新経済連盟　第二回国際動向勉強会

ガバメントアクセスとデータ保護

株式会社野村総合研究所　コンサルティング事業本部
CXコンサルティング部

エキスパート研究員　渡辺翔太

※本報告内容はあくまで報告者の個人的な見解であり、
報告者の属する組織等を代表するものではありません。

2022年9月15日

NRI

Share the Next Values!

1．ガバメントアクセスとは何か？

ガバメントアクセスとは？

政府機関等の公的機関による、民間部門が保有する情報への強制力を持ったアクセス

■民間部門

- 企業、NGO、個人

■強制力を持った

- 法的な（de jure）強制力のほか、**事実上の（de facto）強制も含む趣旨**
  ※事実上の強制とは、例えば法的な強制力はないもののアクセス要求に応じないと事業上の不利益を受ける場合などを想定

■アクセス

- 情報を入手すること

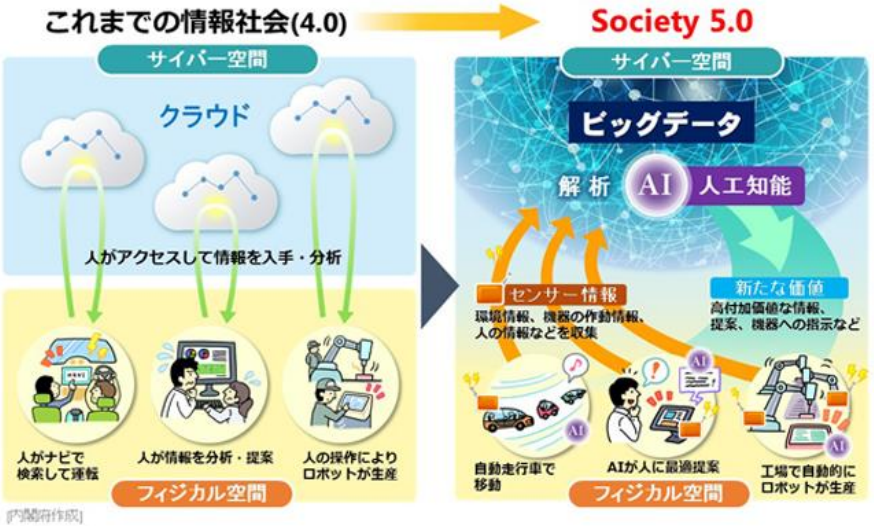
■射程外のもの

- 諜報活動：経済的なスパイ活動もあるとされるが、その実態が不明であり、研究の対象とならない。この定義では、「強制力」を持つものではないため除外している。

なぜガバメントアクセスが注目されているのか？

データの重要性の高まり　と　民間部門のデータ流通における役割の拡大

データの重要性の高まり



現在のAIは、大量のデータを元にアルゴリズムを作成する機械学習（DLなど）が主流であり、AIの競争力強化に向けて大量（かつ良質）のデータが必要になる。

民間部門のデータ流通における役割の拡大

- APP
- PF
- NW
- HW

データ流通では、すべてのレイヤで民間企業が支配的な地位にある

２．ガバメントアクセスに関する海外動向：米欧中印

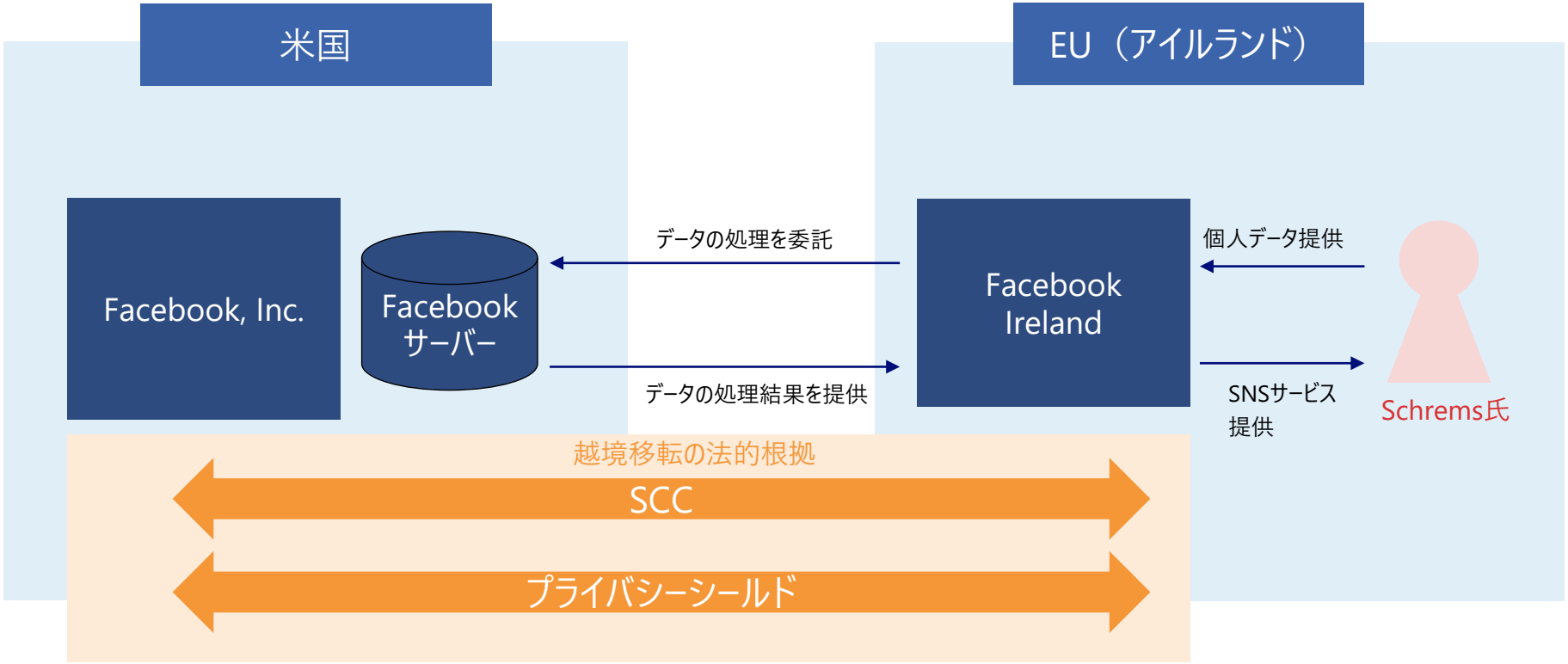
元々は米国発端：GA問題の始まりとしてのスノーデン事件と、Schrems I/II事件

- スノーデン事件で明らかにされた米国の諜報活動は、対外諜報活動監視法（FISA）に基づくものである。同法は、諜報機関による通信傍受の違法性を認めた判決への対応や、対外諜報の法整備を目的に、1978年に成立した。
- その後、2001年の同時多発テロをきっかけに政府権限の強化が図られることとなったが、これは同時に諜報機関の裁量の拡大をもたらし、法令が第三者監査を骨抜きにすることとなった。
- 2013年のスノーデン事件を受け、2015年には米国自由法による改正が行われ司法審査が強化されるとともに、PSが成立した。その後2回のレビューを経て十分性が維持されたものの、2020年にSchrems II事件で再度無効と判断。

時期	主なできごと
1978年	対外諜報活動監視法（FISA)が成立
2001年	愛国者法による権限強化
2008年	法改正により、米国民に対する権利保護強化と外国人に対する諜報活動の緩和
2013年	スノーデン事件発生
2015年	セーフハーバー無効判決（ECJ）：Schrems事件
	米国自由法によるFISAの改正
	プライバシーシールド（PS）成立
2017年	プライバシーシールド第1回レビュー実施（欧州委員会が十分性を維持）
2018年	プライバシーシールド第2回レビュー実施（欧州委員会が十分性を維持）
2020年	PS無効判決（ECJ）：Schrems II事件
2022年	米EU、PSの後継となるThe Trans-Atlantic Data Privacy Frameworkに合意

本事件の図式は下図の通りとなる。個人データがFacebookのアイルランド支社から米本社に移転されていること、SCCとPSという2つの移転の根拠がある点がポイント。

- EU市民はFacebookのアイルランド法人と契約し、アイルランド法人と同社米国法人がデータ処理契約を締結（アイルランド：管理者、米国：処理者）している。サーバーは米国のものを利用し、法人間でのデータ越境移転が成立している。
- 越境移転の根拠は、①Facebook法人間のSCC、②米EUプライバシーシールド、の2つが考えられる。



２．ガバメントアクセスに関する海外動向：米国　Schrems II判決の概要と評価

SCCは条件付きで有効、PSは無効と判断された。

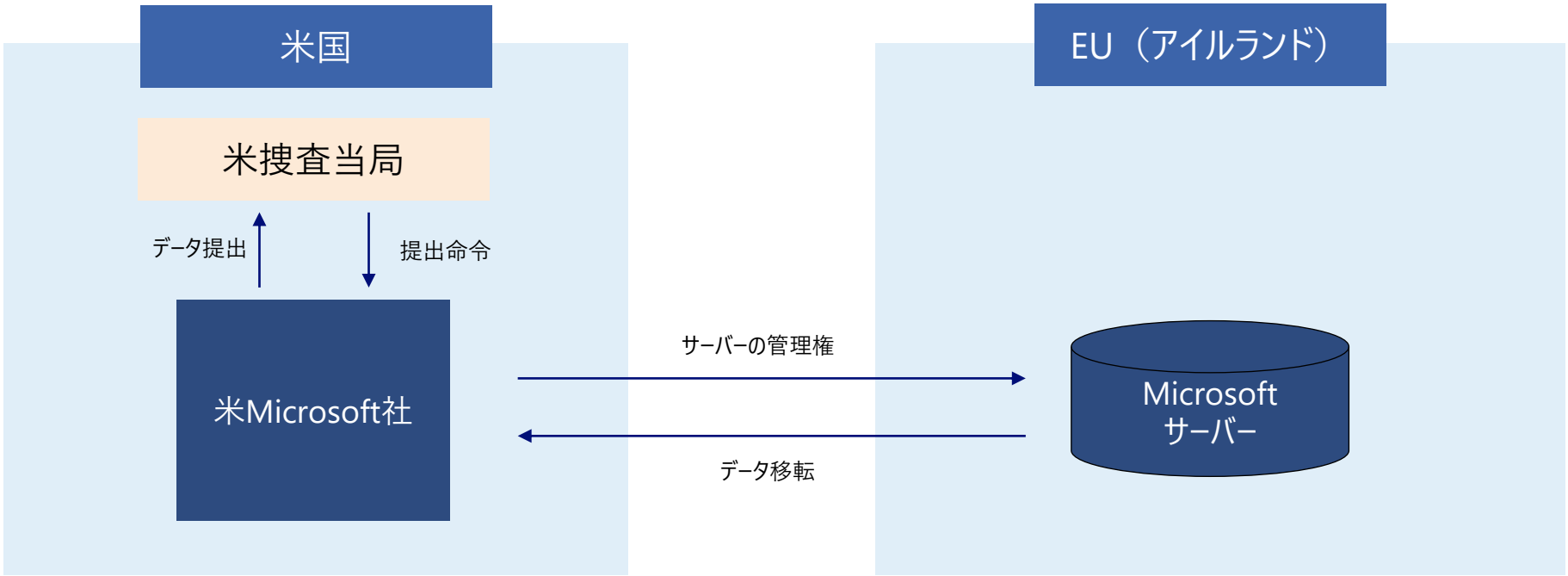
#	論点	概要	結論
1	★安全保障例外の該当性	• EUと加盟国の権限配分を定めるリスボン条約4条2項において「国の安全保障は、各加盟国の排他的な責任のもとに留保される」と規定しており、そもそも第三国において安保を目的とした諜報活動は同条約に基づいて立法されたGDPRの範囲外なのではないか？	• TEU（リスボン条約）における権限配分はEU加盟国を念頭に置いたものであり、第三国には該当しない。 • 次に、GDPR第2条2項はGDPRの適用除外を定めるが、本件データ移転は私企業によるビジネス上の個人データ移転であり、いずれにも該当しない。 • したがって、GDPRが適用される。
2	☆SCCの有効性	• SCCの有効性を判断するEU法上の保護水準（GDPR、基本権憲章）は何か？ • SCCはEU法上の保護水準に照らしてEUと同等の保護を提供しているか？	• 保護水準はEUと同等なものが求められる。 • SCCについては、移転が違法な場合にはDPAが差し止めできるため、SCCの規定自体がGDPRに反するものではない。 • 移転先の適切な体制構築が求められ、必要に応じて追加的保護措置（Additional safeguard）が求められる⇒改訂版のSCCの公表（詳細は略）
3	★DPAの権限	• SCCが締結されている場合、当局は欧州委員会が決定したSCCについてなおデータの移転中止を命じることができるか？	• DPAはSCCに従っている場合であっても、具体的な事案において、個別の苦情処理の権限に基づいて、データ管理者へのデータ処理に関する執行を行うことができる。
4	☆PSの有効性	• PSはEU法上の保護水準（GDPR、基本権憲章）に照らしてEUと同等の保護を提供しているか？	• PSは比例性、救済等の点でEUと同等ではなく、PSはEU法に反しているため、無効である。 ⇒EUと米国で新たな枠組みを交渉中

２．ガバメントアクセスに関する海外動向：米国

他国所在データへのガバメントアクセスとCLOUD法

- CLOUD Act（Clarifying Lawful Overseas Use of Data Act）は、2018年3月に成立した。CLOUD Act が持つ主な意義は、次の二点と指摘される。これらは、従来の刑事共助条約（MLAT）の使い勝手の悪さを補うもの。
- 第一に、SCAに基づく令状等により、米国政府が、米国の管轄権に服するプロバイダに対し、米国外に保有するデータの開示を強制できることを**明確化した**。ただし、プロバイダは①当該データのデータ主体が米国に居住していない米国人以外、かつ、②開示に応じることで米国と行政協定を締結した外国政府の法令に違反する重大なリスクを伴うと合理的に信じる場合、米国裁判所に対して、当該開示命令の修正又は取消しを求めることが可能。
- 第二に、米国政府と外国政府が行政協定を締結することで、米国の管轄権に服するプロバイダが外国政府からの直接の命令に応じてデータを開示しても米国法上違法と評価されないこととなった。

出所）西村高等法務研究所「CLOUD Act (クラウド法) 研究会報告書」



補足：CLOUD法対抗としての欧州での主権クラウドの発展＋Privacy Shield 2.0の動向

欧州（独仏）における主権クラウドの議論（⇒社会基盤としてのクラウド）

米CLOUD法への懸念から、独仏では欧州データ空間の基盤となるGAIA-Xと絡めて、主権クラウド（Sovereign Cloud）のコンセプトを提唱し、それを実現に移しつつある。主権クラウドは主に下記の要素を満たすクラウドサービスを指す（フランス、SecNumCloud認証の例）；

①クラウド運営者の所有及び管理制限：EU外の株主は25％以上所有することができない
②強制的ローカライゼーションとローカルスタッフ：プロバイダは全ての顧客データを EU 内で保管・処理すること、サービスの運営と監督はEU内から行われなければならない、技術的データをEU内で保管・処理しなければならないことを定めている

⇒GCPやAzureが現地企業（T Systems（独）やOrange（仏））と合弁形成（やり口が中国に近い、との米産業界からの批判もある。）

出所）https://www.meti.go.jp/meti_lib/report/2021FY/000018.pdf

Privacy Shieldの改正動向

2022年3月、欧米当局（欧州委員会及び米商務省）は、PSに代わり、The Trans-Atlantic Data Privacy Frameworkを合意したと発表した。米側は大統領令で必要な国内担保措置をとるとしているが、この中では、新たに「データ保護裁判所（Data Protection Review Court）」を新設するとともに、米諜報機関の監査体制を強化し、実体的にも必要かつ相当性のある範囲にデータアクセスを限定する新たな規則を作成するとしている。
ただし、3月以降の進捗は不明である。

２．ガバメントアクセスに関する海外動向：中国

■ 国家情報法

- 国家情報法（2017年6月1日施行）が、幅広いガバメントアクセスの権限を中国政府に与えている。同法施行以前は、政府による組織的アクセスを規律する法令や規範は無かった。
- 電子政府の構築に伴い、国家安全保障、公共の安全、検閲、徴税を目的に、様々な法律が、民間企業が保有するデータ（金融、貿易、旅行、娯楽等）へのアクセス権限を中国政府に与えている。

出所）Zhizheng Wang, “Systematic Government Access to Private-Sector Data in China”(2012)2/4 International Data Privacy Law

■ サイバーセキュリティ法（又はインターネット安全法、「网络安全法」）

- 同法が、ネットワークを流通する個人情報を含むデータのセキュリティを規定する一般法として、2017年6月より施行されている。
- 同法においても、ガバメントアクセスを認める条項が規定されている。

２．ガバメントアクセスに関する海外動向：中国

中国国家情報法（抜粋）

第1 章：総則（第1 条～第9 条）

第7 条

いかなる組織及び国民も、法に基づき国家情報活動に対する支持、援助及び協力を行い、知り得た国家情報活動についての秘密を守らなければならない。

国は、国家情報活動に対し支持、援助及び協力を行う個人及び組織を保護する。

第2 章：国家情報活動機構の職権（第10 条～第19 条）

第15 条

国家情報活動機構は、業務上の必要に基づき、国の関係規定に従い、厳格な許可手続を経て、技術的偵察措置(註：通信傍受のこと) 及び身分保護措置 を講ずることができる。

第16 条

国家情報活動機構の活動要員は、法に従い任務を遂行するに当たり、国の関係規定に基づき、許可を得て、必要な証明文書を提示することにより、立入りが制限されている関係区域・場所に立ち入り、関係する機関、組織及び個人に対し関係する状況について聴取又は質問を行い、関係する公文書、資料及び物品を閲覧又は押収することができる。

第17 条

国家情報活動機構の活動要員は、緊急の任務を遂行する必要がある場合、必要な証明文書を提示することにより、通行の便宜を受けることができる。

国家情報活動機構の活動要員は、業務上の必要に基づき、国の関係規定に従い、関係する機関、組織及び個人の交通手段、通信手段及び土地建物を優先的に使用又は法により接収することができ、必要な場合、関連の活動場所及び施設・設備を設置することができる。任務の終了後は、速やかに返却又は原状回復し、かつ、規定に従い相応の費用を支払わなければならず、損失を生じさせたときは、補償しなければならない。

第18 条

国家情報活動機構は、業務上の必要に基づき、国の関係規定に従い、税関、出入国検査等の機関に対し検査免除等の便宜供与を求めることができる。

第19 条

国家情報活動機構及びその活動要員は、法に厳格に従って業務を行わなければならず、職権を逸脱若しくは濫用し、国民及び組織の合法的権利利益を侵害し、職務上の便宜を利用して本人若しくは他人の私利を貪り、又は国家機密、営業秘密若しくは個人情報を漏えいすることがあってはならない。

第3 章：国家情報活動の保障（第20 条～第27 条）

第4 章：法的責任（第28 条～第31 条）

第5 章：附則（第32 条）

出所）国立国会図書館　調査及び立法考査局　主任調査員　海外立法情報調査室　　岡村　志嘉子「中国の国家情報法」 外国の立法 274（2017.12）

2．ガバメントアクセスに関する海外動向：中国

中国サイバーセキュリティ法

章	義務	条	NW運営者	重要情報インフラ運営者	NW製品及びサービス提供者
3章 NW運営上の安全	サイバーセキュリティ等級（レベル）保護の履行 - NW運営ログの6ヶ月以上保存	21条	○	○	○
	NW製品・サービスが国の強制標準への適合性確保	22条	○	○	○
	NW製品・サービスの安全性の保障				○
	実名制の実施 - ユーザの本人確認 - 国とNW運営者間での本人確認の相互認証の促進	24条	○	○	○
	安全管理責任者の設置、従業員の教育	34条		○	
	（国の安全に影響をもたらすおそれのあるとき）国の安全審査への合格	35条		○	
	個人情報及び重要データの中国国内での保管、及び越境移転の制限	37条	△	○	
	毎年1回以上のNWの安全リスクについて検査・評価の実施、担当機関への報告	38条		○	
4章 NW上の情報の安全	個人情報保護マネジメントの確立	41-42条	○	○	○
	苦情・通報制度の確立 国の監督検査への協力	49条	○	○	○

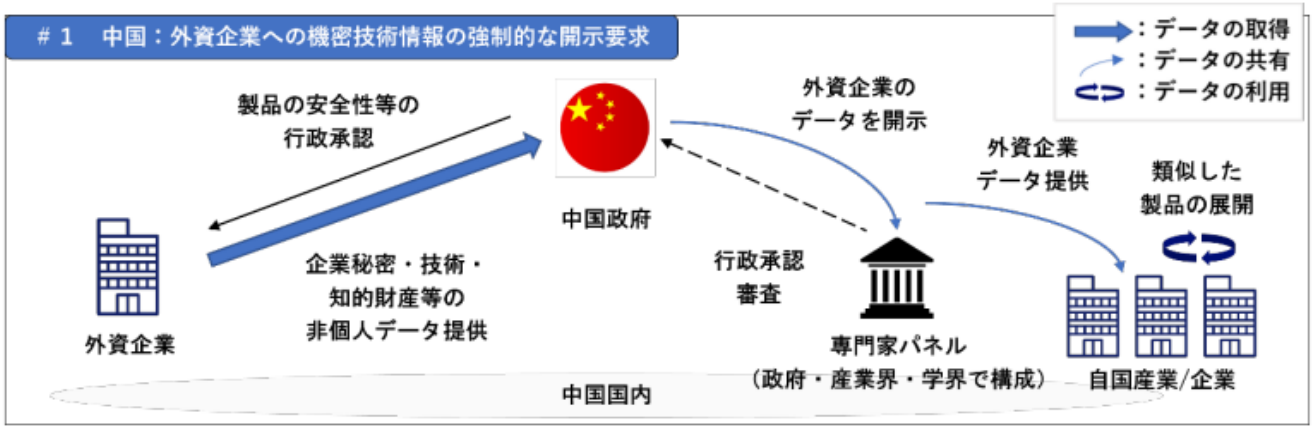
※赤字は、ガバメントアクセスに特に関係すると思われる義務

出所）JETRO「中国におけるサイバーセキュリティ法規制にかかわる対策マニュアル」2018年2月、及び大地法律事務所・サイバーセキュリティ法仮訳をもとに作成

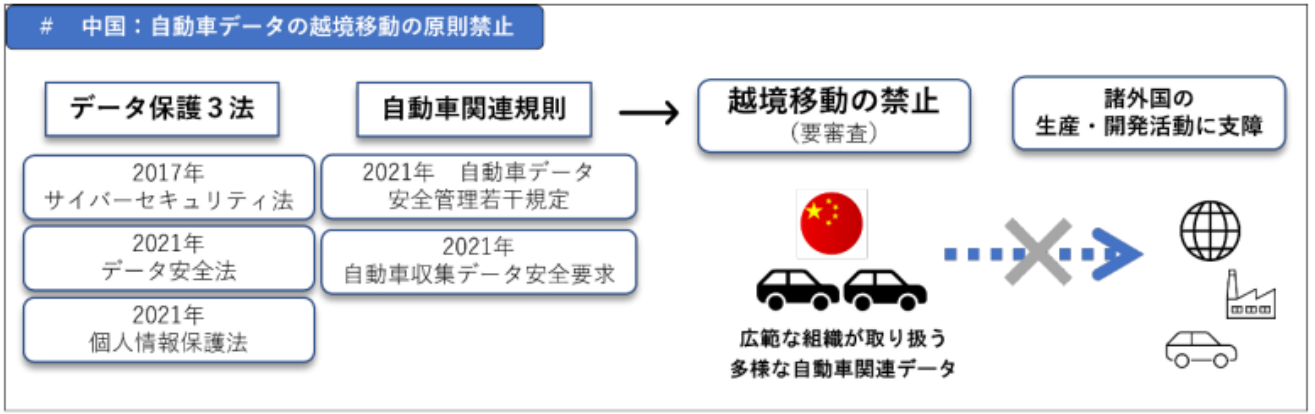
2．ガバメントアクセスに関する海外動向：中国

（参考）中国における産業政策としてのガバメントアクセス

■これらは「強制技術移転」とも呼ばれる類型である。



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", 2018.

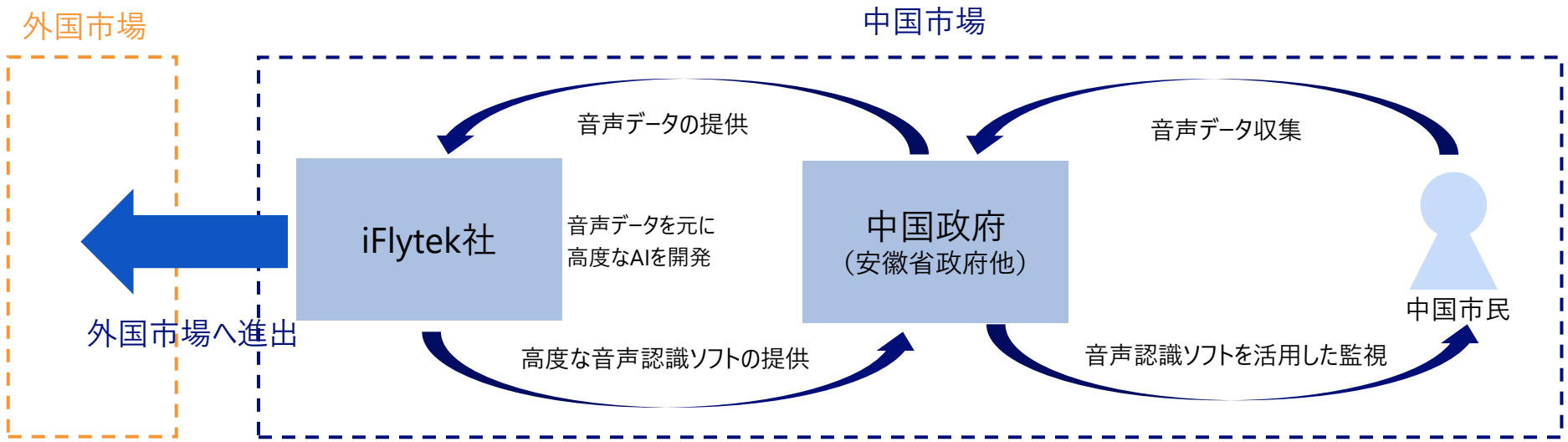


出典：国家互联网信息办公室『汽车数据安全管理若干规定（试行）』(2021年) 全国信息安全标准化技术委员会『信息安全技术 汽车采集数据的安全要求』(2021年)

出所）「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」（https://www.cfiec.jp/jp/pdf/gov/gov-2022-05-20.pdf）
※上記資料は現在の日本におけるGA議論の1つの到達点を示すもの

中国iFlytek社は、国家安全保障を目的に政府から提供を受けた音声データから高度な音声認識ソフトを開発し、それを海外を含む民間市場に展開している。

- iFlytek社は中国安徽省に本拠を置く、音声認識精度で世界第一位とも目される音声認識ソフトの提供者であり、日系企業のソフトウェアにもコンポーネントとして採用されている。
- 中国では国家安全保障目的のため、分析が遅れていた音声認識を強化すべく、2012年から大規模な音声データベースの作成に着手した。ここでは、安徽省を含む地域がパイロット地区として選定された。
  - また、中国語のスピーキングテストの音声データを元に、AI判別によるスピーキングテスト用ソフトの開発等も政府から受託してきた。
- 安徽省政府は入手した大量の音声データを提供し、iFlytek社に対して音声認識ソフトの開発を委託し、同社はこれを元に安徽省政府等に対してAIを活用した音声認識ソフトを納入した。
  - さらに、この音声認識ソフトは日本を含む海外市場に展開している。



出所）ヒューマンライツウォッチ（HRW）「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」よりNRI作成
（https://www.hrw.org/ja/news/2017/10/23/310343）

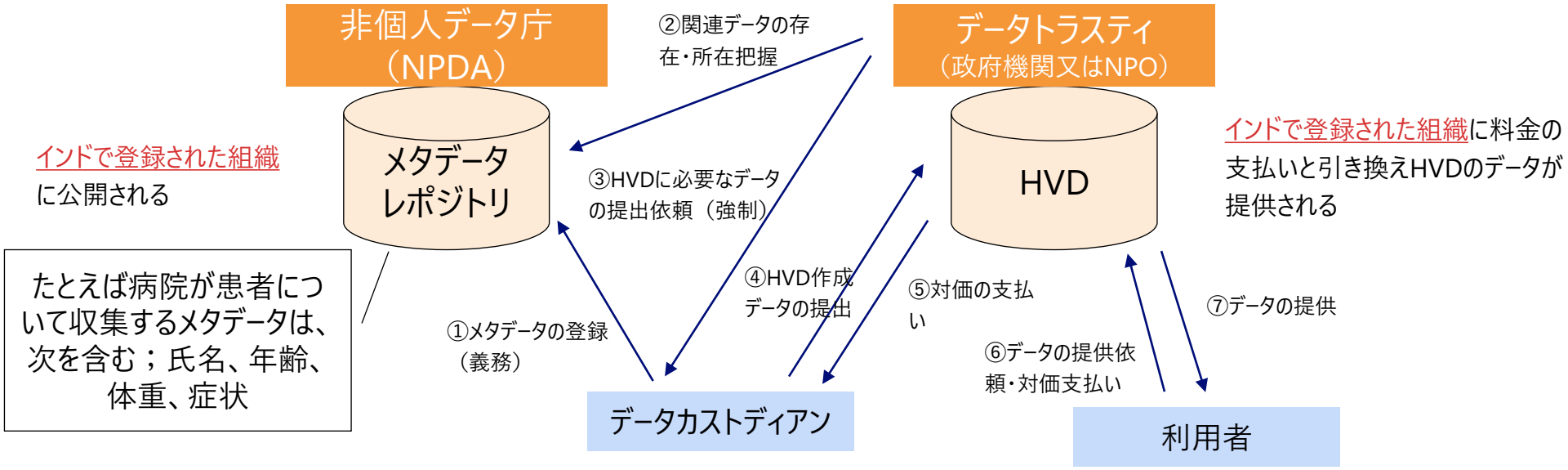
２．ガバメントアクセスに関する海外動向：欧州・インド

非個人データ（産業データ）のGA⇒共有を進めている

欧州：データ法案 厳密な必要性を規定しつつ、補償等を定める	• データ法案は公共部門が特定の公益目的のために必要な民間部門が保有するデータにアクセスし利用すること(ガバメントアクセス)に係る調和された枠組みを規定している。 • 【適用場面】公共部門が特定のデータを使用する例外的必要性があるものの、新しい法律の制定又は既存の報告義務によって適時にデータを市場で取得できない場合にのみ適用される（第14条及び15条） • 【アクセス要件】アクセス権限の濫用防止及び公共部門のデータの利用に関する説明責任の観点から、アクセス要求は目的を明確に示し、比例的であり、企業の利益を尊重する必要がある。また、当局は透明性と一般への公開を保証すること、またその結果として生じる苦情に対応する（第17条及び19条）。 • 【補償】公共の緊急事態（公衆衛生上の緊急事態、大規模自然災害や人災等）に対応する例外的な必要がある場合、データは無料で使用可能である。 その他の例外的な必要性（公的緊急事態の予防、緊急事態からの回復等）がある場合、アクセスを受ける民間のデータ保有者は、関連データを使用可能にするための費用に合理的なマージンを加えた補償を受ける権利を有する。
インド：非個人データガバナンス枠組	• インド電子情報技術省（MeitY）がインドのデータ政策の一環として有識者委員会を組織し、同委員会が取りまとめたものである。 • 民間保有のデータを公共財とみなし、「インドのデータをインドのために」、をコンセプトとして非個人データに関する強制的な共有を規定。インド政府のデータ主権を強調する。 • 後述の通り、内外差別的な規定が含まれるものであり、過去の国有化の事例と同様、データの「収容」に近い運用がなされる可能性も考えられる。 • インドは新興国のルール形成に影響力を持つ国であり、他国への波及に留意する必要。

メタデータレポジトリを元に、データトラスティがカストディアンに対してデータ共有を求め、これが任意に応じられない場合には非個人データ庁が介入し、要求が正当な場合には強制する。

- 本枠組みにおいては、高付加価値データセット（HVD）が一種の公共財として作成・開放され、インドで登録された組織が同データに対して自由にアクセスできる。
- 高付加価値データセット（HVD）の作成手順は次の通りであり、データカストディアンは共有を強制される。



3． 日本におけるガバメントアクセス関連規制動向

データの越境移転や法の域外適用に対する規律は強化。消費者向けには同意取得における透明性向上、企業向けには海外事業者との競争条件の平等を目的としている。

■ 域外適用とは、外国の事業者に対し日本法を適用すること。越境移転とは、日本から国外の事業者に対する個人情報の第三者提供を指す。現行法上越境移転は原則禁止され、①同意、②相当措置、または③十分性認定がある場合のみ許容される（以下、これらを総称して「越境移転オプション」と呼ぶ）。

越境移転における情報提供義務の拡大

（１）越境移転の同意取得に際して、下記の情報提供が義務化（第24条第2項）

- 移転先国の個人情報保護制度
- 移転先組織の個人情報保護措置、等

以上の追加的な情報提供義務については、施行日より適用され、遡及しない（附則第4条）

（２）本法上事業者が講ずべき措置に相当する措置（相当措置）に基づく移転の場合には、相当措置に関する情報提供が義務化（同条第3項）

本人がより適切に移転先の国や組織のリスクを認識して同意を与えられることとなる

域外適用における委員会の執行能力の強化

個人情報保護委員会に下記の権限が追加

- 外国に所在する事業者に対する報告徴収、立入検査、命令の権限（第75条）
- 送達規定（第58条の3）
- 公示送達（期間は6週間）（第58条の4）

域外適用が認められる電気通信事業法と同様、海外事業者とのイコールフッティングを主な目的とする。

越境移転における透明性強化は世界的に珍しい立法であったが、Schrems IIの議論を先取りしていた。

- 情報開示の強化はGDPR水準を超え国際的に前例がない。移転先国の政策によって個人データに関する権利が制限されたり不適切に利用されるリスクを本人に明示し、本人の関与を拡大することが立法趣旨である。
- 上記規律強化に対応する日本企業には、DFFTとの関係を意識して、**特にローカライゼーションやガバメントアクセス（GA）等に関する情報提供が求められることとなると考えられる。**
  - 現時点の提供すべき情報として、移転先国名、個人情報保護制度などが想定。制度について、事業者が移転先の環境を認識するために企業独自の取組が望まれるが、委員会も参考情報を提供予定（令和2年6月4日参議院、其田局長答弁）。

法改正の背後にある諸外国のデータ関連政策が引き起こすリスクと法改正における対応方針

諸外国のデータ関連政策とその引き起こすリスク	
データ・ローカライゼーション政策	本人による消去請求に越境移転先事業者が対応できないリスク
外国政府による無制限なガバメント・アクセス	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リスク

法改正におけるリスク対応の方針

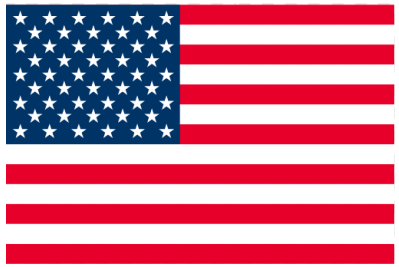
- 2019年G20会合でDFFT概念が合意された。
- 国家間では相互に信頼性を確保した自由なデータ流通を促進する必要性あり
- **個人データのフリー・フローを支える信頼を事業者と本人の間においても確保することが重要**

出所）個人情報保護委員会「制度改正大綱」よりNRI作成

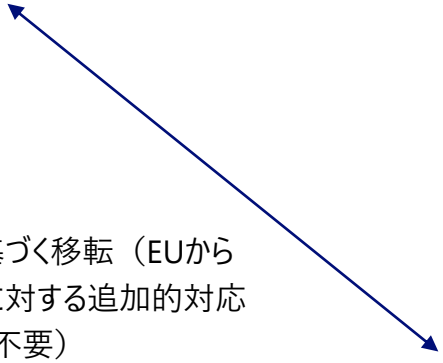
法改正と並行し、個人情報保護委員会はDFFT形成に向け、日欧米3極によるデータ自由流通圏を構築しつつあるが、欧米対立は収束していない。

米EUプライバシーシールド（PS）に基づく移転が不可能に

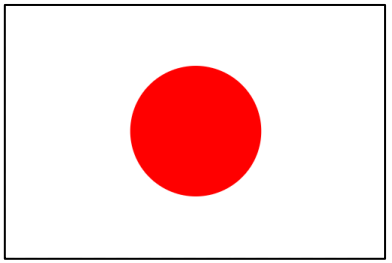
米国の現行法には越境移転規制がなく、対応不要

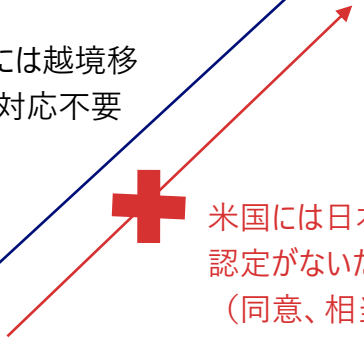


米国の現行法には越境移転規制がなく、対応不要



相互認証に基づく移転（EUからの移転データに対する追加的対応を除いて対応不要）





米国には日本からの十分性認定がないため対応が必要（同意、相当措置）

3．日本におけるガバメントアクセス関連規制動向

経済安全保障推進法：外国におけるガバメントアクセスの脅威が審査されることになる？

サプライチェーン強靭化

概要

1．特定重要物資の安定供給確保に関する基本指針を策定

2．特定重要物資の指定（政令指定）

特定重要物資	国民の生存に必要不可欠又は広く国民生活・経済活動が依拠している重要な物資で、当該物資又はその原材料等を外部に過度に依存し、又は依存するおそれがある場合において、外部の行為により国家及び国民の安全を損なう事態を未然に防止するため、安定供給の確保を図ることが特に必要と認められる物資

3．安定供給確保取組方針の策定

・所管大臣が特定重要物資又はその原材料等の安定供給確保を図るための取組方針を策定。

4．民間事業者による供給確保計画の策定と支援措置

・民間事業者は、特定重要物資等の安定供給確保のための取組（※）に関する計画を作成し、所管大臣の認定を受けることが可能。認定を受けた事業者は、以下の支援を受けることが可能。

（※）生産基盤の整備、供給源の多様化、備蓄、生産技術開発、代替物資開発　等

(1) 安定供給確保支援法人等による助成等の支援
　① 認定供給確保事業者の取組への助成
　② 認定供給確保事業者へ融資を行う金融機関への利子補給
(2) 株式会社日本政策金融公庫法の特例（ツーステップローン）
(3) 中小企業投資育成株式会社法の特例
(4) 中小企業信用保険法の特例

日本における国産クラウド（主権クラウド）の育成？

サプライチェーン強靭化

概要

1．基幹インフラ役務の安定的な提供の確保に関する基本指針を策定

・対象事業者の指定に関する基本的な事項（当該指定に関し経済的社会的観点から留意すべき事項を含む）
・配慮すべき事項（重要設備等を定める主務省令の立案に当たって配慮すべき事項を含む）
・対象事業者その他の関係者との連携に関する事項　等

2．審査対象

(1) 対象分野（法律で対象事業の外縁を示した上で、政令で絞り込み）

電気	ガス	石油	水道	鉄道
貨物自動車運送	外航貨物	航空	空港	電気通信
放送	郵便	金融	クレジットカード	

(2) 対象事業者・・・主務大臣が指定

・対象事業を行う者のうち、①重要設備（具体的な重要設備は主務省令で指定）の機能が停止・低下した場合に、②役務の安定的な提供に支障が生じ、③国家・国民の安全（国民の生存・社会経済秩序の平穏）を損なうおそれが大きいものとして主務省令で定める基準に該当する者

3．審査（重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されるおそれが大きいかどうか）

(1) 重要設備の導入・維持管理等の委託に関する計画書の事前届出

＜計画書の記載事項の例＞
①導入の場合　重要設備の概要、内容・時期、供給者、重要設備の部品等
②維持管理等の委託の場合　重要設備の概要、内容・期間、委託の相手方、再委託等

(2) 事前審査期間（原則として届出受理から30日間）

・審査の必要がないときは短縮可。
・審査や勧告・命令に必要なときは延長可（届出受理から最長４月間）。

4．勧告・命令（妨害行為を防止するため必要な措置）

・審査の結果、重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されるおそれが大きいと認めるときは、妨害行為を防止するため必要な措置（重要設備の導入・維持管理等の内容の変更・中止等）を勧告。

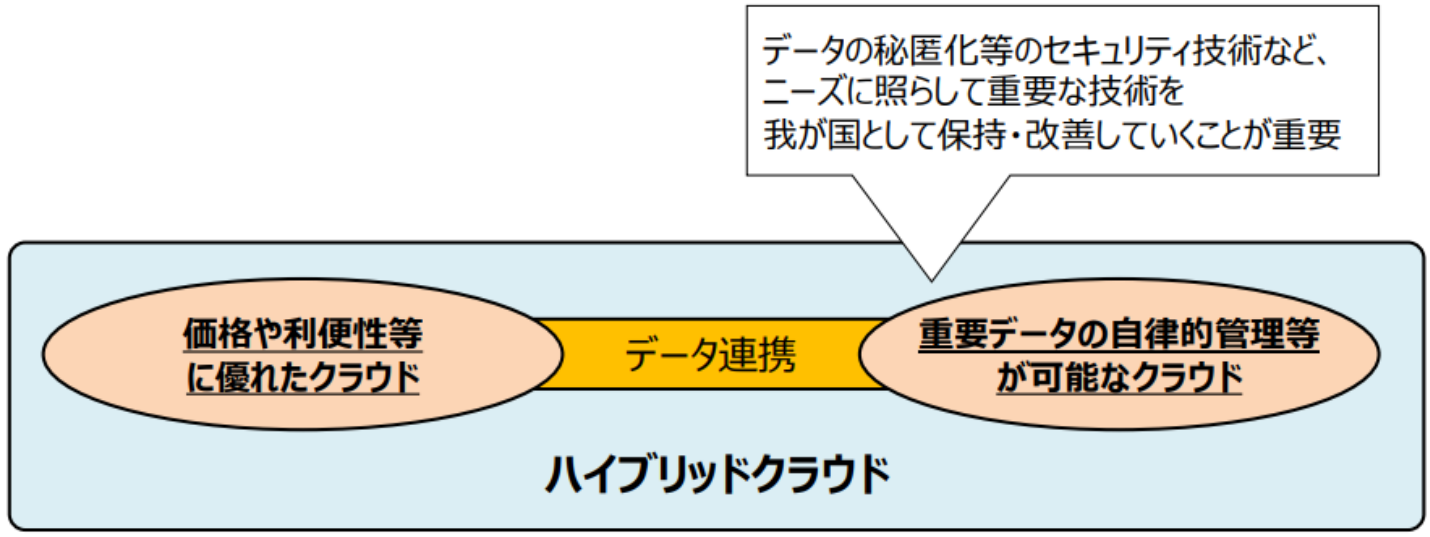
重要設備としてのクラウドと、データ越境移転（ガバメントアクセスのリスク）の審査？

出所）「経済安全保障推進法の概要」（https://www.cas.go.jp/jp/houan/220225/siryou1.pdf）

クラウド産業育成を担う経済産業省は、ハイブリッドクラウドの推進を目指す。

足下のクラウド産業基盤の確保に向けて

- 今後の計算需要の高まりに応える次世代情報処理基盤を構築するためにも、**足下のクラウド産業基盤の確保が重要**。
- 価格や利便性等に優れたクラウドと、我が国として保護すべき重要データの自律的な管理等が可能なクラウドを組み合わせて利用する、**「ハイブリッドクラウド」を促進**していく中で、データ秘匿化等のセキュリティ技術など、**機密性の高いデータを扱うクラウドに求められる技術等の開発を促進するとともに、政府調達等を進めていくことが重要**。



19

出所）経済産業省「第６回半導体・デジタル産業戦略検討会議　資料3」（2022年7月20日）

OECDでのTrusted Government Accessに関する議論（TGA）

■ 日本個人情報保護委員会の後押しで、OECDプライバシーガイドラインの改訂作業の一環として、TGAに関する議論が開始された。2020年12月、下記の声明が公表され、OECDにおいて各国のプラクティスから抽出したハイレベルの原則又は政策ガイダンスが作成されることとなった。

- “the Committee decided to conduct further work to deepen the understanding of approaches in OECD countries and to examine the possibility of developing, as a matter of priority, **an instrument setting out high-level principles or policy guidance for trusted government access to personal data held by the private sector**. Such work would bring together and elaborate a set of common and coherent good practices and legal guarantees from across OECD countries for best reconciling law enforcement and national security needs for data with protection of individual rights. **These may include safeguards relating to: the legal bases upon which governments may compel access to personal data; requirements that access meet legitimate aims and be carried out in a necessary and proportionate manner; transparency; approvals for and constraints placed on government access; limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards; independent oversight; and effective redress.** Such safeguards and their application would facilitate the promotion and protection of **data free flow with trust.**”

今までの議論のまとめ

データ関連政策を理解する「横軸」としてのガバメントアクセスの重要性；データ保護、クラウド、産業政策・・・。

民間が持つデータの重要性＋
データの価値の高まり

↓

各国ごとにデータを社会でどう共有し、利用するのが望ましいのか、政策的な検討が進む

↓

政府主導でデータを取得して利用又は共有するプラクティスが増加する中、
有用性を担保しつつ濫用をどう防止するか？

↓

新しいルール形成が国内、国際（OECD、通商など）の場面で進む

４．日本企業が注意すべきこと

以降の記載はあくまで現時点での報告者の一案でしかありませんので、
ぜひ意見交換させていただけますと幸いです。

４．日本企業が注意すべきこと

ガバメントアクセスへの対抗：リスク評価
例えば、サーバーの所在地やデータの移転の必要性を検討する必要がある。

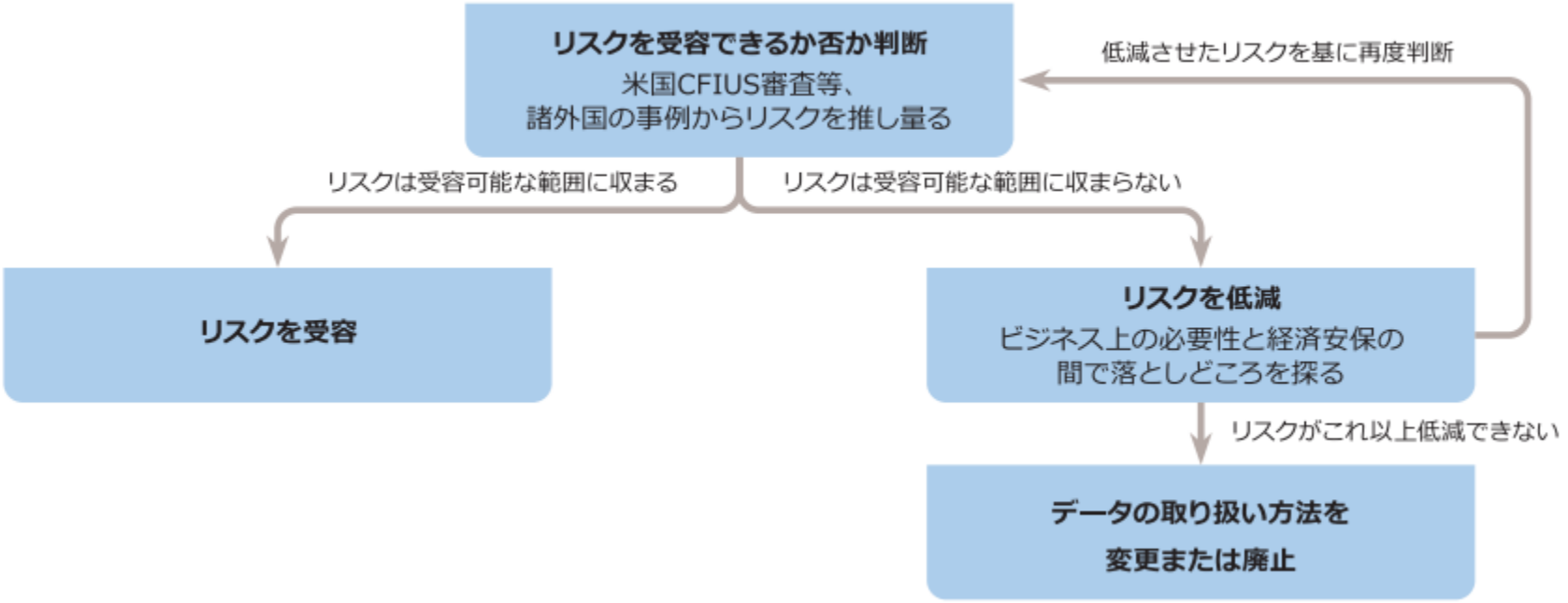
図表２　経済安全保障を加えた自社のリスク評価手順

	個人情報保護	個人情報保護＋経済安全保障
経済安全保障の観点を取り入れたデータマッピングの実施	【調査対象】 ●個人データ 【調査項目】 ●取り扱いの目的や法的根拠 ●第三者提供の有無 ●越境移転の有無・移転先国等	【調査対象】 ●個人／非個人データ 【調査項目】（左記に加え） ●データの件数 ●技術情報を含むかどうか等
リスク評価項目の設定	●本人のプライバシーを保護する観点からリスクを評価	（左記に加え） ●データが経済安全保障に与える影響、例えば選挙介入に利用される可能性や軍事転用可能な技術開発に利用される可能性を考慮してリスクを評価
リスク評価の実施	●データマッピングの結果について、リスク評価項目に基づく評価を実施	●同左

出所）NRI 作成

ガバメントアクセスへの対抗：リスクの評価・低減
CSPへの確認や、データ流通の再配置などを検討する必要がある

図表３　経済安全保障リスクへの対処手順



出所）NRI 作成

４．日本企業が注意すべきこと

ガバメントアクセスは常に悪ではなく、内容が適切であれば、データを大量に保有する企業の社会的責任として応じるのも一案：適切なセーフガードがあるか？が問題。

報道関係者各位

厚生労働省とヤフーは「新型コロナウイルス感染症のクラスター対策に資する情報提供に関する協定」を締結しました

本日、厚生労働省は、クラスター対策を迅速かつ効果的に実施し、クラスターの発生を封じ込めること等により、新型コロナウイルス拡大を防止する取組を進めるため、ヤフーと「新型コロナウイルス感染症のクラスター対策に資する情報提供に関する協定」（以下「本協定」）を締結しました。

政府においては、３月３１日に、民間事業者等に対して、新型コロナウイルス感染症の感染拡大防止に資するデータの政府への提供の要請を行っていたところ、今回、ヤフーから本要請の趣旨に賛同いただけるとの連絡があり、本協定の締結に至ったものです。

（参考）新型コロナウイルス感染症の感染拡大防止に資する統計データ等の提供の要請について（令和２年３月３１日報道発表資料）
https://www.mhlw.go.jp/stf/newpage_10621.html

本協定に基づき、ヤフーは、同社のサービス等の利用者の位置情報等を分析して作成した統計情報のうち、クラスター対策に資する情報を厚生労働省に提供します。

また、厚生労働省は、ヤフーから提供いただいた情報について、新型コロナウイルス感染症の感染拡大防止の目的において利用します。

今後も、民間事業者等と協定を締結した場合は、順次公表いたします。

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）

18

公共性の高い民間データのアクセスに際しては、以下の原理・原則を踏まえた制度設計が必要ではないか

1. 社会的意義（公益）の明確化（社会的意義の明確化）
   どんな公益が見込まれているか、およ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（プライバシー・知財保護）
   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（意図しない利用防止）
   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（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（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（ガバナンス）
   #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（データ取扱い方法説明）
   #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扱い状況の継続的な説明

- 営利目的のデータ利活用と比較すると、情報提供者への直接の便益が小さい（外部性の高い）データ利活用も多く、
  - 社会的意義（公益）の明確化
  - 目的合理性のある最小限のデータアクセス
  - 理解・納得可能なデータ取扱い方法の説明

  が、データ提供者の不安払拭と納得した上でのデータ提供のために重要なのではないか

出所）左）https://www.mhlw.go.jp/stf/newpage_10828.html
右）https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kousou/2021/dai6/siryou6.pdf

特に悪質なガバメントアクセスについては、国際ルールや国内ルールに基づく対抗を

区分	条約/法令の例	
国際法	TRIPS協定	知的財産権の侵害として日本政府の協力を仰ぎ、相手国をWTOに提訴する（例：中国の強制技術移転）
	補助金協定	ガバメントアクセス後のデータ共有において、物品貿易における市場歪曲がある場合には
	投資条約（FTA/EPAを含む）	収用として補償を求める
国内法	憲法/行政法	収用として補償を求める
	GAの根拠法令	違法なGAとして行為の停止を求める