛り込まれている。

[50] ICC “ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector”, April 2022.

３．１　GPA８原則[51]

- 目的：プライバシー保護と法の支配の促進
- 策定主体：Global Privacy Assembly（GPA）
- 対象範囲：個人データに対する安全保障及び公共安全を目的としたガバメントアクセスを対象としている。
- 原則の内容：世界各国のデータ保護機関から構成される GPA によって公表された原則であり、個人情報保護委員会など日本、フランス、カナダのプライバシー保護当局がスポンサーとなっている。
  内容としては、規律要素よりもプライバシー保護に寄せた内容と分析がされ、例えばアクセス権・訂正・消去権というデータ主体の権利が規定される点が異なっている。
  各項目については、以下の表を参照。

GPA８原則
1. 法的根拠（Legal basis）
個人データへのガバメントアクセスは公衆による議論と立法者による審議を経た適切な法令に基づいて、正式に許可されなければならない。法令はデータ保護及びプライバシーその他の人権を尊重し、無差別でなければならない。
2. ガバメントアクセスに適用される明確かつ適切な法令 （Clear and precise legislation applying to government access）
個人情報へのアクセス権限を与える法令は次を満たすべきである： a）公衆が利用可能、b） 明確かつ平易に理解できる言語で規定されている、及び c） アクセスを認める個人情報の範囲とアクセスの条件が明確かつ具体的である。
3. 一般原則としての必要性と比例性 （General principle of necessity and proportionality）
公的機関による機微情報を含む個人データへのアクセスが正当化されるには、個人情報の特定の利用が政府の明確に必要な機能や活動と明らかに関係づけられ、侵害が問題とされる目的に比例したものでなくてはならない。
4. 透明性（Transparency）

[51] 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”, October 2021, https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf, accessed 2022/08/22.

法令による権限付与から生じるガバメントアクセスに向けた合意や取り決めが、関連する政府機関に対して能動的な最低限の公的な報告や公に利用可能なアカウンタビリティ手続を有し、また、民主社会において必要かつ比例的な範囲の制限を除き、影響を受ける個人に情報が提供されることを許容されるべきである。
5. データ主体の権利（Data subject rights）
個人データへのガバメントアクセス（に関する制度）が、安全保障や公共の安全上の要求を考慮しつつ、公的機関への要求を直接行うことを含め、データ主体が自らの権利を行使する枠組みを持つべきである。特に、民主社会において必要かつ比例的な範囲の制限を除き、個人は個人データに関するアクセス、訂正又は消去の権利を持つべきである。
6. 独立（Independent oversight）
アクセスを認める法令が、特定のガバメントアクセスによって生じる個人の基本権や自由への影響の重大性と深刻さを考慮して、独立した事前の監督（例えば事前の司法機関による権限付与）と事後的な審査（例えば独立した規制機関による手続き）を与えるよう考慮すること。
7. 政府機関による取得データの利用に関する法令上の制限 （Statutory limitation on government's use of data acquired）
ある目的についてガバメントアクセスを認める法令が、他の目的による（データの）利用や再移転について規制しており、個人データの継続的な保護のための一般原則を規定していること。
8. 影響を受ける個人に利用可能な実効的な救済 （Effective remedies and redress available to the individuals affected）
個人データへのガバメントアクセスには、影響を受ける個人が実効的な救済を求める規定が伴わなければならない。

3．2　欧州 B2G（Business to Government）データ共有原則 [52]

- 目的：公共部門のための民間部門のデータへのアクセスの改善と、その使用のためのより柔軟な枠組みを設計するため
- 策定主体：欧州委員会
- 対象範囲：非個人データに関する民間と政府のデータ共有を対象としている。欧州 B2G（Business to Government）データ共有原則の問題意識は、「民間企業等が保有す

[52] European Commission, "Towards a Common European Data Space", COM/2018/232 final.

る私的な非個人データについて、政府等による公益目的での的活用を可能にするべき」にあり、具体的な公益的活用方法として、感染病の流行（epidemics）へのより的を絞った対応、より良い都市計画、交通安全と交通管理の改善、さらにはより良い環境保護、市場監視又は消費者保護等が想定されている。

- 原則の内容[53]：以下の表を参照。

欧州 B2G データ共有原則
1. 民間部門データの使用における比例性 （Proportionality in the use of private-sector data）
民間データの提供・利用の要請は、明確かつ実証可能な公共の利益によって正当化されるべきである。要求される民間データは、追求される意図された公益について、必要かつ関連性があり、データの種類、詳細度、量、アクセス頻度などの点で比例している必要がある。民間データの提供と利用に要するコストと労力は、期待される公共の利益に対して合理的かつ比例的なものでなければならない。
2. データ使用の制限（Data-use limitation ）
B2G 共働契約（Collaboration agreement）又はデータ共有を要求する決定は、意図された公益目的及びデータ使用権（例：データで何ができるか、期限を定めたもの）を明確に規定する必要がある。
3. リスクの軽減と保護措置（Risk mitigation and safeguards ）
民間企業や市民団体は、対象となるデータの品質や、公的機関による公益目的での利用について責任を負うべきでない。B2G データ共働に関する合意や決定には、利害関係者、特にデータを使用される個人の権利（プライバシー、データセキュリティ、無差別など）を保護するために、民間データの使用に関して適切な保護措置を含むべきである。
4. 補償（Compensation）
B2G データ共働は、公共部門に優遇措置を与えることで公益目的を認識しつつ、相互に利益をもたらすようにすべきである。
5. 非差別（Non-discrimination ）
B2G データ共働契約は、民間企業は、同様の機能を果たしている又は、同じ課題に取り組んでいる公的機関を、同等の状況で非差別的に扱うべきである。

[53] 原則の内容は、ハイレベル専門家グループによる最終報告を参照。
European Commission, Directorate-General for Communications Networks, Content and Technology, “Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest: Final Report Prepared by the High-Level Expert Group on Business-to-Government Data Sharing”, Publications Office, 2021, https://data.europa.eu/doi/10.2759/731415, accessed 2022/08/22.

6. 民間部門データの制約緩和 （Mitigate limitations of private-sector data）
潜在的な固有のバイアスを含む、民間部門のデータの潜在的な制約に対処するために、民間企業及び市民団体は、規定された目的のために、必要に応じて、データの検証の可能性を含め、規定の目的（例：種類、細かさ、正確さ、適時性、形式）に応じたデータの質の評価を支援するための合理的かつ相応の支援を提供するべきである。民間企業や市民団体は、無償でデータの質を向上させることを要求されるべきではない。
7. 透明性と社会参加 （ Transparency and societal participation ）
B2G データ共働は、連携の当事者とその目的について透明性を確保するべきである。また、公共機関は、民間企業や市民団体に対し、データの利用によってどのような公益がもたらされたのか、及び、データが利用されなかった場合についても、事後的に透明性を確保する必要がある。公共機関は、必要に応じて、民間企業のデータの機密性を損なうことなく、国民のフィードバックと社会参加を活性化するメカニズムを確保する必要がある。
8. アカウンタビリティ（Accountability）
B2G データ共働におけるすべてのパートナーは、責任を持って合法的な方法でデータを使用・共有する説明責任を負い、コンプライアンスを示さなければならいない。
9. 公正・倫理的なデータ使用（Fair and ethical data-use ）
データは、倫理的、合法的、公正かつ包括的な方法で共有・利用されるべきであり、データの利用方法に関する個人の選択を十分に尊重しなければならない。

３．３　日本「公共性の高い民間データアクセスのルールの原則」[54]（検討中）

- 目的：データ提供者への不安感の払拭や動機付けの在り方に対処するルールを策定することで、データ流通を拡大するため
- 策定主体：内閣官房 情報通信技術（IT）総合戦略室
- 対象範囲：公共性の高い民間データへの政府機関によるアクセス（「公共性の高い」の内容については検討中）
- 原則の内容：以下の表を参照。

[54] 内閣官房情報通信技術（IT）総合戦略室・内閣府知的財産戦略推進事務局「民間保有データの利活用を促進するためのデータ取扱いルールの検討状況」（2021 年 3 月）p.18
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kousou/2021/dai6/siryou6.pdf（2022 年 8 月 22 日閲覧）

日本「公共性の高い民間データアクセスのルールの原則」（検討中）
1. 社会的意義（公益）の明確化
どんな公益が見込まれているか、及び公益の達成状況についての継続的な説明
2. プライバシー・知財の保護
データ提供者及び提供されるデータの生成に関与した者のプライバシー・知財の保護に必要な、制度・契約・技術上の措置
3. 意図しないデータ流通・利用の防止
データ提供者が意図していないデータ流通・利用を防止するための、制度・契約・技術上の措置
4. 目的合理性のある最小限のデータアクセス
公益達成に必要最小限の範囲（対象データ・期間・対象者）でデータを利用
5. コスト負担の合理性
データ生成・提供に要する投資に配慮したコスト分担
6. データガバナンスの構築
上記２～４を実効たらしめるデータガバナンス構築（責任者指名と体制の構築・データ取り扱いポリシーの策定・人材育成プランの作成と実行、所管する機関や委託先に対する適切な管理・監督等）
7. 理解・納得可能なデータ取扱い方法の説明
上記２～６についてデータ提供者及び提供されるデータの生成に関与した者が理解・納得可能な、データ取扱い方法及びデータ取り扱い状況の継続的な説明

３．４　Trusted Cloud Principles [55]

- 目的：クラウド事業者として顧客データのプライバシーやセキュリティを確保するため、政府に対してクラウド時代の最低限の保障基準を提供するため
- 策定主体：Amazon、Google、Microsoft 等のクラウド事業者
- 対象範囲：特に限定はないが、顧客を特定できることを前提とした記載となっているため、個人データについて、クラウド事業者へのガバメントアクセスを念頭に置いていると考えられる。
- 原則の内容：以下の表を参照。

[55] Amazon et al., “Trusted Cloud Principles”, 2021, https://trustedcloudprinciples.com/, accessed 2022/08/22.

Trusted Cloud Principles
1. 政府は初めに顧客とやり取りすべきであり、この例外は限定されるべきである
例外的な状況を除き、政府はクラウド事業者よりも企業顧客へ直接データ提出を要求すべきである。
2. 顧客は通知を受ける権利を持つべきである
政府が クラウド事業者から直接データを収集する場合、 クラウド事業者 の顧客は自らのデータへのガバメントアクセスに関して事前に通知を受ける権利を有するべきであり、これは例外的な状況でのみ遅延が許されるべきである。
3. クラウド事業者は顧客の利益を守る権利を持つべきである
関連するデータ保護当局への通知を含め、 クラウド事業者が顧客データへのガバメントアクセスの要求に対する異議申立て（challenge）を行う明確なプロセスが存在するべきである。
4. 政府は抵触法（Conflicts of Law）について調整すべきである
クラウド事業者のある国における法令順守が別の国での違法行為となることがないよう、諸政府は相互にこのような抵触を問題提起・解決できるメカニズムを創設すべきである。
5. 政府は越境データ流通を支持すべきである
イノベーション、効率性、安全性及びデータ保管義務を回避するための原動力として、政府は越境データ流通を支持すべきである。

4. 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）については、以下のものがあると考えられる。個人情報保護に関連する規律要素については、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である。項目 1 から 7 までは、OECD が 2020 年 12 月に個人情報保護に関連する規律要素として言及した公開資料を基礎にしているが、本報告書では、個人データと非個人データを区別せず、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を提示した。なお、OECD を基礎として部分は、2020 年の公開資料にのみ基づいており本稿の自邸で検討途上にあるため、のちに変更されることがある。

4．1　本報告書が提案する 14 の規律要素

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法的根拠を明確にすることで、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データ主体や民間事業者に対して予見可能性を向上させる。政府側の規律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うる。

他の要素との関係：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、予見可能性を担保するルールでもあるため、「透明性」の規律要素との重複も生じうるが、ここでは政府側の法的根拠を明示させることで恣意的な権限行使を抑制することに重点を置いている一方、「透明性」の規律要素では、アクセスを受けるデータ主体や民間事業者への影響を小さくすることに、より重点を置いている。

他の国際ルールとの関係：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（自由権規約）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。ここでは正当性の判断基準は、政治体制によって多様であって構わない。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うる手段がないこと、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要素であり、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データ主体や民間事業者の法的に保護された利益が侵害されることがないように、その目的を達成するのに必要かつ合理的な範囲にとどめるために必要とされる。

他の要素との関係：「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」という経済的合理性は、本要素に内包されうる。

他の国際ルールとの関係：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（関税及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）。

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が判断基準となる。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や民間事業者に通知されることも判断対象である。

意義と役割：アクセスされるデータ主体や民間事業者にとって、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な要素である。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可能にする。データ主体や民間事業者等への通知は、彼ら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」と重複があるが、その差異については、「１）法的根拠」の記載を参照されたい。

また、予見可能性についても本要素に統合している。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考えられるからである。

他の国際ルールとの関係：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、独立の司法機関又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データ主体や民間事業者の権利利益の侵害を未然に防止する意義がある。

適正手続き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、データ主体や民間事業者が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：適正手続きは、自由権規約第 9 条が規定している。

5） 制限 （Limitations）

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下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するとともに、データ主体や民間事業者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：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データ主体や民間事業者への権利利益の侵害を含む影響を事後的に見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、データ主体や民間事業者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：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：前掲のアクセス・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主体や民間事業者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データ主体や民間事業者が、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は後掲「12）補償」を参照。

他の国際ルールとの関係：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きを維持し、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している。

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：「運用の一律性」と重複する部分があるが、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：GATT をはじめとする国際通商法は無差別原則を規定している（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うる。

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、国際的なデータ流通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が必要である。

他の要素との関係：前掲「８）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い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：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している。

10） 公正性（Fair and equitable treatment）

判断基準： 恣意的で不公正、不正義又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（北米自由貿易協定＜NAFTA＞ 第 1105 条）。

11） 経済的合理性（Economic rationality）

判断基準：民間事業者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：アクセスを受ける民間事業者に対し、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、当該民間事業者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：「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、民間事業者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。

12） 補償（Compensation）

判断基準：データの経済的価値の対価として、データ提供元のデータ主体や民間事業者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って制限される不適切なガバメントアクセスが認められるわけではない。

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、データ主体や民間事業者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、民間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、民間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ならなくなる）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、補償の必要が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、「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。
他の国際ルールとの関係：国際慣習法上、データ主体や民間事業者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付けられている。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一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民間事業者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、民間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：EU の B2G データシェアリング要素では、免責について「民間企業や市民団体は、対象となるデータの品質や、公的機関による交易目的での利用について責任を負うべきでない[56]」と規定している。

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、その調整を民間事業者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、民間事業者が進出を躊躇する、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：EU のデータガバナンス法案は、第 31 条国際アクセスにて、公的機関や民間事業者は、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うることを規定している。

[56] 前掲注（53） p 82、c) 参照。

4．2　各要素の関係整理

上記の 14 項目の規律要素は意味の重複や包含関係についての可能性を排除せず、求められる規律の全体像をもれなく描写することを念頭に置いて整理してきたものである。したがって、規律要素とその記述の中に現れる個々の概念間の関係性についても留意して個別に分析を記載してあるが、その中から特に注意すべき要素と概念の関係整理について記載する。

１）比例性の意味

複数の「比例性」の解釈がありうるためここで整理しておきたい。「比例性」は 2020 年の CDEP 声明においては副次的な要素として記載され、その指す内容も声明には記載がない。他方、GPA8 原則の中では必要性と並んでガバメントアクセス規律要素の中核の一つとされている。ここでは、比例性はガバメントアクセスの重要な規律要素との考えから、規律要素の一つとして明確に取り上げることとした。

なお、比例原則は EU 法特有の概念であるとの指摘もあるが、本ルールで記載した比例性については我が国の憲法解釈等にも通底するものであり、より汎用的な概念であるため規律要素として盛り込むこととした。

２）補償と救済の関係

補償と救済も一見、重複しているように見えるが、ここでは、救済はデータ主体や民間事業者が規律要素を遵守しないガバメントアクセスによって被った権利利益の侵害に対して、侵害行為を停止したり被った損害を賠償したりする機能を想定している。

他方、補償については必ずしもルール違反を想定せず、適法なガバメントアクセスであったとしても、ガバメントアクセスを受けてデータを提出した民間事業者に対して、データ提供の対価として経済価値等に基づく相当なデータ提供の対価を支払うべきではないかという考えに基づく。ここではデータの経済価値に着目しており、今回の検討で新たに特定された規律要素であるといえる。ただし、補償については常に必要とされるわけではなく、この点でも救済とは異なっている。

3）公平性、公正性及び公正かつ衡平の関係

公平性と公正性についても、両者を区別すべきか類似の概念とすべきかが問題となる。この点、公平性は競争歪曲の防止を中心とした経済的な概念であるのに対して、公正性は差別のほか、人権や不正義などより広範な規律範囲を有しており両者を区別すべきである。

上記の通り区別された公平性と公正性であるが、特に公正性については文脈や時代に応じて非常に多義的な内容を指すものであり、規律要素として十分固まったものではない面もあるが、公正性の具体的な内容として国際ルールにおいては公正と衡平（fair and equitable）が用いられているため、この用語を採用することとした。

5. 検討結果のまとめと展望

5. 1　非個人データに求められる規律の特性

個人データを対象にする場合に比べ、非個人データを含む規律要素ではガバメントアクセスの目的[57]、すなわち政府側の利益と、それを受けるデータ主体や民間事業者の保護されるべき利益の関係が複雑になる。結果、両者をどの程度厳密に調整するかについてもさまざまな事例を念頭に置く必要があり、ガバメントアクセスの必要性を評価して代替手段を求めることがどこまで妥当か、ガバメントアクセス規律について審査基準のあり方が多様な事例について一律でよいかとの論点がある。特に第２章（2.3）の表の中で「その他『公益』目的」として示した事例では、国民や世界全体の人の安全の維持（例えばパンデミック対策）の利益のためにデータを使うことになる。制度設計では社会全体の利益の増大に向けてどのような理由であればデータが提供されてよいと思えるかという視点が重要になり、法執行やテロ対策等の安全保障とは制度設計の考え方が違ってくるかもしれない。

目的の正当性に関する判断基準も論点である。第１章（1.2）の検討の指針で記載した「グローバルなルール形成を目指す観点から、特定の国家（例えば特定の政治体制を持つ国等）を一律に排除することがないようなルール形成を図ることを基本的な方針とした」点にも関連す

[57] この点、特に公的機関における調査権限（本検討におけるガバメントアクセスの権限）をまとめた資料として、一般財団法人情報法制研究所（JILIS）捜査関係事項照会問題研究タスクフォース「（資料）調査権一覧」（2020年１月）https://www.jilis.org/proposal/pages/2020-03-17/sousa_01_shiryoichiran.pdf（2022 年 8 月 22 日閲覧）が参考になるとの指摘がなされた。

るが、目的の正当性の中で特定の政治体制（例えば独裁政権）を維持するためのガバメントアクセスを適切なものとみなすか、といった論点も生じる。

以上 2 点について、ガバメントアクセスの理解と、それに基づく審査基準の変化という観点からさらなる検討が必要になるだろう。国際通商協定では、政策目的を限定列挙してその審査基準を変える規定方法（GATT や GATS 型）と、政策目的は正当性だけを抽象的に規定し、その審査基準も一律にする規定方法（TPP 協定第 14 章・電子商取引の例外等）があり、ガバメントアクセスの規律要素の規定方法についても、それが一部をなす通商ルールの規定方法に依存する可能性がある。双方の規定方法について、安全保障例外は別に定められている点にも留意すべきである。

国際交渉では、個人データが非個人データより重要と考えられているが、本報告書では非個人データも含めたため新たな規律要素が加わった。特に、中国との関係については「国家情報法」をどう扱うかが大きな問題であり、今後の検討が必要である。今回の分析を行う事例は何らかの形で強制性を伴うものに限定したため、記載した規律要素の考え方にもその限定が付される。しかし、例えば、今回は検討外であったが Yahoo! JAPAN が新型コロナウイルス対策を理由として政府から任意のデータ提供を求められ、任意提供に係る契約を締結した事例もある。このような事例は政府によるデータ活用の一環として今後も増加が見込まれるため、民間事業者が政府にデータを任意提供する場面も含むガバメントアクセス規律要素の検討が必要である。

最後に、経済安全保障の観点から我が国においてもガバメントアクセスの権限を規定する法案について議論がなされる可能性もある。外国の政府によるガバメントアクセスから我が国のデータ主体や民間事業者の権利利益を守る規律も重要だが、同時に規律要素は懸念の対象とされる国・地域だけでなく、自国や友好国にも適用されることを前提としなくてはならない。適切な補償の対象が個人情報を想定したものだけではなく、中小規模の企業に損害が生じた場合にも考慮されることが民間事業者からは望まれるだろう。

5．2　ガバメントアクセスルールの通商ルール適用に向けた論点

通商ルール上の課題としてガバメントアクセスを捉えると、いくつかの点で個人情報を中心とした議論とは異なる検討が必要となる。

第一に、ガバメントアクセス規律要素の遵守が認められない国への対抗措置として何を認めるかが論点である。極端な例を挙げると、当該国に自国からのデータ移転を認めないことが考えられるが（データ越境移転の禁止）、それ以外にも当該国内の移転先にする特別な安全管理措置等を課すこと（例えばGDPRにおけるSchrems II事件判決を踏まえたSCC上の対応）、同意取得時に当該国のガバメントアクセスリスクを明示させること（我が国における令和2年改正個人情報保護法）などの措置が考えられる。相互主義を前提としつつも、自由な越境データ流通の主張を損なわないため、継続的な検討が必要とされる。

第二に、既存の通商ルールとの関係整理を進める必要がある。TRIPS協定等既存の通商ルールでガバメントアクセスに対処できる範囲を明らかにすることが効果的である。それにより不足しているルールの存在が明らかになり、ガバメントアクセスについて新たな規律要素を定めることの必要性が明確になる。

第三に、ガバメントアクセスルールと既存の通商ルールの抵触にも配慮する必要がある。例として挙げたガバメントアクセス規律要素の遵守が認められない国へのデータ越境移転を禁じる場合、TPP協定の規定（第14章・電子商取引）への抵触も一つの例である[58]。また、公平性における市場歪曲はWTOの補助金協定やGATT/GATS上の無差別原則においてカバーされる部分もあるが、守備範囲の重なりや矛盾が生じないかなど関係性を整理しておくことが必要になる。

5．3　今後のルール形成に向けた進め方

本報告書は通商ルール形成に向けた基礎的検討として、ガバメントアクセスルールの規律要素に関する考え方を整理したものである。

ガバメントアクセス規律要素の検討は今後も継続されていくことが予想され、既に議論が進むOECDのほか、G20や、2023年に日本で開催されるG7やインターネットガバナンスフォーラム（IGF）など様々なフォーラムでの議論が想定されうる。ルール形成の中で、我が国の政策立案者や企業実務者、諸外国の専門家が本報告書を参照することを期待する。また、今後

[58] ただし、TPP協定の電子商取引章は、例外となる正当な公共政策目的を達成するために必要であり、恣意的または不当な差別を構成しない等、一定の条件を満たす場合には例外的にデータの移転制限を認めるため、この例外との関係性も必要となる。

はルール形成に求められるエビデンスが重要で、ガバメントアクセスに係る経済的なインパクト等の収集と分析が行われ、それに基づく検討がなされることが期待される。

グローバルなガバメントアクセスのルール形成には相応に時間がかかることが想定されるが、今回取り上げた措置のうち、既存の国内法や国際通商協定によって規律できるものも存在する。例えば、事例 1 の中国における行政承認と引き換えの機密技術情報の開示要求には医薬品の生産事業も含まれるが、医薬品の試験データは TRIPS 協定第 39 条 3 項で保護されている。また、ブラジル議会では、製薬企業の保有するノウハウを含めた情報の共有を強制することの是非が議論されてきた。これはガバメントアクセスの一例といえるが、この同項に違反する可能性がある。一方で、既存の国内・国際ルールをいかに活用できるか検討することも重要である。FTA や投資保護協定も活用可能性を検討する余地がある。既存の国際ルールに関する紛争解決の事例を積み重ねることで、日本がリードして国際協定の解釈に関する一定の相場観を形成することが可能である。これは紛争解決によるルール形成を促し、国家間合意を要する新規ルールの補完につながる。

民間事業者では、ガバメントアクセスを受けた場合の対応として社内専門家がその適切性を判断するだろうが、その際に参考になるルールが求められる。ここで提案した規律要素はその一つとなりうるが、抽象的な表現にとどまるので、企業実務との間を埋めるガイドラインの作成も検討すべきである。

非個人データの保護には、グローバルなルールが定まっていない事項が存在する。いわゆるビッグデータと呼ばれる、AI のアルゴリズムやデータ解析のために集積される大量のデータの集合である。創作性がない点で著作権として保護されず、特許等の申請がなされていないことも多く、営業秘密としても保護されない場合も多い。

知的財産権としては保護されないデータを保護すべきか、保護するならどのような権利があるかについて国際的な議論が続いている（EU のデータ法案における Data Ownership＜データ所有権＞の議論、日本の限定提供データ等）。保護されるべき権利利益の考え方は、非個人データの規律要素を検討する上で重要である。今後も議論動向を注視し、ガバメントアクセスの規律要素の検討に取り込んでいく必要がある。